II

(Actos no legislativos)

DECISIONES

DECISIÓN DE EJECUCIÓN (UE) 2022/254 DE LA COMISIÓN

de 17 de diciembre de 2021

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 la República de Corea en virtud de la Ley sobre la protección de la información personal

[notificada con el número C(2021) 9316]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

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

Considerando lo siguiente:

1. INTRODUCCIÓN

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

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

(3) Tal como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación ha de basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que contemple tanto las normas aplicables a los importadores de datos como las limitaciones y salvaguardias en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «equivalente en lo esencial» al ofrecido en la Unión Europea [considerando 104 del Reglamento (UE) 2016/679]. Esto debe evaluarse con arreglo a la legislación de la Unión, en concreto el Reglamento (UE) 2016/679, así como a la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) ([3]).

([1]) DO L 119 de 4.5.2016, p. 1.
([2]) Véase el considerando 101 del Reglamento (UE) 2016/679.
([3]) Véase, más recientemente, el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems (*Schrems II*), ECLI:EU:C:2020:559.

(4) Tal como ha precisado el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico ([4]). En particular, los medios de que se sirve el tercer país en cuestión para la protección de los datos personales pueden ser diferentes de los aplicados en la Unión, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ([5]). Por consiguiente, el nivel de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión. Se trata más bien de determinar si, a través de la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el ordenamiento en cuestión ofrece, en su conjunto, el nivel de protección exigido ([6]). Las referencias sobre adecuación del Comité Europeo de Protección de Datos, que pretenden aclarar esta norma, también proporcionan orientación a este respecto ([7]).

(5) La Comisión ha analizado detenidamente la legislación y las prácticas coreanas. Sobre la base de las constataciones expuestas en los considerandos 8 a 208, la Comisión concluye que la República de Corea garantiza un nivel adecuado de protección de los datos personales transferidos desde un responsable o encargado del tratamiento en la Unión ([8]) a entidades (por ejemplo, personas físicas o jurídicas, organizaciones o instituciones públicas) de Corea que entran en el ámbito de aplicación de la Ley sobre la protección de la información personal (Ley n.º 10465 de 29 de marzo de 2011, modificada en último lugar por la Ley n.º 16930 de 4 de febrero de 2020). Esto incluye tanto a los responsables como a los encargados del tratamiento (denominados «proveedores externos» ([9])) en el sentido del Reglamento (UE) 2016/679. La constatación de adecuación no abarca el tratamiento de datos personales para actividades misioneras por parte de organizaciones religiosas ni para el nombramiento de candidatos por parte de partidos políticos ni el tratamiento de información crediticia personal con arreglo a la Ley de información crediticia por parte de los responsables del tratamiento que estén sujetos a la supervisión de la Comisión de Servicios Financieros.

(6) Esta conclusión tiene en cuenta las salvaguardias adicionales establecidas en la Nota n.º 2021-5 (anexo I) y las declaraciones, las garantías y los compromisos oficiales del Gobierno coreano a la Comisión (anexo II).

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

2. NORMATIVA APLICABLE AL TRATAMIENTO DE DATOS PERSONALES

2.1 El marco de protección de datos en la República de Corea

(8) El régimen jurídico que rige la privacidad y la protección de datos en Corea tiene sus raíces en la Constitución coreana, promulgada el 17 de julio de 1948. Si bien el derecho a la protección de los datos personales no está expresamente contemplado en la Constitución, sí se reconoce como un derecho fundamental, derivado de los derechos constitucionales a la dignidad humana y a la búsqueda de la felicidad (artículo 10), a la vida privada (artículo 17) y a la privacidad de las comunicaciones (artículo 18). Esto ha sido confirmado tanto por el Tribunal Supremo ([10]) como por el Tribunal Constitucional ([11]). Las restricciones de los derechos y libertades fundamentales (incluido el derecho a la privacidad) solo pueden imponerse por ley, cuando sea necesario para la seguridad nacional o para el mantenimiento del orden público en aras del bienestar público, y no pueden afectar al contenido esencial del derecho o la libertad en cuestión (artículo 37, apartado 2).

([4]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, apartado 73.
([5]) *Schrems*, apartado 74.
([6]) 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. 6-7.
([7]) Referencias sobre adecuación del Comité Europeo de Protección de Datos, WP 254, rev. 01, disponible en el siguiente enlace: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) La presente Decisión es pertinente a efectos del EEE. El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, «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. A efectos de la Decisión, debe entenderse, por tanto, que las referencias a la UE y a los Estados miembros de la UE también incluyen a los Estados del EEE.
([9]) Véase la sección 2.2.3 de la presente Decisión.
([10]) Véase, por ejemplo, la Resolución 2014Da77970 del Tribunal Supremo, de 15 de octubre de 2015 (el resumen en inglés está disponible en el enlace «Lawmaker's disclosure of teachers' trade union members case» en https://www.privacy.go.kr/eng/enforcement_01.do) y la jurisprudencia citada, incluida la Resolución 2012Da49933, de 24 de julio de 2014.
([11]) Véanse, en particular, la Resolución 99Hun-ma513 del Tribunal Constitucional, de 26 de mayo de 2005 (el resumen en inglés está disponible en http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) y la Resolución 2014JHun-ma449 2013 Hun-Ba68 (consolidada), de 23 de diciembre de 2015 (el resumen en inglés está disponible en el enlace «Change of residence registration number case» en https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Aunque la Constitución hace referencia en varios lugares a los derechos de los ciudadanos coreanos, el Tribunal Constitucional ha dictaminado que los extranjeros también son sujetos de derechos fundamentales ([12]). En particular, el Tribunal sostuvo que la protección de la dignidad y el valor como ser humano, así como el derecho a buscar la felicidad, son derechos de todo ser humano, no solo de los ciudadanos ([13]). Además, según las declaraciones oficiales del Gobierno coreano ([14]), está generalmente reconocido que los artículos 12 a 22 de la Constitución (que incluyen los derechos de privacidad) prevén los derechos humanos fundamentales ([15]). Aunque hasta ahora no existe una jurisprudencia específica sobre el derecho a la privacidad de los extranjeros, su fundamento en la protección de la dignidad humana y la búsqueda de la felicidad respalda esta conclusión ([16]).

(10) Por otra parte, Corea ha promulgado una serie de leyes en el ámbito de la protección de datos que ofrecen salvaguardias para todas las personas, independientemente de su nacionalidad ([17]). A efectos de la presente Decisión, las leyes pertinentes son:

— La Ley sobre la protección de la información personal (LPIP),

— la Ley sobre el uso y la protección de la información crediticia ([18]),

— la Ley sobre la protección de la privacidad de las comunicaciones.

(11) La LPIP establece el marco jurídico general para la protección de datos en la República de Corea. Se complementa con un Decreto de Ejecución (Decreto Presidencial n.º 23169, de 29 de septiembre de 2011, modificado por última vez por el Decreto Presidencial n.º 30892, de 4 de agosto de 2020) (Decreto de Ejecución de la LPIP), que, al igual que la LPIP, es jurídicamente vinculante y ejecutable.

(12) Además, las «Notas» reglamentarias adoptadas por la Comisión de Protección de la Información Personal (CPIP) establecen normas adicionales sobre la interpretación y aplicación de la LPIP. Sobre la base del artículo 5 (Obligaciones del Estado) y del artículo 14 (Cooperación internacional) de la LPIP, la CPIP adoptó la Nota n.º 2021-5, de 1 de septiembre de 2020 (modificada por la Nota n.º 2021-1, de 21 de enero de 2021, y la Nota n.º 2021-5, de 16 de noviembre 2021, Nota n.º 2021-5), sobre la interpretación, aplicación y ejecución de determinadas disposiciones de la LPIP. Esta Nota contiene aclaraciones que se aplican a cualquier tratamiento de datos personales en virtud de la LPIP, así como salvaguardias adicionales para los datos personales transferidos a Corea sobre la base de la presente Decisión. La Notificación es jurídicamente vinculante para los responsables del tratamiento de información personal y ejecutable tanto por la CPIP como por los órganos jurisdiccionales ([19]). Una infracción de las normas establecidas en la Nota supone una infracción de las disposiciones pertinentes de la LPIP que complementan. Por consiguiente, el contenido de las salvaguardias adicionales se analiza en el marco de la evaluación de los artículos pertinentes de la LPIP. Por último, en el Manual de la LPIP y las directrices aprobadas por la CPIP se ofrece más orientación sobre la LPIP y su Decreto de Ejecución, que guía la aplicación y el cumplimiento de las normas de protección de datos por parte de la CPIP ([20]).

([12]) Resolución 93 Hun-MA120 del Tribunal Constitucional, 29 de diciembre de 1994.
([13]) Resolución 99HeonMa494 del Tribunal Constitucional, 29 de noviembre de 2001.
([14]) Véase la sección 1.1 del anexo II.
([15]) Véase también el artículo 1 de la Ley sobre la protección de la información personal, que se refiere expresamente a «las libertades y los derechos de las personas». Más concretamente, establece que la finalidad de dicha Ley es «disponer el tratamiento y la protección de la información personal para proteger la libertad y los derechos de las personas y reconocer aún más la dignidad y el valor de las mismas». Asimismo, el artículo 5, apartado 1, de la Ley sobre la protección de la información personal establece la responsabilidad del Estado de «formular políticas para prevenir las consecuencias perjudiciales de la recogida más allá del propósito, el abuso y el uso indebido de la información personal, la vigilancia indiscreta y la persecución, etc. y de mejorar la dignidad de los seres humanos y la privacidad individual».
([16]) Además, el artículo 6, apartado 2, de la Constitución establece que la condición de los extranjeros está garantizada según lo prescrito por el Derecho y los tratados internacionales. Corea es parte de varios acuerdos internacionales que garantizan el derecho a la privacidad, como el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención sobre los Derechos de las Personas con Discapacidad (artículo 22) y la Convención sobre los Derechos del Niño (artículo 16).
([17]) Esto incluye normas que son pertinentes para la protección de los datos personales, pero no se aplican en una situación en la que los datos personales se recogen en la Unión y se transfieren a Corea en virtud del Reglamento (UE) 2016/679, por ejemplo, en la Ley sobre la protección, el uso, etc. de la información sobre la ubicación.
([18]) La finalidad de esta Ley es fomentar una sólida actividad de información crediticia, promover la utilización eficiente y la gestión sistemática de la información crediticia y proteger la privacidad contra el uso indebido y el abuso de la información crediticia (artículo 1 de la Ley).
([19]) Por ejemplo, los órganos jurisdiccionales coreanos se han pronunciado sobre el cumplimiento de las Notificaciones reglamentarias en varios casos, incluso responsabilizando a los responsables del tratamiento coreanos de las violaciones de una Notificación (véase, por ejemplo, la Resolución 2018Da219406 del Tribunal Supremo, de 25 de octubre de 2018, en la que el Tribunal ordenó a un responsable del tratamiento que pagara una indemnización a los particulares por los daños sufridos como consecuencia de una violación de la «Notificación de la norma relativa a las medidas para garantizar la seguridad de la información personal»; véanse también la Resolución 2018Da219352 del Tribunal Supremo, de 25 de octubre de 2018; la Resolución 2011Da24555 del Tribunal Supremo, de 16 de mayo de 2016; la Resolución 2014Gahap511956 del Tribunal del Distrito Central de Seúl, de 13 de octubre de 2016; la Resolución 2009Gahap43176 del Tribunal del Distrito Central de Seúl, de 26 de enero de 2010).
([20]) Artículo 12, apartado 1, de la LPIP.

(13) Además, la Ley sobre el uso y la protección de la información crediticia (LIC) establece normas específicas que se aplican tanto a los operadores comerciales «ordinarios» como a las entidades especializadas dentro del sector financiero cuando tratan información crediticia personal, es decir, información necesaria para determinar la solvencia de las partes de transacciones financieras o comerciales. Esto incluye, en particular, el nombre, los datos de contacto, las transacciones financieras, la calificación crediticia, la situación de seguro o el saldo de préstamos cuando dicha información se utilice para determinar la solvencia de una persona ([21]). En cambio, cuando dicha información se utiliza para otros fines (tales como recursos humanos), la LPIP se aplica en su totalidad. En cuanto a las disposiciones específicas de protección de datos de la LIC, el cumplimiento es supervisado en parte por el CPIP (para las organizaciones comerciales, véase el artículo 45-3 de la LIC) y en parte por la Comisión de Servicios Financieros ([22]) (para el sector financiero, incluidas las agencias de calificación crediticia, los bancos, las compañías de seguros, las cajas mutuas de ahorros, las instituciones financieras de crédito especializadas, las empresas de servicios de inversión financiera, las empresas financieras de valores, las cooperativas de crédito, etc., véanse el artículo 45, apartado 1, de la LIC, en relación con el artículo 36-2 del Decreto de Ejecución de la LIC, y el artículo 38 de la Ley de la Comisión de Servicios Financieros). A este respecto, el ámbito de aplicación de la presente Decisión se limita a los operadores comerciales sujetos a la supervisión de la CPIP ([23]). Las normas específicas de la LIC que se aplican en este contexto (las normas generales de la LPIP se aplican cuando no existen normas específicas) se describen en el apartado 2.3.11.

2.2 **Ámbito de aplicación material y personal de la LPIP**

(14) Salvo que se disponga expresamente lo contrario en otras leyes, la protección de los datos personales se rige por la LPIP (artículo 6). El ámbito de aplicación material y personal está determinado por los conceptos definidos de «información personal», «tratamiento» y «responsable del tratamiento de información personal».

2.2.1 *Definición de «datos personales»*

(15) El artículo 2, apartado 1, de la LPIP define «información personal» como la información relativa a una persona viva que permite identificarla directamente, por ejemplo, por su nombre, número de registro de residente o imagen, o de manera indirecta, a saber, cuando la información que por sí sola no permite identificar a un particular determinado puede combinarse fácilmente con otra información. El hecho de si la información puede combinarse «fácilmente» depende de si dicha combinación es razonablemente probable, teniendo en cuenta la posibilidad de obtener otra información, así como el tiempo, el coste y la tecnología necesarios para identificar a un particular.

(16) Además, la información seudonimizada, es decir, la información que no permite identificar a un particular concreto sin utilizarse o combinarse con información adicional para devolverla a su estado original, se considera datos personales en virtud de la LPIP [artículo 2, apartado 1, letra c), de la LPIP]. En cambio, la información totalmente «anonimizada» queda excluida del ámbito de aplicación de la LPIP (artículo 58-2 de la LPIP). Este es el caso de la información que no permite identificar a un particular concreto, aunque se combine con otra información, teniendo en cuenta el tiempo, el coste y la tecnología razonablemente necesarios para la identificación.

(17) Esto corresponde al ámbito de aplicación material del Reglamento (UE) 2016/679 y a sus conceptos de «datos personales», «seudonimización» ([24]) e «información anonimizada» ([25]).

([21]) Artículo 2, apartado 1, de la LIC.

([22]) La Comisión de Servicios Financieros es la autoridad de supervisión de Corea para el sector financiero y, como tal, también ejecuta la LIC.

([23]) Si esto cambiase en el futuro, por ejemplo, ampliando la jurisdicción de la CPIP a todo el tratamiento de información crediticia personal en virtud de la LIC, podría considerarse modificar la decisión de adecuación para incluir también a las entidades que actualmente están sujetas a la supervisión de la Comisión de Servicios Financieros.

([24]) En la LPIP, el «tratamiento seudonimizado» se considera como el tratamiento por métodos tales como la supresión parcial o la sustitución parcial o total de datos personales de tal modo que no pueda reconocerse a ninguna persona concreta sin información adicional (artículo 2, apartados 1 y 2, de la LPIP). Esto corresponde a la definición de «seudonimización» del artículo 4, apartado 5, del Reglamento (UE) 2016/679, que se refiere al «tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».

([25]) En particular, el considerando 26 del Reglamento (UE) 2016/679 aclara que el Reglamento no se aplica a la información anónima, es decir, la información que no guarda relación con una persona física identificada o identificable. Esto, a su vez, depende de todos los medios que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen tales medios, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

2.2.2 *Definición de «tratamiento»*

(18) En la LPIP, el concepto de «tratamiento» se define de manera general como «la recogida, la generación, la conexión, la interrelación, el registro, el almacenamiento, la conservación, el tratamiento con valor añadido, la edición, la recuperación, la producción, la corrección, la recuperación, la utilización, el suministro, la divulgación y la destrucción de información personal y otras actividades similares» ([26]). Aunque algunas disposiciones de la LPIP solo se refieren a tipos específicos de tratamiento, tales como el «uso», el «suministro» o la «recogida» ([27]), el concepto de «uso» se interpreta en el sentido de que incluye cualquier tipo de tratamiento distinto de la «recogida» o el «suministro» (de terceros). Esta amplia interpretación del concepto de «utilización» garantiza que no haya lagunas en la protección con respecto a determinadas actividades de tratamiento. Por consiguiente, el concepto de «tratamiento» corresponde al mismo concepto del Reglamento (UE) 2016/679.

2.2.3 *Responsable del tratamiento de información personal y «proveedor externo»*

(19) La LPIP se aplica a los «responsables del tratamiento de información personal» (responsable del tratamiento). Al igual que el Reglamento (UE) 2016/679, esto incluye a toda institución pública, persona jurídica, organización o persona física que trate datos personales directa o indirectamente para gestionar ficheros de datos personales como parte de sus actividades ([28]). En este contexto, por «fichero de información personal» se entiende cualquier «conjunto o conjuntos de información personal dispuestos u organizados de manera sistemática sobre la base de una norma determinada para facilitar el acceso a la información personal» (artículo 2, apartado 4, de la LPIP) ([29]). En el ámbito interno, el responsable del tratamiento tiene la obligación de formar a las personas que intervienen en el tratamiento bajo su dirección, como los ejecutivos o los empleados de empresas, y de ejercer el control y la supervisión adecuados (artículo 28, apartado 1, de la LPIP).

(20) Se aplican obligaciones específicas cuando un responsable del tratamiento («externalizador») externaliza el tratamiento de datos personales a un tercero («proveedor externo»). En particular, la externalización debe regirse por un acuerdo jurídicamente vinculante (por lo general, un contrato) ([30]) que establezca el alcance del trabajo externalizado, la finalidad del tratamiento, las salvaguardias técnicas y de gestión que deben aplicarse, la supervisión por parte del responsable del tratamiento, la responsabilidad (como la indemnización por los daños y perjuicios causados por un incumplimiento de las obligaciones contractuales), así como las limitaciones de cualquier subtratamiento ([31]) (artículo 26, apartados 1 y 2, de la LPIP, en relación con el artículo 28, apartado 1, del Decreto de Ejecución) ([32]).

(21) Además, el responsable del tratamiento debe publicar y actualizar constantemente los datos sobre el trabajo externalizado y la identidad del proveedor externo o, en la medida en que el tratamiento externalizado se refiera a actividades de comercialización directa, notificar directamente a las personas la información pertinente (artículo 26, apartados 2 y 3, de la LPIP, en relación con el artículo 28, apartados 2 a 5, del Decreto de Ejecución) ([33]).

(22) Además, de conformidad con el artículo 26, apartado 4, de la LPIP, en relación con el artículo 28, apartado 6, del Decreto de Ejecución, el responsable del tratamiento tiene la obligación de «educar» al proveedor externo sobre las medidas de seguridad necesarias y supervisar, incluso mediante inspecciones, si cumple todas las obligaciones del responsable del tratamiento en virtud de la LPIP ([34]) y del contrato de externalización. Cuando el proveedor externo cause daños debido a una infracción de la LPIP, sus acciones u omisiones se atribuirán al responsable del tratamiento a efectos de responsabilidad, como en el caso de un empleado (artículo 26, apartado 6, de la LPIP).

([26]) Artículo 2, apartado 2, de la LPIP.

([27]) Por ejemplo, los artículos 15 a 19 de la LPIP solo se refieren a la recogida, la utilización y el suministro de información personal.

([28]) Artículo 2, apartado 5, de la LPIP. Entre las instituciones públicas en el sentido de la LPIP se encuentran todos los departamentos o agencias de la administración central y sus organismos asociados, los gobiernos locales, las escuelas y las empresas públicas locales participadas por el Gobierno, los órganos administrativos de la Asamblea Nacional y el poder judicial (también el Tribunal Constitucional) (artículo 2, apartado 6, de la LPIP, en relación con el artículo 2 del Decreto de Ejecución de la LPIP).

([29]) Esto corresponde al ámbito de aplicación material del Reglamento (UE) 2016/679. De conformidad con el artículo 2, apartado 1, del Reglamento (UE) 2016/679, el Reglamento se aplica «al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». El artículo 4, apartado 6, del Reglamento (UE) 2016/679 define «fichero» como «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados». En consonancia con esto, el considerando 15 explica que «la protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento».

([30]) Véase el Manual de la LPIP, capítulo III, sección 2, sobre el artículo 26 (pp. 203-212), donde se explica que el artículo 26, apartado 1, de la LPIP se refiere a acuerdos vinculantes, tales como contratos o acuerdos similares.

([31]) De conformidad con el artículo 26, apartado 5, de la LPIP, se prohíbe al encargado del tratamiento utilizar cualquier información personal más allá del alcance del trabajo externalizado o facilitar información personal a un tercero. El incumplimiento de este requisito puede dar lugar a una sanción penal con arreglo al artículo 71, apartado 2, de la LPIP.

([32]) El incumplimiento de este requisito puede dar lugar a la imposición de una multa (véase el artículo 75, apartado 4, punto 4, de la LPIP).

([33]) El incumplimiento de este requisito puede dar lugar a la imposición de una multa (véase el artículo 75, apartado 2, punto 1, y apartado 4, punto 5, de la LPIP).

([34]) Véase también el artículo 26, apartado 7, de la LPIP, según el cual los artículos 15 a 25, 27 a 31, 33 a 38 y 50 se aplican, *mutatis mutandis*, al encargado del tratamiento.

(23) Aunque la LPIP no utiliza, por tanto, conceptos diferentes para «responsables del tratamiento» y «encargados del tratamiento», las normas sobre la externalización establecen obligaciones y salvaguardias esencialmente equivalentes a las que regulan la relación entre los responsables y los encargados del tratamiento en virtud del Reglamento (UE) 2016/679.

2.2.4 *Disposiciones especiales para los proveedores de servicios de información y comunicación*

(24) Si bien la LPIP se aplica al tratamiento de datos personales por parte de cualquier responsable del tratamiento, algunas disposiciones contienen normas específicas (como *lex specialis*) para el tratamiento de los datos personales de «usuarios» por parte de «proveedores de servicios de información y comunicación» ([35]). El concepto de «usuarios» abarca a los particulares que utilizan servicios de información y comunicación [artículo 2, apartado 1, punto 4, de la Ley de promoción de la utilización de redes de información y comunicaciones y la protección de la información (Ley de redes)]. Esto requiere que la persona utilice directamente servicios de telecomunicaciones prestados por un operador coreano de telecomunicaciones o utilice servicios de información ([36]) prestados comercialmente (es decir, con ánimo de lucro) por una entidad que, a su vez, depende de los servicios de un operador de telecomunicaciones con licencia/registrado en Corea ([37]). En ambos casos, la entidad vinculada por las disposiciones específicas de la LPIP es aquella que ofrece un servicio en línea directamente a un particular (es decir, a un usuario).

(25) Por el contrario, una constatación de adecuación se refiere exclusivamente al nivel de protección de los datos personales transferidos desde un responsable o encargado del tratamiento en la Unión a una entidad de un tercer país (en este caso, la República de Corea). En este último escenario, las personas físicas de la Unión normalmente solo tendrán una relación directa con el «exportador de datos» de la Unión y no con algún proveedor coreano de servicios de información y comunicación ([38]). Por consiguiente, las disposiciones específicas de la LPIP con respecto a los datos personales de los usuarios de servicios de información y comunicación solo se aplicarán, a lo sumo, en situaciones limitadas a los datos personales transferidos en virtud de la presente Decisión.

2.2.5 *Exención de determinadas disposiciones de la LPIP*

(26) El artículo 58, apartado 1, de la LPIP excluye la aplicación de una parte de la LPIP (es decir, los artículos 15 a 57) con respecto a cuatro categorías de tratamiento de datos ([39]). En particular, no son de aplicación las partes de la LPIP que tratan de los motivos específicos del tratamiento, determinadas obligaciones en materia de protección de datos, las normas detalladas para el ejercicio de los derechos individuales ni las normas que rigen la resolución de conflictos por parte del Comité de mediación de conflictos relacionados con la información personal. Otras disposiciones básicas de la LPIP siguen siendo aplicables, especialmente las disposiciones generales sobre los principios de protección de datos (artículo 3 de la LPIP) —entre ellos, por ejemplo, los principios de legalidad, especificación y limitación de la finalidad, minimización de los datos, exactitud y seguridad de los datos— y los derechos individuales (de acceso, rectificación, supresión y suspensión, véase el artículo 4 de la LPIP). Además, el artículo 58, apartado 4, de la LPIP impone obligaciones específicas a dichas actividades de tratamiento, en particular con respecto a la minimización de los datos, la conservación de datos durante un período limitado, las medidas de seguridad y la tramitación de las reclamaciones ([40]). En consecuencia, los particulares pueden presentar una reclamación ante la CPIP si no se respetan estos principios y obligaciones y la CPIP está facultada para adoptar medidas de ejecución en caso de incumplimiento.

([35]) Véanse, en particular, el artículo 18, apartado 2, y el capítulo VI de la LPIP.

([36]) Los servicios de información incluyen tanto el suministro de información como los servicios de intermediación para el suministro de información.

([37]) Véase el artículo 2, apartado 1, punto 3 (en relación con el artículo 2, apartado 1, puntos 2 y 4), de la Ley de redes y el artículo 2, apartados 6 y 8, de la Ley del sector de las telecomunicaciones.

([38]) En la medida en que los proveedores coreanos de servicios de información y comunicación tengan una relación directa con personas físicas de la UE (ofreciendo servicios en línea), esto podría conducir a la aplicación directa del Reglamento (UE) 2016/679, de conformidad con su artículo 3, apartado 2, letra a).

([39]) Además, el artículo 58, apartado 2, de la LPIP establece que los artículos 15, 22, 27, apartados 1 y 2, así como los artículos 34 y 37, no se aplican a la información personal tratada mediante dispositivos de tratamiento de datos visuales instalados y operados en lugares abiertos. Dado que esta disposición se refiere al uso de la videovigilancia en Corea, es decir, la recogida directa de información personal de particulares en Corea, no es pertinente a efectos de la presente Decisión, que abarca las transferencias de datos personales desde los responsables o encargados del tratamiento en la UE a entidades en Corea. Además, de conformidad con el artículo 58, apartado 3, de la LPIP, el artículo 15 (recogida y utilización de la información personal), el artículo 30 (obligación de establecer una política de privacidad pública) y el artículo 31 (obligación de nombrar a un responsable de la protección de la privacidad) no se aplican a la información personal tratada para gestionar grupos o asociaciones de amistad (por ejemplo, clubes de aficionados). Dado que estos grupos se consideran de carácter personal, sin relación con una actividad profesional o comercial, no se requiere ninguna base jurídica específica (como el consentimiento de los particulares afectados) para recoger y utilizar su información en este contexto. Sin embargo, siguen siendo de aplicación todas las demás disposiciones de la LPIP (por ejemplo, minimización de los datos, limitación de la finalidad, licitud del tratamiento, seguridad y derechos individuales). Además, cualquier tratamiento de la información personal que vaya más allá de la finalidad de crear un grupo social no puede acogerse a la excepción.

([40]) Más concretamente, el artículo 58, apartado 4, de la LPIP establece la obligación de limitar el tratamiento de la información personal a lo estrictamente necesario para lograr el fin previsto, limitar la duración del tratamiento al mínimo necesario y adoptar las medidas necesarias para la gestión segura y el tratamiento adecuado de dicha información personal. Este último punto comprende salvaguardias técnicas, físicas y administrativas, así como medidas para garantizar el tratamiento adecuado de las reclamaciones individuales.

(27) En primer lugar, la exención parcial abarca los datos personales recogidos con arreglo a la Ley de Estadística para su tratamiento por parte de las instituciones públicas. Según las aclaraciones recibidas del Gobierno coreano, los datos personales tratados en este contexto suelen estar relacionados con nacionales coreanos y solo pueden incluir excepcionalmente información sobre extranjeros, en particular en el caso de las estadísticas sobre la entrada y la salida del territorio o sobre las inversiones extranjeras. Sin embargo, incluso en estas situaciones, estos datos no suelen transferirse desde los responsables o encargados del tratamiento en la Unión, sino que son recogidos directamente por las autoridades públicas coreanas ([41]). Además, de manera similar a lo que se establece en el considerando 162 del Reglamento (UE) 2016/679, el tratamiento de datos con arreglo a la Ley de Estadística está sujeto a varias condiciones y salvaguardias. En particular, la Ley de Estadística impone obligaciones específicas, tales como garantizar la exactitud, la coherencia y la imparcialidad; garantizar la confidencialidad de los particulares; proteger la información de los encuestados en las consultas estadísticas, incluso con vistas a evitar que dicha información se utilice para fines distintos de la elaboración de estadísticas, y someter a los miembros del personal a requisitos de confidencialidad ([42]). Las autoridades públicas que tratan estadísticas también deben cumplir, entre otras cosas, los principios de minimización de los datos, limitación de la finalidad y seguridad (artículos 3 y 58, apartado 4, de la LPIP) y permitir a las personas ejercer sus derechos (de acceso, rectificación, supresión y suspensión, véase el artículo 4 de la LPIP). Por último, los datos deben tratarse de forma anonimizada o seudonimizada si esto permite cumplir la finalidad del tratamiento (artículo 3, apartado 7, de la LPIP).

(28) En segundo lugar, el artículo 58, apartado 1, de la LPIP se refiere a los datos personales recogidos o solicitados para el análisis de información relacionada con la seguridad nacional. El alcance y las consecuencias de esta exención parcial se describen con más detalle en el considerando 149.

(29) En tercer lugar, la exención parcial se aplica al tratamiento temporal de datos personales cuando esto resulte urgentemente necesario por motivos de seguridad pública, incluida la salud pública. Esta categoría es interpretada en sentido estricto por la CPIP y, según la información recibida, nunca se ha utilizado. Solo se aplica en situaciones de emergencia que requieran medidas urgentes, por ejemplo, para rastrear agentes infecciosos o para rescatar y ayudar a las víctimas de catástrofes naturales ([43]). Incluso en esas situaciones, la exención parcial solo abarca el tratamiento de datos personales durante un período limitado para ejecutar dichas medidas. Las situaciones en que esto podría aplicarse a las transferencias de datos objeto de la presente Decisión son aún más limitadas, habida cuenta de la baja probabilidad de que los datos personales transferidos desde la Unión a operadores coreanos sean del tipo que podría hacer que su tratamiento posterior sea «urgentemente necesario» para tales situaciones de emergencia.

(30) Por último, la exención parcial se aplica a los datos personales recogidos o utilizados por la prensa, para actividades misioneras por parte de organizaciones religiosas o para el nombramiento de candidatos por parte de partidos políticos. La exención solo se aplica cuando los datos personales son tratados por la prensa, las organizaciones religiosas o los partidos políticos para esos fines específicos (es decir, las actividades periodísticas, la labor misionera y el nombramiento de candidatos políticos). Cuando dichas entidades traten datos personales para otros fines, tales como la gestión de recursos humanos o la administración interna, la LPIP se aplica en su totalidad.

(31) Con respecto al tratamiento de datos personales por parte de la prensa para actividades periodísticas, el equilibrio entre la libertad de expresión y otros derechos (incluido el derecho a la privacidad) se establece en la Ley de arbitraje y recursos, etc. para los daños causados por los informes de prensa (Ley de prensa) ([44]). En particular, el

([41]) A este respecto, el artículo 33 de la Ley de Estadística exige a las instituciones públicas que protejan la información de los encuestados en las consultas estadísticas, incluso con vistas a evitar que dicha información se utilice para fines distintos de la elaboración de estadísticas.

([42]) Artículo 2, apartados 2 y 3; artículo 30, apartado 2, y artículos 33 y 34 de la Ley de Estadística.

([43]) Manual de la LPIP, sección sobre el artículo 58.

([44]) Por ejemplo, el artículo 4 de la Ley de prensa establece que los informes de prensa deben ser imparciales, objetivos y de interés público, respetar la dignidad y el valor humanos y no pueden difamar a otras personas ni vulnerar sus derechos, la moral pública o la ética social.

artículo 5 de la Ley de prensa establece que la prensa (es decir, cualquier organismo de radiodifusión, diario, revista o periódico en línea), cualquier servicio de noticias en internet o cualquier organismo de radiodifusión multimedia por internet no pueden vulnerar la privacidad de los particulares. Si, a pesar de todo, se produce una vulneración de la privacidad, esta debe subsanarse sin demora de conformidad con los procedimientos específicos establecidos en la Ley. A este respecto, la Ley concede a las personas que sufran daños debido a un informe de prensa una serie de derechos, tales como la publicación de una corrección de una declaración falsa, una rectificación mediante una declaración contradictoria o un informe adicional (cuando un informe de prensa esté relacionado con acusaciones de delitos de los que la persona sea absuelta posteriormente) ([45]). Las reclamaciones de particulares pueden ser resueltas por los medios de prensa directamente (a través de un defensor del pueblo) ([46]), mediante conciliación o arbitraje (ante una Comisión de Arbitraje de la Prensa especializada) ([47]) o ante los tribunales. Los particulares también pueden obtener una indemnización cuando sufran perjuicios económicos, la vulneración de un derecho de la personalidad o cualquier otra angustia emocional a causa de un acto ilícito de la prensa (por dolo o negligencia) ([48]). La prensa queda exenta de responsabilidad con arreglo a la Ley en la medida en que un informe de prensa que interfiera con los derechos de una persona no sea contrario a los valores sociales y se publique con el consentimiento de la persona afectada o en interés del público (y haya motivos suficientes para considerar que el informe corresponde a la verdad) ([49]).

(32) Si bien el tratamiento de datos personales por parte de la prensa para actividades periodísticas está sujeto, por tanto, a salvaguardias específicas derivadas de la Ley de prensa, no existen salvaguardias adicionales de este tipo que regulen el uso de las excepciones para las actividades de tratamiento por parte de organizaciones religiosas y partidos políticos de manera comparable a los artículos 85, 89 y 91 del Reglamento (UE) 2016/679. Por consiguiente, la Comisión considera apropiado excluir del ámbito de aplicación de la presente Decisión a las organizaciones religiosas en la medida en que traten datos personales para sus actividades misioneras y a los partidos políticos en la medida en que traten datos personales en el marco del nombramiento de candidatos.

2.3 **Salvaguardias, derechos y obligaciones**

2.3.1 *Licitud y lealtad del tratamiento*

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

(34) Este principio está establecido en el artículo 3, apartados 1 y 2, de la LPIP y se ve reforzado por el artículo 59 de la LPIP, que prohíbe el tratamiento de datos personales «de manera fraudulenta, inadecuada o injusta», «sin autoridad jurídica» o «más allá de la autoridad correspondiente» ([50]). Estos principios generales de tratamiento lícito se exponen en los artículos 15 a 19 de la LPIP, que establecen las distintas bases jurídicas para el tratamiento (recogida, utilización y suministro a terceros), incluidas las circunstancias en las que esto pueda implicar un cambio de finalidad (artículo 18 de la LPIP).

([45]) Artículos 15 a 17 de la Ley de prensa.

([46]) Cada medio de prensa o de comunicación debe tener su propio defensor del pueblo para prevenir y subsanar cualquier posible daño causado por la prensa (por ejemplo, recomendando la corrección de informes de prensa que sean falsos o dañen la reputación de otras personas), artículo 6 de la Ley de prensa.

([47]) La Comisión consta de entre 40 y 90 comisarios de arbitraje, designados por el ministro de Cultura, Deporte y Turismo entre personas cualificadas como jueces, abogados, personas involucradas en la recogida o la difusión de noticias durante al menos diez años u otras personas con experiencia relacionada con la prensa. Los comisarios de arbitraje no pueden ser al mismo tiempo funcionarios públicos, miembros de partidos políticos o periodistas. De conformidad con el artículo 8 de la Ley de prensa, los comisarios de arbitraje deben desempeñar sus funciones de manera independiente y no pueden estar sujetos a ninguna dirección o instrucción con respecto a dichas funciones. Además, existen normas específicas para prevenir los conflictos de intereses, por ejemplo, mediante la exclusión de comisarios concretos de la gestión de casos específicos de los que su cónyuge o sus familiares formen parte (artículo 10 de la Ley de prensa). La Comisión puede tratar los conflictos mediante conciliación o arbitraje, pero también puede formular recomendaciones para subsanar las infracciones (artículo 5 de la Ley de prensa).

([48]) Artículo 30 de la Ley de prensa.

([49]) Artículo 5 de la Ley de prensa.

([50]) El artículo 59 de la LPIP prohíbe a cualquier persona «que trate o haya tratado alguna vez información personal» «adquirir información personal u obtener el consentimiento para el tratamiento de información personal de manera fraudulenta, inadecuada o injusta», «divulgar información personal adquirida en el curso de las actividades o suministrarla para el uso de terceros sin autoridad» o «dañar, destruir, alterar, falsificar o divulgar la información personal de otra persona sin autoridad jurídica o más allá de la autoridad correspondiente». Una infracción de esta prohibición puede dar lugar a sanciones penales, véanse el artículo 71, apartados 5 y 6, y el artículo 72, apartado 2, de la LPIP. Además, el artículo 70, apartado 2, de la LPIP permite imponer una sanción penal por la obtención de información personal tratada por terceros de manera fraudulenta o por otros medios o métodos injustos, o por el suministro de dicha información a un tercero con fines lucrativos o injustos, así como por la complicidad en tales conductas o la organización de las mismas.

(35) De conformidad con el artículo 15, apartado 1, de la LPIP, un responsable del tratamiento solo puede recoger datos personales (dentro del alcance de la finalidad de la recogida) sobre la base de un número limitado de fundamentos jurídicos. Estos son 1) el consentimiento del interesado ([51]) (punto 1); 2) la necesidad de ejecutar y cumplir un contrato con el interesado (punto 4); 3) una autorización especial por ley o la necesidad de dar cumplimiento a una obligación legal (punto 2); la necesidad ([52]) de que una institución pública lleve a cabo las tareas que le competen según lo prescrito por la ley; 4) la necesidad manifiesta de proteger la vida, la integridad física o los intereses patrimoniales del interesado o de un tercero contra un peligro inminente (solo si el interesado no está en condiciones de expresar su intención o no se puede obtener el consentimiento previo) (punto 5); 5) la necesidad de alcanzar el «interés justificable» del responsable del tratamiento si este es «manifiestamente superior» a los intereses del interesado (y solo cuando el tratamiento guarde una «relación sustancial» con el interés legítimo y no exceda de lo razonable) (punto 6) ([53]). Estos motivos de tratamiento son esencialmente equivalentes a los establecidos en el artículo 6 del Reglamento (UE) 2016/679, en particular el motivo de «interés justificable» que equivale al motivo de «interés legítimo» del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679.

(36) Una vez recogidos, los datos personales pueden utilizarse dentro del alcance de la finalidad de la recogida (artículo 15, apartado 1, de la LPIP) o «dentro del alcance razonablemente relacionado» con la finalidad de la recogida, teniendo en cuenta las posibles desventajas que puedan surgir para el interesado y siempre que se hayan adoptado las medidas de seguridad necesarias (por ejemplo, el cifrado) (artículo 15, apartado 3, de la LPIP). Para determinar si la finalidad de la utilización está «razonablemente relacionada» con la finalidad de la recogida original, el Decreto de Ejecución establece criterios específicos, los cuales son similares a los del artículo 6, apartado 4, del Reglamento (UE) 2016/679. En particular, debe existir una pertinencia considerable para la finalidad original; la utilización uso adicional debe ser previsible (por ejemplo, a la luz de las circunstancias en las que se recogió la información); y, en la medida de lo posible, los datos deben seudonimizarse ([54]). Los criterios específicos utilizados por el responsable del tratamiento para esta evaluación deben revelarse de antemano en la política de privacidad ([55]). Además, el responsable de la protección de la privacidad (véase el considerando 94) está específicamente obligado a examinar si la utilización posterior tiene lugar dentro de esos parámetros.

([51]) El consentimiento debe darse libremente, ser informado y específico y expresarse en una de las distintas maneras predeterminadas por ley. En cualquier caso, el consentimiento no puede obtenerse de manera fraudulenta, inadecuada o injusta (artículo 59, apartado 1, de la LPIP). En primer lugar, de conformidad con el artículo 4, apartado 2, de la LPIP, los interesados tienen derecho a «dar o no su consentimiento» y a «elegir el alcance del consentimiento», y deben ser informados de ello (artículo 15, apartado 2; artículo 16, apartados 2 y 3; artículo 17, apartado 2, y artículo 18, apartado 3, de la LPIP). El artículo 22, apartado 5, de la LPIP contiene una salvaguardia adicional que prohíbe al responsable del tratamiento denegar el suministro de bienes o servicios cuando ello pueda socavar la libertad de elección del particular a la hora de dar su consentimiento. Lo anterior abarca situaciones en las que solo determinados tipos de tratamiento requieren consentimiento (mientras que otros se basan en un contrato), y también abarca el tratamiento ulterior de los datos personales recogidos en el contexto del suministro de bienes o servicios. En segundo lugar, de conformidad con el artículo 15, apartado 2; el artículo 17, apartados 2 y 3, y el artículo 18, apartado 3, de la LPIP, a la hora de solicitar el consentimiento, el responsable del tratamiento debe informar al interesado de los «detalles» de los datos personales en cuestión [por ejemplo, que se trata de datos sensibles, véase el artículo 17, apartado 2, punto 2, letra a), del Decreto de Ejecución de la LPIP], la finalidad del tratamiento, el período de conservación y cualquier destinatario de los datos. Toda solicitud de este tipo se hará «de manera explícitamente reconocible», de forma que se distingan los asuntos que requieren consentimiento de otros asuntos (artículo 22, apartados 1 a 4, de la LPIP). En tercer lugar, el artículo 17, apartado 1, puntos 1 a 6, del Decreto de Ejecución de la LPIP establece los métodos específicos mediante los cuales el responsable del tratamiento debe obtener el consentimiento, tales como el consentimiento por escrito con la firma del interesado o el consentimiento por correo electrónico (de respuesta). Si bien la LPIP no confiere específicamente a los particulares un derecho general a retirar el consentimiento, los particulares tienen derecho a la suspensión del tratamiento de los datos que les conciernen, el cual, cuando se ejerza, dará lugar a la finalización del tratamiento y a la supresión de los datos (véase el considerando 78 sobre el derecho a la suspensión).

([52]) Según la información recibida de la CPIP, las instituciones públicas solo pueden acogerse a este motivo si el tratamiento de la información personal es inevitable, es decir, debe ser imposible o excesivamente difícil para la institución desempeñar sus funciones sin tratar los datos.

([53]) El artículo 39-3 de la LPIP impone obligaciones específicas (más estrictas) a los proveedores de servicios de información y comunicación con respecto a la recogida y el uso de la información personal de sus usuarios. En particular, exige que el proveedor obtenga el consentimiento del usuario, tras facilitar información sobre la finalidad de la recogida o la utilización, las categorías de información personal que deben recogerse y el período durante el cual se tratará la información (artículo 39-3, apartado 1, de la LPIP). Lo mismo se aplica cuando cambia alguno de estos aspectos. El incumplimiento de la obligación de obtener el consentimiento para la recogida de información es objeto de sanciones penales (artículo 71, apartados 4 y 5, de la LPIP). De forma excepcional, la información personal de los usuarios puede ser recogida o utilizada por los proveedores de servicios de información y comunicación sin obtener el consentimiento previo. Este es el caso 1) cuando resulta claramente difícil obtener el consentimiento normal en relación con la información personal necesaria para ejecutar el contrato que rige la prestación de servicios de información y comunicación por razones económicas y tecnológicas (por ejemplo, cuando los datos personales se crean inevitablemente en el proceso de ejecución de un contrato, tales como la información de facturación, los registros de acceso y los registros de pago); 2) cuando sea necesario para la liquidación de cargos tras la prestación de servicios de información y comunicación; o 3) si lo permiten otras leyes (por ejemplo, el artículo 21, apartado 1, punto 6, de la Ley de protección de los consumidores en el ámbito del comercio electrónico establece que los operadores económicos pueden recoger información personal sobre los tutores legales de un menor para confirmar si se ha obtenido un consentimiento válido en nombre del menor) (artículo 39-3, apartado 2, de la LPIP). En todos los casos, los proveedores de servicios de información y comunicación no pueden negarse a prestar servicios simplemente porque el usuario no facilite más información personal que el mínimo requerido (es decir, la información necesaria para realizar los elementos esenciales del servicio en cuestión) (véase el artículo 39-3, apartado 3, de la LPIP).

([54]) Véase el artículo 14-2 del Decreto de Ejecución de la LPIP.

([55]) Artículo 14-2, apartado 2, del Decreto de Ejecución de la LPIP.

(37) Se aplican normas similares (aunque un poco más estrictas) al suministro de datos a un tercero. De conformidad con el artículo 17, apartado 1, de la LPIP, el suministro de datos personales a un tercero está permitido sobre la base del consentimiento ([56]) o, en el marco de la finalidad de la recogida, cuando la información se haya recogido sobre la base de uno de los fundamentos jurídicos contemplados en el artículo 15, apartado 1, puntos 2, 3 y 5, de la LPIP. Esto excluye, en particular, cualquier divulgación basada en el «interés justificable» del responsable del tratamiento. Además, el artículo 17, apartado 4, de la LPIP permite el suministro a terceros «dentro del alcance razonablemente relacionado» con la finalidad de la recogida, teniendo en cuenta una vez más las posibles desventajas que puedan surgir para el interesado y siempre que se hayan adoptado las medidas de seguridad necesarias (como el cifrado). Deben tenerse en cuenta los mismos factores que los descritos en el considerando 36 para evaluar si el suministro entra en el alcance razonablemente relacionado con la finalidad de la recogida y se aplican las mismas salvaguardias (por ejemplo, con respecto a la transparencia a través de la política de privacidad y la participación del responsable de la protección de la privacidad).

(38) La recepción de datos personales de la Unión por parte de un responsable del tratamiento de datos coreano se considera una «recogida» en el sentido del artículo 15 de la LPIP. La Nota n.º 2021-5 (sección I del anexo I de la presente Decisión) aclara que la finalidad para la que fueron transferidos los datos por la entidad de la UE en cuestión constituye la finalidad de la recogida para el responsable del tratamiento de datos coreano. En consecuencia, los responsables del tratamiento de datos coreanos que reciban datos personales de la Unión están, en principio, obligados a tratar dicha información dentro del alcance de la finalidad de la transferencia, de conformidad con el artículo 17 de la LPIP.

(39) Se aplican limitaciones especiales en caso de que el responsable del tratamiento pretenda utilizar los datos personales o facilitarlos a un tercero para una finalidad distinta de la de su recogida ([57]). De conformidad con el artículo 18, apartado 2, de la LPIP, un responsable del tratamiento privado puede, en casos excepcionales ([58]), utilizar los datos personales o facilitarlos a un tercero para una finalidad diferente: 1) sobre la base del consentimiento adicional (es decir, por separado) del interesado; 2) cuando así lo prevean disposiciones legales especiales; o 3) cuando esto sea manifiestamente necesario para proteger la vida, la integridad física o los intereses patrimoniales del interesado o de un tercero contra un peligro inminente (solo si el interesado no está en condiciones de expresar su intención y no se puede obtener el consentimiento previo) ([59]).

(40) Las instituciones públicas también pueden utilizar los datos personales o facilitarlos a un tercero para fines distintos en determinadas situaciones. Esto abarca los casos en que, de lo contrario, sería imposible para las instituciones públicas cumplir con sus deberes estatutarios según lo prescrito por la ley, previa autorización de la CPIP. Además, las instituciones públicas pueden facilitar datos personales a otra autoridad u órgano jurisdiccional cuando sea necesario para la investigación y el enjuiciamiento de delitos o una acusación; para que un órgano jurisdiccional desempeñe sus funciones relacionadas con procedimientos judiciales en curso; o para la ejecución de una sanción penal o una orden de cuidado o de custodia ([60]). También pueden proporcionar datos personales a un Gobierno extranjero o una organización internacional para cumplir una obligación legal derivada de un tratado o convenio internacional, en cuyo caso también deben cumplir los requisitos para las transferencias de datos transfronterizas (véase el considerando 90).

(41) Por consiguiente, los principios de licitud y lealtad del tratamiento se aplican en el marco jurídico coreano de manera esencialmente equivalente al Reglamento (UE) 2016/679, al permitir el tratamiento solo sobre la base de motivos legítimos y claramente definidos. Además, en todos los casos mencionados, el tratamiento solo está permitido si no es probable que «vulnere deslealmente» los intereses del interesado o de un tercero, lo que requiere encontrar un equilibrio entre los diferentes intereses. Asimismo, el artículo 18, apartado 5, de la LPIP establece salvaguardias adicionales cuando el responsable del tratamiento facilita los datos personales a un tercero, lo cual puede comprender una solicitud para restringir la finalidad y el método de utilización o adoptar medidas de seguridad específicas. A su vez, el tercero está obligado a aplicar las medidas solicitadas.

([56]) Las infracciones del artículo 17, apartado 1, punto 1, de la LPIP pueden dar lugar a la imposición de sanciones penales (artículo 71, apartado 1, de la LPIP).

([57]) La «finalidad prevista» es la finalidad para la que se recogió la información. Por ejemplo, cuando la información se recoge sobre la base del consentimiento del particular afectado, la finalidad perseguida es la que se comunica al particular en virtud del artículo 15, apartado 2, de la LPIP.

([58]) Véase el artículo 18, apartado 1, de la LPIP. Las infracciones del artículo 18, apartados 1 y 2, pueden dar lugar a la imposición de sanciones penales (artículo 71, apartado 2, de la LPIP).

([59]) El uso de la información personal o su suministro a un tercero por parte de los proveedores de servicios de información y comunicación para una finalidad distinta de la original solo puede tener lugar por los motivos establecidos en el artículo 18, apartado 2, puntos 1 y 2, de la LPIP (es decir, cuando se obtenga un consentimiento adicional o cuando existan disposiciones especiales en la legislación). Véase el artículo 18, apartado 2, de la LPIP.

([60]) Salvo cuando el tratamiento sea necesario para la investigación de delitos, la acusación y el enjuiciamiento, las instituciones públicas que utilicen información personal o la faciliten a un tercero para un fin distinto del de la recogida (por ejemplo, cuando esté expresamente permitido por la ley o sea necesario para cumplir un tratado) están obligadas a publicar los fundamentos jurídicos del tratamiento, su finalidad y el alcance en su sitio web o en el Boletín Oficial y a llevar registros (artículo 18, apartado 4, de la LPIP, junto con el artículo 15 del Decreto de Ejecución de la LPIP).

(42) Por último, el artículo 28-2 de la LPIP permite el tratamiento (ulterior) de información seudonimizada sin el consentimiento de la persona afectada con fines estadísticos, de investigación científica ([61]) y de archivo en interés público, sujeto a salvaguardias específicas. Por lo tanto, al igual que el Reglamento (UE) 2016/679 ([62]), la LPIP facilita el tratamiento (ulterior) de datos personales para tales fines en un marco que prevé las salvaguardias adecuadas para proteger los derechos de las personas. En lugar de basarse en la seudonimización como posible salvaguardia, la LPIP la impone como condición previa para llevar a cabo determinadas actividades de tratamiento con fines estadísticos, de investigación científica y de archivo en interés público (como poder tratar los datos sin consentimiento o combinar diferentes conjuntos de datos).

(43) Además, la LPIP impone una serie de salvaguardias específicas, especialmente en lo que se refiere a las medidas técnicas y organizativas necesarias, el mantenimiento de registros, las limitaciones del intercambio de datos y la manera de abordar posibles riesgos de reidentificación. La combinación de las distintas salvaguardias descritas en los considerandos 44 a 48 garantiza que el tratamiento de los datos personales en este contexto esté sujeto a protecciones esencialmente equivalentes a las que se requerirían de conformidad con el Reglamento (UE) 2016/679.

(44) En primer lugar, y lo más importante, el artículo 28-5, apartado 1, de la LPIP prohíbe el tratamiento de información seudonimizada con el fin de identificar a un particular determinado. No obstante, si se generase información que permitiera identificar a un particular durante el tratamiento de información seudonimizada, el responsable del tratamiento debe suspender de inmediato el tratamiento y destruir dicha información (artículo 28-5, apartado 2, de la LPIP). El incumplimiento de estas disposiciones es objeto de multas administrativas y constituye una infracción penal ([63]). Esto significa que, incluso en aquellas situaciones en las que sería *prácticamente* posible reidentificar al particular, dicha reidentificación está *legalmente* prohibida.

(45) En segundo lugar, cuando se realice un tratamiento (ulterior) de información seudonimizada para tales fines, el responsable del tratamiento debe adoptar medidas tecnológicas, físicas y de gestión específicas para garantizar la seguridad de la información (incluidos el almacenamiento y la gestión por separado de la información necesaria para restaurar la información seudonimizada a su estado original) ([64]). Además, deben llevarse registros de la información seudonimizada tratada, la finalidad del tratamiento, el historial de utilización y cualquier tercero destinatario (artículo 29-5, apartado 2, del Decreto de Ejecución de la LPIP).

(46) En tercer y último lugar, la LPIP prevé salvaguardias específicas para evitar la identificación de particulares por parte de terceros en caso de que se comparta la información. En particular, cuando se suministre información seudonimizada a un tercero con fines estadísticos, de investigación científica o de archivo en interés público, los responsables del tratamiento no pueden incluir información que pueda utilizarse para identificar a una persona concreta (artículo 28-2, apartado 2, de la LPIP) ([65]).

(47) Más concretamente, si bien la LPIP permite la combinación de información seudonimizada (tratada por diferentes responsables del tratamiento) con fines estadísticos, de investigación científica o de archivo en interés público, reserva esta facultad a instituciones especializadas equipadas con instalaciones de seguridad específicas (artículo 28-3, apartado 1, de la LPIP) ([66]). Al solicitar una combinación de datos seudonimizados, el responsable del tratamiento debe presentar documentación, entre otras cosas, sobre los datos que deben combinarse, la finalidad

([61]) En el artículo 2, apartado 8, de la LPIP, «investigación científica» se define como «la investigación que aplica métodos científicos, tales como el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado». Estas categorías corresponden a las establecidas en el considerando 159 del Reglamento (UE) 2016/679.

([62]) Véanse el artículo 5, apartado 1, letra b); el artículo 89, apartados 1 y 2, y los considerandos 50 y 157 del Reglamento (UE) 2016/679.

([63]) Véanse el artículo 28-6, apartado 1; el artículo 71, apartado 4-3, y el artículo 75, apartado 2, punto 4-4, de la LPIP.

([64]) Artículo 28-4 de la LPIP y artículo 29-5 del Decreto de Ejecución de la LPIP. El incumplimiento de esta obligación es objeto de sanciones administrativas y penales (véanse el artículo 73, apartado 1, y el artículo 75, apartado 2, punto 6, de la LPIP).

([65]) Las infracciones de estos requisitos pueden dar lugar a la imposición de sanciones penales (artículo 71, apartado 2, de la LPIP). La CPIP comenzó de inmediato a aplicar estas nuevas normas, por ejemplo, en su Decisión de 28 de abril de 2021, en la que impuso una multa y medidas correctoras a una empresa que, entre otras infracciones de la LPIP, no cumplía el requisito del artículo 28-2, apartado 2 (véase https://www.CPIP.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8).

([66]) Para ser designada como institución especializada (una «agencia especializada en la combinación de datos»), debe presentarse una solicitud a la CPIP junto con documentos justificativos en los que se detallen, entre otras cosas, las instalaciones y los equipos aplicados para combinar de forma segura los datos seudonimizados y se confirme que el solicitante cuenta con al menos tres empleados a tiempo completo con cualificaciones o experiencia relacionadas con la protección de datos personales (artículo 29-2, apartados 1 y 2, del Decreto de Ejecución de la LPIP). Los requisitos detallados, por ejemplo, con respecto a las cualificaciones del personal, las instalaciones disponibles, las medidas de seguridad, las políticas y los procedimientos internos, así como los requisitos financieros, se establecen en la Nota n.º 2020-9 de la CPIP sobre la combinación y la divulgación de información seudonimizada (apéndice I). Una designación como agencia especializada en la combinación de datos puede ser revocada por la CPIP (tras celebrar una audiencia) por determinados motivos, por ejemplo, si la agencia ya no cumple las normas de seguridad necesarias para la designación o si se ha producido una violación de la seguridad de los datos en el contexto de la combinación de datos (artículo 29-2, apartados 5 y 6, del Decreto de Ejecución de la LPIP). La CPIP debe publicar cada designación (o revocación de la designación) de una agencia especializada en la combinación de datos (artículo 29-2, apartado 7, del Decreto de Ejecución de la LPIP).

de la combinación y las medidas de seguridad propuestas para el tratamiento de los datos combinados ([67]). Para permitir la combinación, el responsable del tratamiento debe enviar los datos que deben combinarse a la institución especializada y proporcionar una «clave de combinación» (es decir, la información que se ha utilizado para la seudonimización) a la Agencia de Internet y Seguridad de Corea ([68]). Esta última genera «datos de enlace de claves de combinación» (que permiten vincular las claves de combinación de diferentes solicitantes para conseguir la combinación de los conjuntos de datos) y los proporciona a la institución especializada ([69]).

(48) El responsable del tratamiento que solicita la combinación puede analizar la información combinada en las instalaciones de la institución especializada, en un espacio en el que se apliquen medidas de seguridad técnicas, físicas y administrativas específicas (artículo 29-3 del Decreto de Ejecución de la LPIP). Los responsables del tratamiento que aporten un conjunto de datos para una combinación de este tipo solo pueden sacar los datos combinados de la institución especializada tras una seudonimización o anonimización adicional de los datos combinados y con la aprobación de dicha institución (artículo 28-3, apartado 2, de la LPIP) ([70]). A la hora de determinar si concede o no dicha aprobación, la institución evaluará el vínculo entre los datos combinados y la finalidad del tratamiento y si se ha elaborado un plan de seguridad específico para la utilización de dichos datos ([71]). No se permitirá exportar la información combinada fuera de la institución si la información contiene datos que permitan identificar a una persona ([72]). Por último, la CPIP supervisa la combinación y la divulgación de datos seudonimizados por parte de la institución especializada (artículo 29-4, apartado 3, del Decreto de Ejecución de la LPIP).

2.3.2 *Tratamiento de categorías especiales de datos personales*

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

(50) La LPIP contiene normas específicas con respecto al tratamiento de datos sensibles ([73]), que se definen como datos personales que revelan información sobre la ideología, las creencias, la admisión en un sindicato o partido político o la retirada de los mismos, las opiniones políticas, la salud y la vida sexual de una persona, así como otra información personal que pueda amenazar «notablemente» la privacidad del interesado y que haya sido prescrita como información sensible por Decreto Presidencial ([74]). Según las aclaraciones recibidas de la CPIP, la vida sexual se interpreta en el sentido de que también abarca la orientación o las preferencias sexuales de la persona ([75]). Además, el artículo 18 del Decreto de Ejecución añade otras categorías al alcance de los datos sensibles, especialmente la información relativa al ADN obtenida a partir de pruebas genéticas y los datos que constituyen antecedentes penales. La reciente modificación del Decreto de Ejecución de la LPIP ha ampliado aún más el concepto de «datos sensibles», incluyendo también datos personales que revelen el origen racial o étnico y la información biométrica ([76]). Tras esta modificación, el concepto de «datos sensibles» en virtud de la LPIP es esencialmente equivalente al del artículo 9 del Reglamento (UE) 2016/679.

(51) De conformidad con el artículo 23, apartado 1, de la LPIP y de forma similar a lo dispuesto en el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el tratamiento de datos sensibles está generalmente prohibido, salvo que se aplique una de las excepciones enumeradas ([77]). Estas limitan el tratamiento a los casos en que el responsable del tratamiento informe al interesado de conformidad con los artículos 15 y 17 de la LPIP y obtenga

([67]) Artículo 8, apartados 1 y 2, de la Notificación 2020-9 sobre la combinación y la divulgación de información seudonimizada.
([68]) Artículo 2, apartados 3 y 6, y artículo 9, apartado 1, de la Notificación 2020-9 sobre la combinación y la divulgación de información seudonimizada.
([69]) Artículo 2, apartado 4, y artículo 9, apartados 2 y 3, de la Notificación 2020-9 sobre la combinación y la divulgación de información seudonimizada. Tras la combinación, la institución especializada debe destruir de inmediato los datos de enlace de claves de combinación (artículo 9, apartado 4, de la Nota).
([70]) Las infracciones de los requisitos para la combinación de conjuntos de datos pueden dar lugar a la imposición de sanciones penales (artículo 71, apartado 4-2, de la LPIP). Véase también el artículo 29-2, apartado 4, del Decreto de Ejecución de la LPIP.
([71]) El procedimiento para aprobar la divulgación de datos combinados se establece en el artículo 11 de la Nota n.º 2020-9 sobre la combinación y la divulgación de información seudonimizada. En particular, la institución especializada debe crear un «comité de revisión de la divulgación», compuesto por miembros con conocimientos y experiencia importantes en materia de protección de datos.
([72]) Artículo 29-2, apartado 4, del Decreto de Ejecución de la LPIP y artículo 11 de la Nota n.º 2020-9.
([73]) El Tribunal Constitucional de Corea también ha reconocido la necesidad de establecer medidas de protección específicas para el tratamiento de datos sensibles, tales como los datos relativos a la salud o al comportamiento sexual (véase la Resolución HunMa 1139 del Tribunal Constitucional, de 31 de mayo de 2007).
([74]) Artículo 23, apartado 1, de la LPIP.
([75]) Véase también el Manual de la LPIP, capítulo III, sección 2 sobre el artículo 23 (pp. 157-164).
([76]) Es decir, información personal resultante del tratamiento técnico específico de datos relativos a las características físicas, fisiológicas o de comportamiento de una persona con el fin de identificarla de manera unívoca.
([77]) El incumplimiento de estos requisitos puede dar lugar a sanciones con arreglo al artículo 71, punto 3, de la LPIP.

un consentimiento por separado (es decir, independiente del consentimiento para el tratamiento de otros datos personales) o cuando el tratamiento sea exigido o permitido por la ley. Las autoridades públicas también pueden tratar la información biométrica, la información relativa al ADN obtenida a partir de pruebas genéticas, la información personal que revele el origen racial o étnico y los datos que constituyan antecedentes penales por los motivos que estén exclusivamente a su disposición (por ejemplo, cuando sea necesario para la investigación de delitos o para que un tribunal proceda con un caso) ([78]). Como tales, las bases jurídicas disponibles para el tratamiento de datos sensibles son más limitadas que para otros tipos de datos personales, e incluso más restrictivas en la legislación coreana que en el artículo 9, apartado 2, del Reglamento (UE) 2016/679.

(52) Además, el artículo 23, apartado 2, de la LPIP —cuyo incumplimiento puede dar lugar a sanciones ([79])— subraya la especial importancia de garantizar una seguridad adecuada a la hora de gestionar datos sensibles para que «no puedan ser extraviados, robados, divulgados, falsificados, alterados o dañados». Si bien este es un requisito general en virtud del artículo 29 de la LPIP, el artículo 3, apartado 4, deja claro que el nivel de seguridad debe adaptarse al tipo de datos personales que se está tratando, lo que implica que deben tenerse en cuenta los riesgos particulares que conlleva el tratamiento de datos sensibles. Por otra parte, el tratamiento de datos siempre deberá realizarse «de forma que se reduzca al mínimo la posibilidad de vulnerar» la privacidad del interesado y, si es posible, «manteniendo el anonimato» (artículo 3, apartados 6 y 7, de la LPIP). Estos requisitos son especialmente importantes cuando el tratamiento se refiere a datos sensibles.

2.3.3 *Limitación de la finalidad*

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

(54) Este principio está garantizado por el artículo 3, apartados 1 y 2, de la LPIP, según el cual el responsable del tratamiento «especificará y explicitará» la finalidad del tratamiento, tratará los datos personales de la manera adecuada necesaria para tal fin y no los utilizará más allá de dicha finalidad. El principio general de limitación de la finalidad también se confirma en el artículo 15, apartado 1; el artículo 18, apartado 1, y el artículo 19 y, en el caso de los encargados del tratamiento (los denominados «proveedores externos»), en el artículo 26, apartado 1, punto 1, y apartados 5 y 7, de la LPIP En particular, los datos personales solo pueden, en principio, utilizarse y facilitarse a terceros dentro del alcance de la finalidad para la que fueron recogidos (artículo 15, apartado 1, y artículo 17, apartado 1, punto 2). El tratamiento para una finalidad compatible, es decir, «dentro del alcance razonablemente relacionado con la finalidad inicial de la recogida», solo puede tener lugar si no afecta negativamente a los interesados de que se trate y si se adoptan las medidas de seguridad necesarias (como el cifrado) (artículo 15, apartado 3, y artículo 17, apartado 4, de la LPIP). A fin de determinar si el tratamiento ulterior es para una finalidad compatible, el Decreto de Ejecución de la LPIP enumera una serie de criterios específicos similares a los previstos en el artículo 6, apartado 4, del Reglamento (UE) 2016/679 (véase el considerando 36).

(55) Como se explica en el considerando 38, la finalidad de la recogida en el caso de los responsables del tratamiento coreanos que reciben datos personales de la Unión es la finalidad para la que se transfieren los datos. El cambio de finalidad por parte del responsable del tratamiento solo está permitido de manera excepcional en casos específicos (enunciados) (artículo 18, apartado 2, puntos 1 a 3, de la LPIP; véase también el considerando 39). En la medida en que la ley autorice un cambio de finalidad, estas leyes, a su vez, deben respetar el derecho fundamental a la privacidad y a la protección de datos, así como los principios de necesidad y proporcionalidad establecidos en la Constitución coreana. Además, el artículo 18, apartados 2 y 5, de la LPIP prevé salvaguardias adicionales, especialmente el requisito de que tal cambio de finalidad no «vulnere deslealmente los intereses de un interesado», por lo que siempre se requiere encontrar un equilibrio entre los diferentes intereses. Esto ofrece un nivel de protección esencialmente equivalente al previsto en el artículo 5, apartado 1, letra b), y en el artículo 6, en relación con el considerando 50 del Reglamento (UE) 2016/679.

2.3.4 *Exactitud y minimización de los datos*

(56) Los datos personales deben ser exactos y, en caso necesario, se han de mantener actualizados. También deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

([78]) El artículo 18 del Decreto de Ejecución de la LPIP establece que las categorías de datos allí enumeradas quedan excluidas de la disposición del artículo 23, apartado 1, de la Ley cuando sean tratadas por una institución pública de conformidad con el artículo 18, apartado 2, puntos 5 a 9, de la LPIP.

([79]) Véanse el artículo 73, punto 1, y el artículo 75, apartado 2, punto 6, de la LPIP.

(57) El principio de exactitud se reconoce asimismo en el artículo 3, apartado 3, de la LPIP, que exige que los datos personales sean «exactos, completos y actualizados en la medida necesaria con respecto a los fines» para los que se traten. La minimización de los datos se exige en el artículo 3, apartados 1 y 6, y en el artículo 16, apartado 1, de la LPIP, que estipulan que el responsable del tratamiento (solo) recogerá datos personales «en la medida mínima necesaria» para alcanzar la finalidad perseguida y asumirá la carga de la prueba a este respecto. Si es posible cumplir la finalidad de la recogida mediante el tratamiento de información de forma anonimizada, los responsables del tratamiento deben esforzarse por hacerlo (artículo 3, apartado 7, de la LPIP).

2.3.5 *Limitación del plazo de conservación*

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

(59) El principio de limitación del plazo de conservación se establece de forma similar en el artículo 21, apartado 1, de la LPIP ([80]), que exige que el responsable del tratamiento «destruya» ([81]) los datos personales sin demora una vez lograda la finalidad del tratamiento o cuando expire el período de conservación (si esta última fecha es anterior), salvo que la ley exija una retención ulterior ([82]). En este último caso, los datos personales pertinentes «se almacenarán y gestionarán separados de otros datos personales» (artículo 21, apartado 3, de la LPIP).

(60) El artículo 21, apartado 1, de la LPIP no se aplica cuando los datos seudonimizados se tratan con fines estadísticos, de investigación científica o de archivo en interés público ([83]). Para garantizar el principio de conservación limitada de los datos también en este caso, la Notificación 2021-5 exige que los responsables del tratamiento anonimicen la información de conformidad con el artículo 58-2 de la LPIP si los datos no se han destruido una vez lograda la finalidad específica del tratamiento ([84]).

2.3.6 *Seguridad de los datos*

(61) 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 el estado de la técnica, los costes conexos y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos de las particulares.

(62) Un principio de seguridad similar se establece en el artículo 3, apartado 4, de la LPIP, que exige a los responsables del tratamiento «gestionar la información personal de manera segura según los métodos, tipos, etc. de tratamiento de la información personal, teniendo en cuenta la posibilidad de que se vulneren los derechos de los interesados y la gravedad de los riesgos pertinentes». Además, el responsable del tratamiento «tratará la información personal de manera que se reduzca al mínimo la posibilidad de vulnerar la privacidad de un interesado» y, en este contexto, procurará tratar los datos personales de forma anónima o seudonimizada, si es posible (artículo 3, apartados 6 y 7, de la LPIP).

(63) Estos requisitos generales se exponen de manera más detallada en el artículo 29 de la LPIP, de conformidad con el cual todo responsable del tratamiento «adoptará las medidas técnicas, físicas y administrativas, tales como el establecimiento de un plan de gestión interna y la conservación de los registros de conexión, etc., que sean necesarias para garantizar la seguridad según lo prescrito por el Decreto Presidencial de manera que los datos

([80]) Artículo 8 (en relación con el artículo 8-2 del Decreto de Ejecución), artículo 11 (en relación con el artículo 12, apartado 2, del Decreto de Ejecución).

([81]) En relación con los métodos para destruir la información personal, véase el artículo 16 del Decreto de Ejecución de la LPIP. El artículo 21, apartado 2, de la LPIP aclara que esto comprenderá «las medidas necesarias para impedir la recuperación y la reactivación».

([82]) El incumplimiento de estos requisitos puede dar lugar sanciones penales (artículo 73, apartados 1 y 2, de la LPIP). El artículo 39-6 de la LPIP impone un requisito adicional a los proveedores de servicios de información y comunicación de suprimir la información personal de los usuarios que no hayan hecho uso de los servicios de información y comunicación ofrecidos durante al menos un año (salvo que la ley exija una conservación ulterior o que el particular afectado así lo solicite). Los particulares deben ser informados de la intención de suprimir su información treinta días antes de la expiración del plazo de un año (artículo 39-6, apartado 2, de la LPIP y artículo 48-5, apartado 3, del Decreto de Ejecución de la LPIP). Si la ley exige una retención ulterior, los datos conservados deben almacenarse separados de otra información de los usuarios y solo pueden utilizarse o divulgarse de conformidad con dicha ley (artículo 48-5, apartados 1 y 2, del Decreto de Ejecución de la LPIP).

([83]) Artículo 28-7 de la LPIP.

([84]) Nota n.º 2021-5 (anexo I), sección 4.

personales no puedan ser extraviados, robados, divulgados, falsificados, alterados o dañados». El artículo 30, apartado 1, del Decreto de Ejecución de la LPIP especifica dichas medidas haciendo alusión a 1) la elaboración y la aplicación de un plan de gestión interna para el tratamiento seguro de los datos personales, 2) los controles y las restricciones de acceso, 3) la adopción de tecnología de cifrado para almacenar y transmitir los datos personales de manera segura, 4) los registros de conexión, 5) los programas de seguridad y 6) medidas físicas tales como un sistema de almacenamiento o bloqueo seguro ([85]).

(64) Además, se aplican obligaciones específicas si se produce una violación de los datos (artículo 34 de la LPIP, en relación con los artículos 39 y 40 del Decreto de Ejecución de la LPIP) ([86]). En particular, el responsable del tratamiento está obligado a notificar sin demora a los interesados perjudicados los detalles de la violación ([87]), incluida la información sobre las contramedidas (obligatorias) adoptadas por el responsable del tratamiento y lo que pueden hacer los interesados para minimizar el riesgo de daños (artículo 34, apartados 1 y 2, de la LPIP) ([88]). Cuando la violación de la seguridad de los datos afecte a 1 000 interesados, como mínimo, el responsable del tratamiento también comunicará sin demora la violación de la seguridad de los datos y las contramedidas adoptadas a la CPIP y a la Agencia de Internet y Seguridad de Corea, que podrán prestar asistencia técnica (artículo 34, apartado 3, de la LPIP, en relación con el artículo 39 del Decreto de Ejecución de la LPIP). Los responsables del tratamiento son responsables de los daños causados por las violaciones de los datos, de conformidad con las disposiciones de la Ley civil sobre responsabilidad civil (véase también la sección 2.5 sobre las vías de recurso) ([89]).

(65) En el cumplimiento de sus obligaciones de seguridad, el responsable del tratamiento debe estar asistido por un responsable de la protección de la privacidad, cuyas tareas comprenden, entre otras, la creación de un sistema de control interno «para prevenir la divulgación, el abuso y el uso indebido de la información personal» (artículo 31, apartado 2, punto 4, de la LPIP). Además, el responsable del tratamiento tiene la obligación de llevar a cabo «el control y la supervisión adecuados» de los miembros de su personal que traten datos personales, incluso en lo que se refiere a su gestión segura; esto abarca la formación («educación») necesaria de los empleados (artículo 28, apartados 1 y 2, de la LPIP). Por último, en el caso del subtratamiento, el responsable del tratamiento debe imponer requisitos al «proveedor externo», entre otras cosas, en lo que se refiere a la gestión segura de los datos personales («salvaguardias técnicas y administrativas») y debe supervisar la manera en que se aplican mediante inspecciones (artículo 26, apartados 1 y 4, de la LPIP, en relación con el artículo 28, apartado 1, puntos 3 y 4, y apartado 6, del Decreto de Ejecución de la LPIP).

2.3.7 *Transparencia*

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

([85]) Con respecto al tratamiento de datos personales por parte de los proveedores de servicios de información y comunicación, el artículo 39-5 de la LPIP establece explícitamente que el número de personas que manejan la información personal de los usuarios deberá limitarse al mínimo. Además, los proveedores de servicios de información y comunicación deberán garantizar que la información personal de los usuarios no esté expuesta al público a través de la red de información y comunicaciones (artículo 39-10, apartado 1, de la LPIP). La información expuesta debe suprimirse o bloquearse a petición de la CPIP (artículo 39-10, apartado 2, de la LPIP). De manera más general, los proveedores de servicios de información y comunicación (y los terceros que reciben datos personales de los usuarios) están sujetos a obligaciones de seguridad adicionales, especificadas en el artículo 48-2 del Decreto de Ejecución de la LPIP, por ejemplo, el desarrollo y la aplicación de un plan de gestión interna con respecto a las medidas de seguridad, las medidas para garantizar el control de acceso, el cifrado, el uso de programas informáticos para detectar programas maliciosos, etc.

([86]) Además, existe una prohibición general de dañar, destruir, alterar, falsificar o filtrar información personal sin autoridad jurídica (véase el artículo 59, apartado 3, de la LPIP).

([87]) El requisito de notificar a la persona no se aplica en la medida en que se produzca una violación de los datos con respecto a la información seudonimizada tratada con fines estadísticos, de investigación científica o de archivo en interés público (artículo 28-7 de la LPIP, que establece una exención del artículo 34, apartado 1, y del artículo 39-4 de la LPIP). Garantizar la notificación individual requeriría que el responsable del tratamiento en cuestión identificase a los particulares del conjunto de datos seudonimizado, lo cual está expresamente prohibido en virtud del artículo 28-5 de la LPIP. Sin embargo, sigue siendo de aplicación el requisito general de notificación de las violaciones de la seguridad de los datos (a la CPIP).

([88]) Los requisitos de notificación, incluidos el momento en que se realiza y la posibilidad de una notificación «por etapas», se especifican con más detalle en el artículo 40 del Decreto de Ejecución de la LPIP. Se aplican normas más estrictas a los proveedores de servicios de información y comunicación que están obligados a notificar al interesado y a la CPIP en un plazo de veinticuatro horas tras haber tenido conocimiento de que la información personal ha sido extraviada, robada o filtrada (artículo 39-4, apartado 1, de la LPIP). Esta notificación debe incluir los detalles de la información personal que ha sido filtrada, el momento en que esto ha ocurrido, las medidas que puede adoptar el usuario, las medidas de respuesta adoptadas por el proveedor y los datos de contacto del departamento al que el usuario puede dirigir preguntas (artículo 39-4, apartado 1, puntos 1 a 5, de la LPIP). Si existe un motivo justificable, por ejemplo, no contar con los datos de contacto del usuario, pueden utilizarse otros medios de notificación, por ejemplo, poner la información a disposición del público en un sitio web (artículo 39-4, apartado 1, de la LPIP, en relación con el artículo 48-4, apartado 4 y siguientes, del Decreto de Ejecución de la LPIP). En tal caso, la CPIP debe ser informada de los motivos (artículo 34-4, apartado 3, de la LPIP).

([89]) Véanse, por ejemplo, las Resoluciones del Tribunal Supremo 2011Da59834, 2011Da59858 y 2011Da59841, de 26 de diciembre de 2012. Un resumen en inglés está disponible en el siguiente enlace: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Esto se garantiza de distintas maneras en el sistema coreano. Además del derecho a la información en virtud del artículo 4, apartado 1 (en general), y el artículo 20, apartado 1, de la LPIP (para los datos personales recogidos de terceros), así como el derecho de acceso en virtud del artículo 35 de la LPIP, la LPIP incluye un requisito general de transparencia con respecto a la finalidad del tratamiento (artículo 3, apartado 1, de la LPIP) y requisitos específicos de transparencia en caso de que el tratamiento se base en el consentimiento (artículo 15, apartado 2; artículo 17, apartado 2, y artículo 18, apartado 3, de la LPIP) ([90]). Además, el artículo 20, apartado 2, de la LPIP exige que determinados responsables del tratamiento —aquellos cuyo tratamiento supera ciertos umbrales ([91])— notifiquen al interesado cuyos datos personales hayan recibido de un tercero la fuente de información, la finalidad del tratamiento y el derecho del interesado a solicitar la suspensión del tratamiento, salvo que dicha notificación resulte imposible debido a la falta de información de contacto. Se aplican excepciones para determinados ficheros de datos personales que obran en poder de las autoridades públicas, sobre todo los que contienen datos tratados por razones de seguridad nacional, otros intereses nacionales particularmente importantes («graves») o a efectos de control de la aplicación del Derecho penal o cuando la notificación pueda atentar contra la vida o la integridad física de un tercero o vulnere deslealmente los intereses patrimoniales y otros intereses de un tercero, pero solo cuando los intereses públicos o privados en juego sean «manifiestamente superiores» a los derechos de los interesados afectados (artículo 20, apartado 4, de la LPIP). Para ello, se requiere encontrar un equilibrio entre los diferentes intereses.

(68) Además, el artículo 3, apartado 5, de la LPIP establece que los responsables del tratamiento deberán hacer pública su política de privacidad (y otras cuestiones relacionadas con el tratamiento de datos personales). Este requisito se especifica con más detalle en el artículo 30 de la LPIP, en relación con el artículo 31 del Decreto de Ejecución de la LPIP. Según estas disposiciones, la política de privacidad pública debe incluir, entre otras cosas, 1) los tipos de datos personales tratados, 2) la finalidad del tratamiento, 3) el período de conservación, 4) si los datos personales se facilitan a un tercero ([92]), 5) cualquier subtratamiento, 6) información sobre los derechos del interesado y cómo ejercerlos y 7) información de contacto (incluido el nombre del responsable de la protección de la privacidad o el departamento interno responsable de garantizar el cumplimiento de las normas de protección de datos y la tramitación de las reclamaciones). La política de privacidad debe ponerse a disposición del público de tal manera que los interesados «puedan reconocerla con facilidad» (artículo 30, apartado 2, de la LPIP) ([93]) y debe actualizarse constantemente (artículo 31, apartado 2, del Decreto de Ejecución de la LPIP).

(69) Las instituciones públicas están sujetas a una obligación adicional de registrar, en particular, la siguiente información con la CPIP: 1) el nombre de la institución pública, 2) los motivos y finalidades del tratamiento de los ficheros de datos personales, 3) los detalles de los datos personales registrados, 4) el método de tratamiento, 5) el período de conservación, 6) el número de interesados cuyos datos personales se conservan, 7) el departamento que tramita las solicitudes de los interesados y 8) los destinatarios de los datos personales cuando estos últimos se facilitan de forma rutinaria o repetitiva (artículo 32, apartado 1, de la LPIP) ([94]). La CPIP hace públicos los ficheros de datos personales registrados, a los cuales las instituciones públicas también deben hacer referencia en su política de privacidad (artículo 30, apartado 1, y artículo 32, apartado 4, de la LPIP).

(70) A fin de aumentar la transparencia para los interesados de la Unión cuyos datos personales se transfieren a Corea sobre la base de la presente Decisión, la sección 3, incisos i) y ii), de la Nota n.º 2021-5 (anexo I) impone requisitos de transparencia adicionales. En primer lugar, cuando se reciban datos personales de la Unión sobre la base de la presente Decisión, los responsables del tratamiento coreanos deben notificar sin demora injustificada a los interesados de que se trate (y, en cualquier caso, a más tardar un mes después de la transferencia) el nombre y los datos de contacto de las entidades que transfieren y reciben la información, los datos personales (o las categorías de datos personales) transferidos, la finalidad de la recogida por parte del responsable del tratamiento

([90]) En particular, cuando la información personal se trate con el consentimiento de una persona, el responsable del tratamiento debe informar a esa persona de la finalidad del tratamiento, de los detalles de la información que será tratada, del destinatario de la información, del período durante el cual se conservará y utilizará la información personal, así como de que la persona tiene derecho a negar el consentimiento (y cualquier desventaja que pueda derivarse de ello).

([91]) De conformidad con el artículo 15-2, apartado 1, del Decreto de Ejecución de la LPIP, esto concierne a los responsables del tratamiento que tratan información sensible de, al menos, 50 000 interesados, o información personal «normal» de, al menos, un millón de interesados. El artículo 15-2, apartado 2, del Decreto de Ejecución de la LPIP establece los métodos y el momento de notificación, y el artículo 15-2, apartado 3, el requisito de mantener determinados registros al respecto. Además, se aplican normas específicas a determinadas categorías de proveedores de servicios de información y comunicación (aquellos que generaron ingresos por ventas de 10 000 millones de won, como mínimo, durante el ejercicio anterior o aquellos que almacenaron o gestionaron datos personales de al menos un millón de usuarios al día, por término medio, durante los tres meses precedentes al final del ejercicio anterior), que están obligados a notificar periódicamente a los usuarios el historial de utilización de sus datos personales, salvo que resulte imposible debido a la falta de información de contacto (artículo 39-8 de la LPIP y artículo 48-6 del Decreto de Ejecución de la LPIP).

([92]) Según la información recibida del Gobierno coreano, esto implica la obligación de indicar a los destinatarios en la política de privacidad pública de forma individual.

([93]) En el artículo 31, apartado 3, del Decreto de Ejecución de la LPIP se establecen otras modalidades.

([94]) El requisito de registro no se aplica a determinados tipos de ficheros de información personal, por ejemplo, los que registran cuestiones relacionadas con la seguridad nacional, los secretos diplomáticos, las investigaciones penales, el enjuiciamiento, las penas, las investigaciones de delitos relacionados con la fiscalidad o los ficheros relacionados exclusivamente con el desempeño de funciones internas (artículo 32, apartado 2, de la LPIP).

coreano, el período de conservación y los derechos disponibles en virtud de la LPIP. En segundo lugar, cuando se faciliten a terceros datos personales recibidos de la Unión sobre la base de la presente Decisión, los interesados deben ser informados, entre otras cosas, sobre el destinatario, los datos personales o las categorías de datos personales que deben facilitarse y el país al que se facilitan los datos (si procede), así como los derechos disponibles en virtud de la LPIP ([95]). De este modo, la Nota garantiza que los particulares de la UE sigan estando informados de los responsables específicos del tratamiento de su información y puedan ejercer sus derechos frente a las entidades correspondientes.

(71) La sección 3, inciso iii), de la Nota (anexo I) permite algunas excepciones limitadas y con reservas a estas obligaciones de transparencia adicionales que son esencialmente equivalentes a las previstas en el Reglamento (UE) 2016/679. En particular, no es obligatorio notificar a los interesados de la Unión 1) cuando sea necesario restringir la notificación por determinadas razones de interés público (por ejemplo, cuando la información se trate con fines de seguridad nacional o investigaciones penales en curso), en la medida en que estos objetivos de interés público sean manifiestamente superiores a los derechos del interesado; 2) cuando el interesado ya disponga de la información; 3) cuando la notificación pueda atentar contra la vida o la integridad física del particular o de un tercero o vulnerar deslealmente los intereses patrimoniales de un tercero, en el caso de que dichos derechos o intereses sean manifiestamente superiores a los derechos del interesado; o 4) cuando no se disponga de los datos de contacto de los particulares de que se trate o cuando sea necesario un esfuerzo desproporcionado para notificarlas. A la hora de determinar si es posible o no ponerse en contacto con el interesado o si ello supone un esfuerzo excesivo, se tendrá en cuenta la posibilidad de cooperar con el exportador de datos en la Unión.

(72) Las normas de los considerandos 67 a 71 garantizan, por tanto, un nivel de protección con respecto a la transparencia esencialmente equivalente al previsto en el Reglamento (UE) 2016/679.

2.3.8 *Derechos individuales*

(73) Los interesados deben tener ciertos derechos que puedan hacer valer ante el responsable o el encargado del tratamiento, en concreto, el derecho de acceso a los datos, el derecho de rectificación, el derecho a oponerse al tratamiento y el derecho de supresión de datos. Al mismo tiempo, estos derechos pueden estar sujetos a limitaciones, en la medida en que dichas limitaciones sean necesarias y proporcionadas para salvaguardar objetivos importantes de interés público general.

(74) De conformidad con el artículo 3, apartado 5, de la LPIP, el responsable del tratamiento deberá garantizar los derechos de los interesados mencionados en el artículo 4 de la LPIP y especificados con más detalle en los artículos 35 a 37, 39 y 39-2 de la LPIP.

(75) En primer lugar, los particulares tienen derecho a la información y derecho de acceso. Cuando el responsable del tratamiento recoja datos personales de un tercero —que siempre será el caso cuando los datos se transfieran desde la Unión—, los interesados tienen generalmente derecho a recibir información sobre 1) la «fuente» de los datos personales recogidos (es decir, el transferente), 2) la finalidad del tratamiento y 3) el hecho de que el interesado tiene derecho a solicitar la suspensión del tratamiento (artículo 20, apartado 1, de la LPIP). Se aplican excepciones limitadas, a saber, cuando dicha notificación pueda atentar contra la vida o la integridad física de un tercero o «vulnere deslealmente los intereses patrimoniales y otros intereses» de un tercero, pero solo cuando dichos intereses de terceros sean «explícitamente superiores» a los derechos del interesado (artículo 20, apartado 4, punto 2, de la LPIP).

(76) Además, el artículo 35, apartados 1 y 3, de la LPIP, en relación con el artículo 41, apartado 4, del Decreto de Ejecución de la LPIP, otorga a los interesados el derecho de acceso a su información personal ([96]). El derecho de acceso abarca la confirmación del tratamiento, información sobre el tipo de datos tratados, la finalidad del tratamiento y el período de conservación, así como cualquier divulgación a terceros y el suministro de una

([95]) Nota n.º 2021-5, sección 3, inciso ii) (anexo I).

([96]) De conformidad con el artículo 35, apartado 3, de la LPIP, en relación con el artículo 42, apartado 2, del Decreto de Ejecución de la LPIP, el responsable del tratamiento puede aplazar el acceso por «causa justificada» (es decir, por motivos justificados, por ejemplo, si se necesita más tiempo para evaluar si puede facilitarse el acceso), pero debe notificar al interesado dicha justificación en un plazo de diez días y proporcionar información sobre cómo recurrir esta decisión; tan pronto como deje de existir el motivo del aplazamiento, deberá concederse el acceso.

copia de la información personal tratada (artículo 4, apartado 3, de la LPIP, en relación con el artículo 41, apartado 1, del Decreto de Ejecución de la LPIP) ([97]). El acceso puede limitarse (acceso parcial) ([98]) o denegarse únicamente cuando así lo disponga la ley ([99]), cuando pueda atentar contra la vida o la integridad física de un tercero, o pueda dar lugar a una vulneración injustificada de los intereses patrimoniales y otros intereses de un tercero (artículo 35, apartado 4, de la LPIP) ([100]). Esto último implica que debe encontrarse un equilibrio entre los derechos y las libertades del particular protegidos por la Constitución, por una parte, y los de otras personas, por otra. Cuando se limite o deniegue el acceso, el responsable del tratamiento debe notificar al interesado los motivos y la forma de recurrir la decisión (artículo 41, apartado 5, y artículo 42, apartado 2, del Decreto de Ejecución de la LPIP).

(77) En segundo lugar, los interesados tienen derecho a la rectificación o supresión ([101]) de sus datos personales, «salvo que otras leyes dispongan expresamente lo contrario» (artículo 36, apartados 1 y 2, de la LPIP) ([102]). Cuando reciba una solicitud, el responsable del tratamiento debe investigar el asunto sin demora, adoptar las medidas necesarias ([103]) y notificar al respecto al interesado en un plazo de diez días; cuando no pueda accederse a la solicitud, este requisito de notificación abarca los motivos de la denegación y las vías de recurso (véase el artículo 36, apartado 4, de la LPIP, en relación con el artículo 43, apartado 3, del Decreto de Ejecución de la LPIP) ([104]).

(78) Por último, los interesados tienen derecho a solicitar la suspensión del tratamiento de sus datos personales, sin demora ([105]), salvo que se aplique una de las excepciones mencionadas (artículo 37, apartados 1 y 2, de la LPIP) ([106]). El responsable del tratamiento puede denegar la solicitud 1) cuando esté expresamente autorizado por la ley o sea necesario («inevitable») para cumplir obligaciones legales, 2) cuando la suspensión pueda atentar contra la vida o la integridad física de un tercero o dar lugar a una vulneración injustificada de los intereses patrimoniales y otros intereses de un tercero, 3) cuando sea imposible para una institución pública desempeñar sus funciones según lo establecido por la ley sin el tratamiento de la información, o 4) cuando el interesado no rescinda expresamente el contrato subyacente con el responsable del tratamiento, a pesar de que sería impracticable ejecutar el contrato sin el tratamiento de los datos. En este caso, el responsable del tratamiento debe notificar sin demora al interesado los motivos de la denegación y las vías de recurso (artículo 37, apartado 2, de la LPIP, en relación con el artículo 44, apartado 2, del Decreto de Ejecución de la LPIP). De conformidad con el artículo 37, apartado 4, de la LPIP, el responsable del tratamiento debe «adoptar sin demora las medidas necesarias, incluida la destrucción de la información personal pertinente» a efectos del cumplimiento de la solicitud de suspensión ([107]).

(79) El derecho a la suspensión también se aplica cuando los datos personales se utilizan con fines de comercialización directa, es decir, para promover bienes o servicios o solicitar su compra. Además, este tratamiento ulterior suele requerir el consentimiento expreso (adicional) del interesado (véanse el artículo 15, apartado 1, punto 1, y el artículo 17, apartado 2, punto 1, de la LPIP) ([108]). Al solicitar este consentimiento, el responsable del tratamiento debe informar al interesado especialmente de la utilización prevista de los datos para fines de comercialización

([97]) El acceso a la información personal tratada por una institución pública puede obtenerse directamente de la institución o de forma indirecta presentando una solicitud a la CPIP, que la transmitirá sin demora (artículo 35, apartado 2, de la LPIP y artículo 41, apartado 3, del Decreto de Ejecución de la LPIP).

([98]) De conformidad con el artículo 42, apartado 1, del Decreto de Ejecución de la LPIP, el responsable del tratamiento está obligado a conceder un acceso parcial cuando al menos una parte de la información no esté cubierta por los motivos de la denegación.

([99]) A su vez, dicha ley debe respetar el derecho fundamental a la privacidad y a la protección de datos, así como los principios de necesidad y proporcionalidad establecidos en la Constitución coreana.

([100]) Además, las instituciones públicas pueden denegar el acceso si tal acceso puede causar graves dificultades para desempeñar determinadas funciones, incluidas las auditorías en curso o la imposición, la recaudación o el reembolso de impuestos (artículo 35, apartado 4, de la LPIP).

([101]) En este caso, el responsable del tratamiento debe adoptar medidas para impedir la recuperación de la información personal (véase el artículo 36, apartado 3, de la LPIP).

([102]) Tales leyes deben cumplir los requisitos de la Constitución de que un derecho fundamental solo puede restringirse cuando sea necesario por razones de seguridad nacional o para el mantenimiento del orden público en aras del bienestar público y no puede afectar al contenido esencial de la libertad o el derecho (artículo 37, apartado 2, de la Constitución).

([103]) El artículo 43, apartado 2, del Decreto de Ejecución de la LPIP establece un procedimiento especial en caso de que el responsable del tratamiento trate ficheros de información personal facilitados por otro responsable del tratamiento.

([104]) La falta de adopción de las medidas necesarias para rectificar o suprimir la información personal y el uso continuo o el suministro de dicha información a un tercero pueden dar lugar a sanciones penales (artículo 73, apartado 2, de la LPIP).

([105]) De conformidad con el artículo 44, apartado 2, del Decreto de Ejecución de la LPIP, el responsable del tratamiento deberá informar al interesado de que ha suspendido debidamente el tratamiento en un plazo de diez días a partir de la recepción de la solicitud.

([106]) En cuanto a las instituciones públicas, el derecho a la suspensión del tratamiento puede ejercerse con respecto a la información contenida en los ficheros registrados de información personal (artículo 37, en relación con el artículo 32 de la LPIP). Este registro no es obligatorio en un número limitado de situaciones, por ejemplo, cuando los ficheros de información personal están relacionados con la seguridad nacional, investigaciones penales, relaciones diplomáticas, etc. (artículo 32, apartado 2, de la LPIP).

([107]) La falta de suspensión del tratamiento puede dar lugar sanciones penales (artículo 73, apartado 3, de la LPIP).

([108]) El Comité de mediación de conflictos (véase el considerando 133) ha tratado varios casos en los que particulares se quejaron del uso de sus datos con fines de comercialización directa sin consentimiento, lo cual, por ejemplo, ha dado lugar al pago de una indemnización y a la supresión de datos personales por parte del responsable del tratamiento correspondiente [véanse, por ejemplo, Comité de mediación de conflictos 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)].

directa —es decir, del hecho de que puede ser contactado para promocionar bienes o servicios o solicitar su compra— de «manera explícitamente reconocible» (artículo 22, apartados 2 y 4, de la LPIP, en relación con el artículo 17, apartado 2, punto 1, del Decreto de Ejecución de la LPIP).

(80) A fin de facilitar el ejercicio de los derechos individuales, el responsable del tratamiento debe establecer procedimientos específicos y anunciarlos públicamente (artículo 38, apartado 4, de la LPIP) ([109]). Esto incluye los procedimientos para formular objeciones contra la denegación de una solicitud (artículo 38, apartado 5, de la LPIP). El responsable del tratamiento debe garantizar que el procedimiento para el ejercicio de los derechos sea «fácil para los interesados» y que no sea más difícil que el procedimiento para la recogida de los datos personales; esto también incluye la obligación de facilitar información sobre el procedimiento en su sitio web (artículo 41, apartado 2; artículo 43, apartado 1, y artículo 44, apartado 1, del Decreto de Ejecución de la LPIP) ([110]). Los particulares pueden autorizar a un representante para que presente dicha solicitud (artículo 38, apartado 1, de la LPIP, en relación con el artículo 45 del Decreto de Ejecución de la LPIP). Si bien el responsable del tratamiento tiene derecho a cobrar un canon (y, en caso de que se solicite el envío de copias de los datos personales, franqueo), el importe debe determinarse «dentro de los gastos reales necesarios para el tratamiento de [la solicitud]»; no podrá imponerse ningún canon (ni franqueo) cuando el responsable del tratamiento haya originado la solicitud (artículo 38, apartado 3, de la LPIP, en relación con el artículo 47 del Decreto de Ejecución de la LPIP).

(81) La LPIP y su Decreto de Ejecución 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, en lo que respecta a los datos personales que hayan sido recogidos en la Unión, 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 ([111]). Esto comprende los escenarios de transferencias en los que el tratamiento lo lleva a cabo un operador económico extranjero (por ejemplo, coreano) que actúa como agente (encargado) por cuenta del responsable de la Unión (o como subencargado que actúa por cuenta del encargado de la Unión, que haya recibido los datos del responsable de la Unión 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.

(82) Como excepción, las disposiciones relativas a la transparencia previa solicitud (artículo 20) y los derechos individuales (artículos 35 a 37), así como el requisito de notificación individual para los proveedores de servicios de información y comunicación (artículo 39-8 de la LPIP), no se aplican con respecto a la información seudonimizada, cuando se trate con fines estadísticos, de investigación científica o de archivo en interés público (artículo 28-7 de la LPIP) ([112]). En consonancia con el enfoque del artículo 11, apartado 2 (en relación con el considerando 57), del Reglamento (UE) 2016/679, esto se justifica por el hecho de que, para garantizar la transparencia o conceder derechos individuales, el responsable del tratamiento tendría que identificar si alguno de los datos (y, en su caso, cuál) está relacionado con la persona que presenta la solicitud, lo cual está expresamente prohibido por la LPIP (artículo 28-5, apartado 1, de la LPIP). Además, si dicha reidentificación implica revertir la seudonimización de la totalidad del conjunto de datos (seudonimizados), expondría la información personal de todas las demás personas afectadas a mayores riesgos. Si bien el Reglamento (UE) 2016/679 hace referencia a situaciones en las que la reidentificación es prácticamente imposible, la LPIP adopta un enfoque más estricto al prohibir expresamente la reidentificación en todas las situaciones en las que se trate información seudonimizada.

(83) Por consiguiente, el sistema coreano, tal como se describe en los considerandos 74 a (82), contiene normas sobre los derechos de los interesados que proporcionan un nivel de protección esencialmente equivalente al previsto en el Reglamento (UE) 2016/679.

([109]) Véase también el artículo 30, apartado 1, punto 5, de la LPIP sobre la política de privacidad, que, entre otras cosas, deberá contener información sobre los derechos de que dispone la persona y cómo ejercerlos.

([110]) Véase también el artículo 39-7, apartado 2, de la LPIP con respecto a los proveedores de servicios de información y comunicación.

([111]) Por el contrario, puede existir excepcionalmente una relación directa entre el operador económico coreano y el interesado de la UE, lo que suele ser 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 económico coreano 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.

([112]) Véase también la Nota n.º 2021-5, que confirma que la sección III de la LPIP (incluido el artículo 28-7) solo se aplica cuando la información seudonimizada se trata con fines estadísticos, de investigación científica o de archivo en interés público (véase la sección 4 del anexo I de la presente Decisión).

2.3.9 *Transferencias ulteriores*

(84) El nivel de protección de los datos personales que se transfieren desde la Unión a responsables del tratamiento en la República de Corea no debe verse comprometido por la transferencia ulterior de dichos datos a destinatarios que se encuentran en un tercer país.

(85) Estas «transferencias ulteriores» constituyen transferencias internacionales desde la República de Corea, desde la perspectiva del responsable del tratamiento coreano. A este respecto, la LPIP distingue entre la externalización del tratamiento a un proveedor externo (es decir, un encargado del tratamiento) y el suministro de datos personales a terceros ([113]).

(86) En primer lugar, cuando el tratamiento de datos personales se externaliza a una entidad ubicada en un tercer país, el responsable del tratamiento coreano debe garantizar el cumplimiento de las disposiciones de la LPIP en materia de externalización (artículo 26 de la LPIP). Esto incluye la creación de un instrumento jurídicamente vinculante que, entre otras cosas, limite el tratamiento por parte del proveedor externo a la finalidad del trabajo externalizado, imponga salvaguardias técnicas y administrativas y limite el subtratamiento (véase el artículo 26, apartado 1, de la LPIP); y la publicación de información sobre el trabajo externalizado. Además, el responsable del tratamiento tiene la obligación de «educar» al proveedor externo sobre las medidas de seguridad necesarias y supervisar, incluso mediante inspecciones, si cumple todas las obligaciones del responsable del tratamiento en virtud de la LPIP ([114]) y del contrato de externalización.

(87) Si el proveedor externo causa daños al tratar los datos personales en contravención de la LPIP, esto se atribuirá al responsable del tratamiento a efectos de responsabilidad, como sería el caso de los empleados del responsable del tratamiento (artículo 26, apartado 6, de la LPIP). Por consiguiente, el responsable del tratamiento coreano sigue siendo responsable de los datos personales que se han externalizado y debe garantizar que el encargado del tratamiento extranjero trate la información de conformidad con la LPIP. Si el proveedor externo trata la información en contravención de la LPIP, el responsable del tratamiento coreano puede ser considerado responsable del incumplimiento de su obligación de garantizar el cumplimiento de la LPIP, por ejemplo, a través de su supervisión del proveedor externo. Las salvaguardias previstas en el contrato de externalización y la responsabilidad del responsable del tratamiento coreano en relación con las acciones del proveedor externo garantizan la continuidad de la protección cuando el tratamiento de datos personales se externaliza a una entidad fuera de Corea.

(88) En segundo lugar, los responsables del tratamiento coreanos pueden facilitar datos personales a un tercero ubicado fuera de Corea. Si bien la LPIP incluye una serie de fundamentos jurídicos que permiten el suministro a terceros en general, si el tercero está ubicado fuera de Corea, el responsable del tratamiento, en principio ([115]), debe obtener el consentimiento del interesado ([116]) tras haberle proporcionado información sobre 1) el tipo de datos personales, 2) el destinatario de los datos personales, 3) la finalidad de la transferencia en el sentido de la finalidad del tratamiento perseguida por el destinatario, 4) el período de conservación para el tratamiento por parte del destinatario y 5) el hecho de que el interesado puede negar su consentimiento (artículo 17, apartados 2 y 3, de la LPIP). La Nota n.º 2021-5, en su sección sobre la transparencia (véase el considerando 70), exige que se informe a los particulares sobre el tercer país al que se proporcionarán sus datos. Esto garantiza que los interesados de la Unión puedan tomar una decisión con pleno conocimiento de causa sobre si dar o no su consentimiento para un suministro internacional. Además, el responsable del tratamiento no debe celebrar ningún contrato con el tercero destinatario en violación de la LPIP, lo que significa que el contrato no debe contener obligaciones que contradigan los requisitos impuestos por la LPIP al responsable del tratamiento ([117]).

([113]) Se aplican normas específicas a los proveedores de servicios de información y comunicación. De conformidad con el artículo 39-12 de la LPIP, los proveedores de servicios de información y comunicación deben, en principio, obtener el consentimiento del usuario para toda transferencia internacional de información personal. En caso de que se transfiera información personal como parte de la externalización de las operaciones de tratamiento, también por lo que se refiere al almacenamiento, no se requiere el consentimiento si los particulares afectados han sido informados con antelación, directamente o mediante anuncio público de una manera que permita un fácil acceso, de 1) los detalles de la información que debe transferirse, 2) el país al que se transferirá la información (así como la fecha y el método de la transferencia), 3) el nombre del destinatario y 4) la finalidad de la utilización y la conservación por parte del destinatario (artículo 39-12, apartado 3, de la LPIP). Además, en ese caso, se aplicarán los requisitos generales para la externalización. Para cada transferencia, deben establecerse salvaguardias específicas con respecto a la seguridad, la gestión de reclamaciones y litigios, así como otras medidas necesarias para proteger la información de los usuarios (artículo 48-10 del Decreto de Ejecución de la LPIP).

([114]) Véase también el artículo 26, apartado 7, de la LPIP, según el cual los artículos 15 a 25, 27 a 31, 33 a 38 y 50 se aplican *mutatis mutandis* al encargado del tratamiento.

([115]) En caso de que los proveedores de servicios de información y comunicación faciliten información personal de los usuarios a terceros, siempre se requiere el consentimiento del usuario (artículo 39-12, apartado 2, de la LPIP).

([116]) Como se explica con más detalle en la nota al pie de página 51, para que dicho consentimiento sea válido, este debe darse de forma libre, informada y específica.

([117]) Véase también el artículo 39-12, apartado 1, de la LPIP con respecto a los proveedores de servicios de información y comunicación.

(89) Sin el consentimiento del particular, los datos personales pueden facilitarse a un tercero (extranjero) cuando la finalidad de la divulgación se mantenga «dentro del alcance razonablemente relacionado» con la finalidad inicial de la recogida (artículo 17, apartado 4, de la LPIP, véase el considerando 36). Sin embargo, a la hora de decidir si se divulgan (o no) los datos personales para una finalidad «relacionada», el responsable del tratamiento debe tener en cuenta si la divulgación ocasiona desventajas para el particular y si se han adoptado las medidas de seguridad necesarias (como el cifrado). Dado que el tercer país al que se transfieren los datos personales puede no ofrecer protecciones similares a las previstas en la LPIP, la sección 2 de la Nota n.º 2021-5 reconoce que tales desventajas pueden surgir y solo pueden evitarse si el responsable del tratamiento coreano y el destinatario extranjero, a través de un instrumento jurídicamente vinculante (como un contrato), garantizan un nivel de protección equivalente al previsto en la LPIP, incluso con respecto a los derechos de los interesados.

(90) Se aplican normas especiales a la divulgación «fuera de la finalidad», es decir, el suministro de datos a un tercero para una nueva finalidad (no relacionada), que solo puede tener lugar por uno de los motivos mencionados en el artículo 18, apartado 2, de la LPIP, como se describe en el considerando 39. Sin embargo, incluso en esas condiciones, el suministro a terceros queda excluido si es probable que «vulnere deslealmente» los intereses del interesado o de un tercero, lo que requiere encontrar un equilibrio entre los diferentes intereses. Además, de conformidad con el artículo 18, apartado 5, de la LPIP, el responsable del tratamiento debe aplicar salvaguardias adicionales, las cuales pueden comprender solicitar al tercero que restrinja la finalidad y el método del tratamiento o que establezca medidas de seguridad específicas. Una vez más, dado que el tercer país al que se transfieren los datos personales puede no ofrecer protecciones similares a las previstas en la LPIP, la sección 2 de la Nota n.º 2021-5 reconoce que tal «vulneración desleal» de los intereses del particular o de un tercero puede ocurrir y solo puede evitarse si el responsable del tratamiento coreano y el destinatario extranjero, a través de un instrumento jurídicamente vinculante (como un contrato), garantizan un nivel de protección equivalente al previsto en la LPIP, incluso con respecto a los derechos de los interesados.

(91) Por consiguiente, las normas de los considerandos 86 a 90 garantizan la continuidad de la protección cuando los datos personales se transfieren ulteriormente (a un «proveedor externo» o a un tercero) desde la República de Corea de una manera esencialmente equivalente a la prevista en el Reglamento (UE) 2016/679.

2.3.10 *Responsabilidad*

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

(93) De conformidad con el artículo 3, apartados 6 y 8, de la LPIP, el responsable del tratamiento deberá tratar los datos personales «de manera que se reduzca al mínimo la posibilidad de vulnerar» la privacidad del interesado y procurará obtener la confianza del interesado mediante la observación y el desempeño de tales funciones y responsabilidades según lo previsto en la LPIP y otras leyes conexas. Esto abarca el establecimiento de un plan de gestión interna (artículo 29 de la LPIP), así como la formación y supervisión adecuadas del personal (artículo 28 de la LPIP).

(94) Como medio para garantizar la responsabilidad, el artículo 31 de la LPIP, en relación con el artículo 32 del Decreto de Ejecución de la LPIP, establece una obligación para los responsables del tratamiento de designar a un responsable de la protección de la privacidad que «se haga cargo de manera global del tratamiento de la información personal». En particular, este responsable de la protección de la privacidad se encarga de desempeñar las siguientes funciones: 1) establecimiento y aplicación de un plan de protección de los datos personales y elaboración de la política de privacidad, 2) realización de encuestas periódicas sobre el estado y las prácticas del tratamiento de los datos personales, con vistas a mejorar cualquier deficiencia, 3) tramitación de reclamaciones y compensación correctora, 4) establecimiento de un sistema de control interno para evitar la divulgación, el abuso o el uso indebido de los datos personales, 5) preparación y aplicación de un programa educativo, 6) protección, control y gestión de los ficheros de datos personales y 7) destrucción de los datos personales una vez lograda la finalidad del tratamiento o expirado el período de conservación. En el desempeño de estas funciones, el responsable de la protección de la privacidad puede inspeccionar el estado del tratamiento de los datos personales y de los sistemas relacionados, y solicitar información al respecto (artículo 31, apartado 3, de la LPIP). Si el responsable de la protección de la privacidad tiene conocimiento de alguna infracción de la LPIP u otras leyes pertinentes en materia de protección de datos, adoptará de inmediato medidas correctoras e informará de ellas a la dirección («jefe») del responsable del tratamiento, en caso necesario (artículo 31, apartado 4, de la LPIP). De conformidad con el artículo 31, apartado 5, de la LPIP, el responsable de la protección de la privacidad no debe sufrir desventajas injustificadas como consecuencia del desempeño de estas funciones.

(95) Además, los responsables del tratamiento deben esforzarse proactivamente por llevar a cabo una evaluación del impacto sobre la privacidad en caso de que la gestión de ficheros de datos personales implique un riesgo para la misma (artículo 33, apartado 8, de la LPIP). Sobre la base del artículo 33, apartados 1 y 2, de la LPIP, en relación con los artículos 35, 36 y 38 del Decreto de Ejecución de la LPIP, los factores como el tipo y la naturaleza de los datos tratados (en particular si constituyen información sensible), su volumen, el período de conservación y la probabilidad de violaciones de la seguridad de los datos serán pertinentes para evaluar el grado de riesgo para los derechos de los interesados. El objetivo de la evaluación del impacto sobre la privacidad es garantizar que se analicen los factores de riesgo para la privacidad, así como cualquier contramedida de seguridad o de otra índole, e indicar los aspectos que deben mejorarse (véase el artículo 33, apartado 1, de la LPIP, en relación con el artículo 38 del Decreto de Ejecución de la LPIP).

(96) Las instituciones públicas tienen la obligación de llevar a cabo una evaluación de impacto cuando traten determinados ficheros de datos personales que presenten un mayor riesgo de posibles violaciones de la privacidad (artículo 33, apartado 1, de la LPIP). De conformidad con el artículo 35 del Decreto de Ejecución de la LPIP, este es el caso, entre otros, de los ficheros que contienen información sensible sobre al menos 50 000 interesados, los ficheros que irán acompañados de otros y, en consecuencia, contendrán información sobre al menos 500 000 interesados, o los ficheros que contienen información sobre un millón de interesados, como mínimo. El resultado de una evaluación de impacto realizada por una institución pública debe comunicarse a la CPIP (artículo 33, apartado 1, de la LPIP), que puede emitir un dictamen (artículo 33, apartado 3, de la LPIP).

(97) Por último, el artículo 13 de la LPIP estipula que la CPIP establecerá las políticas necesarias para promover y apoyar las «actividades de autorregulación en materia de protección de datos» realizadas por los responsables del tratamiento, entre otras cosas, mediante la educación en materia de protección de datos, la promoción y el apoyo a las organizaciones dedicadas a la protección de datos, y ayudando a los responsables del tratamiento a establecer y aplicar normas de autorregulación. Además, introducirá y facilitará el sistema de marcado ePRIVACY. A este respecto, el artículo 32-2 de la LPIP, en relación con los artículos 34-2 a 34-8 del Decreto de Ejecución de la LPIP, prevé la posibilidad de certificar que el sistema o los sistemas de protección y tratamiento de datos personales del responsable del tratamiento cumplen los requisitos de la LPIP. Según estas normas, puede concederse una certificación ([118]) (por un período de tres años) si el responsable del tratamiento cumple los criterios de certificación determinados por la CPIP, incluido el establecimiento de salvaguardias técnicas, físicas y de gestión para proteger los datos personales ([119]). La CPIP debe examinar los sistemas del responsable del tratamiento pertinentes para la certificación al menos una vez al año para mantener su eficacia, lo cual puede dar lugar a la revocación de la certificación (artículo 32, apartado 4, de la LPIP, en relación con el artículo 34-5 del Decreto de Ejecución de la LPIP; la denominada «gestión de seguimiento»).

(98) Por consiguiente, el marco coreano aplica el principio de responsabilidad de manera que se garantice un nivel de protección esencialmente equivalente al previsto en el Reglamento (UE) 2016/679, incluso previendo diferentes mecanismos para garantizar y demostrar el cumplimiento de la LPIP.

2.3.11 *Normas especiales para el tratamiento de la información crediticia personal*

(99) Tal como se describe en el considerando 13, la Ley sobre el uso y la protección de la información crediticia (LIC) establece normas específicas para el tratamiento de la información crediticia personal por parte de los operadores comerciales. Por consiguiente, a la hora de tratar información crediticia personal, los operadores comerciales deben cumplir los requisitos generales de la LPIP, salvo que la LIC contenga normas más específicas. Este será el caso, por ejemplo, cuando traten información relacionada con una tarjeta de crédito o cuenta bancaria en el contexto de una transacción comercial con un particular. Como legislación sectorial para el tratamiento de la información crediticia (tanto personal como no personal), la LIC no solo impone salvaguardias específicas de protección de datos (por ejemplo, en términos de transparencia y seguridad), sino que también regula de manera más general las circunstancias específicas en las que puede tratarse la información crediticia personal. Esto se ve reflejado, en particular, en los requisitos detallados para la utilización, el suministro de datos a un tercero y la conservación de dichos datos.

(100) Al igual que la LPIP, la LIC refleja los principios de licitud y proporcionalidad. En primer lugar, como requisito general, el artículo 15, apartado 1, de la LIC solo permite la recogida de información crediticia personal por medios razonables y justos, y en la menor medida necesaria para responder a una finalidad específica, de conformidad con el artículo 3, apartados 1 y 2, de la LPIP En segundo lugar, la LIC regula específicamente la licitud del tratamiento de la información crediticia personal, al limitar su recogida, utilización y suministro a terceros y, en general, al vincular dichas actividades de tratamiento al requisito de consentimiento de la persona de que se trate.

([118]) Además, si el responsable del tratamiento pretende hacer referencia a la certificación o promoverla en sus operaciones comerciales, puede utilizar la marca de protección de la información personal establecida por la CPIP. Véase el artículo 34-7 del Decreto de Ejecución de la LPIP.

([119]) Desde noviembre de 2018, se ha desarrollado el «Sistema de Gestión de la Información Personal y la Seguridad de la Información» (SGSI-P), que certifica que los responsables del tratamiento aplican un sistema de gestión global.

(101) La información crediticia personal puede recogerse sobre la base de uno de los motivos previstos por la LPIP o por motivos específicos establecidos en la LIC. Dado que el artículo 45 del Reglamento (UE) 2016/679 presupone una transferencia de datos personales por parte de un responsable o un encargado del tratamiento en la Unión, pero no abarca la recogida directa (por ejemplo, de un particular o de un sitio web) por un responsable del tratamiento en Corea, solo el consentimiento y los motivos disponibles en virtud de la LPIP son pertinentes para la presente Decisión. Estos motivos incluyen, en particular, los escenarios en que la transferencia es necesaria para ejecutar un contrato con la persona o para los intereses legítimos del responsable del tratamiento coreano (artículo 15, apartado 1, puntos 4 y 6, de la LPIP) ([120]).

(102) Una vez recogida, la información crediticia personal puede utilizarse 1) para la finalidad original con la que fue facilitada (directamente) por la persona ([121]); 2) para un fin compatible con la finalidad original de la recogida ([122]); 3) para determinar si se establece o mantiene una relación comercial solicitada por la persona ([123]); 4) para fines estadísticos, de investigación y de archivo en interés público ([124]) si la información está seudonimizada ([125]); 5) si se obtiene un consentimiento adicional o 6) de conformidad con la ley.

(103) Si un operador comercial tiene la intención de divulgar información crediticia personal a un tercero, debe obtener el consentimiento de la persona ([126]) tras informarla del destinatario de los datos, la finalidad del tratamiento por parte del destinatario, los detalles de los datos que se han de facilitar, el período de conservación por parte del destinatario y el derecho a negar el consentimiento (artículo 32, apartado 1, de la LIC y artículo 28, apartado 2, del Decreto de Ejecución de la LIC) ([127]). Este requisito de consentimiento no se aplica en situaciones específicas, a saber, cuando la información crediticia personal se divulgue ([128]): 1) a un proveedor externo con fines de externalización ([129]); 2) a un tercero en caso de traspaso, división o fusión de una empresa; 3) para fines estadísticos, de investigación y de archivo en interés público si la información está seudonimizada; 4) para un fin compatible con la finalidad original de la recogida; 5) a un tercero que utilice la información para recaudar una deuda de la persona ([130]); 6) para cumplir una resolución judicial; 7) a un fiscal o agente de la policía judicial

([120]) La LIC también contiene otras bases jurídicas para la recogida, por ejemplo, cuando así lo exija la legislación, cuando la información sea publicada por una institución pública con arreglo a la legislación en materia de libertad de información o cuando la información esté disponible en una red social. Para que el operador comercial pueda acogerse a este último motivo, debe poder demostrar que la recogida se mantiene dentro del alcance del consentimiento del interesado, sobre la base de una interpretación («objetiva») razonable y teniendo en cuenta la naturaleza de los datos, la intención y la finalidad de ponerlos a disposición en la red social, si la finalidad de la recogida es «muy pertinente» para ese fin, etc. (artículo 13 del Decreto de Ejecución de la LIC). Sin embargo, como se explica en el considerando 101, estos motivos no serán, en principio, pertinentes en un escenario de transferencia.

([121]) Por ejemplo, cuando la información crediticia se genera o facilita en el contexto de una transacción comercial con la persona. Sin embargo, este motivo no puede invocarse para utilizar la información crediticia personal con fines de comercialización directa (véase el artículo 33, apartado 1, punto 3, de la LIC).

([122]) Para determinar si la finalidad de uso es compatible con la finalidad original de la recogida, deben tenerse en cuenta los siguientes factores: 1) la relación («pertinencia») entre las dos finalidades; 2) la forma en que se recogió la información; 3) el impacto de la utilización sobre el particular y 4) si se han aplicado las medidas de seguridad adecuadas, tales como la seudonimización (véase el artículo 32, apartado 6, punto 9-4 de la LIC).

([123]) Por ejemplo, un responsable del tratamiento puede tener que tomar en cuenta la información crediticia personal que haya recibido de una persona para decidir si se amplía el plazo de un préstamo a dicha persona.

([124]) Artículo 33 de la LIC, en relación con su artículo 32, apartado 6, puntos 9-2, 9-4 y 10.

([125]) El artículo 2, apartado 15, de la LIC define la seudonimización como el tratamiento de información crediticia personal de tal manera que las personas ya no puedan ser identificadas a partir de la información, salvo en combinación con información adicional. Aunque la LIC contiene salvaguardias específicas para el tratamiento de información seudonimizada con fines estadísticos, de investigación y de archivo en interés público (artículo 40-2 de la LIC), estas normas no se aplican a las organizaciones comerciales. En su lugar, estas últimas siguen estando sujetas a los requisitos específicos de la sección III de la LPIP, tal como se describe en los considerandos 42 a 48. Además, el artículo 40-3 de la LIC exime al tratamiento de la información crediticia seudonimizada —cuando se lleve a cabo con fines estadísticos, de investigación científica o de archivo en interés público— de los requisitos en materia de transparencia y derechos individuales, de forma similar a la excepción establecida en el artículo 28-7 de la LPIP y con sujeción a las salvaguardias de la sección III de la LPIP, tal como se describe con más detalle en los considerandos 42 a 48.

([126]) Esto no se aplica cuando la información se facilite a un tercero a fin de mantener la información crediticia personal exacta y actualizada, siempre que el suministro se mantenga dentro de la finalidad original del tratamiento (artículo 32, apartado 1, de la LIC). Esto puede ocurrir, por ejemplo, cuando se facilite información actualizada a una agencia de calificación crediticia para garantizar que sus registros sean exactos.

([127]) Si no resulta práctico facilitar la información antes mencionada, puede ser suficiente remitir a la persona al tercero destinatario para obtener la información necesaria.

([128]) Dado que la LIC no regula específicamente la comunicación internacional de información crediticia personal, dicha comunicación debe cumplir las salvaguardias para las transferencias ulteriores impuestas por la sección 2 de la Nota n.º 2021-5.

([129]) La externalización del tratamiento de la información crediticia personal solo puede tener lugar sobre la base de un contrato escrito y de conformidad con los requisitos del artículo 26, apartados 1 a 3 y apartado 5, de la LPIP, tal como se describe en el considerando 20 (artículo 17 de la LIC y artículo 14 del Decreto de Ejecución de la LIC). El proveedor externo no puede utilizar la información más allá del alcance de las funciones externalizadas y la empresa de externalización debe establecer requisitos de seguridad específicos (por ejemplo, el cifrado) y educar al proveedor externo sobre cómo evitar que la información crediticia sea extraviada, robada, divulgada o alterada o se vea comprometida.

([130]) Véase también el artículo 28, apartado 10, puntos 1, 2 y 6, del Decreto de Ejecución de la LIC.

en una situación de emergencia en la que la vida de la persona esté en peligro o se prevea que sufra lesiones corporales y no se disponga de tiempo para emitir una orden judicial ([131]); 8) a las autoridades tributarias competentes para cumplir la legislación fiscal; o 9) de conformidad con otras leyes. En caso de divulgación por alguno de estos motivos, deberá notificarse previamente al interesado (artículo 32, apartado 7, de la LIC).

(104) La LIC también regula específicamente la duración del tratamiento de la información crediticia personal sobre la base de uno de esos motivos de uso o suministro a un tercero una vez finalizada la relación comercial con la persona ([132]). Solo puede conservarse la información que era necesaria para establecer o mantener dicha relación, con sujeción a salvaguardias adicionales (debe mantenerse separada de la información crediticia relativa a las personas con quienes existe una relación comercial en curso, estar protegida mediante medidas de seguridad específicas y ser accesible únicamente por personas autorizadas) ([133]). Todos los demás datos deben suprimirse (artículo 17-2, apartado 1, punto 2, del Decreto de Ejecución de la LIC). Para determinar qué datos eran necesarios para la relación comercial, deben tenerse en cuenta diferentes factores, por ejemplo, si habría sido posible establecer la relación sin los datos y si estos están directamente relacionados con los bienes o servicios suministrados al particular (artículo 17-2, apartado 2, del Decreto de Ejecución de la LIC).

(105) Incluso en los casos en que, en principio, la información crediticia personal pueda conservarse más allá del fin de la relación comercial, debe suprimirse en un plazo de tres meses a partir de la consecución de la finalidad adicional del tratamiento ([134]) o, en cualquier caso, al cabo de cinco años (artículo 20-2 de la LIC). En un número limitado de circunstancias, la información crediticia personal puede conservarse durante más de cinco años, en particular cuando esto sea necesario para cumplir una obligación legal, cuando sea necesario para los intereses vitales en relación con la vida, la integridad física o la propiedad de un particular, para el archivo de información seudonimizada (utilizada con fines estadísticos, de investigación científica o de archivo en interés público) o con fines de aseguramiento (en particular, para los pagos de seguros o para prevenir los fraudes a seguros) ([135]). En estos casos excepcionales, se aplican salvaguardias específicas (como la notificación al particular de la utilización ulterior, la separación de la información conservada de la información relativa a los particulares con las que aún existe una relación comercial y la limitación de los derechos de acceso, véase el artículo 17-2, apartados 1 y 2, del Decreto de Ejecución de la LIC).

(106) La LIC también especifica con más detalle los principios de exactitud y calidad de los datos, exigiendo que la información crediticia personal «se registre, modifique y gestione» para mantener su exactitud y actualizarla (artículo 18, apartado 1, de la LIC y artículo 15, apartado 3, del Decreto de Ejecución de la LIC) ([136]). Cuando faciliten información crediticia a otras entidades (como las agencias de calificación crediticia), los operadores comerciales también están obligados específicamente a verificar la exactitud de la información para garantizar que el destinatario solo registre y gestione información exacta (artículo 15, apartado 1, del Decreto de Ejecución de la LIC, en relación con el artículo 18, apartado 1, de la LIC). De manera más general, la LIC exige que se mantengan registros sobre la recogida, la utilización, la divulgación a terceros y la destrucción de información crediticia personal (artículo 20, apartado 2, de la LIC) ([137]).

(107) Además, el tratamiento de la información crediticia personal está sujeto a requisitos específicos con respecto a la seguridad de los datos. En particular, la LIC exige la aplicación de medidas tecnológicas, físicas y organizativas para evitar el acceso ilícito a los sistemas informáticos, así como la alteración, la destrucción o cualquier otro riesgo para los datos tratados (por ejemplo, mediante controles de acceso, véase el artículo 19 de la LIC y el artículo 16 del Decreto de Ejecución de la LIC). Asimismo, cuando se intercambie información crediticia personal con un tercero, debe celebrarse un acuerdo que establezca las medidas de seguridad específicas (artículo 19, apartado 2, de la LIC). Si se produce una violación de la información crediticia personal, deben adoptarse medidas para minimizar los daños y debe notificarse sin demora a los particulares de que se trate (artículo 39-4, apartados 1 y 2, de la LIC). Además, debe informarse a la CPIP de la notificación enviada a los particulares y de las medidas que se han aplicado (artículo 39-4, apartado 4, de la LIC).

([131]) En tal caso, debe solicitarse sin demora una orden judicial. Si la orden no se emite en el plazo de treinta y seis horas, los datos recibidos deben suprimirse de inmediato (artículo 32, apartado 6, punto 6, de la LIC).

([132]) Por ejemplo, porque se han cumplido las obligaciones contractuales, una de las partes ejerció su derecho de rescisión, etc. (véase el artículo 17-2, apartado 5, del Decreto de Ejecución de la LIC).

([133]) Artículo 20-2, apartado 1, de la LIC y artículo 17-2, apartado 1, punto 1, del Decreto de Ejecución de la LIC.

([134]) Este período tiene en cuenta que, a menudo, no es posible llevar a cabo la supresión de inmediato, sino que normalmente es preciso adoptar determinadas medidas (por ejemplo, separar los datos que deben suprimirse de otros datos y realizar la supresión sin que ello afecte a la estabilidad de los sistemas de información) que requieren cierto tiempo.

([135]) Artículo 20-2, apartado 2, de la LIC.

([136]) El artículo 18, apartado 2, de la LIC y el artículo 15, apartado 4, del Decreto de Ejecución de la LIC establecen normas más específicas con respecto a este requisito de mantenimiento de registros, por ejemplo, para los registros relativos a información que pueda suponer una desventaja para una persona, como la información relacionada con la morosidad y la quiebra.

([137]) Por lo que se refiere a otros mecanismos de exigencia de responsabilidades, la LIC exige a determinadas organizaciones (por ejemplo, las cooperativas y las empresas públicas, véase el artículo 21, apartado 2, del Decreto de Ejecución de la LIC) que designen a un «administrador/guardián de la información crediticia» que se encargue de supervisar el cumplimiento de la LIC y lleve a cabo las tareas del «responsable de la protección de la privacidad» en virtud de la LPIP (artículo 20, apartados 3 y 4, de la LIC).

(108) La LIC también impone obligaciones específicas de transparencia a la hora de obtener el consentimiento para el uso o suministro de información crediticia personal (artículo 32, apartado 4, y artículo 34-2 de la LIC y artículo 30-3 del Decreto de Ejecución de la LIC) y, de manera más general, antes de facilitar información a un tercero (artículo 32, apartado 7, de la LIC) ([138]). Además, las personas tienen derecho a obtener, previa solicitud, información sobre la utilización y el suministro de su información crediticia a terceros en los tres años anteriores a la solicitud (incluidas la finalidad y las fechas de dicha utilización o dicho suministro) ([139]).

(109) En virtud de la LIC, las personas también tienen derecho a acceder a su información crediticia personal (artículo 38, apartado 1, de la LIC) y a obtener la rectificación de los datos inexactos (artículo 38, apartados 2 y 3, de la LIC) ([140]). Por otra parte, además del derecho general a la supresión en virtud de la LPIP (véase el considerando 77), la LIC prevé un derecho específico a la supresión de la información crediticia personal que se haya conservado más allá de los períodos de conservación mencionados en el considerando 104, es decir, cinco años (para la información crediticia personal que era necesaria para establecer o mantener una relación comercial) o tres meses (para otros tipos de información crediticia personal) ([141]). Excepcionalmente, puede denegarse una solicitud de supresión cuando sea necesaria una conservación ulterior en las circunstancias descritas en el considerando 105. Si un particular solicita la supresión, pero se aplica una de las excepciones, deben aplicarse salvaguardias específicas a la información crediticia en cuestión (artículo 38-3, apartado 3, de la LIC y artículo 33-3 del Decreto de Ejecución de la LIC). Por ejemplo, la información debe mantenerse separada de otra información, solo puede ser consultada por una persona autorizada y debe estar sujeta a medidas de seguridad específicas.

(110) Además de los derechos mencionados en el considerando 109, la LIC garantiza a los particulares el derecho a solicitar a un responsable del tratamiento que deje de ponerse en contacto con ellos con fines de comercialización directa (artículo 37, apartado 2, de la Ley) y el derecho a la portabilidad de los datos. En relación con este último, la LIC permite a los particulares solicitar la transmisión de su información crediticia personal a sí mismos o a determinados terceros (tales como instituciones financieras y empresas de calificación crediticia). La información crediticia personal debe tratarse y transmitirse al tercero en un formato que pueda ser procesado por un dispositivo de tratamiento de información (por ejemplo, un ordenador).

(111) Por consiguiente, en la medida en que la LIC contenga normas específicas en comparación con la LPIP, la Comisión considera que también estas normas garantizan un nivel de protección esencialmente equivalente al ofrecido en virtud del Reglamento (UE) 2016/679.

2.4 **Supervisión y cumplimiento de las normas**

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

2.4.1 *Supervisión independiente*

(113) En la República de Corea, la autoridad independiente encargada de supervisar la LPIP y de hacerla cumplir es la CPIP. La CPIP está compuesta por un presidente, un vicepresidente y siete comisarios. El presidente y el vicepresidente son nombrados por el presidente de la República de Corea, previa recomendación del primer ministro. De los comisarios, dos son nombrados por el presidente de la República por recomendación del presidente de la CPIP y cinco por recomendación de la Asamblea Nacional [dos de los cuales por recomendación del partido

([138]) Esto incluye un requisito general de notificación (artículo 32, apartado 7, de la LIC) y una obligación específica de transparencia en caso de que se facilite información mediante la cual pueda determinarse la solvencia de una persona a ciertas entidades, tales como las agencias de calificación crediticia y las agencias de recopilación de información crediticia (artículo 35-3 de la LIC y artículo 30-3 del Decreto de Ejecución de la LIC), o cuando se deniegue o ponga fin a una relación de transacción comercial sobre la base de la información crediticia personal recibida de un tercero (artículo 36 de la LIC y artículo 31 del Decreto de Ejecución de la LIC).

([139]) Artículo 35 de la LIC. Algunas organizaciones comerciales, como las cooperativas y las empresas públicas (artículo 21, apartado 2, del Decreto de Ejecución de la LIC), están sujetas a requisitos de transparencia adicionales, por ejemplo, poner a disposición del público cierta información (artículo 31 de la LIC) e informar a los particulares de las posibles desventajas para su calificación crediticia cuando realicen transacciones financieras que conlleven riesgos crediticios (artículo 35-2 de la LIC).

([140]) Por lo que se refiere a las condiciones y excepciones a los derechos de acceso y rectificación, se aplican las normas de la LPIP (descritas en los considerandos 76 y 77). Además, se establecen otras modalidades en el artículo 38, apartados 4 a 8, de la LIC y en el artículo 33 del Decreto de Ejecución de la LIC. En concreto, un operador comercial que haya rectificado o suprimido información crediticia inexacta deberá notificarlo al particular. Asimismo, deberá notificarse a cualquier tercero al que se haya comunicado dicha información en los seis meses anteriores y deberá informarse de ello al particular de que se trate. Si un particular no está satisfecho con la manera en que se ha tramitado una solicitud de rectificación, puede presentar una solicitud a la CPIP, que verifica las acciones del responsable del tratamiento y puede imponer medidas correctoras.

([141]) Artículo 38-3 de la LIC.

político al que pertenece el presidente de la República y tres por recomendación de otros partidos políticos (artículo 7-2, apartado 2, de la LPIP), lo cual contribuye a contrarrestar el partidismo en el proceso de nombramiento] ([142]). Este procedimiento está en consonancia con los requisitos aplicables al nombramiento de los miembros de las autoridades de protección de datos en la Unión [artículo 53, apartado 1, del Reglamento (UE) 2016/679]. Además, todos los comisarios deben abstenerse de cualquier actividad empresarial con fines de lucro o actividad política y de ocupar cargos en la administración pública o en la Asamblea Nacional (artículos 7-6 y 7-7, apartado 1, punto 3, de la LPIP) ([143]). Todos los comisarios están sujetos a normas específicas que les impiden participar en las deliberaciones en caso de un posible conflicto de intereses (artículo 7-11 de la LPIP). La CPIP está asistida por una secretaría (artículo 7-13) y puede crear subcomisiones (compuestas por tres comisarios) para tratar infracciones menores y asuntos recurrentes (artículo 7-12 de la LPIP).

(114) Cada miembro de la CPIP es nombrado por tres años y su mandato puede ser renovado una sola vez (artículo 7-4, apartado 1, de la LPIP). Los comisarios solo pueden ser destituidos en circunstancias específicas, a saber, si ya no están en condiciones de desempeñar sus funciones debido a una discapacidad física o mental a largo plazo, actúan en violación de la ley o cumplen uno de los motivos de anulación del mandato ([144]) (artículo 7-5 de la LPIP). Esto les proporciona protección institucional en el ejercicio de sus funciones.

(115) De manera más general, el artículo 7, apartado 1, de la LPIP garantiza explícitamente la independencia de la CPIP, y el artículo 7-5, apartado 2, de la LPIP exige que los comisarios desempeñen sus funciones de manera independiente, según la ley y su conciencia ([145]). Las salvaguardias institucionales y procedimentales descritas, incluso en relación con el nombramiento y la destitución de sus miembros, garantizan que la CPIP actúe con total independencia, sin injerencias ni instrucciones externas. Además, como organismo administrativo central, la CPIP propone anualmente su propio presupuesto (que es revisado por el Ministerio de Finanzas como parte del presupuesto nacional global antes de su adopción por la Asamblea Nacional) y se encarga de la gestión de su propio personal. La CPIP cuenta con un presupuesto actual de aproximadamente 35 millones de euros y 154 miembros del personal (incluidos 40 empleados especializados en tecnologías de la información y la comunicación, 32 empleados dedicados a la investigación y 40 expertos jurídicos).

(116) Las funciones y competencias de la CPIP se establecen principalmente en los artículos 7-8 y 7-9, así como en los artículos 61 a 66 de la LPIP ([146]). En particular, las tareas de la CPIP incluyen el asesoramiento sobre las leyes y los reglamentos relacionados con la protección de datos, el desarrollo de políticas y directrices en materia de protección de datos, la investigación de las vulneraciones de los derechos individuales, la tramitación de reclamaciones y la mediación de conflictos, la ejecución del cumplimiento de la LPIP, el aseguramiento de la educación y la promoción en el ámbito de la protección de datos, así como el intercambio y la cooperación con las autoridades de protección de datos de terceros países ([147]).

(117) Sobre la base del artículo 68 de la LPIP, en relación con el artículo 62 del Decreto de Ejecución de la LPIP, se han delegado determinadas tareas de la CPIP en la Agencia de Internet y Seguridad de Corea, a saber: 1) la educación y las relaciones públicas, 2) la formación de especialistas y la elaboración de criterios para las evaluaciones de impacto sobre la privacidad, 3) la tramitación de las solicitudes de designación de una institución de evaluación del impacto sobre la privacidad, 4) la tramitación de las solicitudes de acceso indirecto a los datos personales en poder de las autoridades públicas (artículo 35, apartado 2, de la LPIP) y 5) la tarea de solicitar materiales y llevar a

([142]) Solo las personas que cumplan los siguientes criterios pueden ser nombradas comisarios de la CPIP: altos funcionarios responsables de asuntos relacionados con la información personal; antiguos jueces, fiscales o abogados que hayan ejercido durante al menos diez años; antiguos directivos con experiencia en protección de datos que hayan trabajado en una institución u organización pública durante más de tres años o que hayan sido recomendados por dicha institución u organización; y antiguos profesores asociados con conocimientos profesionales en el ámbito de la protección de datos que hayan trabajado durante al menos cinco años en una institución académica (artículo 7-2 de la LPIP).

([143]) Véase también el artículo 4-2 del Decreto de Ejecución de la LPIP.

([144]) Véase el artículo 7-7 de la LPIP, según el cual los extranjeros y los miembros de partidos políticos no pueden ser miembros de la CPIP. Lo mismo se aplica a los particulares que han sido objeto de determinados tipos de sanciones penales, han sido destituidos por medio de una sanción disciplinaria en los últimos cinco años, etc. (artículo 7-7 de la LPIP, en relación con el artículo 33 de la Ley de cargos públicos).

([145]) Si bien el artículo 7, apartado 2, de la LPIP hace referencia a la facultad general del primer ministro en virtud del artículo 18 de la Ley sobre la organización del Gobierno para suspender o revocar, con la aprobación del presidente de la República, cualquier disposición ilícita o injusta de un organismo administrativo central, no se otorga tal facultad con respecto a las facultades de investigación o ejecución de la CPIP (véase el artículo 7, apartado 2, puntos 1 y 2, de la LPIP). Según las explicaciones recibidas del Gobierno coreano, el artículo 18 de la Ley sobre la organización del Gobierno tiene por objeto ofrecer al primer ministro la posibilidad de actuar en circunstancias extraordinarias, por ejemplo, para mediar en caso de desacuerdo entre diferentes organismos gubernamentales. Sin embargo, el primer ministro nunca ha hecho uso de esta facultad desde que se adoptó esta disposición en 1963.

([146]) Cuando resulte necesario para llevar a cabo las tareas previstas en el artículo 7-9, apartado 1, de la LPIP, la CPIP puede solicitar las opiniones de los funcionarios públicos pertinentes, expertos en protección de datos, organizaciones cívicas y los operadores económicos pertinentes. Además, la CPIP puede solicitar los materiales que resulten pertinentes, formular recomendaciones de mejora e inspeccionar su aplicación (artículo 7-9, apartados 2 a 5, de la LPIP).

([147]) Véanse también el artículo 9 (plan director trienal para la protección de la información personal), el artículo 12 (directrices normalizadas para la protección de la información personal) y el artículo 13 (políticas para el fomento y el apoyo de la autorregulación) de la LPIP.

cabo inspecciones con respecto a las reclamaciones recibidas a través del denominado «Centro de atención telefónica sobre privacidad». En el contexto de la tramitación de las reclamaciones a través del Centro de atención telefónica sobre privacidad, la Agencia de Internet y Seguridad de Corea transmite el caso a la CPIP o al Ministerio Fiscal si constata que se ha producido una infracción de la ley. La posibilidad de presentar una reclamación ante el Centro de atención telefónica sobre privacidad no impide que las personas presenten una reclamación directamente ante la CPIP o que se dirijan a ella si consideran que su reclamación no ha sido tramitada satisfactoriamente por la Agencia de Internet y Seguridad de Corea.

2.4.2 *Ejecución, en particular las sanciones*

(118) Con el fin de garantizar el cumplimiento de la LPIP, el legislador ha otorgado a la CPIP facultades tanto de investigación como de ejecución, que abarcan desde las recomendaciones hasta las multas administrativas. Además, estas facultades se complementan con un régimen de sanciones penales.

(119) Por lo que se refiere a las facultades de investigación, si se sospecha o se ha denunciado una infracción de la LPIP o si resulta necesario para la protección de los derechos de los interesados contra a las infracciones, la CPIP puede realizar inspecciones *in situ* y solicitar todos los materiales pertinentes (tales como objetos y documentos) a los responsables del tratamiento de los datos personales (artículo 63 de la LPIP, en relación con el artículo 60 del Decreto de Ejecución de la LPIP) ([148]).

(120) Por lo que se refiere a la ejecución, en virtud del artículo 61, apartado 2, de la LPIP, la CPIP puede asesorar a los responsables del tratamiento sobre la manera de mejorar el nivel de protección de los datos personales de determinadas actividades de tratamiento. Los responsables del tratamiento deben esforzarse de buena fe para aplicar estos consejos y están obligados a informar a la CPIP del resultado. Asimismo, cuando existan motivos razonables para creer que se ha producido una infracción de la LPIP y sea probable que la inacción cause daños difíciles de reparar, la CPIP podrá imponer medidas correctoras (artículo 64, apartado 1, de la LPIP) ([149]). La sección 5 de la Notificación 2021-5 (anexo I) aclara, con efecto vinculante, que estas condiciones se cumplen con respecto a la infracción de cualquier disposición de la LPIP que proteja los derechos de privacidad de las personas en relación con la información personal ([150]). Entre las medidas que la CPIP está facultada para adoptar se incluye ordenar el cese de la conducta que causa la infracción, la suspensión temporal del tratamiento de datos o cualquier otra medida necesaria. El incumplimiento de una medida correctora puede dar lugar a una sanción mediante una multa de un importe máximo de 50 millones de won (artículo 75, apartado 2, punto 13, de la LPIP).

(121) Con respecto a determinadas autoridades públicas (como la Asamblea Nacional, los organismos administrativos centrales, los organismos gubernamentales locales y los órganos jurisdiccionales), el artículo 64, apartado 4, de la LPIP establece que la CPIP puede «recomendar» cualquiera de las medidas correctoras mencionadas en el considerando 120 y que estas autoridades están obligadas a cumplir dicha recomendación, salvo que existan circunstancias extraordinarias. Según el punto 5 de la Nota n.º 2021-5, esto se refiere a circunstancias extraordinarias de hecho o de derecho de las que la CPIP no tenía conocimiento a la hora de formular su recomendación. La autoridad pública en cuestión solo puede invocar tales circunstancias extraordinarias si demuestra con claridad que no se ha producido ninguna infracción y la CPIP determina que efectivamente no es así. De lo contrario, la autoridad pública debe seguir la recomendación de la CPIP y «adoptar una medida correctora, por ejemplo, la suspensión inmediata de la acción, e indemnizar por daños y perjuicios en el caso excepcional de que se haya cometido un acto ilícito».

(122) La CPIP también puede solicitar a otros organismos administrativos con competencia específica conforme a la legislación sectorial (por ejemplo, salud y educación) que lleven a cabo una investigación —solos o conjuntamente con la CPIP— sobre las (presuntas) violaciones de la privacidad por parte de los responsables del tratamiento que operan en estos sectores bajo su jurisdicción, y que impongan medidas correctoras (artículo 63, apartados 4 y 5, de la LPIP). En ese caso, la CPIP determina los motivos, el objeto y el alcance de la investigación ([151]). A su vez, el organismo administrativo competente debe presentar a la CPIP un plan de inspección y notificarle el resultado de la inspección. La CPIP puede recomendar la adopción de una medida correctora específica, que el organismo correspondiente debe esforzarse por aplicar. En cualquier caso, tal solicitud no limita la competencia de la CPIP para llevar a cabo su propia investigación o imponer sanciones.

([148]) Además, la CPIP puede entrar en los locales del responsable del tratamiento para inspeccionar la situación de las operaciones comerciales, los registros, los documentos, etc. (artículo 63, apartado 2, de la LPIP). Véanse también el artículo 45-3 de la LIC y el artículo 36-4 del Decreto de Ejecución de la LIC con respecto a las facultades de la CPIP en virtud de dicha Ley.

([149]) Véanse también el artículo 45-4 de la LIC con respecto a las facultades de la CPIP en virtud de dicha Ley.

([150]) La sección 5 de la Notificación establece que «una razón fundada para considerar que se ha producido una infracción con respecto a la información personal y que es probable que la falta de adopción de medidas cause daños difíciles de reparar en el sentido del artículo 64, apartados 1 y 2, de la LPIP se refiere a una violación de cualquiera de los principios, derechos y obligaciones incluidos en la legislación para proteger los derechos de las personas relativos a la información personal». Lo mismo se aplica a las facultades de la CPIP en virtud del artículo 45-4 de la LIC.

([151]) Artículo 60 del Decreto de Ejecución de la LPIP.

(123) Además de sus facultades correctivas, la CPIP puede imponer multas administrativas de entre 10 y 50 millones de won por las infracciones de diversos requisitos de la LPIP (artículo 75 de la LPIP) ([152]). Entre otras cosas, se incluyen el incumplimiento de los requisitos de licitud del tratamiento, la no adopción de las medidas de seguridad necesarias, la falta de notificación a los interesados en caso de violación de la seguridad de los datos, el incumplimiento de los requisitos para el subtratamiento, la falta de establecimiento y divulgación de una política de privacidad, la no designación de un responsable de la protección de la privacidad o la falta de respuesta a una solicitud de un interesado en el ejercicio de sus derechos individuales, así como determinadas infracciones de procedimiento (falta de cooperación durante una investigación). En caso de que el mismo responsable del tratamiento infrinja varias disposiciones de la LPIP, podrá imponerse una multa por cada infracción y se tendrá en cuenta el número de personas afectadas a la hora de fijar el importe de la multa.

(124) Además, cuando existan motivos razonables para sospechar una infracción de la LPIP o de cualquier otra «ley relacionada con la protección de datos», la CPIP puede presentar una denuncia penal ante el órgano de investigación competente (por ejemplo, un fiscal, véase el artículo 65, apartado 1, de la LPIP). Además, la CPIP puede recomendar al responsable del tratamiento que adopte medidas disciplinarias contra la persona responsable (incluido el directivo encargado, véase el artículo 65, apartado 2, de la LPIP). Tras recibir dichas recomendaciones, el responsable del tratamiento debe cumplirlas ([153]) y notificar el resultado por escrito a la CPIP (artículo 65 de la LPIP, en relación con el artículo 58 del Decreto de Ejecución de la LPIP).

(125) Por lo que se refiere al asesoramiento con arreglo al artículo 61, las medidas correctoras con arreglo al artículo 64, la acusación o el asesoramiento para la adopción de medidas disciplinarias con arreglo al artículo 65 y la imposición de multas administrativas con arreglo al artículo 75 de la LPIP, la CPIP puede dar a conocer los hechos, es decir, la infracción, la entidad que haya infringido la ley y la(s) medida(s) impuesta(s), publicándolos en su sitio web o en un periódico general de ámbito nacional (artículo 66 de la LPIP, en relación con el artículo 61, apartado 1, del Decreto de Ejecución de la LPIP) ([154]).

(126) Por último, el cumplimiento de los requisitos de protección de datos establecidos en la LPIP (así como en otras «leyes relacionadas con la protección de datos») está respaldado por un régimen de sanciones penales. A este respecto, los artículos 70 a 73 de la LPIP contienen disposiciones sobre sanciones que pueden dar lugar a la imposición de una multa (de entre veinte y cien millones de won) o una pena de prisión (cuya duración máxima oscila entre dos y diez años). Entre las infracciones importantes figuran la utilización de datos personales o el suministro de tales datos a un tercero sin el consentimiento necesario, el tratamiento de información sensible en contra de la prohibición establecida en el artículo 23, apartado 1, de la LPIP, el incumplimiento de los requisitos de seguridad aplicables que dé lugar a la pérdida, el robo, la divulgación, la falsificación, la alteración o el daño de los datos personales, la no adopción de las medidas necesarias para corregir, suprimir o suspender los datos personales o la transferencia ilícita de datos personales a un tercer país ([155]). De conformidad con el artículo 74 de la LPIP, en cada uno de estos casos, será responsable el empleado, agente o representante del responsable del tratamiento, así como el propio responsable del tratamiento ([156]).

(127) Además de las sanciones penales previstas en la LPIP, el uso indebido de los datos personales también puede constituir un delito con arreglo a la Ley penal. Este es el caso, en particular, de la violación del secreto de la correspondencia, los documentos o los registros electrónicos (artículo 316), la divulgación de información sujeta al secreto profesional (artículo 317), el fraude mediante el uso de ordenadores (artículo 347-2), así como la malversación y el abuso de confianza (artículo 355).

(128) Por consiguiente, el sistema coreano combina diferentes tipos de sanciones, desde medidas correctoras y multas administrativas hasta sanciones penales, que pueden tener un efecto disuasorio especialmente importante sobre los responsables del tratamiento y los particulares que manejan los datos. Inmediatamente después de su creación en 2020, la CPIP empezó a hacer uso de sus facultades. El informe anual de 2021 de la CPIP muestra que la CPIP

([152]) Además, cuando los sistemas de tratamiento y protección de la información personal gestionados por un responsable del tratamiento hayan sido certificados como conformes con la LPIP, pero no se hayan cumplido los criterios de certificación con arreglo al artículo 34-2, apartado 1, del Decreto de Ejecución de la LPIP, o en caso de infracción grave de cualquier «ley relativa a la protección de la información [personal]», la CPIP podrá revocar la certificación (artículo 32-2, apartados 3 y 5, de la LPIP). La CPIP notificará dicha revocación al responsable del tratamiento y la anunciará públicamente o la publicará en su sitio web o en el Boletín Oficial (artículo 34-4 del Decreto de Ejecución de la LPIP). También están previstas multas administrativas (artículo 52 de la LIC) y sanciones penales (artículo 50 de la LIC) en caso de infracciones de la LIC.

([153]) De conformidad con el artículo 58, apartado 2, del Decreto de Ejecución de la LPIP, en caso de que circunstancias especiales hagan «impracticable» el cumplimiento de las recomendaciones, el responsable del tratamiento debe proporcionar una justificación razonada a la CPIP.

([154]) A la hora de decidir si se hace pública dicha información, la CPIP tendrá en cuenta el fondo y la gravedad de la infracción, su duración y frecuencia, así como sus consecuencias (alcance de los daños). Se informará previamente a la entidad afectada y se le ofrecerá la posibilidad de defenderse. Véase el artículo 61, apartados 2 y 3, del Decreto de Ejecución de la LPIP.

([155]) Véase el artículo 71, apartado 2, en relación con el artículo 18, apartado 1, de la LPIP (incumplimiento de las condiciones del artículo 17, apartado 3, de la LPIP, al que se refiere el artículo 18, apartado 1). Véase también el artículo 75, apartado 2, punto 1, en relación con el artículo 17, apartado 2, de la LPIP (no facilitación de la información necesaria al particular afectado con arreglo al artículo 17, apartado 2, de la LPIP, al que se refiere el artículo 17, apartado 3).

([156]) Además, el artículo 74-2 de la LPIP permite el decomiso de cualquier dinero, bien u otro beneficio obtenido como consecuencia de la infracción o, si el decomiso es imposible, la «recogida» del beneficio obtenido ilícitamente.

ya ha formulado una serie de recomendaciones, ha impuesto multas administrativas y ha emitido órdenes correctivas, tanto contra el sector público (alrededor de 34 autoridades públicas) como contra operadores privados (alrededor de 140 empresas) ([157]). Algunos casos significativos incluyen, por ejemplo, la imposición de una multa de 6 700 millones de won en diciembre de 2020 a una empresa por infringir distintas disposiciones de la LPIP (incluidos los requisitos de seguridad, los requisitos de consentimiento para el suministro a terceros y la transparencia) ([158]) y una multa de 103,3 millones de won en abril de 2021 a una empresa de tecnología de IA (por infringir, entre otras disposiciones, las normas sobre la licitud del tratamiento, en particular el consentimiento, y el tratamiento de información seudonimizada) ([159]). En agosto de 2021, la CPIP finalizó otra investigación sobre las actividades de tres empresas, la cual dio lugar a medidas correctoras y a la imposición de multas de hasta 6 470 millones de won (entre otras cosas, por no haber informado a los particulares sobre la divulgación de datos personales a terceros, incluidas las transferencias a terceros países) ([160]). Asimismo, ya antes de la reciente reforma, Corea del Sur tenía un sólido historial de ejecución y las autoridades responsables hacían uso de toda la gama de medidas de ejecución, incluidas las multas administrativas, las medidas correctoras y el «nombramiento e intercambio» con respecto a una variedad de responsables del tratamiento, incluidos los proveedores de servicios de comunicación (Comisión de Comunicaciones de Corea), así como los operadores comerciales, las instituciones financieras, las autoridades públicas, las universidades y los hospitales (Ministerio del Interior y de Seguridad) ([161]). Sobre esta base, la Comisión concluye que el sistema coreano garantiza el cumplimiento efectivo de las normas de protección de datos en la práctica, garantizando así un nivel de protección esencialmente equivalente al previsto en el Reglamento (UE) 2016/679.

2.5 **Vías de recurso**

(129) 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.

(130) El sistema coreano ofrece a los particulares diversos mecanismos para hacer valer eficazmente sus derechos y obtener reparación (judicial).

(131) Como primer paso, los particulares que consideren que se han vulnerado sus derechos o intereses de protección de datos pueden dirigirse al responsable del tratamiento correspondiente. De conformidad el artículo 30, apartado 1, punto 5, de la LPIP, la política de privacidad del responsable del tratamiento deberá incluir, entre otras cosas, información sobre los derechos de los interesados y la manera de ejercerlos. Además, deberá facilitar información de contacto —como el nombre y el número de teléfono del responsable de la protección de la privacidad o del departamento responsable de la protección de datos— para permitir la presentación de reclamaciones. Dentro de la organización del responsable del tratamiento, el responsable de la protección de la privacidad se encarga de la tramitación de las reclamaciones, la adopción de medidas correctoras en caso de violación de la privacidad y la compensación correctora (artículo 31, apartado 2, punto 3, y apartado 4, de la LPIP). Esta última es pertinente, por ejemplo, en caso de violación de la seguridad de los datos, ya que el responsable del tratamiento debe informar al interesado del punto o puntos de contacto para notificar cualquier daño, entre otros (artículo 34, apartado 1, punto 5, de la LPIP).

(132) Además, la LPIP ofrece a los particulares varias vías de recurso contra los responsables del tratamiento. En primer lugar, cualquier persona que considere que sus derechos o intereses de protección de datos han sido vulnerados por el responsable del tratamiento puede denunciar dicha infracción directamente a la CPIP o a una de las instituciones especializadas designadas por la CPIP para recibir y tramitar las reclamaciones; esto incluye a la Agencia de Internet y Seguridad de Corea, que a tal fin gestiona un centro de llamadas para asuntos relacionados con la información personal (el denominado «Centro de atención telefónica sobre privacidad») (artículo 62, apartados 1 y 2, de la LPIP, en relación con el artículo 59 del Decreto de Ejecución de la LPIP). El Centro de

([157]) Véase el informe anual de 2021 de la CPIP, pp. 50-55 (solo disponible en coreano), en https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Véase (solo disponible en coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Véase (solo disponible en coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Véase (solo disponible en coreano): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Véanse, por ejemplo, el informe anual de 2020 (solo disponible en coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 y los ejemplos facilitados en inglés en https://www.privacy.go.kr/eng/enforcement_02.do.

atención telefónica sobre privacidad investiga y constata las infracciones, ofrece asesoramiento en relación con el tratamiento de datos personales (artículo 62, apartado 3, de la LPIP) y puede notificar infracciones a la CPIP (pero no puede adoptar medidas de ejecución por sí mismo). El Centro de atención telefónica sobre privacidad recibe un gran número de reclamaciones/solicitudes (por ejemplo, 177 457 en 2020, 159 255 en 2019 y 164 497 en 2018) ([162]). Según la información recibida de la CPIP, ella misma recibió alrededor de 1 000 reclamaciones entre agosto de 2020 y agosto de 2021. En respuesta a una reclamación, la CPIP puede formular recomendaciones de mejora, medidas correctoras, una «acusación» ante el órgano de investigación competente (incluidos los fiscales) o recomendaciones de medidas disciplinarias (véanse los artículos 61, 64 y 65 de la LPIP). Las decisiones de la CPIP (tales como la negativa a tramitar una reclamación o la desestimación de una reclamación en cuanto al fondo) pueden impugnarse con arreglo a la Ley de lo contencioso-administrativo ([163]).

(133) En segundo lugar, de conformidad con los artículos 40 a 50 de la LPIP, en relación con los artículos 48-14 a 57 del Decreto de Ejecución de la LPIP, los interesados pueden presentar reclamaciones ante un denominado «Comité de mediación de conflictos», compuesto por representantes designados por el presidente de la CPIP de entre los miembros del servicio ejecutivo superior de la CPIP y por personas físicas nombradas sobre la base de su experiencia en el ámbito de la protección de datos de determinados grupos admisibles (véanse el artículo 40, apartados 2, 3 y 7, de la LPIP y el artículo 48-14 del Decreto de Ejecución de la LPIP) ([164]). La posibilidad de hacer uso de la mediación ante el Comité de mediación de conflictos ofrece una vía alternativa para obtener reparación, pero no limita el derecho de la persona a dirigirse a la CPIP o a los órganos jurisdiccionales. A fin de examinar el caso, el Comité puede solicitar a las partes en conflicto que faciliten los materiales necesarios o convocar a los testigos pertinentes para que comparezcan ante él (artículo 45 de la LPIP). Una vez aclarado el asunto, el Comité prepara un proyecto de laudo de mediación ([165]) con el que debe estar de acuerdo la mayoría de sus miembros. El proyecto de laudo de mediación puede abarcar la suspensión de la infracción, las soluciones necesarias (en particular la restitución o la indemnización), así como cualquier medida necesaria para evitar que vuelva a producirse una infracción idéntica o similar (artículo 47, apartado 1, de la LPIP). Cuando ambas partes estén de acuerdo con el laudo de mediación, este tendrá el mismo efecto que un acuerdo judicial (artículo 47, apartado 5, de la LPIP). Las partes pueden incoar una acción judicial mientras la mediación está en curso, en cuyo caso se suspenderá esta última (véase el artículo 48, apartado 2, de la LPIP) ([166]). Las cifras anuales publicadas por la CPIP muestran que los particulares utilizan regularmente el procedimiento ante el Comité de mediación de conflictos, que a menudo conduce a un resultado satisfactorio. Por ejemplo, en 2020, el Comité trató 126 asuntos, 89 de los cuales se resolvieron ante el Comité (en 77 asuntos, las partes ya habían llegado a un acuerdo antes de que finalizara el proceso de mediación y en 12 asuntos, las partes aceptaron la propuesta de mediación), lo que corresponde a un índice de mediación del 70,6 % ([167]). Del mismo modo, en 2019, el Comité trató 139 asuntos, de los cuales se resolvieron 92, lo que corresponde a una tasa de mediación del 62,2 %.

(134) Además, cuando al menos 50 personas sufran daños o sus derechos de protección de datos hayan sido vulnerados de manera idéntica o similar como consecuencia del mismo (tipo de) incidente ([168]), un interesado o una organización de protección de datos puede solicitar la mediación colectiva en nombre de dicha colectividad; otros interesados pueden solicitar participar en dicha mediación, que el Comité de mediación de conflictos anunciará públicamente (artículo 49, apartados 1 a 3, de la LPIP, en relación con los artículos 52 a 54 del Decreto de Ejecución de la LPIP) ([169]). El Comité de mediación de conflictos puede seleccionar por lo menos a una persona

([162]) Véase el informe anual de 2021 de la CPIP, p. 174. En 2020, estas reclamaciones se referían, por ejemplo, a la recogida de datos sin consentimiento, el incumplimiento de las obligaciones de transparencia, infracciones de la LPIP por parte de los encargados del tratamiento, medidas de seguridad insuficientes, la falta de respuesta a las solicitudes de los interesados, así como consultas generales.

([163]) En particular, las personas pueden recurrir el ejercicio de poderes públicos, o la negativa a ejercerlos, por parte del organismo administrativo (artículo 2, apartado 1, punto 1, y artículo 3, apartado 1, de la Ley de lo contencioso-administrativo). En el considerando 181, se ofrece información más detallada sobre los aspectos procedimentales, entre ellos los requisitos de admisibilidad.

([164]) Todos los miembros tienen un mandato fijo y solo pueden ser destituidos por causa justificada (véanse el artículo 40, apartado 5, y el artículo 41 de la LPIP). Asimismo, el artículo 42 de la LPIP contiene salvaguardias para proteger contra los conflictos de intereses.

([165]) Véase el artículo 44 de la LPIP. Además, puede proponer un proyecto de solución y recomendar una solución sin mediación (véase el artículo 46 del PIPA).

([166]) Por otra parte, el Comité puede rechazar la mediación si considera inadecuado mediar el conflicto en vista de su naturaleza o porque la solicitud de mediación se ha presentado con una finalidad desleal (artículo 48 de la LPIP).

([167]) Véase el informe anual de 2021 de la CPIP, pp. 179-180. Estos asuntos se referían, entre otras cosas, a infracciones del requisito de obtener el consentimiento para la recogida de datos, del principio de limitación de la finalidad y de los derechos de los interesados.

([168]) Véanse el artículo 49, apartado 1, de la LPIP, según el cual los interesados deben sufrir daños o una vulneración de sus derechos «de manera idéntica o similar», y el artículo 52, apartado 2, del Decreto de Ejecución de la LPIP, que establece como requisito que «las cuestiones principales del incidente sean comunes de hecho o de derecho».

([169]) Por otra parte, incluso los terceros pueden beneficiarse de un laudo de mediación colectiva aceptado por el responsable del tratamiento en la medida en que el Comité de mediación de conflictos puede aconsejar al responsable del tratamiento que prepare y presente un plan de compensación que (también) los incluya (artículo 49, apartado 5, de la LPIP).

que represente de la manera más adecuada el interés común como representante (artículo 49, apartado 4, de la LPIP). Si el responsable del tratamiento rechaza la mediación colectiva o no acepta el laudo de mediación, determinadas organizaciones ([170]) pueden presentar una demanda colectiva para abordar la violación (artículos 51 a 57 de la LPIP).

(135) En tercer lugar, en caso de una violación de la privacidad que cause «daños» a la persona, el interesado tiene derecho a obtener una reparación adecuada en un «procedimiento rápido y justo» (artículo 4, punto 5, en relación con el artículo 39 de la LPIP) ([171]). El responsable del tratamiento puede exculparse demostrando la ausencia de culpa («dolo» o negligencia). Si el interesado sufre daños como consecuencia de la pérdida, el robo, la divulgación, la falsificación, la alteración o el daño de sus datos personales, el Tribunal puede determinar una indemnización de hasta tres veces el daño real, teniendo en cuenta una serie de factores (artículo 39, apartados 3 y 4, de la LPIP). Como alternativa, el interesado puede solicitar una indemnización de un «importe razonable» que no exceda de tres millones de won (artículo 39-2, apartados 1 y 2, de la LPIP). Además, de conformidad con la Ley civil, puede solicitarse una indemnización a cualquier persona «que cause pérdidas o lesiones a un tercero debido a un acto ilícito, de forma deliberada o por negligencia» ([172]) o a una persona «que haya lesionado a la persona, haya perjudicado la libertad o la fama de un tercero o haya causado daños morales a un tercero» ([173]). Esta responsabilidad civil derivada de la infracción de las normas de protección de datos ha sido confirmada por el Tribunal Supremo ([174]). Si el daño ha sido causado por una acción ilícita de una autoridad pública, también puede presentarse una reclamación de indemnización con arreglo a la Ley de indemnización estatal ([175]). Las reclamaciones en virtud de la Ley de indemnización estatal pueden presentarse ante un «Consejo de indemnización» especializado o directamente ante los órganos jurisdiccionales coreanos ([176]). La responsabilidad estatal también abarca los daños y perjuicios inmateriales (como el sufrimiento mental) ([177]). Si la víctima es extranjera, la Ley de indemnización estatal se aplica siempre que su país de origen garantice igualmente la indemnización estatal para los nacionales coreanos ([178]).

(136) En cuarto lugar, el Tribunal Supremo ha reconocido que las personas tienen derecho a solicitar medidas cautelares por las vulneraciones de los derechos que les confiere la Constitución, incluido el derecho a la protección de los datos personales ([179]). En este contexto, un órgano jurisdiccional puede, por ejemplo, ordenar a los responsables del tratamiento que suspendan o pongan fin a cualquier actividad ilícita. Además, los derechos de protección de datos, también los protegidos por la LPIP, pueden ejercerse a través de acciones civiles. Esta aplicación horizontal de la protección constitucional de la privacidad a las relaciones entre particulares ha sido reconocida por el Tribunal Supremo ([180]).

([170]) A saber, los grupos de consumidores o las ONG sin ánimo de lucro de un cierto tamaño en términos de afiliación cuyo objetivo declarado es la protección de datos (aunque en el caso de estas últimas con el requisito adicional de que al menos cien interesados que hayan sufrido la misma infracción (o el mismo tipo de infracción) hayan presentado una solicitud para presentar una demanda colectiva). Véase el artículo 51 de la LPIP.

([171]) Los artículos 43 a 43-3 de la LIC también establecen la responsabilidad de indemnizar por los daños y perjuicios derivados de las infracciones de dicha Ley.

([172]) Artículo 750 de la Ley civil.

([173]) Artículo 751, apartado 1, de la Ley civil.

([174]) Véase, por ejemplo, la Resolución del Tribunal Supremo 2015Da251539, 251546, 251553, 251560 y 251577, de 30 de mayo de 2018. Además, el Tribunal Supremo confirmó que las violaciones de la seguridad de los datos pueden dar lugar a la concesión de una indemnización por daños y perjuicios en virtud de la Ley civil, véase la Resolución del Tribunal Supremo 2011Da59834, 59858, 59841, de 26 de diciembre de 2012 (resumen en inglés disponible en http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). En este caso, el Tribunal Supremo aclaró que, para evaluar si un particular ha sufrido una angustia emocional considerada como daño indemnizable, deben tenerse en cuenta varios factores, tales como el tipo y las características de la información filtrada, la identificabilidad del particular a causa de la violación, la posibilidad de acceso a los datos por parte de terceros, la medida en que se difundió la información personal, si esto dio lugar a vulneraciones adicionales de los derechos individuales, cómo se gestionó y protegió la información personal, etc.

([175]) Sobre la base de la Ley de indemnización estatal, las personas pueden solicitar una indemnización por los daños y perjuicios causados por funcionarios públicos debido al ejercicio de sus funciones oficiales en violación de la ley (artículo 2, apartado 1, de la Ley).

([176]) Artículos 9 y 12 de la Ley de indemnización estatal. La Ley establece consejos de distrito (presididos por el fiscal adjunto de la fiscalía correspondiente), un consejo central (presidido por el viceministro de Justicia) y un consejo especial (encargado de las reclamaciones de indemnización por daños y perjuicios causados por el personal militar o los empleados civiles del ejército, presidido por el viceministro de Defensa Nacional). Las reclamaciones de indemnización son, en principio, tramitadas por los consejos de distrito, que, en determinadas circunstancias, deben remitir los asuntos al consejo central o especial, por ejemplo, si la indemnización supera un importe determinado o en caso de que un particular solicite una nueva deliberación. Todos los consejos están formados por miembros nombrados por el ministro de Justicia (por ejemplo, de entre los funcionarios públicos del Ministerio de Justicia, los agentes judiciales, los abogados y las personas con experiencia en materia de indemnización estatal) y están sujetos a normas específicas relativas a los conflictos de intereses (véase el artículo 7 del Decreto de Ejecución de la Ley de indemnización estatal).

([177]) Véase el artículo 8 de la Ley de indemnización estatal (que hace referencia a la Ley civil), así como el artículo 751 de la Ley civil.

([178]) Artículo 7 de la Ley de indemnización estatal.

([179]) Resolución 93Da40614 del Tribunal Supremo, de 12 de abril de 1996, y Resolución 2008Da42430, de 2 de septiembre de 2011 (resumen en inglés disponible en https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

([180]) Véase, por ejemplo, la Resolución 2008Da42430 del Tribunal Supremo, de 2 de septiembre de 2011 (resumen en inglés disponible en https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

(137) Por último, las personas pueden presentar una denuncia penal de conformidad con la Ley de enjuiciamiento criminal (artículo 223) ante un fiscal o un agente de la policía judicial ([181]).

(138) Por consiguiente, el sistema coreano ofrece diversas vías para obtener reparación, desde opciones de fácil acceso y de bajo coste [por ejemplo, ponerse en contacto con el Centro de atención telefónica sobre privacidad o a través de la mediación (colectiva)] hasta vías administrativas (ante la CPIP) y judiciales, incluso con la posibilidad de obtener una indemnización por daños y perjuicios.

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

(139) La Comisión ha evaluado asimismo las limitaciones y salvaguardias previstas, incluidos los mecanismos de supervisión y de recurso disponibles en el Derecho coreano en lo que respecta a la recogida y la utilización ulterior por las autoridades públicas coreanas de los datos personales transferidos a responsables del tratamiento en Corea en aras del interés público, en particular a efectos coercitivos y de seguridad nacional (acceso de las autoridades públicas). A este respecto, el Gobierno coreano 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.

(140) A la hora de evaluar si, con arreglo a la presente Decisión, las condiciones en las que el acceso de las autoridades públicas a los datos transferidos a Corea cumple la prueba de «equivalencia esencial» de conformidad con el artículo 45, apartado 1, del Reglamento (UE) 2016/679, según la interpretación del Tribunal de Justicia de la Unión Europea a la luz de la Carta de los Derechos Fundamentales, la Comisión tuvo en cuenta, en particular, los siguientes criterios.

(141) En primer lugar, cualquier limitación al derecho a la protección de datos personales debe estar prevista por la ley y la base jurídica que permite la injerencia en este derecho debe definir por sí misma el alcance de la limitación al ejercicio del derecho en cuestión ([182]).

(142) En segundo lugar, a fin de satisfacer el requisito de proporcionalidad, según el cual las excepciones y limitaciones a la protección de datos personales deben aplicarse únicamente en la medida en que sea estrictamente necesario en una sociedad democrática para lograr objetivos específicos de interés general equivalentes a los reconocidos por la Unión, la legislación del tercer país en cuestión que permite la interferencia debe establecer normas claras y precisas que regulen el alcance y la aplicación de dichas medidas e imponer salvaguardias mínimas para que las personas cuyos datos se hayan transferido dispongan de garantías suficientes para proteger de manera efectiva sus datos personales contra el riesgo de abuso ([183]). En particular, la legislación debe indicar en qué circunstancias y en qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos ([184]), así como someter el cumplimiento de tales requisitos a una supervisión independiente ([185]).

(143) En tercer lugar, esta legislación y sus exigencias deben ser jurídicamente vinculantes en virtud del Derecho interno. Esto afecta, en primer lugar, a las autoridades del tercer país en cuestión, pero estos requisitos jurídicos también deben ser exigibles ante los tribunales contra dichas autoridades ([186]). En concreto, los interesados deben tener la posibilidad de emprender acciones legales ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión ([187]).

3.1 **Marco jurídico general**

(144) Las limitaciones y salvaguardias que se aplican a la recogida y la utilización ulterior de los datos personales por parte de las autoridades públicas coreanas se derivan del marco constitucional general, de leyes específicas que regulan sus actividades en los ámbitos del cumplimiento del Derecho penal y la seguridad nacional, así como de las normas que se aplican específicamente al tratamiento de datos personales.

([181]) Como se explica en el considerando 127, el uso indebido de los datos puede constituir un delito con arreglo a la Ley penal.

([182]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 174 y 175, y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también el asunto C-623/17 Privacy International/Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 65 (ECLI:EU:C:2020:790), y los asuntos acumulados C-511/18, C-512/18 y C-520/18 La Quadrature du Net y otros/Premier ministre y otros, apartado 175 (ECLI:EU:C:2020:791).

([183]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 176 y 181, y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 68, y La Quadrature du Net y otros, apartado 132.

([184]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 176. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 68, y La Quadrature du Net y otros, apartado 132.

([185]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 179.

([186]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 181 y 182.

([187]) Véase Maximillian Schrems contra Data Protection Commissioner, apartado 95, y Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 194. En ese sentido, el TJUE ha destacado en particular que el cumplimiento del artículo 47 de la Carta de los Derechos Fundamentales, que garantiza el derecho a la tutela judicial efectiva ante un juez independiente e imparcial, «contribuye al nivel de protección exigido dentro la Unión Europea [y] debe ser constatado por la Comisión antes de adoptar una decisión de adecuación en virtud del artículo 45, apartado 1, del Reglamento (UE) 2016/679» (Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 186).

(145) En primer lugar, el acceso a los datos personales por parte de las autoridades públicas coreanas se rige por los principios generales de legalidad, necesidad y proporcionalidad que se derivan de la Constitución coreana ([188]). En particular, los derechos y libertades fundamentales (incluido el derecho a la privacidad en general y el derecho a la privacidad de la correspondencia) ([189]) solo pueden ser restringidos por ley y cuando sea necesario por razones de seguridad nacional o para el mantenimiento del orden público en aras del bienestar público. Estas restricciones no pueden afectar al contenido esencial del derecho o libertad en cuestión. Por lo que se refiere específicamente a los registros e incautaciones, la Constitución establece que solo pueden tener lugar en las condiciones previstas por la ley, sobre la base de una orden emitida por un juez y respetando las garantías procesales ([190]). Por último, las personas pueden invocar sus derechos y libertades ante el Tribunal Constitucional si consideran que han sido vulnerados por las autoridades públicas en el ejercicio de sus competencias ([191]). Del mismo modo, las personas que hayan sufrido daños y perjuicios como consecuencia de un acto ilícito cometido por un funcionario público en el ejercicio de sus funciones oficiales tienen derecho a reclamar una indemnización justa ([192]).

(146) En segundo lugar, como se describe con más detalle en las secciones 3.2.1 y 3.3.1, los principios generales mencionados en el considerando 145 también se reflejan en las leyes específicas que regulan las competencias de las autoridades encargadas de garantizar el cumplimiento de la ley y de las autoridades nacionales de seguridad. Por ejemplo, en lo que respecta a las investigaciones penales, la Ley de enjuiciamiento criminal (LEC) establece que solo pueden adoptarse medidas obligatorias cuando así lo disponga explícitamente la LEC y en la menor medida necesaria para alcanzar el objetivo de la investigación ([193]). Del mismo modo, el artículo 3 de la Ley sobre la protección de la privacidad de las comunicaciones (LPPC) prohíbe el acceso a las comunicaciones privadas, salvo con arreglo a la legislación y con sujeción a las limitaciones y salvaguardias en ella establecidas. En el ámbito de la seguridad nacional, la Ley del Servicio Nacional de Inteligencia (Ley SNI) establece que todo acceso a las comunicaciones o a la información sobre la ubicación debe cumplir la ley y somete a sanciones penales los abusos de poder y las infracciones de la ley ([194]).

(147) En tercer lugar, el tratamiento de datos personales por parte de las autoridades públicas, incluso a efectos de control de la aplicación de la ley y de seguridad nacional, está sujeto a las normas de protección de datos en virtud de la LPIP ([195]). Como principio general, el artículo 5, apartado 1, de la LPIP exige a las autoridades públicas que formulen políticas para prevenir «el abuso y el uso indebido de la información personal, la vigilancia indiscreta y el seguimiento, etc. y mejorar la dignidad de los seres humanos y la privacidad individual». Además, todo responsable del tratamiento debe tratar los datos personales de manera que se reduzca al mínimo la posibilidad de vulnerar la privacidad de un interesado (artículo 3, apartado 6, de la LPIP).

(148) Todos los requisitos de la LPIP, tal como se describen detalladamente en la sección 2, se aplican al tratamiento de datos personales a efectos de control de la aplicación de la ley. Esto incluye los principios fundamentales (como la licitud y la lealtad, la limitación de la finalidad, la exactitud, la minimización de los datos, la limitación del plazo de conservación, la seguridad y la transparencia), las obligaciones (por ejemplo, con respecto a los datos sensibles y la notificación de las violaciones de la seguridad de los datos) y los derechos (acceso, corrección, supresión y suspensión).

(149) Si bien el tratamiento de datos personales por motivos de seguridad nacional está sujeto a un conjunto más limitado de disposiciones en virtud de la LPIP, se aplican los principios fundamentales, así como las normas sobre supervisión, ejecución y reparación ([196]). Más concretamente, los artículos 3 y 4 de la LPIP establecen los principios generales de protección de datos (licitud y lealtad, limitación de la finalidad, exactitud, minimización de los datos, seguridad y transparencia) y los derechos individuales (el derecho a ser informado, el derecho de acceso y los derechos de rectificación, supresión y suspensión) ([197]). Además, el artículo 4, apartado 5, de la LPIP otorga a los particulares el derecho a una reparación adecuada por cualquier daño o perjuicio derivado del tratamiento de sus datos personales en un procedimiento rápido y justo. Esto se complementa con las obligaciones más

([188]) Véase la sección 1.1 del anexo II.

([189]) Artículo 37, apartado 2, de la Constitución.

([190]) Artículos 16 y 12, apartado 3, de la Constitución. Además, el artículo 12, apartado 3, de la Constitución establece las circunstancias excepcionales en las que pueden llevarse a cabo registros o incautaciones sin una orden judicial (aunque sigue siendo necesaria una orden *ex post*), por ejemplo, por delito flagrante o, en el caso de delitos que pueden acarrear penas de privación de libertad de hasta tres años, si existe un riesgo de que se destruyan las pruebas o de que el sospechoso desaparezca.

([191]) Artículo 68, apartado 1, de la Ley del Tribunal Constitucional.

([192]) Artículo 29, apartado 1, de la Constitución.

([193]) Artículo 199, apartado 1, de la LEC. De manera más general, al ejercer las facultades que les confiere la LEC, las autoridades públicas deben respetar los derechos fundamentales de los sospechosos de delitos y de cualquier otra persona afectada (artículo 198, apartado 2, de la LEC).

([194]) Artículo 14 de la Ley SNI.

([195]) Véase la sección 1.2 del anexo II.

([196]) Artículo 58, apartado 1, punto 2, de la LPIP. Véase también la sección 6 de la Nota n.º 2021-5 (anexo I). Esta exención de determinadas disposiciones de la LPIP solo se aplica cuando los datos personales se tratan «con fines de seguridad nacional». Una vez que ha finalizado la situación de seguridad nacional que justifica el tratamiento de datos, ya no puede invocarse la exención y se aplican todos los requisitos de la LPIP.

([197]) Estos derechos solo pueden restringirse cuando así lo disponga la ley, en la medida y durante el tiempo que sea necesario y proporcionado para proteger un objetivo importante de interés público, o cuando la concesión del derecho pueda atentar contra la vida o la integridad física de un tercero o dar lugar a una vulneración injustificada de los intereses patrimoniales y otros intereses de un tercero. Véase el punto 6 de la Nota n.º 2021-5.

específicas de solo tratar los datos personales en la medida mínima necesaria para lograr la finalidad prevista y durante el período mínimo, establecer las medidas necesarias para garantizar una gestión segura de los datos y un tratamiento adecuado (tales como salvaguardias técnicas, físicas y de gestión), así como establecer medidas para la tramitación adecuada de las reclamaciones individuales ([198]). Por último, los principios generales de legalidad, necesidad y proporcionalidad establecidos en la Constitución coreana (véase el considerando 145) también se aplican al tratamiento de datos personales por motivos de seguridad nacional.

(150) Estas limitaciones y salvaguardias generales pueden ser invocadas por particulares ante organismos de supervisión independientes (por ejemplo, la CPIP o la Comisión Nacional de Derechos Humanos, véanse los considerandos 177 y 178) y los órganos jurisdiccionales (véanse los considerandos 179 a 183) para obtener reparación.

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

(151) El Derecho de la República de Corea impone una serie de limitaciones al acceso y la utilización de datos personales a efectos de control de la aplicación del Derecho penal, y proporciona mecanismos de supervisión y reparación que se ajustan a los requisitos mencionados en los considerandos 141 a 143 de la presente Decisión. Las condiciones en las que puede tener lugar dicho acceso y las salvaguardias aplicables a la utilización de estos poderes se precisan en detalle en las siguientes secciones.

3.2.1 *Base jurídica, limitaciones y salvaguardias*

(152) Los datos personales tratados por responsables del tratamiento coreanos que se transferirían desde la Unión en virtud de la presente Decisión ([199]) podrán ser recogidos por las autoridades coreanas a efectos de control de la aplicación del Derecho penal en el contexto de un registro o una incautación (sobre la base de la LEC), accediendo a información sobre las comunicaciones (sobre la base de la LPPC) u obteniendo datos de los abonados a través de solicitudes de divulgación voluntaria (sobre la base de la Ley del sector de las telecomunicaciones, LST) ([200]).

3.2.1.1 Registros e incautaciones

(153) La LEC establece que solo podrá llevarse a cabo un registro o una incautación si una persona es sospechosa de un delito, es necesario para la investigación y se establece una conexión entre la investigación y la persona objeto del registro o el artículo objeto de la inspección o incautación ([201]). Además, solo podrá autorizarse o llevarse a cabo un registro o una incautación (como medida obligatoria) en la menor medida necesaria ([202]). En principio, si un registro concierne a un disco de ordenador u otro soporte de almacenamiento de datos, solo se incautarán los datos necesarios (copiados o impresos) en lugar de todo el soporte ([203]). Este último solo podrá ser incautado cuando se considere sustancialmente imposible imprimir o copiar los datos necesarios por separado o cuando se considere que es sustancialmente impracticable lograr el objetivo del registro de otra manera ([204]). Por consiguiente, la LEC establece normas claras y precisas sobre el alcance y la aplicación de estas medidas, garantizando así que la injerencia en los derechos de los particulares en caso de registro o incautación se limite a lo necesario para una investigación penal específica y sea proporcionada al objetivo perseguido.

([198]) Artículo 58, apartado 4, de la LPIP.

([199]) Véase la sección 2.1 del anexo II. La declaración oficial del Gobierno coreano (sección 2.1 del anexo II) también hace referencia a la posibilidad de recoger información sobre transacciones financieras con el fin de prevenir el blanqueo de capitales y la financiación del terrorismo sobre la base de la Ley sobre la comunicación y el uso de información específica sobre las transacciones financieras (LCUIETF). Sin embargo, la LCUIETF solo impone obligaciones de divulgación de información a los responsables del tratamiento que tratan información crediticia personal con arreglo a la LIC y están sujetos a la supervisión del CSF (véase el considerando 13). Dado que el tratamiento de información crediticia personal por parte de dichos responsables está excluido del ámbito de aplicación de la presente Decisión, la LCUIETF no es pertinente para la presente evaluación.

([200]) El artículo 3 de la LPPC también menciona la Ley de tribunales militares como posible base jurídica para la recogida de datos sobre las comunicaciones. No obstante, dicha Ley regula la recogida de información sobre el personal militar y solo puede aplicarse a civiles en un número limitado de casos (por ejemplo, si el personal militar y los civiles cometen un delito conjuntamente o si un particular comete un delito contra el ejército, puede incoarse un procedimiento ante un tribunal militar, véase el artículo 2 de la Ley de tribunales militares). En cualquier caso, establece disposiciones generales sobre registros e incautaciones similares a las de la LEC (véanse, por ejemplo, los artículos 146 a 149 y 153 a 156 de la Ley de tribunales militares) y, por ejemplo, establece que el correo postal solo podrá recogerse cuando sea necesario para una investigación y sobre la base de una orden del Tribunal Militar. En la medida en que las comunicaciones electrónicas se recojan sobre la base de esta Ley, se aplicarán las limitaciones y salvaguardias de la LPPC. Véanse la sección 2.2.2 y la nota a pie de página n.º 50 del anexo II.

([201]) Artículo 215, apartados 1 y 2, de la LEC. Véanse también el artículo 106, apartado 1, y los artículos 107 y 109 de la LEC, que establecen que los órganos jurisdiccionales pueden realizar registros e incautaciones siempre que se considere que las personas o los objetos afectados están relacionados con un caso concreto. Véase la sección 2.2.1.2 del anexo II.

([202]) Artículo 199, apartado 1, de la LEC.

([203]) Artículo 106, apartado 3, de la LEC.

([204]) Artículo 106, apartado 3, de la LEC.

(154) En cuanto a las salvaguardias procedimentales, la LEC exige que se obtenga una orden judicial para llevar a cabo un registro o una incautación ([205]). Un registro o una incautación sin una orden solo se permite excepcionalmente, a saber, en circunstancias urgentes ([206]), *in loco* en el momento del arresto o la detención de un sospechoso ([207]) o cuando un sospechoso o un tercero deseche o presente voluntariamente un artículo (en relación con los datos personales, por la propia persona afectada) ([208]). Los registros e incautaciones ilícitos están sujetos a sanciones penales ([209]) y cualquier prueba obtenida en violación de la LEC se considerará inadmisible ([210]). Por último, las personas afectadas siempre deben ser informadas sin demora de un registro o una incautación (incluida una incautación de sus datos) ([211]), lo cual, a su vez, facilitará el ejercicio de sus derechos sustantivos y del derecho a la reparación (véase, en particular, la posibilidad de impugnar la ejecución de una orden de incautación; véase el considerando 180).

3.2.1.2 Acceso a la información sobre las comunicaciones

(155) Sobre la base de la LPPC, las autoridades coreanas encargadas de garantizar el cumplimiento del Derecho penal pueden adoptar dos tipos de medidas ([212]): por una parte, la recogida de «datos de confirmación de la comunicación» ([213]), que incluye la fecha de las telecomunicaciones, su hora de inicio y fin, el número de llamadas salientes y entrantes, así como el número de abonados de la otra parte, la frecuencia de uso, los archivos de registro sobre el uso de los servicios de telecomunicaciones y la información sobre la ubicación (por ejemplo, de torres de transmisión en las que se reciben las señales); y, por otra parte, las «medidas de restricción de la comunicación», que abarcan tanto la recogida del contenido del correo tradicional como la interceptación directa del contenido de las telecomunicaciones ([214]).

(156) Solo se podrá acceder a los datos de confirmación de la comunicación cuando sea necesario para llevar a cabo una investigación penal o ejecutar una pena ([215]), sobre la base de una orden emitida por un tribunal ([216]). A este respecto, la LPPC exige que se facilite información detallada tanto en la solicitud de la orden (por ejemplo, sobre los motivos de la solicitud, la relación con el destinatario/abonado y los datos necesarios) como en la propia orden (por ejemplo, sobre el objetivo, el objeto y el alcance de la medida) ([217]). La recogida sin una orden solo podrá llevarse a cabo cuando existan motivos de urgencia que impidan obtener una autorización judicial, en cuyo

([205]) Artículo 215, apartados 1 y 2, y artículo 113 de la LEC. Al solicitar una orden, la autoridad en cuestión debe presentar materiales que demuestren los motivos para sospechar que un particular ha cometido un delito, que el registro, la inspección o la incautación son necesarios, y que existen los objetos pertinentes que deben incautarse (artículo 108, apartado 1, del Reglamento sobre enjuiciamiento criminal). La propia orden debe especificar, entre otras cosas, el nombre del sospechoso y el delito; el lugar, la persona o los objetos que se vayan a registrar o los objetos que se vayan a incautar; la fecha de emisión; y el período efectivo de aplicación (artículo 114, apartado 1, en relación con el artículo 219 de la LEC). Véase la sección 2.2.1.2 del anexo II.

([206]) Es decir, cuando resulta imposible obtener una orden debido a la urgencia en el lugar de una infracción (artículo 216, apartado 3, de la LEC), en cuyo caso debe obtenerse una orden posteriormente sin demora (artículo 216, apartado 3, de la LEC).

([207]) Artículo 216, apartados 1 y 2, de la LEC.

([208]) Artículo 218 de la LEC. Por otra parte, como se explica en el punto 2.2.1.2 del anexo II, los objetos presentados voluntariamente solo se admiten como pruebas en procedimientos judiciales si no existen dudas razonables acerca del carácter voluntario de la divulgación, lo cual debe demostrar el fiscal.

([209]) Artículo 321 de la Ley penal.

([210]) Artículo 308-2 de la LEC. Además, un particular (y su abogado) puede estar presente cuando se ejecuta una orden de registro o incautación y, por consiguiente, también puede formular una objeción en el momento en que se ejecuta la orden (artículos 121 y 219 de la LEC).

([211]) Artículo 121 y 122 de la LEC (con respecto a los registros) y artículo 219, en relación con el artículo 106, apartado 4, de la LEC (con respecto a las incautaciones).

([212]) Véase también la sección 2.2.2.1 del anexo II. Tales medidas pueden adoptarse con la asistencia obligatoria de los operadores de telecomunicaciones después de concederles una autorización por escrito de un tribunal (artículo 9, apartado 2, de la LPPC), la cual deben conservar los operadores (artículo 15-2 de la LPPC y artículo 12 del Decreto de Ejecución de la LPPC). Los proveedores de telecomunicaciones pueden negarse a cooperar cuando la información sobre el particular en cuestión indicado en la autorización escrita del tribunal (por ejemplo, el número de teléfono del particular) sea incorrecta y esté prohibido en cualquier circunstancia revelar las contraseñas utilizadas para las telecomunicaciones (artículo 9, apartado 4, de la LPPC).

([213]) Artículo 2, apartado 11, de la LPPC.

([214]) Véanse el artículo 2, apartado 6, de la LPPC, que hace referencia a la «censura» (la apertura del correo sin el consentimiento de la parte afectada o la adquisición de conocimiento, la grabación o la retención de su contenido por otros medios) y el artículo 2, apartado 7, de la LPPC, que hace referencia a las «escuchas telefónicas» (la adquisición o la grabación del contenido de las telecomunicaciones mediante la escucha o la lectura común de los sonidos, las palabras, los símbolos o las imágenes de las comunicaciones a través de dispositivos electrónicos y mecánicos sin el consentimiento de la parte afectada o la interferencia en su transmisión y recepción).

([215]) Artículo 13, apartado 1, de la LPPC. Véase también la sección 2.2.2.3 del anexo II. Además, los datos de seguimiento de la ubicación en tiempo real y los datos de confirmación de la comunicación relativos a una estación de base específica solo podrán recogerse para la investigación de delitos graves o cuando, de lo contrario, sea difícil impedir la ejecución de un delito o recoger pruebas (artículo 13, apartado 2, de la LPPC). Esto refleja la necesidad de prever salvaguardias adicionales en caso de medidas particularmente intrusivas con la privacidad, en consonancia con el principio de proporcionalidad.

([216]) Artículos 13 y 6 de la LPPC.

([217]) Véase el artículo 13, apartados 3 y 9, en relación con el artículo 6, apartados 4 y 6, de la LPPC.

caso la orden deberá obtenerse y comunicarse al proveedor de telecomunicaciones inmediatamente después de solicitar los datos ([218]). Si el órgano jurisdiccional se niega a conceder una autorización posterior, la información recogida deberá destruirse ([219]).

(157) En cuanto a las salvaguardias adicionales con respecto a la recogida de datos de confirmación de la comunicación, la LPPC impone requisitos específicos de mantenimiento de registros y de transparencia ([220]). En particular, tanto las autoridades policiales ([221]) como los proveedores de telecomunicaciones ([222]) deben mantener registros de las solicitudes y divulgaciones efectuadas. Además, dichas autoridades deben, en principio, notificar a las personas que se han recogido sus datos de confirmación de la comunicación ([223]). Esta notificación solo puede aplazarse en circunstancias excepcionales, previa autorización del director de una fiscalía de distrito competente ([224]). Dicha autorización solo podrá concederse cuando la notificación pueda 1) poner en peligro la seguridad nacional, la seguridad y el orden públicos, 2) causar la muerte o lesiones corporales, 3) impedir un procedimiento judicial justo (por ejemplo, dar lugar a la destrucción de pruebas o a amenazas a los testigos) o 4) difamar al sospechoso, a las víctimas o a otras personas relacionadas con el asunto o invadir su privacidad. En tales casos, la notificación deberá presentarse en un plazo de treinta días una vez que dejen de existir los motivos para el aplazamiento ([225]). Tras la notificación, las personas tienen derecho a obtener información sobre los motivos de la recogida de sus datos ([226]).

(158) Se aplican normas más estrictas con respecto a las medidas de restricción de la comunicación, que solo pueden utilizarse cuando existan razones fundadas para sospechar que se están planificando, se están cometiendo o se han cometido determinados delitos graves mencionados específicamente en la LPPC ([227]). Además, las medidas de restricción de la comunicación solo pueden adoptarse como medida de último recurso y cuando, de otro modo, sea difícil impedir la comisión de un delito, detener a un delincuente o recabar pruebas ([228]). Estas medidas deben interrumpirse de inmediato una vez que ya no sean necesarias, a fin de garantizar que la vulneración de la privacidad de las comunicaciones sea lo más limitada posible ([229]). La información obtenida de manera ilícita a través de medidas de restricción de la comunicación no se admite como prueba en procedimientos judiciales o disciplinarios ([230]).

(159) En cuanto a las salvaguardias procedimentales, la LPPC exige que se obtenga una orden judicial para aplicar medidas de restricción de la comunicación ([231]). Una vez más, la LPPC exige que la solicitud de una orden y la propia orden contengan información detallada ([232]), incluida la justificación de la solicitud, así como las comunicaciones que deben recogerse (que deben ser las del sospechoso objeto de la investigación) ([233]). Tales medidas solo pueden adoptarse sin una orden en caso de una amenaza inminente de delincuencia organizada o cuando sea inminente otro delito grave que pueda causar directamente la muerte o lesiones graves y exista una emergencia

([218]) Artículo 13, apartado 2, de la LPPC.
([219]) Artículo 13, apartado 3, de la LPPC.
([220]) Véase la sección 2.2.2.3 del anexo II.
([221]) Artículo 13, apartados 5 y 6, de la LPPC.
([222]) Artículo 13, apartado 7, de la LPPC. Además, los proveedores de telecomunicaciones deben informar dos veces al año sobre la divulgación de datos de confirmación de la comunicación al Ministerio de Ciencia y TIC.
([223]) Véase el artículo 13-3, apartado 7, en relación con el artículo 9-2 de la LPPC. En particular, debe notificarse a los particulares en un plazo de treinta días a partir de la adopción de la decisión de (no) incoar un procedimiento o en un plazo de treinta días transcurrido un año desde que se haya adoptado la decisión de suspender una acusación (aunque la notificación debe efectuarse, en cualquier caso, en un plazo de treinta días transcurrido un año desde la recogida de la información), véase el artículo 13-3, apartado 1, de la LPPC.
([224]) Artículo 13-3, apartados 2 y 3, la LPPC.
([225]) Artículo 13-3, apartado 4, de la LPPC.
([226]) Artículo 13-3, apartado 5, de la LPPC. A petición del particular, un fiscal o un agente de la policía judicial debe explicar los motivos por escrito en un plazo de treinta días a partir de la recepción de la solicitud, salvo que se aplique una de las excepciones para el aplazamiento de la notificación (artículo 13-3, apartado 6, de la LPPC).
([227]) Por ejemplo, la insurrección, los delitos relacionados con las drogas, aquellos relacionados con explosivos y aquellos relacionados con la seguridad nacional, las relaciones diplomáticas o las bases e instalaciones militares, véase el artículo 5, apartado 1, de la LPPC. Véase también la sección 2.2.2.2 del anexo II.
([228]) Artículo 3, apartado 2, y artículo 5, apartado 1, de la LPPC.
([229]) Artículo 2 del Decreto de Ejecución de la LPPC.
([230]) Artículo 4 de la LPPC.
([231]) Artículo 6, apartados 1, 2, 5 y 6, de la LPPC.
([232]) La solicitud de una orden debe describir 1) las razones fundadas para sospechar (*prima facie*) que uno de los delitos listados está previsto, se está cometiendo o se ha cometido, así como cualquier material de apoyo; 2) las medidas de restricción de la comunicación, así como su objeto, alcance, objetivo y período efectivo; y 3) el lugar en el que se ejecutarían las medidas y cómo se llevarían a cabo (artículo 6, apartado 4, de la LPPC y artículo 4, apartado 1, del Decreto de Ejecución de la LPPC). La propia orden debe especificar las medidas, así como su objeto, alcance, período efectivo, lugar de ejecución y la manera en que deben llevarse a cabo (artículo 6, apartado 6, de la LPPC).
([233]) El objeto de una medida de restricción de la comunicación deben ser envíos postales o telecomunicaciones específicos enviados o recibidos por el sospechoso, o envíos postales o telecomunicaciones enviados o recibidos por el sospechoso durante un período de tiempo determinado (artículo 5, apartado 2, de la LPPC).

que impida seguir el procedimiento ordinario ([234]). No obstante, en tal caso, la solicitud de una orden debe presentarse inmediatamente después de la adopción de la medida ([235]). Las medidas de restricción de la comunicación solo pueden aplicarse durante un período máximo de dos meses ([236]) y solo pueden prorrogarse previa autorización judicial si se siguen cumpliendo las condiciones para la aplicación de las medidas ([237]). El período prorrogado no puede superar un total de un año, o tres años para determinados delitos especialmente graves (como los relacionados con la insurrección, la agresión extranjera y la seguridad nacional) ([238]).

(160) Al igual que en el caso de la recogida de datos de confirmación de la comunicación, la LPPC exige a los proveedores de telecomunicaciones ([239]) y a las autoridades encargadas de garantizar el cumplimiento de la ley ([240]) que lleven registros de la ejecución de las medidas de restricción de la comunicación, y prevé la notificación a la persona afectada, la cual puede aplazarse excepcionalmente cuando sea necesario por motivos importantes de interés público ([241]).

(161) Por último, el incumplimiento de varias de las limitaciones y salvaguardias de la LPPC (incluidas, por ejemplo, las obligaciones de obtención de una orden, mantenimiento de registros y notificación a la persona), tanto en lo que se refiere a la recogida de datos de confirmación de la comunicación como al uso de medidas de restricción de la comunicación, está sujeto a sanciones penales ([242]).

(162) Por lo tanto, las competencias de las autoridades encargadas de garantizar el cumplimiento del Derecho penal para recoger datos relativos a las comunicaciones sobre la base de la LPPC (tanto el contenido de las comunicaciones como los datos de confirmación de la comunicación) están limitadas por normas claras y precisas y están sujetas a una serie de salvaguardias. Estas salvaguardias, en particular, garantizan la supervisión de la ejecución de tales medidas, tanto *ex ante* (a través de la aprobación judicial previa) como *ex post* (a través de requisitos de mantenimiento de registros y requisitos de información), y facilitan el acceso de los particulares a vías de recurso eficaces (garantizando que estén informadas de la recogida de sus datos).

3.2.1.3 Solicitudes de divulgación voluntaria de datos de los abonados

(163) Además de basarse en las medidas obligatorias descritas en los considerandos 153 a 162, las autoridades coreanas encargadas de garantizar el cumplimiento de la ley pueden solicitar a los proveedores de telecomunicaciones «datos de comunicaciones» de forma voluntaria, para apoyar un proceso penal, una investigación o la ejecución de una sentencia (artículo 83, apartado 3, de la LST). Esta posibilidad solo existe con respecto a conjuntos de datos limitados, por ejemplo, el nombre, el número de registro de residente, la dirección y el número de teléfono de los usuarios, las fechas de suscripción o cancelación de la suscripción de los usuarios, así como los códigos de identificación de los usuarios (es decir, los códigos utilizados para identificar al usuario legítimo de sistemas informáticos o redes de comunicación) ([243]). Dado que solo las personas que contratan servicios directamente de un proveedor de telecomunicaciones coreano se consideran «usuarios» ([244]), los ciudadanos de la UE cuyos datos se hayan transferido a la República de Corea normalmente no entrarían en esta categoría ([245]).

(164) Se aplican diferentes limitaciones a estas divulgaciones voluntarias, tanto para el ejercicio de las competencias por parte de la autoridad encargada de garantizar el cumplimiento de la ley como para la respuesta del operador de telecomunicaciones. Como requisito general, las autoridades encargadas de garantizar el cumplimiento de la ley deben actuar de conformidad con los principios constitucionales de necesidad y proporcionalidad (artículo 12, apartado 1, y artículo 37, apartado 2, de la Constitución), incluso cuando soliciten información de forma

([234]) Artículo 8, apartado 1, de la LPPC. No obstante, la recogida de información en situaciones de emergencia debe realizarse siempre de conformidad con una «declaración de censura/escuchas telefónicas de emergencia» y la autoridad que lleve a cabo la recogida debe mantener un registro de toda medida de emergencia (artículo 8, apartado 4, de la LPPC).

([235]) La recogida debe interrumpirse inmediatamente si el organismo encargado de la aplicación de la ley no obtiene la autorización judicial en un plazo de treinta y seis horas (artículo 8, apartado 2, de la LPPC), en cuyo caso, como se explica en la sección 2.2.2.2 del anexo II, la información recogida, en principio, se destruirá. También debe notificarse al órgano jurisdiccional en caso de que las medidas de emergencia se hayan completado en un plazo tan breve que no fuera necesaria una autorización (por ejemplo, si el sospechoso es detenido inmediatamente después de iniciar la interceptación, véase el artículo 8, apartado 5, de la LPPC). En tal caso, debe facilitarse al órgano jurisdiccional información sobre el objetivo, el objeto, el alcance, el período, el lugar de ejecución y el método de recogida, así como los motivos para no presentar una solicitud de autorización judicial (artículo 8, apartados 6 y 7, de la LPPC).

([236]) Artículo 6, apartado 7, de la LPPC. Si el objetivo de las medidas se alcanza antes dentro de ese período, las medidas deben interrumpirse de inmediato.

([237]) Artículo 6, apartados 7 y 8, de la LPPC.

([238]) Artículo 6, apartado 8, de la LPPC.

([239]) Artículo 9, apartado 3, de la LPPC.

([240]) Artículo 18, apartado 1, del Decreto de Ejecución de la LPPC.

([241]) En particular, el fiscal debe notificar a la persona en un plazo de treinta días a partir de la formulación de una acusación o una disposición a no acusar o detener (artículo 9-2, apartado 1, de la LPPC). La notificación puede aplazarse con la aprobación del jefe de la fiscalía de distrito si puede poner en grave peligro la seguridad nacional o perturbar la seguridad y el orden públicos, o cuando pueda atentar gravemente contra la vida y la integridad física de terceros (artículo 9-2, apartados 4 a 6, de la LPPC).

([242]) Artículos 16 y 17 de la LPPC.

([243]) Artículo 83, apartado 3, de la LST. Véase también la sección 2.2.3 del anexo II.

([244]) Artículo 2, apartado 9, de la LST.

([245]) Véase también la sección 2.2.3 del anexo II.

voluntaria. Además, deben cumplir la LPIP, especialmente recogiendo solo datos personales mínimos, en la medida necesaria para lograr una finalidad legítima, de manera que se minimice el impacto sobre la privacidad de los particulares (como el artículo 3, apartados 1 y 6 de la LPIP). Más concretamente, las solicitudes para obtener datos de comunicaciones sobre la base de la LST deben hacerse por escrito e indicar los motivos de la solicitud, el vínculo con el usuario pertinente y el alcance de los datos solicitados ([246]).

(165) Los proveedores de telecomunicaciones no están obligados a acceder a estas solicitudes y solo pueden hacerlo de conformidad con la LPIP. En particular, esto significa que deben encontrar un equilibrio entre los diferentes intereses en juego y no pueden facilitar los datos si ello pudiera vulnerar deslealmente los intereses de la persona o de un tercero ([247]). Este sería el caso, por ejemplo, si fuera evidente que la autoridad requirente abusó de su autoridad ([248]). Los operadores de telecomunicaciones deben mantener registros de las divulgaciones con arreglo a la LST e informar dos veces al año al Ministerio de Ciencia y TIC ([249]).

(166) Además, de conformidad con la sección 3 de la Nota n.º 2021-5 (anexo I), los proveedores de telecomunicaciones deben, en principio, notificar a la persona afectada cuando accedan voluntariamente a una solicitud ([250]). Esto, a su vez, permitirá al particular ejercer sus derechos y, en caso de que sus datos se divulguen de manera ilícita, obtener reparación, ya sea del responsable del tratamiento (por ejemplo, por divulgar los datos en violación de la LPIP o por responder a una solicitud claramente desproporcionada) o de la autoridad encargada de garantizar el cumplimiento de la ley (por ejemplo, por actuar más allá de los límites de lo que resulta necesario y proporcionado o por no respetar los requisitos procedimentales de la LST).

3.2.2 *Utilización ulterior de la información recogida*

(167) El tratamiento de los datos personales recogidos por las autoridades coreanas encargadas de garantizar el cumplimiento del Derecho penal está sujeto a todos los requisitos de la LPIP, incluso con respecto a la limitación de la finalidad (artículo 3, apartados 1 y 2, de la LPIP), la licitud del uso y el suministro a terceros (artículos 15, 17 y 18 de la LPIP), las transferencias internacionales (artículos 17 y 18 de la LPIP, en relación con la sección 2 de la Notificación 2021-5) ([251]), la proporcionalidad/minimización de los datos (artículo 3, apartados 1 y 6 de la LPIP) y la limitación del plazo de conservación (artículo 21 de la LPIP) ([252]).

(168) Con respecto al contenido de las comunicaciones adquiridas mediante la aplicación de medidas de restricción de la comunicación, la LPPC limita su posible uso específicamente a la investigación, el enjuiciamiento o la prevención de delitos graves ([253]); los procedimientos disciplinarios por los mismos delitos; las reclamaciones por daños y perjuicios presentadas por una parte de las comunicaciones o cuando así lo permitan específicamente otras leyes ([254]). Además, el contenido recogido de las telecomunicaciones transmitidas a través de internet solo puede conservarse con la aprobación del órgano jurisdiccional que autorizó las medidas de restricción de la comunicación ([255]), con vistas a utilizarlo para la investigación, el enjuiciamiento o la prevención de delitos graves ([256]). De manera más general, la LPPC prohíbe la divulgación de información confidencial obtenida a través de medidas de restricción de la comunicación y el uso de dicha información para perjudicar la reputación de las personas sujetas a las medidas ([257]).

3.2.3 *Supervisión*

(169) En Corea, las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal son supervisadas por distintos organismos ([258]).

([246]) Artículo 83, apartado 4, de la LST. Cuando sea imposible presentar una solicitud por escrito debido a la urgencia, la solicitud escrita deberá presentarse tan pronto como desaparezca el motivo de la urgencia (artículo 83, apartado 4, de la LST).

([247]) Artículo 18, apartado 2, de la LPIP.

([248]) Resolución n.º 2012Da105482 del Tribunal Supremo, de 10 de marzo de 2016. Véase también el anexo II, sección 2.2.3, de esta Resolución del Tribunal Supremo.

([249]) Artículo 83, apartados 5 y 6, de la LST.

([250]) Este requisito está sujeto a excepciones limitadas y con reservas, en particular siempre y cuando la notificación ponga en peligro una investigación penal en curso o pueda atentar contra la vida o la integridad física de un tercero, en el caso de que esos derechos o intereses sean manifiestamente superiores a los derechos del interesado. Véase la sección 3, inciso iii), punto 1, de la Nota.

([251]) En particular, las autoridades públicas coreanas están obligadas a garantizar, mediante un instrumento jurídicamente vinculante, un nivel de protección equivalente al ofrecido por la LPIP (véase también el considerando 90).

([252]) Véase también la sección 1.2 del anexo II.

([253]) Véase el considerando 158.

([254]) Artículo 12 de la LPPC. Véase la sección 2.2.2.2 del anexo II.

([255]) El fiscal o el agente de policía que ejecute las medidas de restricción de la comunicación debe seleccionar las telecomunicaciones que deben conservarse en un plazo de catorce días a partir de la finalización de las medidas y solicitar una autorización judicial (en el caso de un agente de policía, la solicitud debe presentarse a un fiscal, que, a su vez, presenta la solicitud al órgano jurisdiccional), véase el artículo 12-2, apartados 1 y 2, de la LPPC.

([256]) Las solicitudes de tal autorización deben contener información sobre las medidas de restricción de la comunicación, un resumen de los resultados de las medidas, los motivos de la conservación (junto con materiales de apoyo) y las telecomunicaciones que deben conservarse (artículo 12-2, apartado 3, de la LPPC). Si no se presenta ninguna solicitud, los datos obtenidos deberán suprimirse en un plazo de catorce días a partir de la finalización de la medida de restricción de la comunicación (artículo 12-2, apartado 5, de la LPPC) y, en caso de denegación de la solicitud, en un plazo de siete días (artículo 12-2, apartado 5, de la LPPC). En ambos casos, debe presentarse un informe sobre la supresión al órgano jurisdiccional que autorizó la recogida en un plazo de siete días.

([257]) Artículo 11, apartado 2, del Decreto de Ejecución de la LPPC.

([258]) Véase la sección 2.3 del anexo II.

(170) En primer lugar, la policía está sujeta a la supervisión interna de una Inspección General ([259]), que lleva a cabo un control de la legalidad, incluso con respecto a posibles vulneraciones de los derechos humanos. La Inspección General se creó para aplicar la Ley de auditorías del sector público, que fomenta la creación de organismos de autocontrol y establece requisitos específicos para su composición y sus funciones. En particular, la Ley exige que el jefe de un organismo de auditoría interna sea ajeno a la autoridad en cuestión (como antiguos jueces y profesores), sea designado por un período de dos a cinco años ([260]), solo pueda ser destituido por razones justificadas (por ejemplo, cuando no pueda ejercer sus funciones por motivos de salud o cuando esté sujeto a medidas disciplinarias) ([261]) y que se garantice su independencia en la mayor medida posible ([262]). La obstrucción de una auditoría interna está sujeta a multas administrativas ([263]). Los informes de auditoría (que pueden incluir recomendaciones, solicitudes de medidas disciplinarias y solicitudes de compensación o corrección) se comunican al jefe de la autoridad pública de que se trate, a la Comisión de Control y de Inspección (CCI) ([264]) y, en general, se hacen públicos ([265]). Los resultados de la aplicación del informe también deben notificarse a la CCI ([266]) (véase el considerando 173 sobre la función de supervisión y las competencias de la CCI).

(171) En segundo lugar, la CPIP supervisa la conformidad del tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal con la LPIP y otras leyes que protegen la privacidad de las personas, incluidas las leyes que regulan la recogida de pruebas (electrónicas) a efectos de control de la aplicación del Derecho penal, tal como se describe en la sección 3.2.1 ([267]). En particular, dado que la supervisión de la CPIP abarca la licitud y la lealtad de la recogida y el tratamiento de datos (artículo 3, apartado 1, de la LPIP), que se infringirán si se accede a los datos personales y estos se utilizan en violación de dichas leyes ([268]), la CPIP también puede investigar y hacer cumplir las limitaciones y salvaguardias descritas en la sección 3.2.1 ([269]). En el ejercicio de esta función de supervisión, la CPIP puede hacer uso de todas sus facultades de investigación y correctivas, según se describe detalladamente en el punto 2.4.2. Ya antes de la reciente reforma de la LPIP (es decir, en su anterior función supervisora del sector público), la CPIP llevó a cabo varias actividades de supervisión del tratamiento de datos personales por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, por ejemplo, en el contexto del interrogatorio de sospechosos (asunto n.º 2013-16, de 26 de agosto de 2013), con respecto a la notificación a los particulares sobre la imposición de multas administrativas (asunto n.º 2015-02-04, de 26 de enero de 2015), el intercambio de datos con otras autoridades (asunto n.º 2018-15-146, de 9 de julio de 2018; asunto n.º 2018-25-308, de 10 de diciembre de 2018; asunto n.º 2019-02-015, de 29 de enero de 2019), la recogida de huellas dactilares o fotografías (asunto n.º 2019-17-273, de 9 de septiembre de 2019) y el uso de drones (asunto n.º 2020-01-004, de 13 de enero de 2020). En esos asuntos, la CPIP investigó el cumplimiento de varias disposiciones de la LPIP (por ejemplo, la licitud del tratamiento, los principios de limitación de la finalidad y minimización de los datos), pero también las disposiciones pertinentes de otras leyes, como la Ley de enjuiciamiento criminal, y, en caso necesario, formuló recomendaciones para ajustar el tratamiento a los requisitos de protección de datos.

(172) En tercer lugar, la supervisión independiente corre a cargo de la Comisión Nacional de Derechos Humanos (CNDH) ([270]), que puede investigar las vulneraciones de los derechos a la privacidad en general y a la privacidad de la correspondencia como parte de su mandato general de proteger los derechos fundamentales establecidos en los artículos 10 a 22 de la Constitución. La CNDH está formada por once comisarios que deben reunir cualificaciones específicas ([271]) y son nombrados por el presidente de conformidad con los procedimientos establecidos por la ley. En particular, cuatro comisarios son designados a propuesta de la Asamblea Nacional, cuatro a propuesta del presidente y tres a propuesta del jefe judicial del Tribunal Supremo ([272]). El presidente de la CNDH es nombrado por el presidente de la República entre los comisarios y debe ser confirmado por la Asamblea Nacional ([273]). Los comisarios (incluido el presidente de la CNDH) son nombrados por un mandato

([259]) Véase la sección 2.3.1 del anexo II. Véase también https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Del mismo modo, los auditores se designan sobre la base de las condiciones específicas establecidas en la Ley, véanse los artículos 16 y siguientes de la Ley de auditorías del sector público.
([261]) Artículos 8 a 11 de la Ley de auditorías del sector público.
([262]) Artículo 7 de la Ley de auditorías del sector público.
([263]) Artículo 41 de la Ley de auditorías del sector público.
([264]) Artículo 23, apartado 1, de la Ley de auditorías del sector público.
([265]) Artículo 26 de la Ley de auditorías del sector público.
([266]) Artículo 23, apartado 3, de la Ley de auditorías del sector público.
([267]) Véanse el artículo 7-8, apartados 3 y 4, y el artículo 7-9, apartado 5, de la LPIP.
([268]) Véase la notificación de la CPIP de la Nota n.º 2021-5, sección 6 (anexo I).
([269]) Véase también la sección 2.3.4 del anexo II.
([270]) Artículo 1 de la Ley de la Comisión Nacional de Derechos Humanos (Ley CNDH).
([271]) Para ser nombrado, un comisario debe 1) haber trabajado durante diez años, como mínimo, en una universidad o un instituto de investigación autorizado, al menos como profesor asociado; 2) haber ejercido como juez, fiscal o abogado durante al menos diez años; 3) haber participado en actividades de derechos humanos durante al menos diez años (por ejemplo, para una organización sin ánimo de lucro, una organización no gubernamental o una organización internacional); o 4) haber sido recomendados por grupos de la sociedad civil (artículo 5, apartado 3, de la Ley CNDH). Además, una vez nombrados, los comisarios tienen prohibido ocupar un cargo simultáneo en la Asamblea Nacional, los consejos locales o cualquier Gobierno estatal o local (como funcionario público), véase el artículo 10 de la Ley CNDH.
([272]) Artículo 5, apartados 1 y 2, de la Ley CNDH.
([273]) Artículo 5, apartado 5, de la Ley CNDH.

renovable de tres años y solo pueden ser destituidos cuando sean condenados a prisión o ya no sean capaces de ejercer sus funciones debido a una debilidad física o mental prolongada (en cuyo caso, dos terceras partes de los comisarios deben estar de acuerdo con la destitución) ([274]). Como parte de una investigación, la CNDH puede solicitar la presentación de los materiales pertinentes, llevar a cabo inspecciones y convocar personas para que testifiquen ([275]). En cuanto a las facultades correctivas, la CNDH puede formular recomendaciones (públicas) para mejorar o corregir políticas y prácticas específicas, a las cuales las autoridades públicas deben responder con una propuesta de un plan de ejecución ([276]). Si la autoridad en cuestión no aplica las recomendaciones, debe informar de ello a la Comisión ([277]), que, a su vez, puede comunicar dicho incumplimiento a la Asamblea Nacional o hacerlo público. Según la declaración oficial del Gobierno coreano (sección 2.3.5 del anexo II), las autoridades coreanas generalmente cumplen las recomendaciones de la CNDH y tienen un fuerte incentivo para hacerlo, ya que su aplicación se ha examinado como parte de una evaluación general y continua bajo la autoridad de la Oficina del Primer Ministro. Las cifras anuales sobre sus actividades muestran que la CNDH supervisa activamente las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, ya sea sobre la base de peticiones individuales o mediante investigaciones de oficio ([278]).

(173) En cuarto lugar, la supervisión general de la legalidad de las actividades de las autoridades públicas es realizada por la CCI, que examina los ingresos y gastos del Estado, pero también, de manera más general, supervisa el cumplimiento de las obligaciones de las autoridades públicas con vistas a mejorar el funcionamiento de la administración pública ([279]). La CCI está establecida formalmente bajo la responsabilidad del presidente de la República de Corea, pero mantiene un estatuto independiente con respecto a sus funciones ([280]). Además, se le concede plena independencia en lo que respecta al nombramiento, la destitución y la organización de su personal, así como a la elaboración de su presupuesto ([281]). La CCI está formada por un presidente (nombrado por el presidente de la República, con el consentimiento de la Asamblea Nacional) ([282]) y seis comisarios (nombrados por el presidente de la República por recomendación del presidente de la CCI) ([283]), que deben reunir las cualificaciones específicas establecidas por la ley ([284]) y solo pueden ser despedidos en caso de proceso de destitución, condena a prisión o incapacidad para ejercer sus funciones debido a una debilidad física o mental a largo plazo ([285]). La CCI lleva a cabo una auditoría general con una periodicidad anual, pero también puede realizar auditorías específicas sobre cuestiones de especial interés. Al llevar a cabo una auditoría o una inspección, la CCI puede solicitar la presentación de documentos y la asistencia de personas ([286]). La CCI puede formular recomendaciones, solicitar medidas disciplinarias o presentar una denuncia penal ([287]).

(174) Por último, la Asamblea Nacional lleva a cabo la supervisión parlamentaria de las autoridades públicas a través de investigaciones e inspecciones ([288]) de sus actividades ([289]). Puede solicitar la divulgación de documentos, exigir la comparecencia de testigos ([290]), recomendar medidas correctoras (si llega a la conclusión de que se han llevado

([274]) Artículo 7, apartado 1, y artículo 8 de la Ley CNDH.

([275]) Artículo 36 de la Ley CNDH. De conformidad con el artículo 6, apartado 7, de la Ley, puede rechazarse la presentación de materiales u objetos si esta perjudicara la confidencialidad del Estado y pudiera tener un efecto considerable sobre la seguridad del Estado o las relaciones diplomáticas o si constituyera un obstáculo importante para una investigación penal o un juicio en curso. En tales casos, la Comisión puede solicitar información adicional al jefe del organismo pertinente (que debe cumplir de buena fe) cuando sea necesario para permitir una revisión de si la negativa a facilitar la información está justificada.

([276]) Artículo 25, apartados 1 y 3, de la Ley CNDH.

([277]) Artículo 25, apartado 4, de la Ley CNDH.

([278]) Por ejemplo, entre 2015 y 2019, la CNDH recibió anualmente entre 1 380 y 1 699 peticiones en contra de las autoridades encargadas de garantizar el cumplimiento del Derecho penal y tramitó un número igual de alto (por ejemplo, tramitó 1 546 denuncias contra la policía en 2018 y 1 249 en 2019); también llevó a cabo varias investigaciones de oficio, tal como se describe con más detalle en el informe anual de 2018 de la CNDH (disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) y en el informe anual de 2019 (disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Artículos 20 y 24 de la Ley de la Comisión de Control e Inspección (Ley CCI). Véase la sección 2.3.2 del anexo II.

([280]) Artículo 2, apartado 1, de la Ley CCI.

([281]) Artículo 2, apartado 2, de la Ley CCI.

([282]) Artículo 4, apartado 1, de la Ley CCI.

([283]) Artículo 5, apartado 1, y artículo 6 de la Ley CCI.

([284]) Por ejemplo, haber ejercido como juez, fiscal o abogado durante al menos diez años, haber trabajado como funcionario o profesor o haber ocupado un cargo más alto en una universidad durante al menos ocho años, o haber trabajado durante al menos diez años en una empresa cotizada o en una institución participada por el Gobierno (de los cuales al menos cinco años como director ejecutivo), véase el artículo 7 de la Ley CCI. Además, los comisarios tienen prohibido participar en actividades políticas y ocupar simultáneamente cargos en la Asamblea Nacional, organismos administrativos, organizaciones sujetas a auditoría e inspección por parte de la CCI o cualquier otro cargo remunerado (artículo 9 de la Ley CCI).

([285]) Artículo 8 de la Ley CCI.

([286]) Véase, por ejemplo, el artículo 27 de la Ley CCI.

([287]) Artículos 24 y 31 a 35 de la Ley CCI.

([288]) Artículo 128 de la Ley de la Asamblea Nacional y artículos 2, 3 y 15 de la Ley de inspección e investigación de la administración del Estado. Esto incluye las inspecciones anuales de los asuntos gubernamentales en su conjunto, pero también las investigaciones de cuestiones específicas.

([289]) Véase la sección 2.2.3 del anexo.

([290]) Artículo 10, apartado 1, de la Ley de inspección e investigación de la administración del Estado. Véanse también los artículos 128 y 129 de la Ley de la Asamblea Nacional.

a cabo actividades ilícitas o inadecuadas) ([291]) y hacer públicos los resultados de sus conclusiones ([292]). Cuando la Asamblea Nacional solicite la adopción de medidas correctoras —que pueden incluir, por ejemplo, la concesión de indemnizaciones, la adopción de medidas disciplinarias o la mejora de los procedimientos internos—, la autoridad pública de que se trate deberá actuar sin demora e informar del resultado a la Asamblea Nacional ([293]).

3.2.4 *Vías de recurso*

(175) El sistema coreano ofrece distintas vías (judiciales) para obtener reparación, entre ellas una indemnización por daños y perjuicios.

(176) En primer lugar, la LPIP otorga a las personas un derecho de acceso, rectificación, supresión y suspensión con respecto a los datos personales tratados a efectos de control de la aplicación del Derecho penal ([294]).

(177) En segundo lugar, los particulares pueden hacer uso de los diferentes mecanismos de recurso ofrecidos por la LPIP si sus datos han sido tratados por una autoridad encargada de garantizar el cumplimiento del Derecho penal en violación de la LPIP o en violación de las limitaciones y salvaguardias que rigen la recogida de datos personales en otras leyes (por ejemplo, la LEC o la LPPC, véase el considerando 171). En particular, las personas físicas pueden presentar una reclamación ante la CPIP (incluso a través del Centro de atención telefónica sobre privacidad gestionado por la Agencia de Internet y Seguridad de Corea ([295])) o el Comité de mediación de conflictos relacionados con la información personal ([296]). Estas posibilidades de recurso no están sujetas a otros requisitos de admisibilidad. Sobre la base de la Ley de lo contencioso-administrativo, las personas también pueden recurrir o impugnar las decisiones o la inacción de la CPIP (véase el considerando 132).

(178) En tercer lugar, cualquier persona ([297]) puede presentar una denuncia ante la CNDH en relación con una vulneración del derecho a la privacidad y a la protección de datos por parte de una autoridad coreana encargada de garantizar el cumplimiento del Derecho penal. La CNDH puede recomendar la rectificación o la mejora de cualquier ley, institución, política o práctica pertinente ([298]), o la aplicación de soluciones como la mediación ([299]), el cese de la vulneración de los derechos humanos, la indemnización por daños y perjuicios y medidas para evitar que vuelvan a producirse infracciones idénticas o similares ([300]). Según la declaración oficial del Gobierno coreano (punto 2.4.2 del anexo II), esto también puede comprender la supresión de datos personales recogidos de manera ilícita. Aunque la CNDH no está facultada para adoptar decisiones vinculantes, ofrece una vía de recurso más informal, de bajo coste y de fácil acceso, especialmente porque, como se explica en el anexo II, sección 2.4.2, no exige demostrar la existencia de un perjuicio para que se investigue una denuncia ([301]). Esto garantiza que las denuncias de particulares relacionadas con la recogida de sus datos puedan investigarse, incluso si una persona no está en condiciones de demostrar que sus datos realmente se han recogido (por ejemplo, porque aún no se ha notificado a la persona). Los informes de actividad anuales de la CNDH muestran que las personas también utilizan esta vía en la práctica para impugnar las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, incluso en lo que respecta al manejo de datos personales ([302]). Si una persona no está satisfecha con el resultado de un procedimiento ante la CNDH, puede impugnar las decisiones de esta

([291]) Artículo 16, apartado 2, de la Ley de inspección e investigación de la administración del Estado.
([292]) Artículo 12-2 de la Ley de inspección e investigación de la administración del Estado.
([293]) Artículo 16, apartado 3, de la Ley de inspección e investigación de la administración del Estado.
([294]) Este derecho puede ejercerse directamente ante la autoridad competente o de forma indirecta a través de la CPIP (artículo 35, apartado 2, de la LPIP). Como se describe con más detalle en los considerandos 76 a 78, las excepciones a estos derechos solo se aplican cuando sea necesario para proteger intereses (públicos) importantes.
([295]) Artículo 62 de la LPIP.
([296]) Artículos 40 a 50 de la LPIP y artículos 48-2 a 57 del Decreto de Ejecución de la LPIP. Véase también la sección 2.4.1 del anexo II.
([297]) Como se explica en el anexo II, sección 2.4.2, aunque el artículo 4 de la Ley CNDH hace referencia a los ciudadanos y extranjeros residentes en la República de Corea, el término «residente» refleja un concepto de jurisdicción y no de territorio. Por consiguiente, si las instituciones nacionales dentro de Corea vulneran los derechos fundamentales de un extranjero fuera de Corea, dicho particular puede presentar una denuncia ante la CNDH. Este sería el caso si las autoridades públicas coreanas accedieran de manera ilícita a los datos personales de un extranjero transferidos a Corea. Véanse, en particular, las explicaciones facilitadas en https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Artículo 44 de la Ley CNDH.
([299]) Una persona también puede solicitar que la denuncia se resuelva mediante mediación (véanse los artículos 42 y siguientes de la Ley CNDH).
([300]) Artículo 42, apartado 4, de la Ley CNDH. Por otra parte, la CNDH puede adoptar medidas de ayuda urgente en caso de una infracción continua que pueda causar daños difíciles de reparar si no se atiende (véase el artículo 48 de la Ley CNDH).
([301]) En principio, la denuncia debe presentarse en el plazo de un año a partir de la infracción, pero la CNDH puede decidir, aun así, investigar una denuncia presentada después de ese plazo, siempre que no haya expirado el régimen de prescripción en virtud del Derecho penal o civil (artículo 32, apartado 1, punto 4, de la Ley CNDH).
([302]) Por ejemplo, la CNDH ha tramitado denuncias en el pasado y ha formulado recomendaciones en relación con las incautaciones ilícitas y el incumplimiento de la obligación de informar a las personas de una incautación (véanse las páginas 80 y 91 del informe anual de 2018 de la CNDH, disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), así como el tratamiento ilícito de información personal por parte de la policía, la fiscalía y los órganos jurisdiccionales (véanse las páginas 157 y 158 del informe anual de 2019 de la CNDH, disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, y la página 76 del informe anual de 2019, disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

última (por ejemplo, una decisión de no continuar la investigación de una denuncia ([303])) y las recomendaciones formuladas ante los órganos jurisdiccionales coreanos en virtud de la Ley de lo contencioso-administrativo (véase el considerando 181) ([304]). Además, un procedimiento ante la CNDH puede facilitar aún más el acceso a los órganos jurisdiccionales, ya que un particular puede recurrir contra la autoridad pública que haya tratado sus datos ilícitamente sobre la base de las constataciones de la CNDH, de conformidad con los procedimientos descritos en los considerandos 181 a 183.

(179) Por último, hay diferentes recursos judiciales disponibles, que permiten a las personas invocar las limitaciones y salvaguardias descritas en la sección 3.2.1 para obtener reparación ([305]).

(180) Con respecto a las incautaciones (incluidos los datos), la LEC prevé la posibilidad de objetar o impugnar la ejecución de una orden a través de una «cuasi reclamación», solicitando al órgano jurisdiccional competente que cancele o modifique una disposición adoptada por un fiscal o un agente de policía ([306]).

(181) De manera más general, las personas pueden impugnar las acciones ([307]) u omisiones ([308]) de las autoridades públicas (incluidas las autoridades encargadas de garantizar el cumplimiento del Derecho penal) en virtud de la Ley de lo contencioso-administrativo ([309]). Una medida administrativa se considera como «disposición impugnable» si afecta directamente los derechos y obligaciones civiles ([310]), que, como ha confirmado el Gobierno coreano (sección 2.4.3 del anexo II), es el caso de las medidas para recoger datos personales, ya sea de forma directa (por ejemplo, interceptando comunicaciones) o mediante solicitudes de divulgación vinculantes (por ejemplo, a un proveedor de servicios) o solicitudes de cooperación voluntaria. Para que una denuncia con arreglo a la Ley de lo contencioso-administrativo sea admisible, una persona debe tener un interés jurídico en presentar la denuncia ([311]). Según la jurisprudencia del Tribunal Supremo, «interés jurídico» se interpreta como un «interés jurídicamente protegido», es decir, un interés directo y específico protegido por las leyes y los reglamentos en los que se basan las disposiciones administrativas (es decir, no intereses generales, indirectos y abstractos del público) ([312]). Los particulares tienen tal interés jurídico en caso de cualquier vulneración de las limitaciones y salvaguardias aplicables a la recogida de sus datos personales a efectos de control de la aplicación del Derecho penal (en virtud de leyes específicas o de la LPIP). Sobre la base de la Ley de lo contencioso-administrativo, un órgano jurisdiccional puede decidir revocar o modificar una disposición ilícita, emitir un dictamen de nulidad (es decir, un dictamen de que la disposición no tiene efectos jurídicos o de su inexistencia en el ordenamiento jurídico) o emitir un dictamen de que una omisión es ilícita ([313]). Una sentencia firme con arreglo a la Ley de lo contencioso-administrativo es vinculante para las partes ([314]).

([303]) Por ejemplo, si excepcionalmente la CNDH no puede inspeccionar determinados materiales o instalaciones porque atañen a secretos de Estado que pueden tener un efecto considerable sobre la seguridad del Estado o las relaciones diplomáticas o cuando la inspección suponga un obstáculo importante para una investigación penal o un juicio en curso y cuando esto impida que la CNDH lleve a cabo la investigación necesaria para evaluar el fondo de la petición recibida, informará a la persona de las razones por las que se desestimó la denuncia, de conformidad con el artículo 39 de la Ley CNDH. En este caso, el particular puede impugnar la decisión de la CNDH con arreglo a la Ley de lo contencioso-administrativo.

([304]) Véanse, por ejemplo, la Resolución 2007NU27259 del Tribunal Superior de Seúl, de 18 de abril de 2008, confirmada por la Resolución 2008Du7854 del Tribunal Supremo, de 9 de octubre de 2008; y la Resolución 2017NU69382 del Tribunal Superior de Seúl, de 2 de febrero de 2018.

([305]) Véase la sección 2.4.3 del anexo II.

([306]) Artículo 417 de la LEC, en relación con su artículo 414, apartado 2. Véase también la Resolución n.º 97Mo66 del Tribunal Supremo, de 29 de septiembre de 1997.

([307]) La Ley de lo contencioso-administrativo hace referencia a una «disposición», es decir, el ejercicio de poderes públicos en un caso concreto o la negativa a ejercerlos.

([308]) En virtud de la Ley de lo contencioso-administrativo, esto se refiere al fracaso prolongado por parte de un organismo administrativo para adoptar una determinada disposición, contrariamente a la obligación legal de hacerlo.

([309]) Una impugnación administrativa puede efectuarse, en primer lugar, ante las comisiones de recursos administrativos establecidas en determinadas autoridades públicas (por ejemplo, el SNI o la CNDH) o ante la Comisión Central de Recursos Administrativos creada bajo los auspicios de la Comisión Anticorrupción y de Derechos Civiles (artículo 6 de la Ley de recursos administrativos y artículo 18, apartado 1, de la Ley de lo contencioso-administrativo), como vía de recurso más informal. Sin embargo, una demanda también puede presentarse directamente ante los órganos jurisdiccionales coreanos sobre la base de la Ley de lo contencioso-administrativo.

([310]) Resolución 98Du18435 del Tribunal Supremo, de 22 de octubre de 1999; Resolución 99Du1113 del Tribunal Supremo, de 8 de septiembre de 2000, y Resolución 2010Du3541 del Tribunal Supremo, de 27 de septiembre de 2012.

([311]) Artículos 12, 35 y 36 de la Ley de lo contencioso-administrativo. Además, deben presentarse una solicitud de revocación o modificación de una disposición y una solicitud de declaración de la ilegalidad de una omisión en un plazo de noventa días a partir de la fecha en que el particular tenga conocimiento de la disposición u omisión y, en principio, a más tardar un año después de la fecha de emisión de la disposición o de que se haya producido la omisión, salvo que existan razones justificables (artículos 20 y 38, apartado 2, de la Ley de lo contencioso-administrativo). El concepto de «razones justificables» ha sido interpretado en sentido amplio por el Tribunal Supremo y requiere evaluar si es socialmente aceptable permitir la presentación de una denuncia tardía, a la luz de todas las circunstancias del asunto (Resolución 90NU6521 del Tribunal Supremo, de 28 de junio de 1991). Tal como ha confirmado el Gobierno coreano en el punto 2.4.3 del anexo II, esto incluye (entre otras cosas) los motivos de retraso de los que la parte afectada no puede ser considerada responsable (es decir, situaciones que escapan al control del denunciante, por ejemplo, cuando no se le ha notificado la recogida de sus datos personales) o de fuerza mayor (por ejemplo, una catástrofe natural o una guerra).

([312]) Resolución n.º 2006Du330 del Tribunal Supremo, de 26 de marzo de 2006.

([313]) Artículos 2 y 4 de la Ley de lo contencioso-administrativo.

([314]) Artículo 30, apartado 1, de la Ley de lo contencioso-administrativo.

(182) Además de impugnar la acción del Gobierno a través de litigios administrativos, las personas también pueden presentar un recurso de inconstitucionalidad ante el Tribunal Constitucional en relación con cualquier vulneración de sus derechos fundamentales debida al ejercicio o al no ejercicio del poder gubernamental (excluidas las sentencias de los órganos jurisdiccionales) ([315]). Si hay otras vías de recurso disponibles, estas deben agotarse primero. Según la jurisprudencia del Tribunal Constitucional, los extranjeros pueden interponer un recurso de inconstitucionalidad en la medida en que sus derechos fundamentales estén reconocidos por la Constitución coreana (véanse las explicaciones en la sección 1.1) ([316]). El Tribunal Constitucional puede invalidar el ejercicio del poder gubernamental que provocó la infracción o confirmar que una determinada omisión es inconstitucional ([317]). En tal caso, la autoridad competente está obligada a adoptar medidas para dar cumplimiento a la resolución del Tribunal.

(183) Además, los particulares pueden obtener una indemnización por daños y perjuicios ante los órganos jurisdiccionales coreanos. Esto incluye, en primer lugar, la posibilidad de reclamar una indemnización por las infracciones de la LPIP cometidas por las autoridades encargadas de garantizar el cumplimiento del Derecho penal, de conformidad con el artículo 39 (véase también el considerando 135). De manera más general, las personas pueden solicitar una indemnización por daños y perjuicios causados por funcionarios públicos debido al ejercicio de sus funciones oficiales en violación de la ley, sobre la base de la Ley de indemnización estatal (véase también el considerando 135) ([318]).

(184) Los mecanismos descritos en los considerandos 176 a 183 ofrecen a los interesados soluciones administrativas y judiciales efectivas que les permiten, en particular, hacer valer sus derechos, en especial el derecho a acceder a sus datos personales o a obtener la rectificación o supresión de dichos datos.

3.3 **Acceso y utilización por parte de las autoridades públicas coreanas con fines de seguridad nacional**

(185) El Derecho de la República de Corea contiene una serie de limitaciones y salvaguardias con respecto al acceso y la utilización de datos personales con fines de seguridad nacional, y proporciona mecanismos de supervisión y reparación que se ajustan a los requisitos mencionados en los considerandos 141 a 143 de la presente Decisión. Las condiciones en las que puede tener lugar dicho acceso y las salvaguardias aplicables al uso de estos poderes se precisan en detalle en las siguientes secciones.

3.3.1 *Base jurídica, limitaciones y salvaguardias*

(186) En la República de Corea, se puede acceder a los datos personales con fines de seguridad nacional sobre la base de la LPPC, la LST y la Ley antiterrorista para la protección de los ciudadanos y la seguridad pública (Ley antiterrorista) ([319]). La principal autoridad ([320]) con competencias en el ámbito de la seguridad nacional es el Servicio Nacional de Inteligencia (SNI) ([321]). La recogida y el uso de datos personales por parte del SNI deben cumplir

([315]) Artículo 68, apartado 1, de la Ley del Tribunal Constitucional. Los recursos de inconstitucionalidad deben presentarse en un plazo de noventa días a partir del momento en que el particular haya tenido conocimiento de la infracción, y en el plazo de un año a partir del momento en que se produjo. Como también se explica en el anexo II, sección 2.4.3, dado que el procedimiento establecido en la Ley de lo contencioso-administrativo se aplica a los litigios en virtud de la Ley del Tribunal Constitucional, de conformidad con su artículo 40, una denuncia seguirá siendo admisible si existen «razones justificables», interpretadas de acuerdo con la jurisprudencia del Tribunal Supremo descrita en la nota a pie de página n.º 312. Si primero hay que agotar otras vías de recurso, un recurso de inconstitucionalidad debe interponerse en un plazo de treinta días a partir de la decisión final sobre dicho recurso (artículo 69 de la Ley del Tribunal Constitucional).

([316]) Resolución n.º 99HeonMa194 del Tribunal Constitucional, de 29 de noviembre de 2001.

([317]) Artículo 75, apartado 3, de la Ley del Tribunal Constitucional.

([318]) Artículo 2, apartado 1, de la Ley de indemnización estatal.

([319]) Véase la sección 3.1 del anexo II.

([320]) Excepcionalmente, la policía y las fiscalías también pueden recoger información personal con fines de seguridad nacional (véase la nota a pie de página n.º 327 y el anexo II, sección 3.2.1.2). Además, la agencia de inteligencia militar coreana (el Comando de Apoyo a la Seguridad de la Defensa, establecido bajo los auspicios del Ministerio de Defensa) tiene competencias en el ámbito de la seguridad nacional. Sin embargo, como se explica en el anexo II, punto 3.1, solo es responsable de la inteligencia militar y solo lleva a cabo la vigilancia de civiles cuando sea necesario para desempeñar sus funciones militares. En particular, únicamente puede investigar al personal militar, a los empleados civiles del ejército, a las personas en formación militar, a las personas en reserva militar o servicio de reclutamiento y a los prisioneros de guerra (artículo 1 de la Ley de tribunales militares). Al recoger información sobre las comunicaciones con fines de seguridad nacional, el Comando de Apoyo a la Seguridad de la Defensa está sujeto a las limitaciones y salvaguardias establecidas por la LLPC y su Decreto de Ejecución.

([321]) El mandato del SNI consiste en recoger, recopilar y distribuir información sobre países extranjeros (por ejemplo, información general sobre las tendencias y la evolución en relación con países extranjeros o las actividades de los agentes estatales); inteligencia relacionada con la lucha contra el espionaje (incluido el espionaje militar e industrial), el terrorismo y las actividades de la delincuencia organizada internacional; inteligencia sobre determinados tipos de delitos dirigidos contra la seguridad pública y nacional (por ejemplo, la insurrección nacional y la agresión extranjera) e inteligencia relacionada con la tarea de garantizar la ciberseguridad y prevenir o contrarrestar los ciberataques y las amenazas (artículo 4, apartado 2, de la Ley SNI). Véase también el punto 3.1 del anexo II.

los requisitos jurídicos pertinentes (incluidas la LPIP y la LPPC) ([322]) y las directrices generales elaboradas por el presidente de la República y revisadas por la Asamblea Nacional ([323]). Como principio general, el SNI debe mantener la neutralidad política y proteger la libertad y los derechos de las personas ([324]). Además, el personal del SNI no debe abusar de sus potestades públicas para obligar a una institución, organización o persona a hacer algo que no estén obligadas a hacer (con arreglo a la ley) ni obstruir el ejercicio de los derechos de ninguna persona ([325]).

3.3.1.1 Acceso a la información sobre las comunicaciones

(187) Sobre la base de la LPPC, las autoridades públicas coreanas ([326]) pueden recoger datos de confirmación de la comunicación (es decir, la fecha de las telecomunicaciones, su hora de inicio y fin, el número de llamadas salientes y entrantes, así como el número de abonados de la otra parte, la frecuencia de uso, los archivos de registro sobre el uso de los servicios de telecomunicaciones y la información sobre la ubicación, véase el considerando 155) y el contenido de las comunicaciones (a través de medidas de restricción de la comunicación, véase el considerando 155) con fines de seguridad nacional (según lo determinado por el mandato del SNI, véase la nota al pie de página n.º 322). Estas competencias abarcan dos tipos de información: 1) comunicaciones en las que una o ambas partes son nacionales coreanos ([327]) y 2) comunicaciones de a) países hostiles a la República de Corea, b) agencias, grupos o nacionales extranjeros sospechosos de participar en actividades anticoreanas ([328]) o c) miembros de grupos que operan en la península de Corea, pero, en la práctica, más allá de la soberanía de la República de Corea y de sus grupos centrales con sede en países extranjeros ([329]). Por consiguiente, las comunicaciones de los ciudadanos de la UE transferidas desde la Unión a la República de Corea sobre la base de la presente Decisión solo pueden recogerse con arreglo a la LPPC con fines de seguridad nacional (con sujeción a las condiciones establecidas en los considerandos 188 a 192) si se trata de comunicaciones entre un ciudadano de la UE y de un nacional coreano o si atañen exclusivamente a comunicaciones entre nacionales no coreanos y entran en una de las tres categorías mencionadas 2a), b) y c).

(188) En ambos escenarios, la recogida de datos de confirmación de la comunicación solo puede realizarse con el fin de prevenir amenazas para la seguridad nacional ([330]), mientras que las medidas de restricción de la comunicación solo pueden adoptarse cuando exista un riesgo grave para la seguridad nacional y la recogida sea necesaria para prevenirlo ([331]). Además, solo puede accederse al contenido de las comunicaciones como medida de último recurso y debe hacerse un esfuerzo para minimizar la violación de la privacidad de las comunicaciones ([332]), garantizando así que siga siendo proporcional al objetivo de seguridad nacional perseguido. La recogida tanto del contenido de las comunicaciones como de los datos de confirmación de la comunicación solo puede durar un período máximo de cuatro meses y debe interrumpirse de inmediato si se alcanza antes el objetivo perseguido ([333]). Si se siguen cumpliendo las condiciones pertinentes, el plazo puede prorrogarse hasta cuatro meses, previa autorización de un órgano jurisdiccional (para las medidas descritas en el considerando 189) o del presidente (para las medidas descritas en el considerando 190) ([334]).

(189) Las mismas salvaguardias procedimentales se aplican a la recogida de datos de confirmación de la comunicación y al contenido de las comunicaciones ([335]). En particular, cuando al menos una de las personas que participan en la comunicación sea un nacional coreano, la agencia de inteligencia debe presentar una solicitud por escrito a la

([322]) Véanse también los artículos 14, 22 y 23 de la Ley SNI.
([323]) Artículo 4, apartado 2, de la Ley SNI.
([324]) Artículo 3, apartado 1; artículo 6, apartado 2, y artículos 11 y 21 de la Ley SNI. Véanse también las normas sobre los conflictos de intereses, en particular los artículos 10 y 12 de la Ley SNI.
([325]) Artículo 13 de la Ley SNI.
([326]) Esto incluye las agencias de inteligencia (es decir, el SNI y el Comando de Apoyo a la Seguridad de la Defensa), la policía y las fiscalías.
([327]) Artículo 7, apartado 1, punto 1, de la LPPC.
([328]) Según ha explicado el Gobierno coreano en la nota a pie de página n.º 244 del anexo II, esto se refiere a actividades que amenazan la existencia y la seguridad de la nación, el orden democrático o la supervivencia y la libertad del pueblo.
([329]) Artículo 7, apartado 1, punto 2, de la LPPC.
([330]) Artículo 13-4 de la LPPC.
([331]) Artículo 7, apartado 1, de la LPPC.
([332]) Artículo 3, apartado 2, de la LPPC. Además, las medidas de restricción de la comunicación deben interrumpirse de inmediato una vez que dejen de ser necesarias, garantizando así que cualquier violación de los secretos de la comunicación del particular se limite al mínimo (artículo 2 del Decreto de Ejecución de la LPPC).
([333]) Artículo 7, apartado 2, de la LPPC.
([334]) La solicitud de autorización para prorrogar las medidas de vigilancia debe presentarse por escrito, indicando los motivos por los que se solicita la prórroga y facilitando materiales de apoyo (artículo 7, apartado 2, de la LPPC y artículo 5 del Decreto de Ejecución de la LPPC).
([335]) Véanse el artículo 13-4, apartado 2, de la LPPC y el artículo 37, apartado 4, del Decreto de Ejecución de la LPPC, según los cuales los procedimientos aplicables a la recogida del contenido de las comunicaciones también se aplican a la recogida de datos de confirmación de la comunicación. Véase también el punto 3.2.1.1.1 del anexo II.

Fiscalía Superior, que, a su vez, debe solicitar una orden de un jefe judicial del Tribunal Superior ([336]). La LPPC indica la información que debe proporcionarse en la solicitud al fiscal, la solicitud de la orden y la propia orden, que incluye, en particular, la justificación de la solicitud y los principales motivos de sospecha, los materiales de apoyo, así como información sobre el objetivo, el objeto (es decir, la persona o personas específicas), el alcance y la duración de la medida propuesta ([337]). La recogida sin una orden solo puede tener lugar si hay un acto de conspiración que amenace la seguridad nacional y existe una emergencia que impida seguir los procedimientos antes mencionados ([338]). No obstante, también en tal caso, la solicitud de una orden debe presentarse inmediatamente después de la adopción de la medida ([339]). Por consiguiente, la LPPC define claramente el alcance y las condiciones de estos tipos de recogida y los somete a salvaguardias (procedimentales) específicas (incluida la previa aprobación judicial), lo cual garantiza que el uso de tales medidas se limite a lo necesario y proporcionado. Además, el requisito de facilitar información detallada tanto en la solicitud de una orden como en la propia orden excluye la posibilidad de acceso indiscriminado.

(190) Para las comunicaciones entre nacionales no coreanos incluidos en una de las tres categorías específicas mencionadas en el considerando 187, debe presentarse una solicitud al director del SNI, quien, tras examinar la adecuación de las medidas propuestas, debe solicitar la aprobación previa por escrito del presidente de la República de Corea ([340]). La solicitud elaborada por la agencia de inteligencia debe incluir la misma información detallada que una solicitud de orden judicial (véase el considerando 189), en particular sobre la justificación de la solicitud y los principales motivos de sospecha, los materiales de apoyo y la información sobre los objetivos, la persona o personas específicas, el alcance y la duración de las medidas propuestas ([341]). En situaciones de emergencia ([342]), debe obtenerse la aprobación previa del ministro al que pertenezca la agencia de inteligencia competente, aunque la agencia de inteligencia debe solicitar la aprobación del presidente inmediatamente después de la adopción de las medidas de emergencia ([343]). Por consiguiente, también con respecto a la recogida de comunicaciones entre nacionales exclusivamente no coreanos, la LPPC limita el uso de tales medidas a lo necesario y proporcionado, al delimitar claramente las categorías limitadas de particulares que pueden ser objeto de tales medidas y al establecer criterios detallados que las agencias de inteligencia deben demostrar para justificar una solicitud de recogida de información. Además, esto descarta una vez más la posibilidad de un acceso indiscriminado. Si bien no existe una aprobación independiente previa de tales medidas, la supervisión independiente está garantizada *ex post*, especialmente por la CPIP y la CNDH (véanse, por ejemplo, los considerandos 199 y 200).

(191) Además, la LPPC impone varias salvaguardias adicionales que contribuyen a la supervisión *ex post* y facilitan el acceso de los particulares a vías de recurso eficaces. En primer lugar, con respecto a cualquier tipo de recogida con fines de seguridad nacional, la LPPC establece diferentes requisitos de mantenimiento de registros y requisitos de información. En particular, a la hora de solicitar la cooperación de operadores privados, las agencias de inteligencia deben facilitar la orden judicial, la autorización presidencial o una copia de la portada de una declaración de censura de emergencia, que la entidad obligada debe conservar en sus archivos ([344]). Cuando los operadores privados se vean obligados a cooperar, tanto la autoridad pública requirente como el operador

([336]) Artículo 6, apartados 5 y 8, y artículo 7, apartado 1, punto 1, y apartado 3, de la LPPC, en relación con el artículo 7, apartados 3 y 4, del Decreto de Ejecución de la LPPC.

([337]) Véanse el artículo 7, apartado 3, y el artículo 6, apartado 4, de la LPPC (para la solicitud de la agencia de inteligencia), el artículo 4 del Decreto de Ejecución de la LPPC (para la solicitud del fiscal) y el artículo 7, apartado 3, y el artículo 6, apartado 6, de la LPPC (para la orden).

([338]) Artículo 8 de la LPPC.

([339]) Artículo 8, apartados 2 y 8, de la LPPC. La recogida debe interrumpirse inmediatamente si no se obtiene la autorización judicial en un plazo de treinta y seis horas a partir del momento en que se adopten las medidas. En los casos en que la vigilancia se complete en poco tiempo y se descarte la autorización judicial, el jefe de la Fiscalía Superior competente debe enviar una notificación de las medidas de emergencia preparada por la agencia de inteligencia al jefe del órgano jurisdiccional competente, que, sobre esta base, puede examinar la legalidad de la recogida (artículo 8, apartados 5 y 7, de la LPPC). En esta notificación deben indicarse el objetivo, el objeto, el alcance, el período, el lugar de ejecución y el método de vigilancia, así como los motivos para no presentar una solicitud antes de adoptar la medida (artículo 8, apartado 6, de la LPPC). De manera más general, las agencias de inteligencia solo pueden adoptar medidas de emergencia de conformidad con una «declaración de censura/escuchas telefónicas de emergencia» y deben mantener registros de tales medidas (artículo 8, apartado 4, de la LPPC).

([340]) Artículo 8, apartados 1 y 2, del Decreto de Ejecución de la LPPC.

([341]) Artículo 8, apartado 3, del Decreto de Ejecución de la LPPC, en relación con el artículo 6, apartado 4, de la LPPC.

([342]) Es decir, en los casos en que la medida esté destinada a un acto de conspiración que amenace la seguridad nacional, no haya tiempo suficiente para obtener la aprobación del presidente y la no adopción de medidas de emergencia pueda perjudicar a la seguridad nacional (artículo 8, apartado 8, de la LPPC).

([343]) Artículo 8, apartado 9, de la LPPC. La recogida debe interrumpirse inmediatamente si no se obtiene la autorización en un plazo de treinta y seis horas a partir del momento en que se realice la solicitud.

([344]) Artículo 9, apartado 2, de la LPPC y artículo 12 del Decreto de Ejecución de la LPPC. Véase el artículo 13 del Decreto de Ejecución de la LPPC sobre la posibilidad de obligar a las oficinas de correos y los proveedores de servicios de telecomunicaciones a prestar asistencia. Los operadores privados a los que se solicita que divulguen información pueden negarse a hacerlo cuando la orden, la autorización o la declaración de censura de emergencia se refieran al identificador incorrecto (por ejemplo, un número de teléfono perteneciente a un particular distinto del identificado). En cualquier caso, tienen prohibido revelar las contraseñas utilizadas para las comunicaciones (artículo 9, apartado 4, de la LPPC).

pertinente deben mantener registros sobre la finalidad y el objeto de las medidas, así como sobre la fecha de ejecución ([345]). Además, las agencias de inteligencia deben informar al director del SNI sobre la información que han recopilado y el resultado de la actividad de vigilancia ([346]).

(192) En segundo lugar, las personas deben ser informadas de la recogida de sus datos (datos de confirmación de la comunicación o contenido de las comunicaciones) con fines de seguridad nacional si se trata de comunicaciones en las que al menos una de las partes es un nacional coreano ([347]). Esta notificación debe presentarse por escrito en un plazo de treinta días a partir de la fecha de finalización de la recogida (incluso cuando los datos se hayan obtenido con arreglo al procedimiento de emergencia) y solo puede aplazarse si pondría en peligro la seguridad nacional o perjudicaría la vida y la seguridad física de las personas ([348]). Con independencia de dicha notificación, los particulares pueden obtener reparación a través de distintas vías, como se explica con más detalle en el punto 3.3.4.

3.3.1.2 Recogida de información sobre sospechosos de terrorismo

(193) La Ley antiterrorista establece que el SNI puede recoger datos sobre los sospechosos de terrorismo ([349]) de conformidad con las limitaciones y salvaguardias establecidas en otras leyes ([350]). En particular, el SNI puede obtener datos de comunicaciones (sobre la base de la LPPC) y otra información personal (a través de una solicitud de divulgación voluntaria) ([351]). Con respecto a la recogida de información de comunicaciones (es decir, el contenido de las comunicaciones o los datos de confirmación de la comunicación), se aplican las limitaciones y salvaguardias descritas en el punto 3.3.1.1, incluido el requisito de obtener una orden judicial. Por lo que se refiere a las solicitudes de divulgación voluntaria de otros tipos de datos personales de los sospechosos de terrorismo, el SNI debe cumplir los requisitos establecidos en la Constitución y la LPIP relativos a la necesidad y la proporcionalidad (véase el considerando 164) ([352]). Los responsables del tratamiento que reciban tales solicitudes pueden acceder voluntariamente en las condiciones establecidas en la LPIP (por ejemplo, de conformidad con el principio de minimización de los datos y limitando el impacto sobre la privacidad de la persona) ([353]). En este caso, también deben cumplir el requisito de notificar al particular de que se trate según la Nota n.º 2021-5 (véase el considerando 166).

([345]) Para las medidas de restricción de la comunicación, estos registros deben conservarse durante tres años (véanse el artículo 9, apartado 3, de la LPPC y el artículo 17, apartado 2, del Decreto de Ejecución de la LPPC). Por lo que se refiere a los datos de confirmación de la comunicación, las agencias de inteligencia deben mantener registros de que se ha realizado una solicitud relativa a tales datos, así como de la propia solicitud escrita y de la institución que se ha amparado en ella (artículo 13, apartado 5, y artículo 13-4, apartado 3, de la LPPC). Los proveedores de servicios de telecomunicaciones deben conservar los registros durante siete años e informar dos veces al año al Ministerio de Ciencia y TIC sobre la frecuencia de estas divulgaciones (artículo 9, apartado 3, de la LPPC, en relación con su artículo 13, apartado 7, y el artículo 37, apartado 4, y el artículo 39 del Decreto de Ejecución de la LPPC).

([346]) Artículo 18, apartado 3, del Decreto de Ejecución de la LPPC.

([347]) Artículo 9-2, apartado 3, y artículo 13-4 de la LPPC. La notificación debe incluir 1) el hecho de que se ha recogido la información, 2) el organismo de ejecución y 3) el período de ejecución.

([348]) Artículo 9-2, apartado 4, de la LPPC. En tal caso, la notificación debe efectuarse en un plazo de treinta días una vez que dejen de existir los motivos para el aplazamiento (véanse el artículo 13-4, apartado 2, y el artículo 9-2, apartado 6, de la LPPC).

([349]) Es decir, los miembros de un grupo terrorista (designado por las Naciones Unidas, véase el artículo 2, apartado 2, de la Ley antiterrorista); las personas que promuevan y difundan las ideas o tácticas de un grupo terrorista, recauden o aporten fondos para el terrorismo o participen en otras actividades de preparación, conspiración, propaganda o instigación del terrorismo; o personas para las que existan motivos fundados para sospechar que han llevado a cabo tales actividades (artículo 2, apartado 3, de la Ley antiterrorista). El término «terrorismo» se define en el artículo 2, apartado 1, de la Ley antiterrorista como conducta llevada a cabo con el fin de impedir el ejercicio de la autoridad del Estado, de un Gobierno local o de un Gobierno extranjero (incluidas las organizaciones internacionales) o con el fin de obligarlos a actuar sin que tengan ninguna obligación legal de hacerlo o de amenazar al público. Esta conducta puede abarcar, por ejemplo, el asesinato, el secuestro o la toma de rehenes; el secuestro, la incautación, la destrucción o el daño de un buque o una aeronave; el uso de armas bioquímicas, explosivas o incendiarias con la intención de provocar muertes, lesiones graves o daños; y el abuso de materiales nucleares o radiactivos.

([350]) Artículo 9, apartados 1 y 3, de la Ley antiterrorista.

([351]) Si bien la Ley antiterrorista también hace referencia a la posibilidad de recoger información sobre la entrada y salida de la República de Corea sobre la base de la Ley de inmigración y la Ley de aduanas, estas leyes actualmente no prevén tal habilitación (véase la sección 3.2.2.1 del anexo II). En cualquier caso, no se aplicarían, en principio, a los datos transferidos sobre la base de la presente Decisión, ya que normalmente afectarían a información que sería recogida directamente por las autoridades coreanas (en lugar del acceso a datos previamente transferidos desde la Unión a los responsables del tratamiento coreanos). Además, la Ley antiterrorista menciona la LCUIETF como base jurídica para la recogida de información sobre transacciones financieras. Sin embargo, como se explica en la nota a pie de página n.º 200, los tipos de datos que podrían obtenerse sobre la base de esta Ley no entran en el ámbito de aplicación de la presente Decisión. Por último, la Ley antiterrorista también establece que el SNI puede recoger información sobre la ubicación a través de solicitudes no vinculantes, en cuyo caso los proveedores de información sobre la ubicación podrían divulgar voluntariamente dicha información en las condiciones establecidas en la LPIP (tal como se describe en el considerando 193) y en la Ley de información sobre la ubicación. No obstante, como también se explica en la nota a pie de página n.º 17, la información sobre la ubicación no se transferiría desde la Unión a los responsables del tratamiento coreanos sobre la base de la presente Decisión, sino que se generaría dentro de Corea.

([352]) Véase la sección 3.2.2.2 del anexo II.

([353]) Véanse el artículo 58, apartado 4, de la LPIP, que exige que la información personal se trate en la medida mínima necesaria para lograr la finalidad prevista, y el artículo 3, apartado 6, de la LPIP, que establece que la información personal debe tratarse de manera que se reduzca al mínimo la posibilidad de vulnerar la privacidad de la persona. Véase también el artículo 59, puntos 2 y 3, de la LPIP, según el cual los responsables del tratamiento tienen prohibido divulgar información personal a terceros sin autoridad.

3.3.1.3 Solicitudes de divulgación voluntaria de datos de los abonados

(194) Sobre la base de la LST, los proveedores de telecomunicaciones pueden divulgar voluntariamente los datos de los abonados (véase el considerando 163) a petición de una agencia de inteligencia que tenga la intención de recoger dicha información para evitar una amenaza para la seguridad nacional ([354]). Por lo que se refiere a estas solicitudes del SNI, se aplican las mismas limitaciones (establecidas en la Constitución, la LPIP y la LST) que en el ámbito de la aplicación del Derecho penal, como se expone en el considerando 164) ([355]). Los proveedores de telecomunicaciones no están obligados a cumplir y solo pueden hacerlo en las condiciones establecidas en la LPIP (en particular, de conformidad con el principio de minimización de los datos y limitando el impacto sobre la privacidad del particular, véase también el considerando 193). Se aplican los mismos requisitos con respecto al mantenimiento de registros y la notificación de la persona afectada que en el ámbito de la aplicación del Derecho penal (véanse los considerandos 165 y 166).

3.3.2 *Utilización ulterior de la información recogida*

(195) El tratamiento de los datos personales recogidos por las autoridades coreanas con fines de seguridad nacional está sujeto a los principios de limitación de la finalidad (artículo 3, apartados 1 y 2, de la LPIP), licitud y lealtad del tratamiento (artículo 3, apartado 1, de la LPIP), proporcionalidad/minimización de los datos (artículo 3, apartados 1 y 6, y artículo 58 de la LPIP), exactitud (artículo 3, apartado 3, de la LPIP), transparencia (artículo 3, apartado 5, de la LPIP), seguridad (artículo 58, apartado 4, de la LPIP)y limitación del plazo de conservación (artículo 58, apartado 4, de la LPIP) ([356]). La posible divulgación de datos personales a terceros (incluidos terceros países) solo puede llevarse a cabo de conformidad con estos principios (en particular, la limitación de la finalidad y la minimización de los datos), tras haber evaluado el cumplimiento de los principios de necesidad y proporcionalidad (artículo 37, apartado 2, de la Constitución) y teniendo en cuenta el impacto sobre los derechos de las personas afectadas (artículo 3, apartado 6, de la LPIP).

(196) Por lo que se refiere al contenido de las comunicaciones y los datos de confirmación de la comunicación, la LPPC limita aún más la utilización de dichos datos a los procedimientos judiciales en los que una parte relacionada con la comunicación se base en ellos para una reclamación por daños y perjuicios; o los usos permitidos en virtud de otras leyes ([357]).

3.3.3 *Supervisión*

(197) Las actividades de las autoridades coreanas de seguridad son supervisadas por distintos organismos ([358]).

(198) En primer lugar, la Ley antiterrorista prevé mecanismos específicos de supervisión de las actividades de lucha contra el terrorismo, incluida la recogida de datos sobre los sospechosos de terrorismo. En particular, en el nivel del poder ejecutivo, las actividades de lucha contra el terrorismo son supervisadas por la Comisión de Lucha contra el Terrorismo ([359]), a la que el director del SNI debe informar sobre las investigaciones y el rastreo de sospechosos de terrorismo para recabar la información o los materiales necesarios para las actividades de lucha contra el terrorismo ([360]). Además, el oficial de protección de los derechos humanos (OPDH) supervisa específicamente la conformidad de las actividades de lucha contra el terrorismo con los derechos fundamentales ([361]). El OPDH es nombrado por el presidente de la Comisión de Lucha contra el Terrorismo entre las personas que reúnen las cualificaciones específicas mencionadas en el Decreto de Ejecución de la Ley antiterrorista ([362]) por un período (renovable) de dos años y solo puede ser destituido de su cargo por motivos específicos y limitados y por causa justificada ([363]). En el ejercicio de su función de supervisión, el OPDH puede formular recomendaciones

([354]) Artículo 83, apartado 3, de la LST.
([355]) Véase también la sección 3.2.3 del anexo II.
([356]) Véase la sección 1.2 del anexo II.
([357]) Artículo 5, apartados 1 y 2, y artículos 12 y 13-5 de la LPPC.
([358]) Véase la sección 3.3 del anexo II.
([359]) Artículo 5, apartado 3, de la Ley antiterrorista. La Comisión está presidida por el primer ministro y está compuesta por varios ministros y jefes de organismos gubernamentales, como los ministros de Asuntos Exteriores, de Justicia, de Defensa Nacional y del Interior y Seguridad, el director del SNI y el comisario general de la Agencia Nacional de Policía (artículo 3, apartado 1, del Decreto de Ejecución de la Ley antiterrorista).
([360]) Artículo 9, apartado 4, de la Ley antiterrorista.
([361]) Artículo 7 de la Ley antiterrorista.
([362]) Es decir, cualquier persona cualificada como abogado con al menos diez años de experiencia laboral o con conocimientos especializados en el ámbito de los derechos humanos y que trabaje o haya trabajado (al menos) como profesor asociado durante al menos diez años o que haya ejercido como funcionario público de rango superior en agencias estatales o Gobiernos locales o con al menos diez años de experiencia laboral en el ámbito de los derechos humanos, por ejemplo, en una organización no gubernamental (artículo 7, apartado 1, del Decreto de Ejecución de la Ley antiterrorista).
([363]) Por ejemplo, cuando se le acuse en un proceso penal relacionado con sus funciones, cuando divulgue información confidencial o por incapacidad mental o física de larga duración (artículo 7, apartado 3, del Decreto de Ejecución de la Ley antiterrorista).

generales para mejorar la protección de los derechos humanos ([364]) y recomendaciones específicas de medidas correctoras en caso de que se haya constatado una vulneración de los derechos humanos ([365]). Las autoridades públicas están obligadas a informar al OPDH sobre el seguimiento dado a sus recomendaciones ([366]).

(199) En segundo lugar, la CPIP supervisa el cumplimiento por parte de las autoridades nacionales de seguridad de las normas de protección de datos, que incluyen tanto las disposiciones aplicables de la LPIP (véase el considerando 149) como las limitaciones y salvaguardias que se aplican a la recogida de datos personales en virtud de otras leyes (la LPPC, la Ley antiterrorista y la LST, véase también el considerando 171) ([367]). En el ejercicio de esta función de supervisión, la CPIP puede hacer uso de todas sus facultades de investigación y correctivas, según se describe detalladamente en el punto 2.4.2.

(200) En tercer lugar, las actividades de las autoridades nacionales de seguridad están sujetas a la supervisión independiente de la CNDH, de conformidad con los procedimientos descritos en el considerando 172 ([368]).

(201) En cuarto lugar, la función de supervisión de la CCI también abarca a las autoridades nacionales de seguridad, aunque, en circunstancias excepcionales, el SNI puede negarse a facilitar determinada información o ciertos materiales, por ejemplo, cuando constituyen secretos de Estado y el conocimiento público tendría graves consecuencias para la seguridad nacional ([369]).

(202) Por último, la supervisión parlamentaria de las actividades del SNI corre a cargo de la Asamblea Nacional (a través de un Comité de Inteligencia especializado) ([370]). La LPPC establece una función de supervisión específica de la Asamblea Nacional con respecto al uso de medidas de restricción de la comunicación con fines de seguridad nacional ([371]). En particular, la Asamblea Nacional puede llevar a cabo inspecciones *in situ* de los equipos de escuchas telefónicas y puede exigir tanto al SNI como a los operadores de telecomunicaciones que hayan divulgado el contenido de las comunicaciones que informen al respecto. La Asamblea Nacional también puede desempeñar sus funciones generales de supervisión (de conformidad con los procedimientos descritos en el considerando 174). La Ley SNI exige al director del SNI que responda sin demora cuando el Comité de Inteligencia solicite un informe sobre un asunto concreto ([372]), con normas específicas para determinada información especialmente sensible. En concreto, el director del SNI solo puede negarse a responder o testificar ante el Comité en circunstancias excepcionales, por ejemplo, si la solicitud se refiere a secretos de Estado relativos a cuestiones militares, diplomáticas o relacionadas con Corea del Norte, cuando el conocimiento público podría tener graves consecuencias para el «destino nacional» del país ([373]). En este caso, el Comité de Inteligencia puede solicitar una explicación al primer ministro y, si no se facilita ninguna explicación en el plazo de siete días, no podrá denegarse la respuesta o el testimonio.

3.3.4 *Vías de recurso*

(203) También en el ámbito de la seguridad nacional, el sistema coreano ofrece distintas vías (judiciales) para obtener reparación, incluida una indemnización por daños y perjuicios. Estos mecanismos ofrecen a los interesados soluciones administrativas y judiciales efectivas que les permiten, en particular, hacer valer sus derechos, en especial el derecho a acceder a sus datos personales o a obtener la rectificación o supresión de dichos datos.

(204) En primer lugar, de conformidad con el artículo 3, apartado 5, y el artículo 4, apartados 1, 3 y 4, de la LPIP, los particulares pueden ejercer sus derechos de acceso, rectificación, supresión y suspensión ante las autoridades nacionales de seguridad. La sección 6 de la Nota n.º 2021-5 (anexo I de la presente Decisión) aclara aún más cómo se aplican estos derechos en el contexto del tratamiento de datos con fines de seguridad nacional. En

([364]) Artículo 8, apartado 1, del Decreto de Ejecución de la Ley antiterrorista.
([365]) Artículo 9, apartado 1, del Decreto de Ejecución de la Ley antiterrorista. El OPDH decide de manera autónoma sobre la adopción de recomendaciones, pero debe informar de ellas al presidente de la Comisión de Lucha contra el Terrorismo.
([366]) Artículo 9, apartado 2, del Decreto de Ejecución de la Ley antiterrorista. Según la declaración oficial del Gobierno coreano, la no aplicación de una recomendación del OPDH se elevaría a la Comisión de Lucha contra el Terrorismo, incluido el primer ministro, aunque hasta ahora no se han registrado casos en los que no se hayan aplicado las recomendaciones del OPDH (véase el punto 3.3.1 del anexo II).
([367]) Anexo II, sección 3.3.4.
([368]) En concreto, con respecto al SNI, la CNDH ha llevado a cabo investigaciones de oficio y tramitado una serie de denuncias individuales. Véase, por ejemplo, el informe anual de 2018 de la CNDH, p. 128 (disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) y el informe anual de 2019 de la CNDH, p. 70 (disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Artículo 13, apartado 1, de la Ley SNI.
([370]) Artículos 36 y 37, apartado 1, punto 15, de la Ley de la Asamblea Nacional.
([371]) Artículo 15 de la LPPC.
([372]) Artículo 15, apartado 2, de la Ley SNI.
([373]) Artículo 17, apartado 2, de la Ley SNI. Los «secretos de Estado» se definen como hechos, bienes o conocimientos (clasificados) que no se divulgarán a ningún otro país u organización con el fin de evitar cualquier perjuicio grave para la seguridad nacional y a los que solo se permite un acceso limitado. Véase el artículo 13, apartado 4, de la Ley SNI.

particular, una autoridad nacional de seguridad solo puede limitar o denegar el ejercicio del derecho en la medida y durante el tiempo necesarios y proporcionados para proteger un objetivo importante de interés público (por ejemplo, en la medida y durante el tiempo que la concesión del derecho ponga en peligro una investigación en curso o amenace la seguridad nacional) o cuando la concesión del derecho pueda atentar contra la vida o la integridad física de un tercero. Por consiguiente, la invocación de tal restricción requiere encontrar un equilibrio entre los derechos e intereses del particular y el interés público pertinente y, en cualquier caso, no puede afectar al contenido esencial del derecho (artículo 37, apartado 2, de la Constitución). En caso de denegación o restricción de la solicitud, el particular debe ser informada sin demora de los motivos.

(205) En segundo lugar, las personas tienen derecho a obtener reparación en virtud de la LPIP si sus datos han sido tratados por una autoridad nacional de seguridad en violación de la LPIP o de las limitaciones y salvaguardias establecidas en otras leyes que regulan la recogida de datos personales (en particular, la LPPC, véase el considerando 171) ([374]). Este derecho puede ejercerse a través de una denuncia ante la CPIP (incluso a través del Centro de atención telefónica sobre privacidad gestionado por la Agencia de Internet y Seguridad de Corea) ([375]). Además, para facilitar el acceso a las vías de recurso contra las autoridades coreanas de seguridad, los ciudadanos de la UE pueden presentar una denuncia ante la CPIP a través de su autoridad nacional de protección de datos ([376]). En este caso, la CPIP lo notificará a la persona a través de la autoridad nacional de protección de datos una vez finalizada la investigación (incluida, en su caso, la información sobre las medidas correctoras impuestas). Sobre la base de la Ley de lo contencioso-administrativo, las personas también pueden recurrir o impugnar las decisiones o la inacción de la CPIP (véase el considerando 132).

(206) En tercer lugar, las personas pueden presentar una denuncia ante el OPDH por la vulneración de su derecho a la privacidad y a la protección de datos en el contexto de las actividades de lucha contra el terrorismo (es decir, de conformidad con la Ley antiterrorista) ([377]), que puede recomendar medidas correctoras. Dado que no existen requisitos de admisibilidad ante el OPDH, una denuncia se tramitará incluso si la persona afectada no puede demostrar que efectivamente ha sufrido daños (por ejemplo, debido a la supuesta recogida ilícita de sus datos por parte de una autoridad nacional de seguridad) ([378]). La autoridad pertinente debe informar al OPDH de cualquier medida adoptada para aplicar sus recomendaciones.

(207) En cuarto lugar, las personas pueden presentar una denuncia ante la CNDH en relación con la recogida de sus datos por parte de las autoridades nacionales de seguridad y obtener reparación de conformidad con el procedimiento descrito en el considerando (178) ([379]).

(208) Por último, hay diferentes recursos judiciales disponibles ([380]), que permiten a las personas invocar las limitaciones y salvaguardias descritas en la sección 3.3.1 para obtener reparación. En particular, los particulares pueden impugnar la legalidad de las acciones de las autoridades nacionales de seguridad sobre la base de la Ley de lo contencioso-administrativo (de conformidad con el procedimiento descrito en el considerando 181 o la Ley del Tribunal Constitucional, véase el considerando 182). Además, pueden obtener una indemnización por daños y perjuicios sobre la base de la Ley de indemnización estatal (como se describe con más detalle en el considerando 183).

4. **CONCLUSIÓN**

(209) La Comisión considera que la República de Corea —a través de la LPIP, las normas especiales aplicables a determinados sectores (como se analiza en el punto 2) y las salvaguardias adicionales previstas en la Nota n.º 2021-5 (anexo I)— garantiza un nivel de protección de los datos personales transferidos desde la Unión Europea sustancialmente equivalente al que garantiza el Reglamento (UE) 2016/679.

(210) Por otra parte, la Comisión estima que, en su conjunto, los mecanismos de supervisión y las vías de recurso previstos en el Derecho coreano permiten detectar y abordar en la práctica las infracciones de las normas de protección de datos cometidas por los responsables del tratamiento en Corea y ofrecen al interesado soluciones legales para obtener acceso a sus datos personales y, en su caso, su rectificación o supresión.

([374]) Artículo 58, apartado 4, y artículo 4, apartado 5, de la LPIP. Véase el punto 3.4.2 del anexo II.
([375]) Artículos 62 y 63, apartado 2, de la LPIP.
([376]) Nota n.º 2021-5 (sección 6, anexo I).
([377]) Artículo 8, apartado 1, punto 2, del Decreto de Ejecución de la Ley antiterrorista.
([378]) Véase la sección 3.4.1 del anexo II.
([379]) Por ejemplo, la CNDH recibe regularmente denuncias contra el Servicio Nacional de Inteligencia, véanse las cifras del informe anual de 2019 de la CNDH relativas al número de denuncias recibidas entre 2015 y 2019, p. 70 (disponible en https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Véase la sección 3.4.4 del anexo II.

(211) Por último, sobre la base de la información disponible acerca del ordenamiento jurídico de Corea, en particular las declaraciones, garantías y compromisos del Gobierno coreano que figuran en el anexo II, la Comisión considera que toda vulneración de interés público, en particular a efectos de control de la aplicación del Derecho penal y de seguridad nacional, por las autoridades públicas coreanas de los derechos fundamentales de los particulares cuyos datos personales sean transferidos desde la Unión Europea a la República de Corea se limitará a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva contra tales vulneraciones.

(212) Por consiguiente, a la luz de las conclusiones de la presente Decisión, debe decidirse que la República de Corea garantiza un nivel de protección adecuado en el sentido del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, para los datos personales transferidos desde la Unión Europea a la República de Corea a responsables del tratamiento de información personal en la República de Corea sujetos a la LPIP, con excepción de las organizaciones religiosas en la medida en que traten datos personales para sus actividades misioneras, los partidos políticos en la medida en que traten datos personales en el contexto de la designación de candidatos y los responsables del tratamiento que estén sujetos a la supervisión de la Comisión de Servicios Financieros para el tratamiento de información crediticia personal de conformidad con la Ley de información crediticia, en la medida en que traten dicha información.

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

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

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

(215) Cabe recordar que, de conformidad con el artículo 58, apartado 5, del Reglamento (UE) 2016/679 y como explicó el Tribunal de Justicia en la sentencia Maximillian Schrems ([381]), cuando una autoridad nacional de protección de datos cuestiona, en especial a raíz de una reclamación, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales de la persona a la privacidad y la protección de los datos, el Derecho nacional debe proporcionarle un recurso legal para presentar esas objeciones ante un tribunal nacional, al que podrá exigirse la presentación de una petición de decisión prejudicial al Tribunal de Justicia ([382]).

6. SEGUIMIENTO Y REVISIÓN DE LA PRESENTE DECISIÓN

(216) De conformidad con la jurisprudencia del Tribunal de Justicia ([383]), y tal como se reconoce en el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión debe supervisar de manera continuada los acontecimientos en el tercer país después de la adopción de una decisión de adecuación, para evaluar si el tercer país todavía garantiza un nivel de protección esencialmente equivalente. Debe procederse obligatoriamente a tal control, en cualquier caso, cuando la Comisión sea informada de algún indicio que genere una duda razonable al respecto.

(217) Por consiguiente, la Comisión debe supervisar de manera continuada la situación en la República de Corea 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 coreanas de las declaraciones, las garantías y los compromisos recogidos en el anexo II. Para facilitar este proceso, se invita a las autoridades coreanas a que informen sin demora a la Comisión de toda novedad pertinente para la presente Decisión, en lo que respecta al tratamiento de datos personales por parte de los operadores económicos y las autoridades públicas, así como a las limitaciones y salvaguardias aplicables al acceso de las autoridades públicas a los datos personales.

([381]) Maximillian Schrems contra Data Protection Commissioner, apartado 65.

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

([383]) Maximillian Schrems contra Data Protection Commissioner, apartado 76.

(218) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de supervisión, los Estados miembros deben informarle de cualquier medida pertinente adoptada por las autoridades nacionales de protección de datos, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la UE en relación con la transferencia de datos personales desde la Unión Europea a los responsables del tratamiento de la República de Corea. La Comisión también debe ser informada de todo indicio de que las acciones de las autoridades públicas coreanas 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.

(219) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679 ([384]), y teniendo en cuenta el hecho de que el nivel de protección que ofrece el ordenamiento jurídico coreano 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 la República de Corea siguen estando justificadas desde el punto de vista factual y legal.

(220) A tal fin, la presente Decisión debe someterse a una primera revisión en un plazo de tres 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, del Reglamento (UE) 2016/679, si debe mantenerse el ciclo de tres años. En cualquier caso, las revisiones posteriores deben realizarse al menos cada cuatro años ([385]). La revisión debe comprender todos los aspectos relativos al funcionamiento de la presente Decisión, y en particular la aplicación de las salvaguardias adicionales que figuran en el anexo I de la presente Decisión prestando especial atención a las protecciones ofrecidas en caso de transferencias ulteriores; los avances pertinentes en la jurisprudencia; las normas sobre el tratamiento de información seudonimizada con fines estadísticos, de investigación científica y de archivo en interés público, así como la aplicación de las excepciones previstas en el artículo 28, apartado 7, de la LPIP; la eficacia del ejercicio de los derechos individuales, también ante la recién reformada CPIP, y la aplicación de excepciones a tales derechos; la aplicación de las exenciones parciales en virtud de la LPIP; así como las limitaciones y salvaguardias con respecto al acceso de las autoridades públicas (según lo establecido en el anexo II de la presente Decisión), incluida la cooperación de la CPIP con las autoridades de protección de datos de la UE en relación con las reclamaciones de particulares. También debe abarcar la eficacia de la supervisión y la ejecución, en lo que respecta a la LPIP y en el ámbito de la aplicación del Derecho penal y la seguridad nacional (en particular, por la CPIP y la CNDH).

(221) Al proceder a la revisión, la Comisión debe reunirse con la CPIP, acompañada, en su caso, de otras autoridades coreanas 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. En el marco de la revisión, 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 salvaguardias relativas al acceso de las autoridades públicas ([386]). La Comisión también debe pedir explicaciones sobre cualquier información pertinente para la presente Decisión que haya recibido, en particular los informes públicos elaborados por las autoridades coreanas u otras partes interesadas en Corea, el Comité Europeo de Protección de Datos, las distintas autoridades de protección de datos, los grupos de la sociedad civil, los informes de los medios de comunicación o cualquier otra fuente de información disponible.

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

7. **SUSPENSIÓN, DEROGACIÓN O MODIFICACIÓN DE LA PRESENTE DECISIÓN**

(223) Cuando la información disponible, en particular la información resultante de la supervisión de la presente Decisión o proporcionada por las autoridades coreanas o de los Estados miembros, revele que el nivel de protección ofrecido por la República de Corea puede no ser el adecuado, la Comisión debe informar sin demora de ello a las autoridades coreanas competentes y solicitar que se tomen medidas adecuadas dentro de un plazo determinado y razonable.

(224) Si, al expirar dicho plazo determinado, las autoridades coreanas competentes no han adoptado dichas medidas o no han demostrado satisfactoriamente de otro modo que la presente Decisión sigue basándose en un nivel de protección adecuado, la Comisión iniciará el procedimiento a que se refiere el artículo 93, apartado 2, del Reglamento (UE) 2016/679 con el fin de suspender o derogar, total o parcialmente, esta Decisión.

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

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

([385]) 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 Comité Europeo de Protección de Datos, *Adequacy Referential*, WP 254 rev. 01.

([386]) Véase el anexo II de la presente Decisión.

(226) En particular, la Comisión debe iniciar el procedimiento de suspensión o derogación en caso de que existan indicios de que las salvaguardias adicionales 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 coreanas no cumplan las declaraciones, garantías y compromisos recogidos en el anexo II de la presente Decisión.

(227) 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 o de otra forma, las autoridades coreanas 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 la República de Corea o en relación con el cumplimiento de la presente Decisión. A este respecto, la Comisión debe tener en cuenta en qué medida puede obtenerse la información pertinente de otras fuentes.

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

8. **CONSIDERACIONES FINALES**

(229) El Comité Europeo de Protección de Datos publicó su dictamen ([387]), que se ha tomado en consideración en la elaboración de la presente Decisión.

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

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

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

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) las organizaciones religiosas en la medida en que traten datos personales para sus actividades misioneras;

b) los partidos políticos en la medida en que traten datos personales en el contexto del nombramiento de candidatos;

c) las entidades que estén sujetas a la supervisión de la Comisión de Servicios Financieros para el tratamiento de información crediticia personal de conformidad con la Ley de información crediticia, en la medida en que traten dicha información.

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 en relación con las transferencias de datos que pertenecen al ámbito de aplicación establecido en el artículo 1 de la presente Decisión, el Estado miembro en cuestión informará sin demora a la Comisión.

Artículo 3

1. La Comisión realizará un seguimiento continuo de la aplicación del marco jurídico en el que se basa la presente Decisión, incluidas las condiciones en que se realizan las transferencias ulteriores, se ejercen los derechos individuales y las autoridades públicas coreanas tienen acceso a los datos transferidos sobre la base de la presente Decisión, a fin de evaluar si la República de Corea sigue garantizando un nivel adecuado de protección a tenor del artículo 1.

([387]) Dictamen 32/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con el Reglamento (UE) 2016/679 sobre el nivel de protección adecuado de los datos personales en la República de Corea, disponible en el siguiente enlace: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

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 coreana competente, no garantice el cumplimiento del marco jurídico en el que se sustenta la presente Decisión.

3. Los Estados miembros y la Comisión se informarán recíprocamente de cualquier indicio de que las injerencias de las autoridades públicas coreanas 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. Tres años después de la fecha de notificación de la presente Decisión a los Estados miembros y posteriormente al menos cada cuatro años, la Comisión evaluará la constatación mencionada en el artículo 1, apartado 1, sobre la base de toda la información disponible, incluida la información recibida como parte de la revisión realizada junto con las autoridades coreanas 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 coreanas competentes. Si es necesario, podrá decidir suspender, modificar o derogar la presente Decisión, o limitar su ámbito de aplicación, de conformidad con el artículo 45, apartado 5, del Reglamento (UE) 2016/679, en particular si existen indicios de que:

a) los responsables del tratamiento en Corea que hayan recibido datos personales de la Unión Europea en virtud de la presente Decisión no cumplen las salvaguardias adicionales que figuran en el anexo I, o de que son insuficientes la supervisión y el control de la aplicación de la legislación en este sentido;

b) las autoridades públicas coreanas no cumplen las declaraciones, garantías y compromisos recogidos en el anexo II, 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 coreanas a efectos de control de la aplicación del Derecho penal o de seguridad nacional.

La Comisión podrá asimismo adoptar tales medidas cuando la falta de cooperación del Gobierno coreano le impida determinar si la República de Corea sigue garantizando un nivel adecuado de protección.

Artículo 4

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 17 de diciembre de 2021.

Por la Comisión
Didier REYNDERS
Miembro de la Comisión

ANEXO I

NORMAS COMPLEMENTARIAS PARA LA INTERPRETACIÓN Y LA APLICACIÓN DE LA LEY SOBRE LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL EN RELACIÓN CON EL TRATAMIENTO DE LOS DATOS PERSONALES TRANSFERIDOS A COREA

Índice

I. **Resumen**

Corea y la Unión Europea (en lo sucesivo, «la UE») han celebrado debates sobre la adecuación, como consecuencia de los cuales la Comisión Europea determinó que Corea garantiza un nivel adecuado de protección de los datos personales con arreglo al artículo 45 del RGPD.

En este contexto, la Comisión de Protección de la Información Personal adoptó la presente Nota sobre la base del artículo 5 (Obligaciones del Estado, etc.) y del artículo 14 (Cooperación internacional) ([1]) de la Ley sobre la protección de la información personal para aclarar la interpretación, la aplicación y la ejecución de determinadas disposiciones de la Ley, en particular en lo que se refiere al tratamiento de los datos personales transferidos a Corea sobre la base de la decisión de adecuación de la UE.

Dado que la presente Nota tiene estatuto de norma administrativa que el organismo administrativo competente establece y anuncia para aclarar las normas para la interpretación, la aplicación y la ejecución de la Ley sobre la protección de la información personal en el sistema jurídico de Corea, tiene fuerza jurídica vinculante para el responsable del tratamiento de la información personal, en el sentido de que cualquier infracción de la presente Nota puede considerarse una infracción de las disposiciones pertinentes de la LPIP. Además, si se vulneran los derechos e intereses personales debido a una violación de la presente Nota, los particulares afectados tienen derecho a obtener reparación de la Comisión de Protección de la Información Personal o de un tribunal.

En consecuencia, si el responsable del tratamiento que trata la información personal transferida a Corea de conformidad con la decisión de adecuación de la UE no adopta medidas conformes a la presente Nota, se considerará «que existe una razón fundada para considerar que se ha producido una infracción con respecto a la información personal y que es probable que la falta de adopción de medidas cause daños difíciles de reparar», de conformidad con el artículo 64, apartados 1 y 2, de la Ley. En tales casos, la Comisión de Protección de la Información Personal o los organismos

([1]) El artículo 14 de la Ley sobre la protección de la información personal estipula la autoridad del Gobierno coreano para establecer políticas destinadas a mejorar el nivel de protección de la información personal en el entorno internacional y prevenir la vulneración de los derechos de los interesados como consecuencia de la transferencia transfronteriza de información personal.

administrativos centrales correspondientes podrán ordenar al responsable del tratamiento de datos personales que adopte medidas correctoras, etc., de acuerdo con la autoridad otorgada por la presente disposición, y, en función de las infracciones específicas de la ley, también podrá imponerse la pena correspondiente (sanciones, multas administrativas, etc.).

II. **Definición de términos**

Las definiciones de los términos utilizados en la presente disposición son las siguientes:

i) Ley: Ley sobre la protección de la información personal (Ley n.º 16930, modificada el 4 de febrero de 2020 y ejecutada el 5 de agosto de 2020).

ii) Decreto presidencial: Decreto de Ejecución de la Ley sobre la protección de la información personal (Decreto presidencial n.º 30509, de 3 de marzo de 2020, por el que se modifican otras leyes).

iii) Interesado: persona identificable a través de la información tratada para convertirse en objeto de dicha información.

iv) Responsable del tratamiento de información personal: institución pública, persona jurídica, organización, particular, etc. que trata información personal directa o indirectamente como parte de sus actividades.

v) UE: UE (a finales de febrero de 2020, veintisiete países miembros [2], a saber, Bélgica, Alemania, Francia, Italia, Luxemburgo, Países Bajos, Dinamarca, Irlanda, Grecia, Portugal, España, Austria, Finlandia, Suecia, Chipre, República Checa, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, Eslovaquia, Eslovenia, Rumanía, Bulgaria y Croacia), así como los países asociados a la UE a través del Acuerdo EEE (Islandia, Liechtenstein, Noruega).

vi) RGPD: legislación general de la UE en materia de protección de la información personal, Reglamento General de Protección de Datos [Reglamento (UE) 2016/679].

vii) Decisión de adecuación: de conformidad con el artículo 45, apartado 3, del RGPD, la Comisión Europea decidió que un tercer país, el territorio de un tercer país, una o varias zonas o una organización internacional garantizan un nivel adecuado de protección de la información personal.

III. **Normas complementarias**

1. **Limitación de la utilización y el suministro de información personal fuera de la finalidad (artículos 3, 15 y 18 de la Ley)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Artículo 3 (Principios para la protección de la información personal) 1) El responsable del tratamiento de información personal especificará explícitamente los fines para los que se trata la información personal y recogerá dicha información de manera lícita y leal, limitándose a lo estrictamente necesario para tales fines.

2) El responsable del tratamiento de la información personal tratará dicha información de manera adecuada atendiendo a los fines para los que se realiza el tratamiento y no utilizará la información con otros fines.

Artículo 15 (Recogida y utilización de la información personal) 1) Un responsable del tratamiento de información personal podrá recoger información personal en cualquiera de las siguientes circunstancias y utilizarla dentro del alcance de la finalidad de la recogida:

1. cuando se obtenga el consentimiento de un interesado;
2. cuando existan disposiciones especiales en la legislación o sea inevitable para cumplir las obligaciones legales;
3. cuando sea inevitable para que una institución pública ejerza las funciones de su competencia, según lo previsto en la legislación, etc.;
4. cuando resulte inevitablemente necesario para ejecutar y cumplir un contrato con un interesado;

[2] Hasta el final del período de transición, esto incluye también al Reino Unido, según lo dispuesto en los artículos 126, 127 y 132 del Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica (2019/C 384 I/01).

5. cuando se considere manifiestamente necesario para la protección de la vida, los intereses corporales o patrimoniales del interesado o de un tercero frente a un peligro inminente, cuando el interesado o su representante legal no estén en condiciones de manifestar su intención o no pueda obtenerse el consentimiento previo debido a direcciones desconocidas, etc.;

6. cuando sea necesario para alcanzar el interés justificable de un responsable del tratamiento de información personal, cuando dicho interés sea manifiestamente superior a los derechos del interesado. En tales casos, el tratamiento solo se permitirá en la medida en que esté sustancialmente relacionado con el interés justificable del responsable del tratamiento de información personal y no vaya más allá de un alcance razonable.

Artículo 18 (Limitación de la utilización y el suministro de información personal fuera de la finalidad) 1) El responsable del tratamiento de información personal no podrá utilizar la información personal más allá del alcance previsto en el artículo 15, apartado 1, y el artículo 39-3, apartados 1 y 2, ni facilitarla a terceros más allá del alcance previsto en el artículo 17, apartados 1 y 3.

2) No obstante lo dispuesto en el apartado 1, cuando sea de aplicación cualquiera de los siguientes párrafos, el responsable del tratamiento de información personal podrá utilizar dicha información o facilitarla a un tercero para otros fines, salvo que ello pueda vulnerar deslealmente los intereses de un interesado o de un tercero: siempre que los proveedores de servicios de información y comunicaciones (según lo dispuesto en el artículo 2, apartado 1, punto 3, de la Ley de promoción de la utilización de redes de información y comunicaciones y la protección de la información, etc.; en lo sucesivo, se aplicará lo mismo) que tratan la información personal de los usuarios (tal como se establece en el artículo 2, apartado 1, punto 4, de la Ley de promoción de la utilización de redes de información y comunicaciones y la protección de la información, etc.; en lo sucesivo, se aplicará lo mismo) solo estén sujetos a lo dispuesto en los puntos 1 y 2, y los puntos 5 a 9 solo se apliquen a las instituciones públicas:

1. cuando se obtenga el consentimiento adicional del interesado;

2. cuando existan otras disposiciones especiales en la legislación;

3. cuando se considere manifiestamente necesario para la protección de la vida, los intereses corporales o patrimoniales del interesado o de un tercero frente a un peligro inminente, cuando el interesado o su representante legal no estén en condiciones de manifestar su intención o no pueda obtenerse el consentimiento previo debido a direcciones desconocidas;

4. Suprimido; <por la Ley n.º 16930, de 4 de febrero de 2020>

5. cuando resulte imposible desempeñar las funciones de su competencia según lo dispuesto en cualquier ley, salvo que el responsable del tratamiento de información personal utilice dicha información para un fin distinto del previsto o la facilite a un tercero y esté sujeto a la deliberación y resolución de la Comisión;

6. cuando sea necesario facilitar información personal a un Gobierno extranjero o a una organización internacional para cumplir un tratado u otra convención internacional;

7. cuando sea necesario para la investigación de un delito, la acusación y el enjuiciamiento;

8. cuando sea necesario para que un órgano jurisdiccional lleve a cabo funciones relacionadas con un juicio;

9. cuando sea necesario para la ejecución de la pena, la libertad vigilada y la detención.

Se suprimen los apartados 3 y 4.

5) Cuando un responsable del tratamiento de información personal facilite este tipo de información a un tercero para fines distintos de los previstos en el apartado 2, el responsable del tratamiento de información personal solicitará al destinatario de dicha información que limite la finalidad y el método de utilización y otros aspectos necesarios o que prepare las salvaguardias necesarias para garantizar la seguridad de la información personal. En tales casos, la persona que reciba dicha solicitud deberá adoptar las medidas necesarias para garantizar la seguridad de la información personal.

i) El artículo 3, apartados 1 y 2, de la Ley establece el principio de que el responsable del tratamiento solo debe recoger la información personal mínima necesaria para cumplir la finalidad del tratamiento de manera lícita y legítima, y no debe utilizarla para fines distintos del previsto ([3]).

ii) Con arreglo a este principio, el artículo 15, apartado 1, de la Ley establece que, cuando un responsable del tratamiento recoja información personal, esta información podrá utilizarse en el marco de la finalidad de la recogida, y el artículo 18, apartado 1, estipula que la información personal no debe utilizarse más allá de la finalidad de la recogida ni facilitarse a terceros.

([3]) Dado que estas disposiciones establecen principios generales que se aplican a todo tratamiento de información personal, incluso cuando dicho tratamiento está regulado específicamente por otras leyes, las aclaraciones de la presente sección también se aplican cuando los datos personales se tratan sobre la base de otras leyes (véase, por ejemplo, el artículo 15, apartado 1, de la Ley de información crediticia, que hace referencia específica a estas disposiciones).

iii) Asimismo, aunque la información personal pueda utilizarse para fines distintos del previsto o facilitarse a un tercero en los casos excepcionales ([4]) descritos en el artículo 18, apartado 2, de la Ley, deberá solicitarse que se restrinja la finalidad o el método de utilización para que la información personal pueda tratarse de forma segura de conformidad con el apartado 5, o que se adopten las medidas necesarias para garantizar la seguridad de la información personal.

iv) Las disposiciones anteriores se aplicarán por igual al tratamiento de toda la información personal recibida de un tercer país dentro de la jurisdicción de la zona de Corea, con independencia de la nacionalidad del interesado.

v) Por ejemplo, si un responsable del tratamiento de información personal en la UE transfiere información personal a un responsable del tratamiento coreano con arreglo a la decisión de adecuación de la Comisión Europea, la finalidad del responsable del tratamiento de la UE de transferir la información personal se considerará como la finalidad del responsable del tratamiento coreano de recoger la información personal y, en tales casos, el responsable del tratamiento coreano solo podrá utilizar la información personal o facilitarla a un tercero en el marco de la finalidad de la recogida, salvo en los casos excepcionales descritos en el artículo 18, apartado 2, de la Ley.

2. **Limitación de las transferencias ulteriores de los datos personales (artículo 17, apartados 3 y 4, y artículo 18 de la Ley)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Artículo 17 (Suministro de información personal) 1) Se omite.

2) El responsable del tratamiento de datos personales informará al interesado de los siguientes aspectos cuando obtenga el consentimiento con arreglo al apartado 1, punto 1. Lo mismo se aplicará cuando se modifique cualquiera de los siguientes elementos:

1. el destinatario de la información personal;
2. la finalidad para la que el destinatario de la información personal utiliza dicha información;
3. los detalles de la información personal que debe facilitarse;
4. el período durante el cual el destinatario conserva y utiliza la información personal;
5. el hecho de que el interesado tiene derecho a denegar el consentimiento y, en su caso, los inconvenientes derivados de dicha denegación.

3) El responsable del tratamiento de información personal informará al interesado de las cuestiones contempladas en el apartado 2 y obtendrá el consentimiento del interesado para facilitar la información personal a un tercero en el extranjero; y no celebrará ningún contrato para la transferencia transfronteriza de información personal que infrinja la presente Ley.

4) El responsable del tratamiento podrá facilitar información personal sin el consentimiento de un interesado dentro del alcance razonablemente relacionado con los fines para los que se recogió inicialmente la información personal, de conformidad con lo dispuesto mediante Decreto presidencial, teniendo en cuenta si se han causado inconvenientes al interesado, si se han adoptado las medidas necesarias para garantizar la seguridad, tales como el cifrado, etc.

※ Véanse las páginas 3, 4 y 5 para consultar el artículo 18.

< **Decreto de Ejecución de la Ley sobre la protección de la información personal**

[(Fecha de ejecución: 5 de febrero de 2021) (Decreto presidencial n.º 30892, de 4 de agosto de 2020, por el que se modifican otras leyes)]>

Artículo 14-2 (Normas sobre la utilización o el suministro adicional de información personal, etc.)

1) Si el responsable del tratamiento utiliza o facilita información personal (en lo sucesivo, «utilización o suministro adicional de información personal») sin el consentimiento del interesado de conformidad con el artículo 15, apartado 3, de la Ley o con el artículo 17, apartado 4, de la Ley, el responsable del tratamiento de información personal considerará los siguientes aspectos:

1. si la utilización o el suministro está razonablemente relacionado con la finalidad original para la que se recogió la información personal;
2. si la utilización uso o el suministro adicional de información personal es previsible a la luz de las circunstancias en las que se recogió la información personal y de las prácticas de tratamiento;
3. si la utilización o el suministro adicional de información personal no vulnera deslealmente los intereses del interesado; y
4. si se han adoptado las medidas necesarias para garantizar la seguridad, tales como la seudonimización o el cifrado.

([4]) Los proveedores de servicios de comunicación de información solo están sujetos a lo dispuesto en el artículo 18, apartado 2, puntos 1 y 2. Los puntos 5 a 9 solo se aplican a las instituciones públicas.

2) El responsable del tratamiento de información personal revelará de antemano los criterios para evaluar las cuestiones a que se refiere el apartado 1 en la política de privacidad, con arreglo al artículo 30, apartado 1, de la Ley, y el responsable de la protección de la privacidad, con arreglo al artículo 31, apartado 1, de la Ley, comprobará si el responsable del tratamiento de información personal utiliza o facilita información personal adicional con arreglo a las normas pertinentes.

i) Si el responsable del tratamiento facilita información personal a un tercero en el extranjero, deberá informar de antemano a los interesados de todas las cuestiones descritas en el artículo 17, apartado 2, de la Ley y obtener su consentimiento, salvo en los casos contemplados en los apartados 1 y 2. No debe celebrarse ningún contrato relacionado con el suministro transfronterizo de datos personales que infrinja la presente Ley.

1) Si se facilita información personal dentro del alcance razonablemente relacionado con la finalidad inicial de la recogida con arreglo al artículo 17, apartado 4, de la Ley. Sin embargo, los casos en los que puede aplicarse esta disposición se limitan a aquellos en los que se cumplen las normas sobre la utilización y el suministro adicionales de información personal, establecidas en el artículo 14-2 del Decreto de Ejecución. Además, el responsable del tratamiento deberá considerar si el suministro de información personal puede causar inconvenientes a los interesados y si ha adoptado las medidas necesarias para garantizar la seguridad, tales como el cifrado.

2) Si puede facilitarse información personal a un tercero en los casos excepcionales mencionados en el artículo 18, apartado 2, de la Ley (véanse las páginas 3 a 5). Sin embargo, incluso en tales casos, si es probable que el suministro de dicha información personal vulnere deslealmente los intereses del interesado o de un tercero, la información personal no podrá facilitarse a un tercero. Además, el proveedor de la información personal deberá solicitar al destinatario que limite la finalidad o el método de utilización de la información personal o que adopte las medidas necesarias para garantizar su seguridad, de modo que la información personal pueda tratarse de forma segura.

ii) Si se facilita información personal a un tercero en el extranjero, esta podría no recibir el nivel de protección garantizado por la Ley sobre la protección de la información personal de Corea debido a las diferencias en los sistemas de protección de la información personal de distintos países. Por consiguiente, estos casos se considerarán «casos en los que podrían causarse inconvenientes al interesado», mencionados en el artículo 17, apartado 4, de la Ley, o «casos en que se vulnera deslealmente el interés de un interesado o de un tercero», mencionados en el artículo 18, apartado 2, de la Ley y en el artículo 14-2 del Decreto de Ejecución de la misma Ley ([5]). Por tanto, para cumplir los requisitos de estas disposiciones, el responsable del tratamiento de información personal y el tercero deberán garantizar explícitamente un nivel de protección equivalente al ofrecido por la Ley, en particular la garantía de que el interesado pueda ejercer sus derechos en documentos jurídicamente vinculantes, como los contratos, incluso después de la transferencia de información personal al extranjero.

3. **Notificación de los datos en caso de que los datos personales no se hayan obtenido del interesado (artículo 20 de la Ley)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Artículo 20 (Notificación de las fuentes, etc. de la información personal recogida de terceros) 1) Cuando un responsable del tratamiento trate información personal recogida de terceros, el responsable del tratamiento de información personal notificará inmediatamente al interesado, a petición de este último, los siguientes aspectos:

1. la fuente de la información personal recogida;

2. la finalidad del tratamiento de la información personal;

3. el hecho de que el interesado tiene derecho a solicitar la suspensión del tratamiento de la información personal, tal como se establece en el artículo 37.

2) No obstante lo dispuesto en el apartado 1, cuando un responsable del tratamiento de información personal que cumpla los criterios establecidos mediante Decreto presidencial, teniendo en cuenta los tipos y la cantidad de información personal tratada, el número de empleados, el volumen de ventas, etc., recoja información personal de terceros y la trate con arreglo al artículo 17, apartado 1, punto 1, el responsable del tratamiento notificará al interesado los aspectos mencionados en el apartado 1: esto no se aplicará cuando la información recogida por el responsable del tratamiento no contenga información personal, como datos de contacto, a través de la cual pueda notificarse al interesado.

([5]) De conformidad con el artículo 18, apartado 2, punto 2, de la LPIP, esto también se aplica cuando se divulga información personal a terceros en el extranjero sobre la base de las disposiciones de otras leyes (por ejemplo, la Ley de información crediticia).

3) Los aspectos necesarios en relación con el momento, el método y el procedimiento de notificación al interesado con arreglo a la frase principal del apartado 2 se establecerán mediante Decreto presidencial.

4) El apartado 1 y la cláusula principal del apartado 2 no se aplicarán a ninguna de las circunstancias siguientes: este será el caso únicamente cuando sea manifiestamente superior a los derechos de los interesados en virtud de la presente Ley:

1. cuando la información personal que sea objeto de una solicitud de notificación esté contenida en los ficheros de información personal a que se refiere cualquiera de los puntos del artículo 32, apartado 2;

2. cuando dicha notificación pueda atentar contra la vida o la integridad física de un tercero o vulnere deslealmente los intereses patrimoniales y otros intereses de un tercero.

i) Si el responsable del tratamiento recibe la información personal transferida desde la UE sobre la base de la decisión de adecuación de esta última ([6]), deberá notificar al interesado la siguiente información mencionada en los puntos 1 a 5, sin demora injustificada y, en cualquier caso, a más tardar un mes después de la transferencia.

1) El nombre y los datos de contacto de las personas que transfieren y reciben la información personal.

2) Los elementos o las categorías de la información personal transferida.

3) La finalidad de la recogida y la utilización de la información personal (según lo establecido por el exportador de los datos con arreglo al punto 1 de la presente Nota).

4) El período de conservación de la información personal.

5) La información sobre los derechos del interesado en relación con el tratamiento de la información personal, el método y el procedimiento para ejercer los derechos, así como cualquier inconveniente causado por el ejercicio de los mismos, si procede.

ii) Asimismo, si el responsable del tratamiento facilita la información personal mencionada en i) a un tercero en la República de Corea o en el extranjero, deberá notificar la información mencionada en los puntos 1 a 5 al interesado antes de facilitar la información personal.

1) El nombre y los datos de contacto de las personas que facilitan y reciben la información personal.

2) Los elementos o las categorías de la información personal facilitada.

3) El país al que se facilitará la información personal, la fecha prevista y el método para facilitarla (limitado a los casos en que la información personal se facilite a un tercero en el extranjero).

4) La finalidad del proveedor de información personal y la base jurídica para facilitar dicha información.

5) La información sobre los derechos del interesado en relación con el tratamiento de información personal, el método y el procedimiento para ejercer los derechos, así como cualquier inconveniente causado por el ejercicio de los mismos, si procede.

iii) El responsable del tratamiento de información personal no podrá aplicar lo indicado en los incisos i) y ii) en ninguno de los siguientes casos mencionados en los puntos 1 a 4.

1) Si la información personal que debe notificarse está incluida en alguno de los ficheros de información personal mencionados en el artículo 32, apartado 2, de la Ley, en la medida en que los intereses protegidos por esta disposición sean manifiestamente superiores a los derechos del interesado, y siempre y cuando la notificación ponga en peligro la defensa de los intereses en juego, por ejemplo, poniendo en peligro investigaciones penales en curso o amenazando la seguridad nacional.

2) Siempre que la notificación pueda atentar contra la vida o la integridad física de un tercero o vulnerar deslealmente los intereses patrimoniales de un tercero, en el caso de que dichos derechos o intereses sean manifiestamente superiores a los derechos del interesado.

3) Si el interesado ya posee la información que el responsable del tratamiento de información personal debe notificar con arreglo a los incisos i) y ii).

4) Si el responsable del tratamiento de información personal no dispone de datos de contacto del interesado o ponerse en contacto con el interesado supone un esfuerzo excesivo, incluso en el contexto del tratamiento en las condiciones establecidas en la sección 3 de la LPIP. A la hora de determinar si es posible o no ponerse en contacto con el interesado o si ello supone un esfuerzo excesivo, debe tenerse en cuenta la posibilidad de cooperar con el exportador de datos en la UE.

([6]) Las obligaciones establecidas en los incisos i), ii) y iii) también se aplican cuando el responsable del tratamiento que recibe información personal de la UE sobre la base de la decisión de adecuación trata dicha información con arreglo otras leyes, como, por ejemplo, la Ley de información crediticia.

4. **Ámbito de aplicación de la exención especial del tratamiento de información seudonimizada (artículos 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, 3 y 58-2 de la Ley)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Capítulo III Tratamiento de la información personal

SECCIÓN 3 Casos especiales relativos a los datos seudonimizados

Artículo 28-2 (Tratamiento de datos seudonimizados) 1) El responsable del tratamiento de información personal podrá tratar información seudonimizada sin el consentimiento de los interesados con fines estadísticos, de investigación científica y de archivo en interés público, etc.

2) El responsable del tratamiento de información personal no incluirá información que pueda utilizarse para identificar a un particular determinado cuando proporcione información seudonimizada a un tercero de conformidad con el apartado 1.

Artículo 28-3 (Restricción de la combinación de datos seudonimizados) 1) No obstante lo dispuesto en el artículo 28-2, la combinación de información seudonimizada tratada por diferentes responsables del tratamiento de información personal con fines estadísticos, de investigación científica y de conservación de registros de interés público, etc. será realizada por una institución especializada designada por la Comisión de Protección o el jefe del organismo administrativo central correspondiente.

2) El responsable del tratamiento de información personal que tenga la intención de divulgar la información combinada fuera de la organización que combinó la información deberá obtener la autorización del jefe de la institución especializada después de tratar la información para producir información seudonimizada o en la manera a que hace referencia el artículo 58-2.

3) Los aspectos necesarios, en particular los procedimientos y métodos de combinación de conformidad con el apartado 1, las normas y los procedimientos para designar o anular la designación de la gestión y supervisión de una institución especializada, así como las normas y los procedimientos de exportación y autorización con arreglo al apartado 2, se establecerán mediante Decreto presidencial.

Artículo 28-4 (Obligación de adoptar medidas de seguridad para los datos seudonimizados) 1) A la hora de tratar información seudonimizada, el responsable del tratamiento de información personal adoptará medidas técnicas, organizativas y físicas, como almacenar y gestionar por separado la información adicional necesaria para la restitución al estado original, según sea necesario para garantizar la seguridad, de conformidad con lo dispuesto mediante Decreto presidencial, de modo que la información personal no pueda extraviarse, robarse, divulgarse, falsificarse, modificarse o dañarse.

2) El responsable del tratamiento de información personal que tenga la intención de tratar la información seudonimizada elaborará y mantendrá registros relativos a los aspectos establecidos por el Decreto Presidencial, en particular la finalidad del tratamiento de la información seudonimizada y un tercero destinatario cuando se facilite información seudonimizada, a fin de gestionar el tratamiento de la información seudonimizada.

Artículo 28-5 (Actos prohibidos en relación con el tratamiento de información seudonimizada) 1) Ninguna persona tratará la información seudonimizada con el fin de identificar a una particular determinado.

2) Cuando se genere información que permita identificar a un particular determinado durante el tratamiento de la información seudonimizada, el responsable del tratamiento de información personal interrumpirá el tratamiento de la información y recuperará y destruirá de inmediato la información.

Artículo 28-6 (Imposición de recargos administrativos por el tratamiento de información seudonimizada) 1) La Comisión podrá imponer una multa equivalente a menos de tres centésimas de las ventas totales a los responsables del tratamiento que hayan tratado datos con el fin de identificar a un particular concreto en violación del artículo 28-5, apartado 1: en caso de que no haya ventas o haya dificultades para calcular los ingresos por ventas, el responsable del tratamiento podrá ser sancionado con una multa de un máximo de 400 millones de won o de tres centésimas del importe del capital, si esta cifra es superior.

2) El artículo 34-2, apartados 3 a 5, se aplicará *mutatis mutandis* a los aspectos necesarios para imponer y recaudar recargos administrativos.

Artículo 28-7 (Ámbito de aplicación) Los artículos 20, 21, 27, 34, apartado 1, 35 a 37, 39-3, 39-4 y 39-6 a 39-8 no se aplicarán a la información seudonimizada.

Capítulo I Disposiciones generales

Artículo 3 (Principios para la protección de la información personal) 1) El responsable del tratamiento de información personal especificará explícitamente los fines para los que se trata la información personal y recogerá dicha información de manera lícita y leal, limitándose a lo estrictamente necesario para tales fines.

2) El responsable del tratamiento de la información personal tratará dicha información de manera adecuada atendiendo a los fines para los que se realiza el tratamiento y no utilizará la información con otros fines.

3) El responsable del tratamiento garantizará que la información personal sea exacta y completa y esté actualizada en la medida necesaria en relación con los fines para los que se trata dicha información.

4) El responsable del tratamiento gestionará la información personal de manera segura según los métodos de tratamiento, tipos, etc. de información personal, teniendo en cuenta la posibilidad de que se vulneren los derechos del interesado y la gravedad de los riesgos pertinentes.

5) El responsable del tratamiento de información personal deberá hacer pública su política de privacidad y otras cuestiones relacionadas con el tratamiento de información personal y garantizará los derechos del interesado, como el derecho de acceso a su información personal.

6) El responsable del tratamiento tratará la información personal de manera que se reduzca al mínimo la posibilidad de que se vulnere la privacidad del interesado.

7) Siempre que el tratamiento de información anonimizada o seudonimizada permita cumplir la finalidad de la recogida de información personal, el responsable del tratamiento procurará tratar la información personal mediante anonimización, cuando sea posible, o seudonimización, si la anonimización no permite cumplir la finalidad de la recogida de información personal.

8) El responsable del tratamiento de información personal procurará obtener la confianza de los interesados mediante la observación y el desempeño de las funciones y responsabilidades previstas en la presente Ley y en otras leyes conexas.

Capítulo IX Disposiciones complementarias

Artículo 58-2 (Exención de la aplicación) La presente Ley no se aplicará a la información que ya no permita identificar a un particular determinado cuando se combine con otra información, teniendo razonablemente en cuenta el tiempo, el coste, la tecnología, etc. <Este artículo fue introducido recientemente por la Ley n.º 16930, de 4 de febrero de 2020>

i) El capítulo III, sección 3 Casos especiales relativos a los datos seudonimizados (artículos 28-2 a 28-7), permite el tratamiento de información seudonimizada sin el consentimiento del interesado con fines de elaboración de estadísticas, de investigación científica, de conservación de registros públicos, etc. (artículo 28-2), pero, en tales casos, son obligatorias las salvaguardias y prohibiciones adecuadas necesarias para proteger los derechos de los interesados (artículos 28-4 y 28-5); podrán imponerse recargos a los infractores (artículo 28-6) y no se aplicarán determinadas salvaguardias disponibles de otro modo en virtud de la LPIP (artículo 28-7).

ii) Estas disposiciones no se aplicarán a los casos en que la información seudonimizada se trate con fines distintos de la elaboración de estadísticas, la investigación científica, la conservación de registros públicos, etc. Por ejemplo, si la información personal de un ciudadano de la UE, transferida a Corea de conformidad con la decisión de adecuación de la Comisión Europea, se seudonimiza para fines distintos de la elaboración de estadísticas, la investigación científica, la conservación de registros públicos, etc., no se aplicarán las disposiciones especiales del capítulo III, sección 3 ([7]).

iii) Cuando un responsable del tratamiento de información personal trate información seudonimizada con fines de elaboración de estadísticas, investigación científica, conservación de registros públicos, etc. y la información seudonimizada no haya sido destruida una vez que se haya cumplido la finalidad específica del tratamiento de conformidad con el artículo 37 de la Constitución y el artículo 3 (Principios para la protección de la información personal) de la Ley, anonimizará la información con el fin de garantizar que deje de permitir la identificación de un particular concreto, por sí sola o combinada con otra información, teniendo en cuenta razonablemente el tiempo, el coste, la tecnología, etc. con arreglo al artículo 58-2 de la LPIP.

5. **Medidas correctoras, etc. (artículo 64, apartados 1, 2 y 4, de la Ley)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Artículo 64 (Medidas correctoras) 1) Cuando la Comisión de Protección considere que existe una razón fundada para considerar que se ha producido una infracción con respecto a la información personal y que es probable que la falta de adopción de medidas cause daños difíciles de reparar podrá ordenar al infractor de esta Ley (salvo los organismos administrativos centrales, los Gobiernos locales, la Asamblea Nacional, el Tribunal Constitucional y la Comisión Nacional Electoral) que adopte cualquiera de las siguientes medidas:

1. suspender la infracción con respecto a la información personal;

2. suspender temporalmente el tratamiento de información personal;

([7]) Del mismo modo, la excepción del artículo 40-3 de la Ley de información crediticia solo se aplica al tratamiento de información crediticia seudonimizada con fines de elaboración de estadísticas, investigación científica y conservación de registros públicos.

3. otras medidas necesarias para proteger la información personal y prevenir la violación de la seguridad de dicha información.

2) Cuando el jefe de un organismo administrativo central competente considere que existe una razón fundada para considerar que se ha producido una infracción con respecto a la información personal y que es probable que la falta de adopción de medidas cause daños difíciles de reparar podrá ordenar a un responsable del tratamiento de información personal que adopte cualquiera de las medidas previstas en el apartado 1 con arreglo a las leyes dentro de la jurisdicción de dicho organismo administrativo central.

4) Cuando un organismo administrativo central, un Gobierno local, la Asamblea Nacional, el Tribunal Constitucional o la Comisión Nacional Electoral infrinjan la presente Ley, la Comisión de Protección podrá recomendar al jefe del organismo correspondiente que adopte cualquiera de las medidas previstas en el apartado 1. En tales casos, al recibir la recomendación, el organismo deberá cumplirla, salvo que ocurran circunstancias extraordinarias.

i) En primer lugar, la jurisprudencia ([8]) ([9]) interpreta el concepto de «daños difíciles de reparar» como un caso en el que se podrían ver perjudicados los derechos personales o la privacidad de una persona.

ii) Por consiguiente, «una razón fundada para considerar que se ha producido una infracción con respecto a la información personal y que es probable que la falta de adopción de medidas cause daños difíciles de reparar», como se establece en el artículo 64, apartados 1 y 2, se refiere a los casos en los que se considera que una infracción de la ley puede vulnerar los derechos y libertades de los particulares en materia de información personal. Esto será aplicable siempre que se vulnere cualquiera de los principios, derechos y obligaciones contemplados en la Ley sobre la protección de la información personal ([10]).

iii) De conformidad con el artículo 64, apartado 4, de la Ley sobre la protección de la información personal, se trata de una medida relativa a «una infracción de la presente Ley», es decir, una acción contra una infracción de la LPIP.

Un organismo administrativo central, etc., en calidad de autoridad pública vinculada al Estado de Derecho, no puede infringir ninguna ley y está obligado a adoptar una medida correctora, incluida la suspensión inmediata de la acción, y a indemnizar por daños y perjuicios en el caso excepcional de que, a pesar de todo, se haya cometido un acto ilícito.

En consecuencia, incluso sin la intervención de la Comisión de Protección, de conformidad con el artículo 64, apartado 4, de la LPIP, un organismo administrativo central, etc., debe adoptar una medida correctora contra las infracciones si tiene conocimiento de alguna infracción de la ley.

En particular, cuando la Comisión de Protección haya recomendado una medida correctora, por lo general será objetivamente claro para el organismo administrativo central, etc., que ha infringido la ley. Por tanto, para justificar por qué considera que no debe seguirse una recomendación de la Comisión de Protección, un organismo administrativo central, etc., debe presentar razones fundadas que puedan demostrar que no ha infringido la ley. La recomendación debe seguirse, a menos que la Comisión de Protección determine que efectivamente no es el caso.

En vista de ello, las «circunstancias extraordinarias» mencionadas en el artículo 64, apartado 4, de la Ley sobre la protección de la información personal deben limitarse estrictamente a las circunstancias extraordinarias en las que existan razones fundadas para que los organismos administrativos centrales, etc., demuestren que «la presente Ley efectivamente no se ha infringido», como los «casos en los que existan circunstancias extraordinarias (de hecho o de derecho)» que la Comisión de Protección desconocía a la hora de formular su recomendación inicialmente y la Comisión de Protección determine que efectivamente no se ha producido ninguna infracción.

6. **Aplicación de la LPIP al tratamiento de datos personales con fines de seguridad nacional, en particular la investigación de infracciones y la ejecución con arreglo a la LPIP (artículos 7-8, 7-9, 58, 3, 4 y 62 de la LPIP)**

<Ley sobre la protección de la información personal

(Ley n.º 16930, parcialmente modificada el 4 de febrero de 2020)>

Artículo 7-8 (El trabajo de la Comisión de Protección) 1) La Comisión de Protección desempeñará las siguientes funciones: […]

3. cuestiones relacionadas con la investigación de vulneraciones de los derechos de los interesados y las disposiciones consiguientes;

4. tramitación de reclamaciones o procedimientos de reparación relacionados con el tratamiento de información personal y mediación de litigios sobre información personal;

[…]

([8]) (Sentencia del Tribunal Supremo 97Da10215,10222, de 26 de enero de 1999) Si los hechos delictivos del acusado se divulgan a través de los medios de comunicación, es probable que causen daños físicos y mentales irreparables no solo a la víctima, es decir, al demandante, sino también a las personas a su alrededor, incluidas las familias.

([9]) (Sentencia del Tribunal Superior de Seúl 2006Na92006, de 16 de enero de 2008) Si se publica un artículo difamatorio, es probable que cause daños irreparables graves a la persona implicada.

([10]) Los mismos principios establecidos en el inciso ii) se aplican al artículo 45-4 de la Ley de información crediticia.

Artículo 7-9 (Cuestiones objeto de deliberación y resolución por la Comisión de Protección) 1) La Comisión de Protección deliberará y decidirá sobre las siguientes cuestiones: […]

5. cuestiones relativas a la interpretación y el funcionamiento del Derecho en materia de protección de información personal;

[…]

Artículo 58 (Exclusión parcial de la aplicación) 1) Los capítulos III a VII no se aplicarán a ninguno de los siguientes datos personales:

1. información personal recogida con arreglo a la Ley de Estadística para su tratamiento por parte de instituciones públicas;
2. información personal recogida o solicitada para el análisis de información relacionada con la seguridad nacional;
3. información personal tratada temporalmente cuando sea urgentemente necesario para la seguridad pública, la salud pública, etc.;
4. información personal recogida o utilizada con fines de presentación de informes por la prensa, actividades misioneras por organizaciones religiosas y designación de candidatos por partidos políticos, respectivamente.

[Se suprimen los apartados 2 y 3]

4) En el caso del tratamiento de información personal con arreglo al apartado 1, el responsable del tratamiento tratará la información personal en la medida mínima necesaria para alcanzar la finalidad perseguida por el período mínimo; y adoptará asimismo las medidas necesarias, tales como salvaguardias técnicas, físicas y administrativas, tramitación individual de reclamaciones y otras medidas necesarias para la gestión segura y el tratamiento adecuado de dicha información personal.

Artículo 3 (Principios para la protección de la información personal) 1) El responsable del tratamiento de información personal especificará explícitamente los fines para los que se trata la información personal y recogerá dicha información de manera lícita y leal, limitándose a lo estrictamente necesario para tales fines.

2) El responsable del tratamiento de la información personal tratará dicha información de manera adecuada atendiendo a los fines para los que se realiza el tratamiento y no utilizará la información con otros fines.

3) El responsable del tratamiento garantizará que la información personal sea exacta y completa y esté actualizada en la medida necesaria en relación con los fines para los que se trata dicha información.

4) El responsable del tratamiento gestionará la información personal de manera segura según los métodos de tratamiento, tipos, etc. de información personal, teniendo en cuenta la posibilidad de que se vulneren los derechos del interesado y la gravedad de los riesgos pertinentes.

5) El responsable del tratamiento de información personal deberá hacer pública su política de privacidad y otras cuestiones relacionadas con el tratamiento de información personal y garantizará los derechos del interesado, como el derecho de acceso a su información personal.

6) El responsable del tratamiento tratará la información personal de manera que se reduzca al mínimo la posibilidad de que se vulnere la privacidad del interesado.

7) Si sigue siendo posible cumplir la finalidad de la recogida de información personal mediante el tratamiento de información anonimizada o seudonimizada, el responsable del tratamiento procurará tratar la información personal mediante anonimización, cuando sea posible, o seudonimización, si resulta imposible cumplir la finalidad de la recogida de información personal mediante anonimización.

8) El responsable del tratamiento de información personal procurará obtener la confianza de los interesados mediante la observación y el desempeño de las funciones y responsabilidades previstas en la presente Ley y en otras leyes conexas.

Artículo 4 (Derechos de los interesados) Un interesado tiene los siguientes derechos en relación con el tratamiento de su propia información personal:

1. el derecho a ser informado del tratamiento de dicha información personal;
2. el derecho a determinar si dar o no su consentimiento y el alcance del mismo en relación con el tratamiento de dicha información personal;
3. el derecho a confirmar si se está tratando o no información personal y a solicitar acceso (también el suministro de copias; en lo sucesivo, se aplicará lo mismo) a dicha información personal;
4. el derecho a suspender el tratamiento de dicha información personal y a solicitar su rectificación, supresión y destrucción;
5. el derecho a una reparación adecuada por cualquier daño o perjuicio derivado del tratamiento de dicha información personal mediante un procedimiento rápido y justo.

Artículo 62 (Denuncia de infracciones) 1) Toda persona que sufra una vulneración de sus derechos o intereses en relación con sus datos personales en el curso del tratamiento de información personal por parte de un responsable del tratamiento podrá denunciar dicha infracción ante la Comisión de Protección.

2) La Comisión de Protección podrá designar una institución especializada para recibir y tramitar eficazmente las reclamaciones de conformidad con el apartado 1, según lo dispuesto mediante Decreto presidencial. En tales casos, dicha institución especializada establecerá y gestionará un centro de llamadas para las infracciones relacionadas con la información personal (en lo sucesivo denominado «Centro de atención telefónica sobre privacidad»).

3) El Centro de atención telefónica sobre privacidad desempeñará las siguientes funciones:

1. recibir reclamaciones y proporcionar asesoramiento en relación con el tratamiento de la información personal;

2. investigar y confirmar incidentes y escuchar las opiniones de las partes relacionadas;

3. funciones inherentes a los puntos 1 y 2.

4) En caso necesario, la Comisión de Protección podrá enviar a su funcionario público a la institución especializada designada en virtud del apartado 2, de conformidad con el artículo 32-4 de la Ley de funcionarios públicos del Estado, con el fin de investigar y confirmar eficazmente los incidentes con arreglo al apartado 3, punto 2.

i) La recogida de información personal con fines de seguridad nacional está regulada por leyes específicas que facultan a las autoridades competentes (por ejemplo, el Servicio Nacional de Inteligencia) para interceptar comunicaciones o solicitar su divulgación en determinadas condiciones y con ciertas salvaguardias (en lo sucesivo, «leyes de seguridad nacional»). Estas leyes de seguridad nacional incluyen, por ejemplo, la Ley sobre la protección de la privacidad de las comunicaciones, la Ley antiterrorista para la protección de los ciudadanos y la seguridad pública o la Ley del sector de las telecomunicaciones. Además, la recogida y el tratamiento ulterior de información personal deben cumplir los requisitos de la LPIP. A este respecto, el artículo 58, apartado 1, punto 2, de la LPIP establece que los capítulos III a VII no se aplicarán a la información personal recogida o solicitada para el análisis de información relacionada con la seguridad nacional. Por consiguiente, esta excepción parcial se aplica al tratamiento de información personal con fines de seguridad nacional.

Al mismo tiempo, el capítulo I (Disposiciones generales), el capítulo II (Establecimiento de políticas de protección de la información personal, etc.), el capítulo VIII (Demandas colectivas por violación de datos), el capítulo IX (Disposiciones complementarias) y el capítulo X (Disposiciones sobre sanciones) de la LPIP se aplican al tratamiento de dicha información personal. Esto abarca los principios generales de protección de datos establecidos en el artículo 3 (Principios de protección de la información personal) y los derechos individuales garantizados por el artículo 4 de la LPIP (Derechos de los interesados).

Además, el artículo 58, apartado 4, de la LPIP establece que dicha información deberá tratarse en la medida mínima necesaria para alcanzar la finalidad perseguida y por el período mínimo; además, exige que el responsable del tratamiento de información personal establezca las medidas necesarias para garantizar una gestión segura de los datos y un tratamiento adecuado, tales como salvaguardias técnicas, físicas y administrativas, así como medidas para la tramitación adecuada de las reclamaciones individuales.

Por último, se aplicarán las disposiciones que regulan las funciones y competencias de la CPIP (incluidos los artículos 60 a 65 de la LPIP sobre la tramitación de reclamaciones y la adopción de recomendaciones y medidas correctoras), así como las disposiciones sobre las sanciones administrativas y penales (artículo 70 y siguientes de la LPIP). De conformidad con el artículo 7-8, apartado 1, puntos 3 y 4, y el artículo 7-9, apartado 1, punto 5, de la LPIP, estas facultades de investigación y corrección, incluso cuando se ejercen en el contexto de la tramitación de reclamaciones, también abarcan las posibles infracciones de las normas contenidas en las leyes específicas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal, tales como las leyes de seguridad nacional. Habida cuenta de los requisitos establecidos en el artículo 3, apartado 1, de la LPIP para la recogida lícita y leal de información personal, y de que su infracción constituye una violación de la «presente Ley» en el sentido de los artículos 63 y 64, la CPIP puede llevar a cabo una investigación y adoptar medidas correctoras ([11]). El ejercicio de estas facultades por parte de la CPIP complementa, pero no sustituye, las facultades de la Comisión Nacional de Derechos Humanos en virtud de la Ley de la Comisión Nacional de Derechos Humanos.

La aplicación de los principios, derechos y obligaciones fundamentales de la LPIP al tratamiento de información personal con fines de seguridad nacional refleja las garantías consagradas en la Constitución para la protección del derecho de un particular a controlar su propia información personal. Tal como reconoce el Tribunal Constitucional, lo anterior comprende el derecho de un particular ([12]) «a decidir personalmente cuándo y en qué medida se divulgará o utilizará su información, a quién se divulgará y quién podrá efectuar la divulgación o usar la información. Es un derecho fundamental ([13]), [...], destinado a proteger la libertad de decisión personal frente al riesgo causado por la ampliación de las funciones estatales y las tecnologías de infocomunicación». Toda restricción a ese derecho, por ejemplo, cuando resulte necesaria para la protección de la seguridad nacional, requiere encontrar un equilibrio entre los derechos e intereses del particular y el interés público pertinente y no puede afectar al contenido esencial del derecho (artículo 37, apartado 2, de la Constitución).

([11]) Por lo que se refiere a las medidas correctoras con arreglo al artículo 64, véase también la sección 5.
([12]) Sentencia del Tribunal Constitucional, 99HunMa513, 2004HunMa190, de 26 de mayo de 2005.
([13]) Sentencia del Tribunal Constitucional, 2003HunMa282, de 21 de julio de 2005.

Por consiguiente, al tratar información personal con fines de seguridad nacional, el responsable del tratamiento (por ejemplo, el SNI) deberá, entre otras cosas:

1) especificar explícitamente los fines para los que se trata la información personal y recoger dicha información de manera lícita y leal en la medida mínima necesaria para tales fines (artículo 3, apartado 1, de la LPIP); en concreto, solo recogerá y tratará ulteriormente la información personal con el fin de ejercer las funciones previstas en las leyes pertinentes, tales como la Ley del Servicio Nacional de Inteligencia;

2) tratar la información personal en la medida mínima y durante el período mínimo necesarios para alcanzar la finalidad perseguida (artículo 58, apartado 4, de la LPIP); una vez alcanzada la finalidad del tratamiento, el responsable del tratamiento destruirá de manera irreversible la información personal, a menos que la ley exija específicamente una conservación ulterior, en cuyo caso la información personal pertinente se almacenará y gestionará separada de otros datos personales, no se utilizará para fines distintos de los especificados en la ley y se destruirá al final del período de conservación;

3) tratar la información personal de la manera adecuada necesaria para los fines para los que se realiza el tratamiento y no la utilizará más allá de dichos fines (artículo 3, apartado 2, de la LPIP);

4) garantizar que la información personal sea exacta, completa y actualizada en la medida necesaria en relación con los fines para los que se trata dicha información (artículo 3, apartado 3, de la LPIP);

5) gestionar la información personal de manera segura según los métodos de tratamiento, tipos, etc. de información personal, teniendo en cuenta la posibilidad de que se vulneren los derechos del interesado y la gravedad de los riesgos pertinentes (artículo 3, apartado 4, de la LPIP);

6) hacer pública su política de privacidad y otras cuestiones relacionadas con el tratamiento de la información personal (artículo 3, apartado 5, de la LPIP);

7) tratar la información personal de manera que se reduzca al mínimo la posibilidad de vulnerar la privacidad de un interesado (artículo 3, apartado 6, de la LPIP).

ii) De conformidad con el artículo 58, apartado 4, de la LPIP, el responsable del tratamiento (por ejemplo, las autoridades competentes en materia de seguridad nacional, como el SNI) adoptará las medidas necesarias, tales como el establecimiento de salvaguardias técnicas, físicas y administrativas, para garantizar el cumplimiento de estos principios y el tratamiento adecuado de la información personal. Esto puede abarcar, por ejemplo, medidas específicas para garantizar la seguridad de la información personal, tales como restricciones al acceso a la información personal, controles de acceso, registros, proporcionar a los empleados formación específica sobre el manejo de la información personal, etc.

Además, de conformidad con el artículo 3, apartado 5, y el artículo 4 de la LPIP, los interesados tendrán, entre otros, los siguientes derechos con respecto a la información personal tratada con fines de seguridad nacional:

1) el derecho a obtener la confirmación de si se está tratando o no su información personal, así como información sobre el tratamiento, y a acceder a dicha información, incluido el suministro de copias (artículo 4, apartados 1 y 3, de la LPIP);

2) el derecho a suspender el tratamiento, así como a la rectificación, supresión y destrucción de la información personal (artículo 4, apartado 4, de la LPIP).

iii) El interesado podrá presentar una solicitud en el ejercicio de estos derechos directamente al responsable del tratamiento o indirectamente a través de la Comisión de Protección, y podrá autorizar a su representante para que lo haga. Cuando el interesado presente una solicitud, el responsable del tratamiento concederá el derecho sin demora; a reserva, sin embargo, de que puede retrasar, limitar o denegar el derecho si está previsto específicamente por otras leyes o resulta inevitable para cumplirlas, en la medida y durante el tiempo necesarios y proporcionados para proteger un objetivo importante de interés público (por ejemplo, en la medida y durante el tiempo que la concesión del derecho ponga en peligro una investigación en curso o amenace la seguridad nacional) o cuando la concesión del derecho pueda atentar contra la vida o la integridad física de un tercero o dar lugar a una vulneración injustificada de los intereses patrimoniales y otros intereses de un tercero. En caso de denegación o restricción de la solicitud, deberá informar al interesado sin demora de los motivos. El responsable del tratamiento preparará el método y el procedimiento para que los interesados puedan presentar solicitudes y los anunciará públicamente para que los interesados puedan tener conocimiento de ellos.

Además, de conformidad con el artículo 58, apartado 4, de la LPIP (Obligación de garantizar la tramitación adecuada de las reclamaciones individuales) y el artículo 4, apartado 5, de la LPIP (Derecho a una reparación adecuada por cualquier daño o perjuicio derivado del tratamiento de información personal, mediante un procedimiento rápido y justo), los interesados tendrán derecho a obtener reparación. Esto incluye el derecho a denunciar una presunta infracción ante el Centro de denuncias de infracciones relacionadas con la información personal (de conformidad con el artículo 62, apartado 3, de la LPIP), a presentar una reclamación ante la CPIP con arreglo al artículo 62 de la LPIP por cualquier vulneración de los derechos o intereses relacionados con la información personal de un particular y a un recurso judicial contra las decisiones o la inacción de la CPIP en virtud de la Ley de lo contencioso-administrativo. Además, los interesados pueden obtener reparación judicial en virtud de la Ley de lo contencioso-administrativo si se ha producido una vulneración de sus derechos o intereses debido a una disposición u omisión del responsable del tratamiento (por ejemplo, la recogida ilícita de datos personales) u obtener una indemnización por daños y perjuicios de conformidad con la Ley de indemnización estatal. Estas vías de recurso están disponibles en caso de posibles infracciones tanto de las normas contenidas en las leyes específicas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal, por ejemplo, las leyes de seguridad nacional, como de la LPIP.

Un ciudadano de la UE puede presentar una reclamación ante la CPIP a través de su autoridad nacional de protección de datos, y la CPIP notificará a la persona a través de la autoridad nacional de protección de datos, una vez finalizadas la investigación y la medida correctora (si procede).

ANEXO II

18 de mayo de 2021

Excmo. D. Didier Reynders, comisario de Justicia de la Comisión Europea

Excelentísimo señor:

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

En respuesta a la petición cursada por la Comisión Europea al Gobierno de Corea, 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 coreanas.

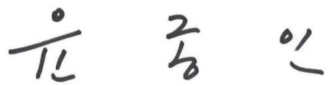
El presente documento atañe a numerosos ministerios y agencias del Gobierno de Corea, y en relación con el contenido del documento, los ministerios y agencias competentes (la Comisión de Protección de la Información Personal, el Ministerio de Justicia, el Servicio Nacional de Inteligencia, la Comisión Nacional de Derechos Humanos de Corea, el Centro Nacional de Lucha contra el Terrorismo, la Unidad de Inteligencia Financiera de Corea) 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,



Yoon Jong In
Presidente de la Comisión de Protección de la Información Personal

El presente documento ha sido elaborado por la Comisión de Protección de la Información Personal y los siguientes ministerios y agencias.

Park Jie Won
Presidente (director), Servicio Nacional de Inteligencia

Lee Jung Soo
Director general, Ministerio de Justicia

Choi Young Ae
Presidenta, Comisión Nacional de Derechos Humanos de Corea

Kim Hyuck Soo
Director, Centro Nacional de Lucha contra el Terrorismo

Kim Jeong Kag
Comisario, Unidad de Inteligencia Financiera de Corea

Marco jurídico para la recogida y la utilización de datos personales por parte de las autoridades públicas coreanas con fines coercitivos y de seguridad nacional

El presente documento ofrece una visión general del marco jurídico para la recogida y la utilización de datos personales por parte de las autoridades públicas coreanas 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 (limitaciones) y las salvaguardias aplicables, así como la supervisión independiente y las posibilidades de reparación individual.

1. PRINCIPIOS JURÍDICOS GENERALES PERTINENTES PARA EL ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

1.1. Marco constitucional

La Constitución de la República de Corea establece el derecho a la privacidad en general (artículo 17) y, en particular, el derecho a la privacidad de la correspondencia (artículo 18). Es obligación del Estado garantizar estos derechos fundamentales ([1]). La Constitución estipula asimismo que los derechos y libertades de los ciudadanos solo pueden ser restringidos por ley y cuando sea necesario por razones de seguridad nacional o para el mantenimiento del orden público en interés del bienestar público ([2]). Incluso cuando se impongan tales restricciones, estas no pueden afectar al contenido esencial de las libertades o de los derechos ([3]). Los órganos jurisdiccionales coreanos han aplicado estas disposiciones en asuntos relativos a la interferencia de las autoridades públicas con la privacidad. Por ejemplo, el Tribunal Supremo consideró que la vigilancia de los ciudadanos vulneraba el derecho fundamental a la privacidad, al hacer hincapié en que los ciudadanos tienen «derecho a la autodeterminación de la información personal» ([4]). En otro asunto, el Tribunal Constitucional declaró que el derecho a la privacidad es un derecho fundamental que brinda protección contra la intervención en la vida privada de los ciudadanos y su vigilancia por parte del Estado ([5]).

La Constitución coreana garantiza asimismo que ninguna persona será arrestada, detenida, registrada o interrogada, ni se incautarán bienes, salvo en los casos previstos por la ley ([6]). Además, los registros e incautaciones solo pueden llevarse a cabo sobre la base de una orden emitida por un juez, a petición de un fiscal, y respetando las garantías procesales ([7]). En circunstancias excepcionales, por ejemplo, cuando se detenga a una persona sospechosa en el momento de la comisión de un delito (delito flagrante), o cuando exista el riesgo de que una persona sospechosa de haber cometido un delito castigado con una pena de prisión de tres años o más pueda escapar o destruir pruebas, las autoridades de investigación podrán llevar a cabo un registro o una incautación sin una orden, que deberán solicitar posteriormente ([8]). Estos principios generales se desarrollan aún más en leyes específicas relativas al procedimiento penal y a la protección de las comunicaciones (véase más adelante para tener una visión de conjunto detallada).

Con respecto a los extranjeros, la Constitución establece que su condición está garantizada según lo dispuesto por el Derecho y los tratados internacionales ([9]). Varios acuerdos internacionales de los que Corea es parte garantizan los derechos de privacidad, como el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención sobre los Derechos de las Personas con Discapacidad (artículo 22) y la Convención sobre los Derechos del Niño (artículo 16). Además, si bien la Constitución hace referencia, en principio, a los derechos de los «ciudadanos», el Tribunal Constitucional ha dictaminado que también los extranjeros son titulares de derechos fundamentales ([10]). En particular, el Tribunal sostuvo que la protección de la dignidad y el valor de una persona como ser humano, así como el derecho a

([1]) Artículo 10 de la Constitución de la República de Corea, promulgada el 17 de julio de 1948 (en lo sucesivo, «la Constitución»).
([2]) Artículo 37, apartado 2, de la Constitución.
([3]) Artículo 37, apartado 2, de la Constitución.
([4]) Resolución n.º 96DA42789 del Tribunal Supremo de Corea, de 24 de julio de 1998.
([5]) Resolución n.º 2002Hun-Ma51 del Tribunal Constitucional, de 30 de octubre de 2003. Del mismo modo, en la Resolución 99Hun-Ma513 y 2004Hun-Ma190 (consolidada), de 26 de mayo de 2005, el Tribunal Constitucional aclaró que «el derecho a controlar la propia información personal es un derecho de la persona a quien concierne la información para decidir personalmente cuándo y en qué medida se divulgará o utilizará su información, a quién se divulgará y quién podrá efectuar la divulgación o usar la información. Es un derecho fundamental, aunque no se especifique en la Constitución, destinado a proteger la libertad de decisión personal frente al riesgo causado por la ampliación de las funciones estatales y las tecnologías de infocomunicación».
([6]) Artículo 12, apartado 1, primera frase, de la Constitución.
([7]) Artículo 16 y artículo 12, apartado 3, de la Constitución.
([8]) Artículo 12, apartado 3, de la Constitución.
([9]) Artículo 6, apartado 2, de la Constitución.
([10]) Resolución n.º 93Hun-MA120 del Tribunal Constitucional, de 29 de diciembre de 1994. Véase también, por ejemplo, la resolución n.º 2014Hun-Ma346 del Tribunal Constitucional (de 31 de mayo de 2018), en la que el Tribunal dictaminó que se había vulnerado el derecho constitucional de un nacional sudanés detenido en el aeropuerto a recibir asistencia letrada. En otro asunto, el Tribunal Constitucional dictaminó que la libertad de elegir el lugar de trabajo está estrechamente relacionada con el derecho a buscar la felicidad, así como con la dignidad y el valor humanos, por lo que no está reservada únicamente a los ciudadanos, sino que también puede garantizarse a los extranjeros que trabajan legalmente en la República de Corea (Resolución n.º 2007Hun-Ma1083 del Tribunal Constitucional, de 29 de septiembre de 2011).

buscar la felicidad, son derechos de todo ser humano, no solo de los ciudadanos ([11]). El Tribunal también aclaró que el derecho a controlar la propia información se considera un derecho fundamental, basado en el derecho a la dignidad y a buscar la felicidad, así como en el derecho a la vida privada ([12]). Aunque hasta ahora la jurisprudencia no se ha ocupado específicamente del derecho a la privacidad de los nacionales no coreanos, es ampliamente aceptado entre los académicos que los artículos 12 a 22 de la Constitución (que abarcan el derecho a la privacidad y a la libertad personal) establecen «los derechos de los seres humanos».

Por último, la Constitución también prevé el derecho a reclamar una indemnización justa a las autoridades públicas ([13]). Además, sobre la base de la Ley del Tribunal Constitucional, cualquier persona cuyos derechos fundamentales garantizados por la Constitución se vean vulnerados por el ejercicio del poder gubernamental (excluidas las sentencias de los órganos jurisdiccionales) podrá presentar un recurso de inconstitucionalidad ante el Tribunal Constitucional ([14]).

1.2. **Normas generales de protección de datos**

La ley general de protección de datos de la República de Corea, la Ley sobre la protección de la información personal (en lo sucesivo, «LPIP»), se aplica tanto al sector público como al privado. Con respecto a las autoridades públicas, la LPIP hace referencia específica a la obligación de formular políticas para prevenir «el abuso y el uso indebido de la información personal, la vigilancia indiscreta y el seguimiento, etc. y mejorar la dignidad de los seres humanos y la privacidad individual» ([15]).

El tratamiento de datos personales a efectos de control de la aplicación de la ley está sujeto a todos los requisitos de la LPIP. Esto significa, por ejemplo, que las autoridades encargadas de garantizar el cumplimiento del Derecho penal deben cumplir las obligaciones de tratamiento lícito, es decir, basarse en una de las bases jurídicas mencionadas en la LPIP para la recogida, la utilización o el suministro de información personal (artículos 15 a 18 de la LPIP), así como los principios de limitación de la finalidad (artículo 3, apartados 1 y 2, de la LPIP), proporcionalidad/minimización de los datos (artículo 3, apartados 1 y 6, de la LPIP), conservación limitada de los datos (artículo 21 de la LPIP), seguridad de los datos, incluida la notificación de las violaciones de la seguridad de los datos (artículo 3, apartado 4, y artículos 29 y 34 de la LPIP) y transparencia (artículo 3, apartados 1 y 5, y artículos 20, 30 y 32 de la LPIP). Se aplican salvaguardias específicas con respecto a la información sensible (artículo 23 de la LPIP). Además, de conformidad con el artículo 3, apartado 5, y los artículos 4 y 35 a 39-2 de la LPIP, los particulares pueden ejercer sus derechos de acceso, rectificación, supresión y suspensión ante las autoridades encargadas de garantizar el cumplimiento de la ley.

Por tanto, si bien la LPIP es plenamente aplicable al tratamiento de datos personales a efectos de control de la aplicación del Derecho penal, contiene una excepción cuando los datos personales se tratan con fines de seguridad nacional. De conformidad con el artículo 58, apartado 1, punto 2, de la LPIP, los artículos 15 a 50 de la LPIP no se aplicarán a la información personal recogida o solicitada para el análisis de información relacionada con la seguridad nacional ([16]). Por el contrario, el capítulo I (Disposiciones generales), el capítulo II (Establecimiento de políticas de protección de la información personal, etc.), el capítulo VIII (Demandas colectivas por violación de la seguridad de los datos), el capítulo IX (Disposiciones complementarias) y el capítulo X (Disposiciones sobre sanciones) de la LPIP seguirán siendo de aplicación. Esto abarca los principios generales de protección de datos establecidos en el artículo 3 (Principios de protección de la información personal) y los derechos individuales garantizados por el artículo 4 de la LPIP (Derechos de los interesados). Esto significa que los principios y derechos fundamentales también están garantizados en este ámbito. Además, el artículo 58, apartado 4, de la LPIP establece que dicha información deberá tratarse en la medida mínima necesaria para alcanzar la finalidad perseguida y por el período mínimo; también exige que el responsable del tratamiento de información personal establezca las medidas necesarias para garantizar una gestión segura de los datos y un tratamiento adecuado, tales como salvaguardias técnicas, físicas y administrativas, así como medidas para la tramitación adecuada de las reclamaciones individuales.

En la Nota n.º 2021-1 sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, la Comisión de Protección de la Información Personal (en lo sucesivo, «la CPIP») aclara con mayor detalle cómo se aplica la LPIP al tratamiento de datos personales con fines de seguridad nacional, a la luz de esta exención parcial ([17]). Esto comprende, en particular, los derechos de las personas (acceso, rectificación, suspensión y supresión) y los motivos y las limitaciones de posibles restricciones de los mismos. De acuerdo con la Nota, la aplicación de los principios, los derechos y las obligaciones fundamentales de la LPIP al tratamiento de datos personales con fines de seguridad nacional refleja las garantías previstas por la Constitución para la protección del

([11]) Resolución n.º 99HeonMa494 del Tribunal Constitucional, de 29 de noviembre de 2001.
([12]) Véase, por ejemplo, la Resolución n.º 99HunMa513 del Tribunal Constitucional.
([13]) Artículo 29, apartado 1, de la Constitución.
([14]) Artículo 68, apartado 1, de la Ley del Tribunal Constitucional.
([15]) Artículo 5, apartado 1, de la LPIP.
([16]) Artículo 58, apartado 1, punto 2, de la LPIP.
([17]) Nota n.º 2021-1 de la CPIP sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, sección III, apartado 6.

derecho de un particular a controlar su propia información personal. Toda restricción a ese derecho, por ejemplo, cuando resulte necesaria para la protección de la seguridad nacional, requiere encontrar un equilibrio entre los derechos e intereses del particular y el interés público pertinente y no puede afectar al contenido esencial del derecho (artículo 37, apartado 2, de la Constitución).

2. ACCESO DE LAS AUTORIDADES PÚBLICAS A EFECTOS DE CONTROL DE LA APLICACIÓN DE LA LEY

2.1. Autoridades públicas competentes en el ámbito del control del cumplimiento de la ley

Sobre la base de la Ley de enjuiciamiento criminal (en lo sucesivo, «LEC»), la Ley sobre la protección de la privacidad de las comunicaciones (en lo sucesivo, «LPPC») y la Ley del sector de las telecomunicaciones (en lo sucesivo, «LST»), la policía, los fiscales y los órganos jurisdiccionales podrán recoger datos personales a efectos de control de la aplicación del Derecho penal. En la medida en que la Ley del Servicio Nacional de Inteligencia también confiera esta facultad al Servicio Nacional de Inteligencia (en lo sucesivo, «SNI»), este deberá cumplir las leyes antes mencionadas ([18]). Por último, la Ley sobre la comunicación y el uso de información específica sobre las transacciones financieras (en lo sucesivo, «LCUIETF») proporciona una base jurídica para que las instituciones financieras revelen información a la Unidad de Inteligencia Financiera de Corea (en lo sucesivo, «UIFC») con el fin de prevenir el blanqueo de capitales y la financiación del terrorismo. Este organismo especializado podrá, a su vez, facilitar dicha información a las autoridades encargadas de garantizar el cumplimiento de la ley. Sin embargo, estas obligaciones de divulgación solo se aplican a los responsables del tratamiento de datos que tratan información crediticia personal de conformidad con la Ley de información crediticia y están sujetos a la supervisión de la Comisión de Servicios Financieros. Dado que el tratamiento de información crediticia personal por parte de dichos responsables está excluido del ámbito de aplicación de la decisión de adecuación, las limitaciones y salvaguardias aplicables en virtud de la LCUIETF no se describen con más detalle en el presente documento.

2.2. Bases jurídicas y limitaciones

La LEC (véase 2.2.1), la LPPC (véase 2.2.2) y la Ley del sector de las telecomunicaciones (véase 2.2.3) proporcionan bases jurídicas para la recogida de información personal a efectos de control de la aplicación de la ley y establecen las limitaciones y salvaguardias aplicables.

2.2.1. *Registros e incautaciones*

2.2.1.1. Base jurídica

Los fiscales y los agentes de alto rango de la policía judicial solo podrán inspeccionar objetos, registrar a personas o incautarse de objetos si 1) una persona es sospechosa de haber cometido un delito (un sospechoso), 2) la investigación así lo requiere y 3) se considera que los objetos por inspeccionar, las personas por registrar y los objetos por incautar están relacionados con el asunto ([19]). Del mismo modo, los órganos jurisdiccionales pueden llevar a cabo registros e incautarse de cualquier objeto que deba ser utilizado como prueba o ser decomisado, siempre que se considere que dichos objetos o personas están relacionados con un asunto concreto ([20]).

2.2.1.2. Limitaciones y salvaguardias

Como obligación general, los fiscales y los agentes de la policía judicial deberán respetar los derechos humanos del sospechoso, así como los de cualquier otra persona afectada ([21]). Además, solo podrán adoptarse medidas obligatorias para alcanzar el objetivo de la investigación cuando así lo disponga explícitamente la LEC y en la menor medida necesaria ([22]).

Los registros, las inspecciones o las incautaciones por parte de agentes de policía o fiscales en el marco de una investigación penal solo podrán llevarse a cabo sobre la base de una orden judicial ([23]). La autoridad que solicite una orden deberá presentar materiales que demuestren los motivos para sospechar que una persona ha cometido un delito, que el registro, la inspección o la incautación son necesarios y que existen los objetos pertinentes que deben incautarse ([24]). En cuanto a la orden, esta debe contener, entre otras cosas, el nombre del sospechoso y el delito; el lugar, la persona o los objetos que se vayan a registrar o los objetos que se vayan a incautar; la fecha de emisión; y el período efectivo de aplicación ([25]). Del mismo modo, cuando, en el marco de un procedimiento judicial en curso, los registros e incautaciones se lleven a cabo fuera de una audiencia pública, deberá obtenerse previamente una orden judicial ([26]). El particular de que se trate y su abogado defensor serán informados con antelación del registro o la incautación y podrán estar presentes en el momento de la ejecución de la orden ([27]).

([18]) Véase el artículo 3 de la Ley SNI (Ley n.º 12948), que hace referencia a las investigaciones penales de determinados delitos, tales como la insurrección, la rebelión y los delitos relacionados con la seguridad nacional (por ejemplo, el espionaje). Los procedimientos de la LEC en materia de registros e incautaciones se aplicarían en este contexto, mientras que la LPPC regiría la recogida de datos de comunicaciones (véase la parte 3 sobre las disposiciones relativas al acceso a las comunicaciones con fines de seguridad nacional).
([19]) Artículo 215, apartados 1 y 2, de la LEC.
([20]) Artículo 106, apartado 1, y artículos 107 y 109 de la LEC.
([21]) Artículo 198, apartado 2, de la LEC.
([22]) Artículo 199, apartado 1, de la LEC.
([23]) Artículo 215, apartados 1 y 2, de la LEC.
([24]) Artículo 108, apartado 1, del Reglamento de procedimiento penal.
([25]) Artículo 114, apartado 1, de la LEC, en relación con su artículo 219.
([26]) Artículo 113 de la LEC.
([27]) Artículos 121 y 122 de la LEC.

En principio, a la hora de llevar a cabo registros o incautaciones y cuando el objeto por registrar sea un disco de ordenador u otro soporte de almacenamiento de datos, solo se incautarán los propios datos (copiados o impresos) en lugar de todo el soporte ([28]). El propio soporte de almacenamiento de datos solo podrá ser incautado cuando se considere sustancialmente imposible imprimir o copiar los datos necesarios por separado o cuando se considere que es sustancialmente impracticable lograr el objetivo del registro de otra manera ([29]). La incautación deberá notificarse sin demora al particular de que se trate ([30]). No hay excepciones a este requisito de notificación con arreglo a la LEC.

Los registros, las inspecciones y las incautaciones sin una orden solo podrán tener lugar en situaciones limitadas. En primer lugar, este es el caso cuando resulta imposible obtener una orden debido a la urgencia en el lugar de una infracción ([31]). No obstante, debe obtenerse una orden posteriormente y sin demora ([32]). En segundo lugar, los registros y las inspecciones sin una orden podrán tener lugar *in loco* cuando se arreste o se detenga a un sospechoso ([33]). Por último, un fiscal o un alto funcionario de la policía judicial podrá incautarse de un objeto sin una orden cuando el objeto haya sido desechado por un sospechoso o un tercero o se haya presentado voluntariamente ([34]).

Las pruebas obtenidas en violación de la LEC se considerarán inadmisibles ([35]). Además, la Ley penal establece que los registros ilícitos de personas o de su lugar de residencia, edificios vigilados, estructuras, automóviles, buques, aeronaves o habitaciones ocupadas son punibles con una pena de prisión de un máximo de tres años ([36]). Por consiguiente, esta disposición también se aplica cuando se incautan objetos, tales como dispositivos de almacenamiento de datos, durante un registro ilícito.

2.2.2. *Recogida de información sobre las comunicaciones*

2.2.2.1. Base jurídica

La recogida de información sobre las comunicaciones se rige por una ley específica, la LPPC. En particular, la LPPC establece la prohibición de censurar cualquier correo, realizar escuchas de cualquier telecomunicación, facilitar datos de confirmación de la comunicación, grabar o escuchar cualquier conversación entre otras personas que no se haga pública, salvo sobre la base de la LEC, la LPPC o la Ley de tribunales militares ([37]). El término «comunicación» en el sentido de la LPPC abarca tanto el correo ordinario como las telecomunicaciones ([38]). A este respecto, la LPPC distingue entre «medidas de restricción de la comunicación» ([39]) y la recogida de «datos de confirmación de la comunicación».

El concepto de «medidas de restricción de la comunicación» abarca la «censura», por ejemplo, la recogida del contenido del correo postal tradicional y las «escuchas telefónicas», es decir, la interceptación directa (adquisición o grabación) del contenido de las telecomunicaciones ([40]). El concepto de «datos de confirmación de la comunicación» abarca los «datos sobre los registros de telecomunicaciones», que incluyen la fecha de las telecomunicaciones, su hora de inicio y fin, el número de llamadas salientes y entrantes, así como el número de abonados de la otra parte, la frecuencia de uso, los archivos de registro sobre el uso de los servicios de telecomunicaciones y la información sobre la ubicación (por ejemplo, de torres de transmisión en las que se reciben las señales) ([41]).

([28]) Artículo 106, apartado 3, de la LEC.
([29]) Artículo 106, apartado 3, de la LEC.
([30]) Artículo 219 de la LEC, en relación con su artículo 106, apartado 4.
([31]) Artículo 216, apartado 3, de la LEC.
([32]) Artículo 216, apartado 3, de la LEC.
([33]) Artículo 216, apartados 1 y 2, de la LEC.
([34]) Artículo 218 de la LEC. Por lo que se refiere a la información personal, esto solo abarca la presentación voluntaria por parte del particular de que se trate, no por un responsable del tratamiento que posea dicha información (lo cual requeriría una base jurídica específica con arreglo a la Ley sobre la protección de la información personal). Los objetos presentados voluntariamente solo se admitirán como pruebas en procedimientos judiciales si no existen dudas razonables acerca del carácter voluntario de la divulgación, lo cual debe demostrar el fiscal. Véase la Resolución n.º 2013Do11233 del Tribunal Supremo, de 10 de marzo de 2016.
([35]) Artículo 308-2 de la LEC.
([36]) Artículo 321 de la Ley penal.
([37]) Artículo 3 de la LPPC. En principio, la Ley de tribunales militares regula la recogida de información sobre el personal militar y solo puede aplicarse a civiles en un número limitado de casos (por ejemplo, si el personal militar y los civiles cometen un delito conjuntamente o si una persona comete un delito contra el ejército, puede incoarse un procedimiento ante un tribunal militar, véase el artículo 2 de la Ley de tribunales militares). Las disposiciones generales que regulan los registros e incautaciones son similares a las de la LEC, véanse, por ejemplo, los artículos 146 a 149 y 153 a 156 de la Ley de tribunales militares. Por ejemplo, el correo postal solo podrá recogerse cuando sea necesario para una investigación y sobre la base de una orden de un tribunal militar. En la medida en que se recojan comunicaciones electrónicas, se aplicarán las limitaciones y salvaguardias de la LPPC.
([38]) Artículo 2, apartado 1, de la LPPC, es decir, «la transmisión o recepción de todo tipo de sonidos, palabras, símbolos o imágenes por cable, de manera inalámbrica, por cable de fibra u otro sistema electromagnético, en particular el teléfono, el correo electrónico, los servicios de información de afiliación, el fax y la radiobúsqueda».
([39]) Artículo 2, apartado 7, y artículo 3, apartado 2, de la LPPC.
([40]) Por «censura» se entiende «la apertura del correo sin el consentimiento de la parte afectada o la adquisición de conocimiento, la grabación o la retención de su contenido por otros medios» (artículo 2, apartado 6, de la LPPC). Por «escuchas telefónicas» se entiende «la adquisición o la grabación del contenido de las telecomunicaciones mediante escucha o lectura colectiva de sonidos, palabras, símbolos o imágenes de las comunicaciones a través de dispositivos electrónicos o mecánicos sin el consentimiento de la parte afectada o la interferencia con su transmisión y recepción» (artículo 2, apartado 7, de la LPPC).
([41]) Artículo 2, apartado 11, de la LPPC.

La LPPC establece las limitaciones y salvaguardias para la recogida de ambos tipos de datos, y el incumplimiento de varios de estos requisitos está sujeto a sanciones penales ([42]).

2.2.2.2. Limitaciones y salvaguardias aplicables a la recogida del contenido de las comunicaciones (medidas de restricción de la comunicación)

La recogida del contenido de las comunicaciones solo podrá tener lugar como medio complementario para facilitar una investigación penal (es decir, como medida de último recurso) y deberán hacerse esfuerzos para minimizar la interferencia con los secretos de las comunicaciones de las personas ([43]). En consonancia con este principio general, solo podrán aplicarse medidas de restricción de la comunicación cuando sea difícil impedir de otro modo la comisión de un delito, detener al delincuente o recabar las pruebas ([44]). Los organismos encargados de la aplicación de la ley que recojan el contenido de las comunicaciones deberán dejar de hacerlo inmediatamente una vez que el acceso continuo ya no se considere necesario, garantizando así que la vulneración de la privacidad de las comunicaciones sea lo más limitada posible ([45]).

Además, las medidas de restricción de la comunicación solo podrán utilizarse cuando existan razones fundadas para sospechar que se están planificando, se están cometiendo o se han cometido determinados delitos graves mencionados específicamente en la LPPC. Entre ellos se incluyen delitos como la insurrección, los delitos relacionados con las drogas o con explosivos, así como los relacionados con la seguridad nacional, las relaciones diplomáticas o las bases e instalaciones militares ([46]). El objeto de una medida de restricción de la comunicación deben ser envíos postales o telecomunicaciones específicos enviados o recibidos por el sospechoso, o envíos postales o telecomunicaciones enviados o recibidos por el sospechoso durante un período de tiempo determinado ([47]).

Incluso cuando se cumplan estos requisitos, la recogida de datos de contenido solo podrá llevarse a cabo sobre la base de una orden judicial. En particular, un fiscal puede pedir al órgano jurisdiccional que permita la recogida de datos de contenido relativos al sospechoso o a la persona investigada ([48]). Del mismo modo, un agente de la policía judicial podrá solicitar autorización a un fiscal, quien, a su vez, podrá solicitar una orden judicial ([49]). La solicitud de una orden deberá hacerse por escrito y contener elementos específicos. En particular, deberá presentar 1) las razones fundadas para sospechar que uno de los delitos listados está previsto, se está cometiendo o se ha cometido, así como cualquier material que demuestre que hay un caso de sospecha aparente; 2) las medidas de restricción de la comunicación, así como su objeto, alcance, objetivo y período efectivo; y 3) el lugar en el que se ejecutarían las medidas y cómo se llevarían a cabo ([50]).

Cuando se cumplan los requisitos legales, el órgano jurisdiccional podrá autorizar por escrito la aplicación de medidas de restricción de la comunicación con respecto al sospechoso o a la persona investigada ([51]). Esta orden especificará los tipos de medidas, así como su objeto, alcance, período efectivo, lugar de ejecución y la manera en que deben llevarse a cabo ([52]).

Las medidas de restricción de la comunicación solo podrán llevarse a cabo durante un período de dos meses ([53]). Si el objetivo de las medidas se alcanza antes dentro de ese período, las medidas deben interrumpirse de inmediato. Por el contrario, si se siguen cumpliendo las condiciones necesarias, podrá presentarse una solicitud para prorrogar el período efectivo de las medidas de restricción de la comunicación dentro del plazo de dos meses. Dicha solicitud deberá contener materiales que justifiquen *prima facie* la prórroga de las medidas ([54]). El período prolongado no podrá superar un total de un año, o de tres años en el caso de determinados delitos especialmente graves (por ejemplo, delitos relacionados con la insurrección, agresiones extranjeras, la seguridad nacional, etc.) ([55]).

Los cuerpos y fuerzas de seguridad podrán exigir la asistencia de los operadores de comunicaciones proporcionándoles la autorización escrita del tribunal ([56]). Los operadores de comunicaciones deberán cooperar y conservar la autorización recibida en sus archivos ([57]). Podrán negarse a cooperar cuando la información sobre la persona en cuestión indicada en la autorización escrita del tribunal (por ejemplo, el número de teléfono de la persona) sea incorrecta. Además, tienen prohibido, en cualquier circunstancia, revelar las contraseñas utilizadas para las telecomunicaciones ([58]).

([42]) Artículos 16 y 17 de la LPPC. Esto se aplica, por ejemplo, a la recogida sin una orden, a la falta de mantenimiento de registros, a la no interrupción de la recogida cuando deja de existir una emergencia o a la falta de notificación al particular de que se trate.
([43]) Artículo 3, apartado 2, de la LPPC.
([44]) Artículo 5, apartado 1, de la LPPC.
([45]) Artículo 2 del Decreto de Ejecución de la LPPC.
([46]) Artículo 5, apartado 1, de la LPPC.
([47]) Artículo 5, apartado 2, de la LPPC.
([48]) Artículo 6, apartado 1, de la LPPC.
([49]) Artículo 6, apartado 2, de la LPPC.
([50]) Artículo 6, apartado 4, de la LPPC y artículo 4, apartado 1, del Decreto de Ejecución de la LPPC.
([51]) Artículo 6, apartado 5, y artículo 6, apartado 8, de la LPPC.
([52]) Artículo 6, apartado 6, de la LPPC.
([53]) Artículo 6, apartado 7, de la LPPC.
([54]) Artículo 6, apartado 7, de la LPPC.
([55]) Artículo 6, apartado 8, de la LPPC.
([56]) Artículo 9, apartado 2, de la LPPC.
([57]) Artículo 15-2 de la LPPC y artículo 12 del Decreto de Ejecución de la LPPC.
([58]) Artículo 9, apartado 4, de la LPPC.

Toda persona que ejecute medidas de restricción de la comunicación o a quien se le solicite cooperar deberá llevar registros en los que se especifiquen los objetivos de las medidas, su ejecución, la fecha en que se prestó la cooperación y el objeto ([59]). Las autoridades encargadas de garantizar el cumplimiento de la ley que apliquen medidas de restricción de la comunicación también deberán mantener registros en los que se expongan los detalles y los resultados obtenidos ([60]). Los agentes de la policía judicial deberán facilitar al fiscal esta información mediante un informe cuando cierren una investigación ([61]).

Cuando un fiscal formule una acusación con respecto a un asunto en el que se hayan utilizado medidas de restricción de la comunicación o adopte una disposición de no acusar o detener al particular en cuestión (es decir, no solo una suspensión del enjuiciamiento), el fiscal deberá notificar al particular sujeto a las medidas de restricción de la comunicación el hecho de que se han ejecutado tales medidas, el organismo de ejecución y el período de ejecución. Dicha notificación deberá presentarse por escrito en un plazo de treinta días a partir de la disposición ([62]). La notificación podrá aplazarse cuando pueda poner en grave peligro la seguridad nacional o perturbar la seguridad y el orden públicos, o cuando pueda atentar gravemente contra la vida y la integridad física de terceros ([63]). Cuando se tenga intención de aplazar la notificación, el fiscal o el agente de la policía judicial deberán obtener la aprobación del jefe de la Fiscalía de distrito ([64]). Una vez que dejen de existir los motivos para el aplazamiento, esto deberá notificarse en un plazo de treinta días a partir de ese momento ([65]).

La LPPC también establece un procedimiento específico para la recogida del contenido de las comunicaciones en situaciones de emergencia. En particular, los organismos encargados de la aplicación de la ley podrán recoger el contenido de las comunicaciones en caso de que sea inminente la planificación o ejecución de delincuencia organizada u otro delito grave que pueda causar directamente la muerte o lesiones graves, y exista una emergencia que impida seguir el procedimiento ordinario (tal como se ha indicado anteriormente) ([66]). En tal situación de emergencia, el agente de policía o el fiscal podrán adoptar medidas de restricción de la comunicación sin previa autorización judicial, pero deberán solicitar dicha autorización inmediatamente después de la ejecución. Si el organismo encargado de la aplicación de la ley no obtiene la autorización judicial en un plazo de treinta y seis horas a partir del momento en que se llevaron a cabo las medidas de emergencia, la recogida deberá interrumpirse de inmediato, y esto normalmente irá seguido de la destrucción de la información recogida ([67]). Los agentes de policía que lleven a cabo una vigilancia de emergencia lo harán bajo el control de un fiscal o, si resultase imposible recibir las instrucciones del fiscal por adelantado debido a la necesidad de actuar con urgencia, la policía deberá obtener la autorización de un fiscal inmediatamente después de comenzar la ejecución ([68]). Las normas sobre la notificación al particular descritas anteriormente también se aplican a la recogida del contenido de las comunicaciones en situaciones de emergencia.

La recogida de información en situaciones de emergencia deberá realizarse siempre de conformidad con una «declaración de censura/escuchas telefónicas de emergencia» y la autoridad que lleve a cabo la recogida deberá mantener un registro de toda medida de emergencia ([69]). La solicitud a un órgano jurisdiccional de que autorice las medidas de emergencia deberá ir acompañada de un documento escrito en el que se indiquen las medidas necesarias de restricción de la comunicación, el objetivo, el objeto, el alcance, el período, el lugar de ejecución, el método y una explicación de la manera en que las medidas pertinentes de restricción de la comunicación cumplen el artículo 5, apartado 1, de la LPPC ([70]), junto con los documentos justificativos.

En los casos en que las medidas de emergencia se completen en poco tiempo, descartando así la autorización judicial (por ejemplo, si el sospechoso es detenido inmediatamente después de iniciar la interceptación, que, por consiguiente, se interrumpe), el jefe de la Fiscalía competente enviará una notificación de las medidas de emergencia al órgano jurisdiccional competente ([71]). La notificación deberá indicar el objetivo, el objeto, el alcance, el período, el lugar de ejecución y el método de recogida, así como los motivos para no presentar una solicitud de autorización judicial ([72]). Esta notificación permite al órgano jurisdiccional receptor examinar la legalidad de la recogida y deberá introducirse en un registro de notificaciones de medidas de emergencia.

([59]) Artículo 9, apartado 3, de la LPPC.
([60]) Artículo 18, apartado 1, del Decreto de Ejecución de la LPPC.
([61]) Artículo 18, apartado 2, del Decreto de Ejecución de la LPPC.
([62]) Artículo 9-2, apartado 1, de la LPPC.
([63]) Artículo 9-2, apartado 4, de la LPPC.
([64]) Artículo 9-2, apartado 5, de la LPPC.
([65]) Artículo 9-2, apartado 6, de la LPPC.
([66]) Artículo 8, apartado 1, de la LPPC.
([67]) Artículo 8, apartado 2, de la LPPC.
([68]) Artículo 8, apartado 3, de la LPPC y artículo 16, apartado 3, del Decreto de Ejecución de la LPPC.
([69]) Artículo 8, apartado 4, de la LPPC.
([70]) Es decir, que existe una razón fundada para sospechar que se están planificando o cometiendo determinados delitos graves, o que se han cometido, y que es impracticable impedir de otro modo la comisión de un delito, detener al delincuente o recabar pruebas.
([71]) Artículo 8, apartado 5, de la LPPC.
([72]) Artículo 8, apartados 6 y 7, de la LPPC.

Como requisito general, el contenido de las comunicaciones adquiridas mediante la aplicación de medidas de restricción de la comunicación sobre la base de la LPPC solo podrá utilizarse para investigar, enjuiciar o prevenir los delitos específicos mencionados anteriormente, en procedimientos disciplinarios por los mismos delitos, una reclamación por daños y perjuicios presentada por una parte de las comunicaciones o cuando así lo permitan otras leyes ([73]).

Cuando se recojan telecomunicaciones transmitidas por internet, se aplicarán salvaguardias específicas ([74]). Dicha información solo podrá utilizarse para investigar los delitos graves mencionados en el artículo 5, apartado 1, de la LPPC. Para conservar la información, deberá obtenerse la autorización del órgano jurisdiccional que autorizó las medidas de restricción de la comunicación ([75]). Las solicitudes de conservación deberán contener información sobre las medidas de restricción de la comunicación, un resumen de los resultados de las medidas, los motivos de la conservación (junto con materiales de apoyo) y las telecomunicaciones por conservar ([76]). A falta de tal solicitud, las telecomunicaciones adquiridas deberán suprimirse en un plazo de catorce días a partir de la finalización de las medidas de restricción de la comunicación ([77]). Si se rechaza una solicitud, las telecomunicaciones deberán destruirse en un plazo de siete días ([78]). Cuando se supriman las telecomunicaciones, deberá presentarse un informe en un plazo de siete días ante el órgano jurisdiccional que autorizó las medidas de restricción de la comunicación, indicando los motivos de la supresión, así como los detalles y el momento en que se realizó.

De manera más general, si la información se obtuvo de manera ilícita a través de medidas de restricción de la comunicación, no se admitirá como prueba en procedimientos judiciales o disciplinarios ([79]). Asimismo, la LPPC prohíbe a toda persona que adopte medidas de restricción de la comunicación divulgar información confidencial obtenida durante la aplicación de tales medidas y utilizar la información obtenida para dañar la reputación de las personas sujetas a las medidas ([80]).

2.2.2.3. Limitaciones y salvaguardias aplicables a la recogida de información de confirmación de la comunicación

Sobre la base de la LPPC, las autoridades encargadas de garantizar el cumplimiento de la ley podrán solicitar a los operadores de telecomunicaciones que faciliten datos de confirmación de la comunicación cuando sea necesario para llevar a cabo una investigación o ejecutar una pena ([81]). A diferencia de la recogida de datos de contenido, la posibilidad de recoger datos de confirmación de la comunicación no se limita a determinados delitos específicos. Sin embargo, como ocurre con los datos de contenido, la recogida de los datos de confirmación de la comunicación requiere la previa autorización escrita de un órgano jurisdiccional, con sujeción a las mismas condiciones descritas anteriormente ([82]). Cuando por motivos de urgencia resulte imposible obtener la autorización judicial, los datos de confirmación de la comunicación podrán recogerse sin una orden, en cuyo caso deberá obtenerse la autorización inmediatamente después de solicitar los datos y deberá comunicarse al proveedor de telecomunicaciones ([83]). Si no se obtiene una autorización posterior, la información recogida deberá destruirse ([84]).

Los fiscales, los agentes de la policía judicial y los órganos jurisdiccionales deberán mantener registros de las solicitudes de datos de confirmación de la comunicación ([85]). Además, los proveedores de telecomunicaciones deberán informar al Ministerio de Ciencia y TIC sobre la divulgación de datos de confirmación de la comunicación dos veces al año y mantener registros al respecto durante siete años a partir de la fecha en que se hayan divulgado los datos ([86]).

En principio, los particulares serán notificados del hecho de que se han recogido datos de confirmación de la comunicación ([87]). El momento para realizar dicha notificación dependerá de las circunstancias de la investigación ([88]). Una vez que se haya tomado una decisión de (no) enjuiciar, la notificación deberá enviarse en un plazo de treinta días. Por el contrario, en caso de suspensión de la acusación, la notificación deberá enviarse en el plazo de treinta días transcurrido un año desde que se haya adoptado tal decisión. En cualquier caso, la notificación deberá enviarse en un plazo de treinta días transcurrido un año desde la recogida de la información.

La notificación podrá aplazarse si puede 1) poner en peligro la seguridad nacional y la seguridad y el orden públicos, 2) causar la muerte o lesiones corporales, 3) impedir un procedimiento judicial justo (por ejemplo, dar lugar a la destrucción de pruebas o a amenazas a los testigos) o 4) difamar al sospechoso, a las víctimas o a otras personas

([73]) Artículo 12 de la LPPC.
([74]) Artículo 12-2 de la LPPC.
([75]) El fiscal o el agente de policía que ejecute las medidas de restricción de la comunicación deberá seleccionar las telecomunicaciones por conservar en un plazo de catorce días a partir de la finalización de las medidas y solicitar una autorización judicial (en el caso de un agente de policía, la solicitud deberá presentarse a un fiscal, quien, a su vez, presentará la solicitud al órgano jurisdiccional), véase el artículo 12-2, apartados 1 y 2, de la LPPC.
([76]) Artículo 12-2, apartado 3, de la LPPC.
([77]) Artículo 12-2, apartado 5, de la LPPC.
([78]) Artículo 12-2, apartado 5, de la LPPC.
([79]) Artículo 4 de la LPPC.
([80]) Artículo 11, apartado 2, del Decreto de Ejecución de la LPPC.
([81]) Artículo 13, apartado 1, de la LPPC.
([82]) Artículos 13 y 6 de la LPPC.
([83]) Artículo 13, apartado 2, de la LPPC. Al igual que en el caso de las medidas urgentes de restricción de la comunicación, deberá elaborarse un documento en el que se expongan los detalles del caso (el sospechoso, las medidas por adoptar, el presunto delito y la urgencia). Véase el artículo 37, apartado 5, del Decreto de Ejecución de la LPPC.
([84]) Artículo 13, apartado 3, de la LPPC.
([85]) Artículo 13, apartados 5 y 6, de la LPPC.
([86]) Artículo 13, apartado 7, de la LPPC.
([87]) Véase el artículo 13-3, apartado 7, en relación con el artículo 9-2 de la LPPC.
([88]) Artículo 13-3, apartado 1, de la LPPC.

relacionadas con el asunto o invadir su privacidad ([89]). El aplazamiento de la notificación por alguno de los motivos mencionados requiere la autorización del director de una fiscalía de distrito competente ([90]). Cuando dejen de existir los motivos para el aplazamiento, esto deberá notificarse en un plazo de treinta días a partir de ese momento ([91]).

Las personas notificadas podrán presentar una solicitud por escrito al fiscal o al agente de la policía judicial en relación con los motivos de la recogida de los datos de confirmación de la comunicación ([92]). En tal caso, el fiscal o el agente de la policía judicial deberán exponer los motivos por escrito en un plazo de treinta días a partir de la recepción de la solicitud, a menos que se aplique uno de los motivos mencionados anteriormente (excepciones para el aplazamiento de la notificación) ([93]).

2.2.3. *Divulgación voluntaria por parte de los operadores de telecomunicaciones*

El artículo 83, apartado 3, de la LST permite a los operadores de telecomunicaciones acceder voluntariamente a una solicitud (formulada en apoyo de un proceso penal, una investigación o la ejecución de una pena) de un órgano jurisdiccional, un fiscal o el jefe de un órgano de investigación de divulgar «datos de comunicaciones». En el contexto de la LST, los «datos de comunicaciones» abarcan el nombre, el número de registro de residente, la dirección y el número de teléfono de los usuarios, las fechas de suscripción o cancelación de la suscripción de los usuarios, así como los códigos de identificación de los usuarios (es decir, los códigos utilizados para identificar al usuario legítimo de sistemas informáticos o redes de comunicación) ([94]). A efectos de la LST, solo se consideran usuarios los particulares que contraten servicios directamente de un proveedor de telecomunicaciones coreano ([95]). En consecuencia, es probable que las situaciones en que los ciudadanos de la UE cuyos datos se hayan transferido a la República de Corea se consideren usuarios con arreglo a la LST sean muy limitadas, ya que estas personas normalmente no celebran un contrato directo con un operador de telecomunicaciones coreano.

Las solicitudes para obtener datos de comunicaciones sobre la base de la LST deberán hacerse por escrito e indicar los motivos de la solicitud, el vínculo con el usuario pertinente y el alcance de los datos solicitados ([96]). Cuando sea imposible presentar una solicitud por escrito debido a la urgencia, la solicitud escrita deberá presentarse tan pronto como desaparezca el motivo de la urgencia ([97]). Los operadores de telecomunicaciones que accedan a solicitudes de divulgación de datos de comunicaciones deberán conservar libros que contengan registros que indiquen que se han facilitado datos de comunicaciones, así como los materiales relacionados, tales como la solicitud escrita ([98]). Además, los operadores de telecomunicaciones deberán informar al ministro de Ciencia y TIC sobre el suministro de datos de comunicaciones dos veces al año ([99]).

Los operadores de telecomunicaciones no están obligados a acceder a las solicitudes de divulgación de datos de comunicaciones en virtud de la LST. Por tanto, el operador deberá evaluar cada solicitud a la luz de los requisitos aplicables de protección de datos con arreglo a la LPIP. En particular, un operador de telecomunicaciones deberá tener en cuenta los intereses del interesado y no podrá divulgar la información si es probable que vulnere deslealmente los intereses de la persona o de un tercero ([100]). Además, de conformidad con la Nota n.º 2021-1 sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, la persona afectada deberá ser informada de la divulgación. En situaciones excepcionales, esta notificación podrá retrasarse, en particular siempre y cuando la notificación ponga en peligro una investigación penal en curso o pueda atentar contra la vida o la integridad física de un tercero, en el caso de que esos derechos o intereses sean manifiestamente superiores a los derechos del interesado ([101]).

En 2016, el Tribunal Supremo confirmó que el suministro voluntario de datos de comunicaciones por parte de los operadores de telecomunicaciones sin una orden, con arreglo a la LST, no vulnera, como tal, el derecho del usuario del servicio de telecomunicaciones a la autodeterminación en materia de información. Al mismo tiempo, el Tribunal aclaró que tal vulneración se produciría si resulta evidente que la agencia solicitante abusó de su autoridad para solicitar la divulgación de datos de comunicaciones, vulnerando así los intereses de la persona afectada o de un tercero ([102]). De manera más general, toda solicitud de divulgación voluntaria por parte de una autoridad encargada de garantizar el cumplimiento de la ley deberá respetar los principios de licitud, necesidad y proporcionalidad que se derivan de la Constitución coreana (artículo 12, apartado 1, y artículo 37, apartado 2).

([89]) Artículo 13-3, apartado 2, de la LPPC.
([90]) Artículo 13-3, apartado 3, de la LPPC.
([91]) Artículo 13-3, apartado 4, de la LPPC.
([92]) Artículo 13-3, apartado 5, de la LPPC.
([93]) Artículo 13-3, apartado 6, de la LPPC.
([94]) Artículo 83, apartado 3, de la LST.
([95]) Artículo 2, apartado 9, de la LST.
([96]) Artículo 83, apartado 4, de la LST.
([97]) Artículo 83, apartado 4, de la LST.
([98]) Artículo 83, apartado 5, de la LST.
([99]) Artículo 83, apartado 6, de la LST.
([100]) Artículo 18, apartado 2, de la LPIP.
([101]) Nota n.º 2021-1 de la CPIP sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, sección III, apartado 2, inciso iii).
([102]) Resolución n.º 2012Da105482 del Tribunal Supremo, de 10 de marzo de 2016.

2.3. **Supervisión**

La supervisión de las autoridades encargadas de garantizar el cumplimiento del Derecho penal se lleva a cabo a través de distintos mecanismos, tanto de manera interna como por órganos externos.

2.3.1. *Auditoría interna*

De conformidad con la Ley de auditorías del sector público, se anima a las autoridades públicas a crear un organismo de auditoría interna, que se encargue, entre otras cosas, de llevar a cabo el control de la legalidad ([103]). Debe garantizarse la independencia de los jefes de tales organismos de auditoría en la mayor medida posible ([104]). Más concretamente, son nombrados desde fuera de la autoridad competente (por ejemplo, antiguos jueces o profesores) por un período de dos a cinco años y solo pueden ser destituidos por razones justificadas (por ejemplo, cuando no puedan ejercer sus funciones debido a un trastorno mental o físico o cuando estén sujetos a medidas disciplinarias) ([105]). Del mismo modo, los auditores son nombrados sobre la base de las condiciones específicas establecidas en la Ley ([106]). Los informes de auditoría podrán incluir recomendaciones o solicitudes de compensación o corrección, así como amonestaciones y recomendaciones o solicitudes de medidas disciplinarias ([107]). Se notifican al jefe de la autoridad pública objeto de la auditoría, así como a la Comisión de Control e Inspección (véase la sección 2.3.2) en un plazo de sesenta días a partir de la finalización de la auditoría ([108]). La autoridad en cuestión deberá aplicar las medidas necesarias e informar de los resultados a la Comisión de Control e Inspección ([109]). Además, los resultados de las auditorías suelen ponerse a disposición del público ([110]). La negativa u obstrucción de una auditoría interna está sujeta a multas administrativas ([111]). En el ámbito de la aplicación del Derecho penal, para cumplir la legislación antes mencionada, la Agencia Nacional de Policía cuenta con un sistema de Inspecciones Generales para llevar a cabo auditorías internas, incluso con respecto a posibles vulneraciones de los derechos humanos ([112]).

2.3.2. *La Comisión de Control e Inspección*

La Comisión de Control e Inspección (en lo sucesivo, «CCI») podrá inspeccionar las actividades de las autoridades públicas y, sobre la base de dichas inspecciones, formular recomendaciones, solicitar medidas disciplinarias o presentar una denuncia penal ([113]). La CCI está establecida bajo la responsabilidad del presidente de la República de Corea, pero mantiene un estatuto independiente con respecto a sus funciones ([114]). Además, la Ley por la que se crea la CCI exige que se le conceda la máxima independencia en lo que respecta al nombramiento, la destitución y la organización de su personal, así como a la elaboración de su presupuesto ([115]). El presidente de la CCI es nombrado por el presidente de la República, con el consentimiento de la Asamblea Nacional ([116]). Los seis comisarios restantes son nombrados por el presidente de la República, previa recomendación del presidente de la CCI, para un mandato de cuatro años ([117]). Los comisarios (incluido el presidente de la CCI) deberán reunir las cualificaciones específicas establecidas por la ley ([118]) y solo podrán ser despedidos en caso de proceso de destitución, condena a prisión o incapacidad para ejercer sus funciones debido a una debilidad física o mental a largo plazo ([119]). Además, los comisarios tienen prohibido participar en actividades políticas y ocupar simultáneamente cargos en la Asamblea Nacional, organismos administrativos, organizaciones sujetas a auditoría e inspección por parte de la CCI o cualquier otro cargo remunerado ([120]).

La CCI lleva a cabo una auditoría general con una periodicidad anual, pero también puede realizar auditorías específicas sobre cuestiones de especial interés. La CCI podrá solicitar la presentación de documentos en el curso de una inspección, así como la asistencia de particulares ([121]). Como parte de una auditoría, la CCI examinará los

([103]) Artículos 3 y 5 de la Ley de auditorías del sector público.
([104]) Artículo 7 de la Ley de auditorías del sector público.
([105]) Artículos 8 a 11 de la Ley de auditorías del sector público.
([106]) Artículos 16 y siguientes de la Ley de auditorías del sector público.
([107]) Artículo 23, apartado 2, de la Ley de auditorías del sector público.
([108]) Artículo 23, apartado 1, de la Ley de auditorías del sector público.
([109]) Artículo 23, apartado 3, de la Ley de auditorías del sector público.
([110]) Artículo 26 de la Ley de auditorías del sector público.
([111]) Artículo 41 de la Ley de auditorías del sector público.
([112]) Véanse, en particular, las divisiones bajo la Dirección General de Auditoría e Inspección: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artículos 24 y 31 a 35 de la Ley de la Comisión de Control e Inspección (en lo sucesivo, «Ley CCI»).
([114]) Artículo 2, apartado 1, de la Ley CCI.
([115]) Artículo 2, apartado 2, de la Ley CCI.
([116]) Artículo 4, apartado 1, de la Ley CCI.
([117]) Artículo 5, apartado 1, y artículo 6 de la Ley CCI.
([118]) Por ejemplo, haber ejercido como juez, fiscal o abogado durante al menos diez años, haber trabajado como funcionario o profesor o haber ocupado un cargo más alto en una universidad durante al menos ocho años, o haber trabajado durante al menos diez años en una empresa cotizada o en una institución participada por el Gobierno (de los cuales al menos cinco años como director ejecutivo), véase el artículo 7 de la Ley CCI.
([119]) Artículo 8 de la Ley CCI.
([120]) Artículo 9 de la Ley CCI.
([121]) Véase, por ejemplo, el artículo 27 de la Ley CCI.

ingresos y gastos del Estado, pero también supervisará el cumplimiento general de las obligaciones de las autoridades y los funcionarios públicos con vistas a mejorar el funcionamiento de la administración pública ([122]). Por lo tanto, su supervisión irá más allá de los aspectos presupuestarios e incluirá asimismo un control de legalidad.

2.3.3. *La Asamblea Nacional*

La Asamblea Nacional podrá investigar e inspeccionar a las autoridades públicas ([123]). Durante una investigación o inspección, la Asamblea Nacional podrá solicitar la divulgación de documentos y exigir a la comparecencia de testigos ([124]). Toda persona que cometa falso testimonio durante una investigación de la Asamblea Nacional estará sujeta a sanciones penales (pena de prisión de hasta diez años) ([125]). El proceso y los resultados de las inspecciones podrán hacerse públicos ([126]). Si la Asamblea Nacional detecta actividades ilícitas o inadecuadas, podrá solicitar a la autoridad pública correspondiente que adopte medidas correctoras, incluidas la concesión de indemnizaciones, la adopción de medidas disciplinarias y la mejora de sus procedimientos internos ([127]). A raíz de tal solicitud, la autoridad deberá actuar sin demora e informar del resultado a la Asamblea Nacional ([128]).

2.3.4. *La Comisión de Protección de la Información Personal*

La Comisión de Protección de la Información Personal (en lo sucesivo, «CPIP») supervisa el tratamiento de la información personal por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal en consonancia con la LPIP. Además, según el artículo 7-8, apartados 3 y 4, y el artículo 7-9, apartado 5, de la LPIP, la supervisión de la CPIP abarca también las posibles infracciones de las normas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal, incluidas aquellas contenidas en las leyes específicas que regulan la recogida de pruebas (electrónicas) a efectos del cumplimiento del Derecho penal (véase la sección 2.2). Habida cuenta de los requisitos establecidos en el artículo 3, apartado 1, de la LPIP para la recogida lícita y leal de información personal, toda infracción de este tipo constituye una violación de la LPIP, lo cual permite a la CPIP llevar a cabo una investigación y adoptar medidas correctoras ([129]).

En el ejercicio de su función de supervisión, la CPIP tendrá acceso a toda la información pertinente ([130]). La CPIP podrá asesorar a las autoridades encargadas de garantizar el cumplimiento de la ley para mejorar el nivel de protección de la información personal de sus actividades de tratamiento, imponer medidas correctoras (por ejemplo, suspender el tratamiento de datos o adoptar las medidas necesarias para proteger la información personal) o recomendar a la autoridad que adopte medidas disciplinarias ([131]). Por último, se prevén sanciones penales para determinadas infracciones de la LPIP, tales como utilizar o divulgar información personal a terceros o tratar información sensible de manera ilícita ([132]). A este respecto, la CPIP podrá remitir el asunto al órgano de investigación competente (incluidos los fiscales) ([133]).

2.3.5. *La Comisión Nacional de Derechos Humanos*

La Comisión Nacional de Derechos Humanos (en lo sucesivo, «CNDH»), un organismo independiente encargado de proteger y promover los derechos fundamentales ([134]), tiene la facultad de investigar y subsanar las infracciones de los artículos 10 a 22 de la Constitución, que incluyen los derechos a la privacidad en general y a la privacidad de la correspondencia. La CNDH está formada por once comisarios, nombrados a propuesta de la Asamblea Nacional (cuatro), el presidente de la República (cuatro) y el jefe judicial del Tribunal Supremo (tres) ([135]). Para ser nombrado, un comisario debe 1) haber trabajado durante diez años, como mínimo, en una universidad o un instituto de investigación autorizado, al menos como profesor asociado; 2) haber ejercido como juez, fiscal o abogado durante al menos diez años; 3) haber participado en actividades de derechos humanos durante al menos diez años (por ejemplo, para una organización sin ánimo de lucro, una organización no gubernamental o una organización internacional); o 4) haber sido recomendado por grupos de la sociedad civil) ([136]). El presidente de la CNDH es nombrado por el presidente de la República entre los

([122]) Artículos 20 y 24 de la Ley CCI.
([123]) Artículo 128 de la Ley de la Asamblea Nacional y artículos 2, 3 y 15 de la Ley de inspección e investigación de la administración del Estado. Esto incluye las inspecciones anuales de los asuntos gubernamentales en su conjunto y las investigaciones de cuestiones específicas.
([124]) Artículo 10, apartado 1, de la Ley de inspección e investigación de la administración del Estado. Véanse también los artículos 128 y 129 de la Ley de la Asamblea Nacional.
([125]) Artículo 14 de la Ley sobre el testimonio, la evaluación, etc. ante la Asamblea Nacional.
([126]) Artículo 12-2 de la Ley de inspección e investigación de la administración del Estado.
([127]) Artículo 16, apartado 2, de la Ley de inspección e investigación de la administración del Estado.
([128]) Artículo 16, apartado 3, de la Ley de inspección e investigación de la administración del Estado.
([129]) Véase la Nota n.º 2021-1 de la CPIP sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal.
([130]) Artículo 63 de la LPIP.
([131]) Artículo 61, apartado 2; artículo 65, apartados 1 y 2, y artículo 64, apartado 4, de la LPIP.
([132]) Artículos 70 a 74 de la LPIP.
([133]) Artículo 65, apartado 1, de la LPIP.
([134]) Artículo 1 de la Ley de la Comisión Nacional de Derechos Humanos (en lo sucesivo, «Ley CNDH»).
([135]) Artículo 5, apartados 1 y 2, de la Ley CNDH.
([136]) Artículo 5, apartado 3, de la Ley CNDH.

comisarios y debe ser confirmado por la Asamblea Nacional ([137]). Los comisarios (incluido el presidente de la CNDH) son nombrados por un mandato renovable de tres años y solo pueden ser destituidos en caso de que sean condenados a prisión o ya no sean capaces de ejercer sus funciones debido a una debilidad física o mental prolongada (en cuyo caso, dos terceras partes de los comisarios deben estar de acuerdo con la destitución) ([138]). Los comisarios de la CNDH tienen prohibido ocupar un cargo simultáneo en la Asamblea Nacional, los consejos locales o cualquier Gobierno estatal o local (como funcionario público) ([139]).

La CNDH podrá iniciar una investigación por iniciativa propia o sobre la base de una petición de un particular. Como parte de su investigación, la CNDH podrá solicitar la presentación de los materiales pertinentes, llevar a cabo inspecciones y convocar personas para que testifiquen ([140]). Después de una investigación, la CNDH podrá formular recomendaciones para mejorar o corregir políticas y prácticas específicas, y podrá hacerlas públicas ([141]). Las autoridades públicas deberán informar a la CNDH de un plan para aplicar dichas recomendaciones en un plazo de noventa días a partir de su recepción ([142]). Además, en caso de no aplicar de las recomendaciones, la autoridad de que se trate deberá informar de ello a la Comisión ([143]). La CNDH podrá, a su vez, divulgar dicho incumplimiento a la Asamblea Nacional o hacerlo público. Las autoridades públicas generalmente cumplen las recomendaciones de la CNDH y tienen un fuerte incentivo para hacerlo, ya que su aplicación se ha examinado como parte de la evaluación general realizada por la Oficina de Coordinación de Políticas Gubernamentales, bajo la autoridad de la Oficina del Primer Ministro.

2.4. **Reparación individual**

2.4.1. *Mecanismos de reparación disponibles en virtud de la LPIP*

Los particulares podrán ejercer sus derechos de acceso, rectificación, supresión y suspensión en virtud de la LPIP con respecto a la información personal tratada por las autoridades encargadas de garantizar el cumplimiento del Derecho penal. El acceso podrá solicitarse directamente a la autoridad correspondiente o de manera indirecta a través de la CPIP ([144]). La autoridad competente podrá limitar o denegar el acceso únicamente cuando así lo disponga la ley, cuando sea probable que atente contra la vida o la integridad física de un tercero, o pueda dar lugar a una vulneración injustificada de los intereses patrimoniales y otros intereses de un tercero (es decir, cuando los intereses del tercero sean superiores a los intereses de la persona que presenta la solicitud) ([145]). Si se deniega una solicitud de acceso, la persona deberá ser informada de los motivos y de las vías de recurso ([146]). Del mismo modo, podrá denegarse una solicitud de rectificación o supresión cuando así lo prevean otras leyes, en cuyo caso deberá informarse a la persona de los motivos subyacentes y de la posibilidad de recurso ([147]).

En lo que respecta a la reparación, los particulares podrán presentar una reclamación ante la CPIP, incluso a través del Centro de atención telefónica sobre privacidad gestionado por la Agencia de Internet y Seguridad de Corea ([148]). Además, una persona podrá obtener una mediación a través del Comité de mediación de conflictos relacionados con la información personal ([149]). Estas vías de recurso están disponibles en caso de posibles infracciones tanto de las normas contenidas en las leyes específicas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal (sección 2.2) como de la LPIP. Además, los particulares podrán impugnar las decisiones o la inacción de la CPIP con arreglo a la Ley de lo contencioso-administrativo (véase la sección 2.4.3).

([137]) Artículo 5, apartado 5, de la Ley CNDH.
([138]) Artículo 7, apartado 1, y artículo 8 de la Ley CNDH.
([139]) Artículo 10 de la Ley CNDH.
([140]) Artículo 36 de la Ley CNDH. De conformidad con el artículo 36, apartado 7, de la Ley, puede rechazarse la presentación de materiales u objetos si esta perjudicara la confidencialidad del Estado y pudiera tener un efecto considerable sobre la seguridad del Estado o las relaciones diplomáticas o si constituyera un obstáculo importante para una investigación penal o un juicio en curso. En tales casos, la Comisión podrá solicitar información adicional al jefe del organismo pertinente (que deberá cumplir de buena fe) cuando sea necesario para revisar si la negativa a facilitar la información está justificada.
([141]) Artículo 25, apartado 1, de la Ley CNDH.
([142]) Artículo 25, apartado 3, de la Ley CNDH.
([143]) Artículo 25, apartado 4, de la Ley CNDH.
([144]) Artículo 35, apartado 2, de la LPIP.
([145]) Artículo 35, apartado 4, de la LPIP.
([146]) Artículo 42, apartado 2, del Decreto de Ejecución de la LPIP.
([147]) Artículo 36, apartados 1 y 2, de la LPIP y artículo 43, apartado 3, del Decreto de Ejecución de la LPIP.
([148]) Artículo 62 de la LPIP.
([149]) Artículos 40 a 50 de la LPIP y artículos 48-2 a 57 del Decreto de Ejecución de la LPIP.

2.4.2. *Reparación ante la Comisión Nacional de Derechos Humanos*

La CNDH tramita las reclamaciones de los particulares (tanto coreanos como extranjeros) relacionadas con vulneraciones de los derechos humanos cometidas por las autoridades públicas ([150]). No existe ningún requisito de legitimación para que los particulares presenten una reclamación ante la CNDH ([151]). En consecuencia, la CNDH tramitará una reclamación incluso cuando el particular de que se trate no pueda demostrar la existencia de un perjuicio en la fase de admisibilidad. Por lo tanto, en el contexto de la recogida de datos personales a efectos de control de la aplicación del Derecho penal, una persona no tendría que demostrar que las autoridades públicas coreanas han accedido efectivamente a su información personal para que la reclamación sea admisible ante la CNDH. Una persona también podrá solicitar que la reclamación se resuelva mediante mediación ([152]).

Para investigar una reclamación, la CNDH podrá hacer uso de sus facultades de investigación, incluso solicitando la presentación de materiales pertinentes, realizando inspecciones y citando a personas para que testifiquen ([153]). Si la investigación revela que se ha producido una infracción de la legislación correspondiente, la CNDH podrá recomendar la aplicación de soluciones o la rectificación o mejora de cualquier ley, institución, política o práctica pertinente ([154]). Las soluciones propuestas podrán incluir la mediación, el cese de la vulneración de los derechos humanos, la indemnización por daños y perjuicios y medidas para evitar que vuelvan a producirse infracciones idénticas o similares ([155]). En el caso de la recogida ilícita de información personal con arreglo a las normas aplicables, las medidas correctoras podrán incluir la supresión de tal información. Si se considera que es muy probable que la infracción esté en curso y que es probable que, si no se atiende, se producirían daños difíciles de reparar, la CNDH podrá adoptar medidas de ayuda urgente ([156]).

Si bien la CNDH no está facultada para obligar, sus decisiones (por ejemplo, la decisión de no continuar la investigación de una reclamación) ([157]) y recomendaciones pueden ser impugnadas ante los órganos jurisdiccionales coreanos con arreglo a la Ley de lo contencioso-administrativo (véase la sección 2.4.3 a continuación) ([158]). Además, si las conclusiones de la CNDH revelan que los datos personales fueron recogidos de manera ilícita por una autoridad pública, una persona podría recurrir ante los órganos jurisdiccionales coreanos contra dicha autoridad pública, por ejemplo, impugnando la recogida con arreglo a la Ley de lo contencioso-administrativo, presentando un recurso de inconstitucionalidad de conformidad con la Ley del Tribunal Constitucional o solicitando una indemnización por daños y perjuicios en virtud de la Ley de indemnización estatal (véase la sección 2.4.3 a continuación).

2.4.3. *Reparación judicial*

Los particulares podrán invocar las limitaciones y salvaguardias descritas en las secciones anteriores para obtener reparación ante los órganos jurisdiccionales coreanos a través de distintas vías.

En primer lugar, de conformidad con la LEC, la afectada persona y su abogado podrán estar presentes cuando se ejecute una orden de registro o incautación y, por consiguiente, podrán formular una objeción en el momento en que se ejecute la orden ([159]). Además, la LEC prevé un denominado mecanismo de «cuasi reclamación», que permite a los particulares solicitar al órgano jurisdiccional competente que cancele o modifique una disposición adoptada por un fiscal o un agente de policía en relación con una incautación ([160]). Esto permite a las personas impugnar las medidas adoptadas para ejecutar una orden de incautación.

([150]) Aunque el artículo 4 de la Ley CNDH hace referencia a los ciudadanos y extranjeros residentes en la República de Corea, el término «residente» refleja un concepto de jurisdicción y no de territorio. Por consiguiente, si las instituciones nacionales dentro de Corea vulneran los derechos fundamentales de un extranjero fuera de Corea, dicho particular puede presentar una denuncia ante la CNDH. Véase, por ejemplo, la pregunta correspondiente en la página de preguntas frecuentes de la CNDH, disponible en https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Este sería el caso si las autoridades públicas coreanas accedieran de manera ilícita a los datos personales de un extranjero transferidos a Corea.

([151]) En principio, la reclamación deberá presentarse en el plazo de un año a partir de la infracción, pero la CNDH podrá decidir, aun así, investigar una reclamación presentada después de ese plazo, siempre que no haya expirado el régimen de prescripción en virtud del Derecho penal o civil (artículo 32, apartado 1, punto 4, de la Ley CNDH).

([152]) Artículos 42 y siguientes de la Ley CNDH.

([153]) Artículos 36 y 37 de la Ley CNDH.

([154]) Artículo 44 de la Ley CNDH.

([155]) Artículo 42, apartado 4, de la Ley CNDH.

([156]) Artículo 48 de la Ley CNDH.

([157]) Por ejemplo, si excepcionalmente la CNDH no puede inspeccionar determinados materiales o instalaciones porque atañen a secretos de Estado que pueden tener un efecto considerable sobre la seguridad del Estado o las relaciones diplomáticas o cuando la inspección suponga un obstáculo importante para una investigación penal o un juicio en curso (véase la nota a pie de página n.º 166) y cuando esto impida que la CNDH lleve a cabo la investigación necesaria para evaluar el fondo de la petición recibida, informará a la persona de las razones por las que se desestimó la reclamación, de conformidad con el artículo 39 de la Ley CNDH. En este caso, el particular puede impugnar la decisión de la CNDH con arreglo a la Ley de lo contencioso-administrativo.

([158]) Véanse, por ejemplo, la Resolución 2007NU27259 del Tribunal Superior de Seúl, de 18 de abril de 2008, confirmada por la Resolución 2008Du7854 del Tribunal Supremo, de 9 de octubre de 2008; y la Resolución 2017NU69382 del Tribunal Superior de Seúl, de 2 de febrero de 2018.

([159]) Artículos 121 y 219 de la LEC.

([160]) Artículo 417 de la LEC, en relación con su artículo 414, apartado 2. Véase también la Resolución n.º 97Mo66 del Tribunal Supremo, de 29 de septiembre de 1997.

Además, los particulares pueden obtener una indemnización por daños y perjuicios ante los órganos jurisdiccionales coreanos. Sobre la base de la Ley de indemnización estatal, las personas podrán solicitar una indemnización por los daños y perjuicios causados por funcionarios públicos debido al ejercicio de sus funciones oficiales en violación de la ley ([161]). Las reclamaciones en virtud de la Ley de indemnización estatal podrán presentarse ante un «Consejo de indemnización» especializado o directamente ante los órganos jurisdiccionales coreanos ([162]). Si la víctima es extranjera, la Ley de indemnización estatal se aplicará siempre que su país de origen garantice igualmente la indemnización estatal para los nacionales coreanos ([163]). Según la jurisprudencia, esta condición se cumple si los requisitos para solicitar una indemnización en el otro país «no están significativamente desequilibrados entre Corea y el otro país» y «no son más estrictos, en general, que los determinados por Corea, sin que haya una diferencia importante y sustantiva» ([164]). La Ley civil regula la responsabilidad de indemnización del Estado, y, por consiguiente, la responsabilidad del Estado también abarca los daños no materiales (por ejemplo, el sufrimiento mental) ([165]).

Para las infracciones de las normas de protección de datos, se prevé una vía de recurso adicional en virtud de la LPIP. De conformidad con el artículo 39 de la LPIP, toda persona que sufra daños como resultado de una infracción de la LPIP o de una pérdida, un robo, una divulgación, una falsificación, una alteración o un daño de su información personal podrá obtener una indemnización por daños y perjuicios ante los órganos jurisdiccionales. No existe un requisito de reciprocidad similar al previsto en la Ley de indemnización estatal.

Además de la indemnización por daños y perjuicios, podrá obtenerse un recurso administrativo contra las acciones u omisiones de los organismos administrativos en virtud de la Ley de lo contencioso-administrativo. Cualquier persona podrá impugnar una disposición (por ejemplo, el ejercicio de poderes públicos, o la negativa a ejercerlos, en un asunto específico) o una omisión (el fracaso prolongado por parte de un organismo administrativo para adoptar una determinada disposición, contrariamente a la obligación legal de hacerlo), lo cual puede dar lugar a la revocación o modificación de una disposición ilícita, a un dictamen de nulidad (es decir, un dictamen de que la disposición no tiene efectos jurídicos o de su inexistencia en el ordenamiento jurídico) o a un dictamen de que una omisión es ilícita ([166]). Para poder impugnar una disposición administrativa, esta debe afectar directamente a los derechos y obligaciones civiles ([167]). Esto incluye las medidas para recoger datos personales, ya sea de manera directa (por ejemplo, interceptando comunicaciones) o mediante una solicitud de divulgación (por ejemplo, a un proveedor de servicios).

Las reclamaciones antes mencionadas podrán presentarse, en primer lugar, ante las comisiones de recursos administrativos establecidas en determinadas autoridades públicas (por ejemplo, el SNI o la CNDH) o ante la Comisión Central de Recursos Administrativos creada bajo los auspicios de la Comisión Anticorrupción y de Derechos Civiles ([168]). Tal recurso administrativo ofrece una vía alternativa más informal para impugnar una disposición u omisión de una autoridad pública. Sin embargo, una reclamación también podrá presentarse directamente ante los órganos jurisdiccionales coreanos, con arreglo a la Ley de lo contencioso-administrativo.

Las solicitudes de revocación o modificación de una disposición en virtud de la Ley de lo contencioso-administrativo podrán ser presentadas por cualquier persona que tenga un interés jurídico en solicitar la revocación o modificación o en que se restablezcan sus derechos mediante la revocación o modificación en caso de que la disposición deje de surtir efecto ([169]). Del mismo modo, los litigios para declarar la nulidad podrán ser iniciados por una persona que tenga un interés jurídico en dicha declaración, mientras que los litigios para declarar la ilegalidad de una omisión podrán ser iniciados por cualquier persona que haya presentado una solicitud de disposición y tenga un interés jurídico en solicitar que se declare la ilegalidad de la omisión ([170]). Según la jurisprudencia del Tribunal Supremo, «interés jurídico» se interpreta como un «interés jurídicamente protegido», es decir, un interés directo y específico protegido por las leyes y los reglamentos en los que se basan las disposiciones administrativas (es decir, no intereses generales, indirectos y abstractos del público) ([171]). Por consiguiente, las personas tendrán un interés jurídico en caso de cualquier vulneración de las limitaciones y salvaguardias con respecto a la recogida de sus datos personales a efectos de control de la aplicación del Derecho penal (en virtud de leyes específicas o de la LPIP). Una sentencia firme con arreglo a la Ley de lo contencioso-administrativo es vinculante para las partes ([172]).

Deberán presentarse una solicitud de revocación o modificación de una disposición y una solicitud de declaración de la ilegalidad de una omisión en un plazo de noventa días a partir de la fecha en que la persona tenga conocimiento de

([161]) Artículo 2, apartado 1, de la Ley de indemnización estatal.
([162]) Artículos 9 y 12 de la Ley de indemnización estatal. La Ley establece consejos de distrito (presididos por el fiscal adjunto de la fiscalía correspondiente), un consejo central (presidido por el viceministro de Justicia) y un consejo especial (presidido por el viceministro de Defensa Nacional y encargado de las reclamaciones de indemnización por daños y perjuicios causados por el personal militar o los empleados civiles del ejército). Las reclamaciones de indemnización son, en principio, tramitadas por los consejos de distrito, que, en determinadas circunstancias, deben remitir los asuntos al consejo central o especial, por ejemplo, si la indemnización supera un importe determinado o en caso de que un particular solicite una nueva deliberación. Todos los consejos están formados por miembros nombrados por el ministro de Justicia (por ejemplo, de entre los funcionarios públicos del Ministerio de Justicia, los agentes judiciales, los abogados y las personas con experiencia en materia de indemnización estatal) y están sujetos a normas específicas relativas a los conflictos de intereses (véase el artículo 7 del Decreto de Ejecución de la Ley de indemnización estatal).
([163]) Artículo 7 de la Ley de indemnización estatal.
([164]) Resolución n.º 2013Da208388 del Tribunal Supremo, de 11 de junio de 2015.
([165]) Véase el artículo 8 de la Ley de indemnización estatal, así como el artículo 751 de la Ley civil.
([166]) Artículos 2 y 4 de la Ley de lo contencioso-administrativo.
([167]) Resolución 98Du18435 del Tribunal Supremo, de 22 de octubre de 1999; Resolución 99Du1113 del Tribunal Supremo, de 8 de septiembre de 2000, y Resolución 2010Du3541 del Tribunal Supremo, de 27 de septiembre de 2012.
([168]) Artículo 6 de la Ley de recursos administrativos y artículo 18, apartado 1, de la Ley de lo contencioso-administrativo.
([169]) Artículo 12 de la Ley de lo contencioso-administrativo.
([170]) Artículos 35 y 36 de la Ley de lo contencioso-administrativo.
([171]) Resolución n.º 2006Du330 del Tribunal Supremo, de 26 de marzo de 2006.
([172]) Artículo 30, apartado 1, de la Ley de lo contencioso-administrativo.

la disposición u omisión y, en principio, a más tardar un año después de la fecha de emisión de la disposición o de que se haya producido la omisión, salvo que existan razones justificables ([173]). Según la jurisprudencia del Tribunal Supremo, el concepto de «razones justificables» debe interpretarse en sentido amplio y requiere evaluar si es socialmente aceptable permitir una reclamación tardía, a la luz de todas las circunstancias del asunto ([174]). Por ejemplo, esto incluye, entre otras cosas, los motivos de retraso de los que la parte afectada no puede ser considerada responsable (es decir, situaciones que escapan al control del reclamante, por ejemplo, cuando no se le ha notificado la recogida de sus datos personales) o de fuerza mayor (por ejemplo, una catástrofe natural o una guerra).

Por último, los particulares también podrán presentar un recurso de inconstitucionalidad ante el Tribunal Constitucional ([175]). Sobre la base de la Ley del Tribunal Constitucional, cualquier persona cuyos derechos fundamentales garantizados por la Constitución se vean vulnerados por el ejercicio o la falta de ejercicio del poder gubernamental (excluidas las sentencias de los órganos jurisdiccionales) podrá solicitar la adjudicación de un recurso de inconstitucionalidad. Si hay otras vías de recurso disponibles, estas deben agotarse primero. Según la jurisprudencia del Tribunal Constitucional, los extranjeros podrán interponer un recurso de inconstitucionalidad en la medida en que sus derechos fundamentales estén reconocidos por la Constitución coreana (véanse las explicaciones en la sección 1.1) ([176]). Los recursos de inconstitucionalidad deben presentarse en un plazo de noventa días a partir del momento en que el particular haya tenido conocimiento de la infracción, y en el plazo de un año a partir del momento en que se produjo. Dado que el procedimiento establecido en la Ley de lo contencioso-administrativo se aplica a los litigios en virtud de la Ley del Tribunal Constitucional ([177]), una reclamación seguirá siendo admisible si existen «razones justificables», interpretadas de acuerdo con la jurisprudencia del Tribunal Supremo descrita anteriormente.

Si primero hay que agotar otras vías de recurso, un recurso de inconstitucionalidad deberá interponerse en un plazo de treinta días a partir de la decisión final sobre dicho recurso ([178]). El Tribunal Constitucional podrá invalidar el ejercicio del poder gubernamental que provocó la infracción o confirmar que una determinada omisión es inconstitucional ([179]). En tal caso, la autoridad competente está obligada a adoptar medidas para dar cumplimiento a la resolución del Tribunal.

3. ACCESO DE LAS AUTORIDADES PÚBLICAS CON FINES DE SEGURIDAD NACIONAL

3.1. Autoridades públicas competentes en el ámbito de la seguridad nacional

La República de Corea cuenta con dos agencias de inteligencia especializadas: el SNI y el Comando de Apoyo a la Seguridad de la Defensa. Además, la policía y las fiscalías también pueden recoger información personal con fines de seguridad nacional.

El SNI se establece en virtud de la Ley del Servicio Nacional de Inteligencia (en lo sucesivo, «Ley SNI») y opera directamente bajo la jurisdicción y supervisión del presidente de la República ([180]). En particular, el SNI recoge, recopila y distribuye información sobre países extranjeros (y Corea del Norte) ([181]), inteligencia relacionada con la lucha contra el espionaje (incluido el espionaje militar e industrial), el terrorismo y las actividades de la delincuencia organizada internacional, inteligencia sobre determinados tipos de delitos dirigidos contra la seguridad pública y nacional (por ejemplo, la insurrección nacional y la agresión extranjera) e inteligencia relacionada con la tarea de garantizar la ciberseguridad y prevenir o contrarrestar los ciberataques y las amenazas ([182]). La Ley SNI, por la que se crea el SNI y se establecen sus funciones, también prevé principios generales que enmarcan todas sus actividades. Como principio general, el SNI debe mantener la neutralidad política y proteger la libertad y los derechos de las personas ([183]). El presidente del SNI se encarga de desarrollar directrices generales que establezcan los principios, el alcance y los procedimientos para el desempeño de las funciones del SNI en relación con la recogida y el uso de información, y debe informar de ellas a la Asamblea Nacional ([184]). La Asamblea Nacional (a través de su Comité de Inteligencia) puede exigir que se corrijan o complementen las directrices si considera que son ilícitas o injustas. De manera más general, en el ejercicio de sus funciones, el director y el personal del SNI no pueden obligar a ninguna institución, organización o persona a hacer algo que no estén obligadas a hacer ni obstruir el ejercicio de los derechos de ninguna persona mediante el abuso de sus potestades públicas ([185]). Además, toda censura del correo, interceptación de las telecomunicaciones, recogida de información sobre la ubicación, recogida de datos de confirmación de la comunicación o grabación

([173]) Artículo 20 de la Ley de lo contencioso-administrativo. Este plazo también se aplica a las reclamaciones para declarar la ilegalidad de una omisión (véase el artículo 38, apartado 2, de la Ley de lo contencioso-administrativo).
([174]) Resolución n.º 90Nu6521 del Tribunal Supremo, de 28 de junio de 1991.
([175]) Artículo 68, apartado 1, de la Ley del Tribunal Constitucional.
([176]) Resolución n.º 99HeonMa194 del Tribunal Constitucional, de 29 de noviembre de 2001.
([177]) Artículo 40 de la Ley del Tribunal Constitucional.
([178]) Artículo 69 de la Ley del Tribunal Constitucional.
([179]) Artículo 75, apartado 3, de la Ley del Tribunal Constitucional.
([180]) Artículo 2 y artículo 4, apartado 2, de la Ley SNI.
([181]) Este concepto no abarca la información sobre las personas, sino la información general sobre países extranjeros (tendencias y evolución) y sobre las actividades de los agentes estatales de terceros países.
([182]) Artículo 3, apartado 1, de la Ley SNI.
([183]) Artículo 3, apartado 1; artículo 6, apartado 2, y artículos 11 y 21. Véanse también las normas sobre los conflictos de intereses, en particular los artículos 10 y 12.
([184]) Artículo 4, apartado 2, de la Ley SNI.
([185]) Artículo 13 de la Ley SNI.

o escucha de comunicaciones privadas por parte del SNI debe cumplir lo dispuesto en la LPPC, la Ley de información sobre la ubicación o la LEC ([186]). Todo abuso de poder o la recogida de información que infrinja estas leyes estarán sujetos a sanciones penales ([187]).

El Comando de Apoyo a la Seguridad de la Defensa es una agencia de inteligencia militar creada bajo los auspicios del Ministerio de Defensa. Es responsable de las cuestiones de seguridad dentro del ejército, de las investigaciones penales militares (sujetas a la Ley de tribunales militares) y la inteligencia militar. En general, el Comando de Apoyo a la Seguridad de la Defensa no lleva a cabo ninguna actividad de vigilancia de civiles, a menos que sea necesario para el desempeño de sus funciones militares. Las personas que pueden ser investigadas son el personal militar, los empleados civiles del ejército, las personas en formación militar, las personas en reserva militar o servicio de reclutamiento y los prisioneros de guerra ([188]). Al recoger información sobre las comunicaciones con fines de seguridad nacional, el Comando de Apoyo a la Seguridad de la Defensa está sujeto a las limitaciones y salvaguardias establecidas por la LLPC y su Decreto de Ejecución.

3.2. **Bases jurídicas y limitaciones**

La LPPC, la Ley antiterrorista para la protección de los ciudadanos y la seguridad pública (en lo sucesivo, «Ley antiterrorista») y la LST proporcionan bases jurídicas para la recogida de información personal con fines de seguridad nacional y establecen las limitaciones y salvaguardias aplicables ([189]). Estas limitaciones y salvaguardias, tal como se describen en las siguientes secciones, garantizan que la recogida y el tratamiento de la información se limiten a lo estrictamente necesario para alcanzar un objetivo legítimo. Queda excluida toda recogida masiva e indiscriminada de información personal con fines de seguridad nacional.

3.2.1. *Recogida de información sobre las comunicaciones*

3.2.1.1. Recogida de información sobre las comunicaciones por las agencias de inteligencia

3.2.1.1.1. Base jurídica

La LPPC faculta a las agencias de inteligencia para recoger datos de comunicaciones y exige a los proveedores de comunicaciones que cooperen con las solicitudes de dichas agencias ([190]). Como se describe en la sección 2.2.2.1, la LPPC distingue entre la recogida del contenido de las comunicaciones (es decir, «medidas de restricción de la comunicación», tales como las «escuchas telefónicas» o las medidas de «censura» ([191])) y la recogida de «datos de confirmación de la comunicación» ([192]).

El umbral para la recogida de estos dos tipos de información difiere, pero los procedimientos y salvaguardias aplicables son, en gran medida, idénticos ([193]). La recogida de datos de confirmación de la comunicación (o metadatos) puede realizarse con el fin de prevenir amenazas para la seguridad nacional ([194]). Se aplica un umbral más elevado para la ejecución de medidas de restricción de la comunicación (es decir, para recoger el contenido de las comunicaciones), que solo pueden adoptarse cuando se prevea que la seguridad nacional se ponga en grave peligro y la recogida de información sea necesaria para prevenir dicho peligro (es decir, si existe un riesgo grave para la seguridad nacional y la recogida es necesaria para prevenirlo) ([195]). Además, el acceso al contenido de las comunicaciones solo puede llevarse a cabo como medida de último recurso para garantizar la seguridad nacional, y deben hacerse esfuerzos para minimizar la vulneración de la privacidad de las comunicaciones ([196]). Incluso cuando se haya obtenido la aprobación o autorización adecuada, tales medidas deben interrumpirse de inmediato una vez que dejen de ser necesarias, garantizando así que cualquier violación de los secretos de las comunicaciones de la persona se limite al mínimo ([197]).

3.2.1.1.2. Limitaciones y salvaguardias aplicables a la recogida de información sobre las comunicaciones en las que participe al menos un nacional coreano

La recogida de información sobre las comunicaciones (tanto contenido como metadatos) cuando una o ambas personas que participan en la comunicación sean nacionales coreanos solo podrá tener lugar con la autorización de un jefe

([186]) Artículo 14 de la Ley SNI.
([187]) Artículos 22 y 23 de la Ley SNI.
([188]) Artículo 1 de la Ley de tribunales militares.
([189]) Al investigar delitos relacionados con la seguridad nacional, la policía y el SNI actuarán sobre la base de la LEC, mientras que el Comando de Apoyo a la Seguridad de la Defensa estará sujeto a la Ley de tribunales militares.
([190]) Artículo 15-2 de la LPPC.
([191]) Artículo 2, apartados 6 y 7, de la LPPC.
([192]) Artículo 2, apartado 11, de la LPPC.
([193]) Véanse también el artículo 13-4, apartado 2, de la LPPC y el artículo 37, apartado 4, del Decreto de Ejecución de la LPPC, que estipulan que los procedimientos aplicables a la recogida del contenido de las comunicaciones se aplicarán *mutatis mutandis* a la recogida de datos de confirmación de la comunicación.
([194]) Artículo 13-4 de la LPPC.
([195]) Artículo 7, apartado 1, de la LPPC.
([196]) Artículo 3, apartado 2, de la LPPC.
([197]) Artículo 2 del Decreto de Ejecución de la LPPC.

judicial del Tribunal Superior ([198]). La solicitud de la agencia de inteligencia deberá presentarse por escrito a un fiscal o a una Fiscalía Superior ([199]). Deberá indicar los motivos de la recogida (por ejemplo, que se prevé que la seguridad nacional se ponga en grave peligro o que la recogida es necesaria para prevenir amenazas para la seguridad nacional), junto con materiales que sustenten dichos motivos y que justifiquen la recogida a primera vista, así como los detalles de la solicitud (es decir, los objetivos, la persona o las personas específicas, el alcance, el período efectivo de la recogida, así como la manera y el lugar en que se realizará la recogida) ([200]). El fiscal o la Fiscalía Superior, a su vez, solicitarán la autorización de un jefe judicial del Tribunal Superior ([201]). El jefe judicial solo podrá conceder una autorización escrita cuando considere justificada la solicitud y la desestimará cuando la considere infundada ([202]). La orden especificará el tipo, el objetivo, el objeto, el alcance y el período efectivo de la recogida, así como el lugar y la manera en que podrá realizarse ([203]).

En el caso de que la medida esté destinada a la investigación de un acto de conspiración que amenace la seguridad nacional y exista una emergencia que impida seguir los procedimientos antes mencionados, se aplicarán normas específicas ([204]). Cuando se cumplan estas condiciones, las agencias de inteligencia podrán aplicar medidas de vigilancia sin previa autorización judicial ([205]). No obstante, inmediatamente después de la ejecución de las medidas de emergencia, la agencia de inteligencia deberá solicitar la autorización del órgano jurisdiccional. Si no se obtiene la autorización en un plazo de treinta y seis horas a partir del momento en que se adopten las medidas, estas deberán suspenderse inmediatamente ([206]). La recogida de información en situaciones de emergencia deberá realizarse siempre de conformidad con una «declaración de censura/escuchas telefónicas de emergencia» y la agencia de inteligencia que lleve a cabo la recogida deberá mantener un registro de toda medida de emergencia ([207]).

En los casos en que la vigilancia se complete en un breve plazo y se descarte la autorización judicial, el jefe de la Fiscalía Superior competente debe enviar una notificación de las medidas de emergencia preparada por la agencia de inteligencia al presidente del órgano jurisdiccional competente, que conserva el registro de las medidas de emergencia ([208]). Esto permite al órgano jurisdiccional examinar la legalidad de la recogida.

3.2.1.1.3. Limitaciones y salvaguardias aplicables a la recogida de información sobre las comunicaciones en las que participen únicamente nacionales no coreanos

Para recoger información sobre las comunicaciones exclusivamente entre nacionales no coreanos, las agencias de inteligencia deberán obtener una autorización previa por escrito del presidente ([209]). Estas comunicaciones solo se recogerán con fines de seguridad nacional si entran en una de las diversas categorías mencionadas, es decir, las comunicaciones entre funcionarios del Gobierno u otras personas de países hostiles a la República de Corea, agencias extranjeras, grupos o nacionales sospechosos de participar en actividades anticoreanas ([210]) o miembros de grupos que operan en la península de Corea, pero, en la práctica, más allá de la soberanía de la República de Corea y de sus grupos centrales con sede en países extranjeros ([211]). En cambio, si una de las partes de una comunicación es un nacional coreano y la otra es un nacional extranjero, se requerirá una autorización judicial de conformidad con el procedimiento descrito en la sección 3.2.1.1.2.

El jefe de una agencia de inteligencia deberá presentar al director del SNI un plan de las medidas que se prevé adoptar ([212]). El director del SNI examinará si el plan es adecuado y, en caso afirmativo, lo someterá a la aprobación del presidente ([213]). La información que deberá incluirse en el plan será la misma que la requerida para solicitar una autorización judicial para recoger información de nacionales coreanos (tal como se ha descrito anteriormente) ([214]). En particular, deberá indicar los motivos de la recogida (por ejemplo, que se prevé que la seguridad nacional se ponga en grave peligro o que la recogida es necesaria para prevenir amenazas para la seguridad nacional) y los principales motivos de sospecha, junto con materiales que sustenten dichos motivos y que justifiquen la recogida a primera vista, así como

([198]) Artículo 7, apartado 1, punto 1, de la LPPC. El órgano jurisdiccional competente será el Tribunal Superior que tenga jurisdicción sobre el lugar del domicilio o de la sede de una o ambas partes sujetas a la vigilancia.
([199]) Artículo 7, apartado 3, del Decreto de Ejecución de la LPPC.
([200]) Artículo 7, apartado 3, y artículo 6, apartado 4, de la LPPC.
([201]) Artículo 7, apartado 4, del Decreto de Ejecución de la LPPC. La solicitud del fiscal al órgano jurisdiccional deberá exponer los principales motivos de sospecha y, en la medida en que se soliciten varias autorizaciones al mismo tiempo, su justificación (véase el artículo 4 del Decreto de Ejecución de la LPPC).
([202]) Artículo 7, apartado 3, y artículo 6, apartados 5 y 9, de la LPPC.
([203]) Artículo 7, apartado 3, y artículo 6, apartado 6, de la LPPC.
([204]) Artículo 8 de la LPPC.
([205]) Artículo 8, apartado 1, de la LPPC.
([206]) Artículo 8, apartado 2, de la LPPC.
([207]) Artículo 8, apartado 4, de la LPPC. Véase la sección 2.2.2.2. para más información sobre las medidas de emergencia en el contexto de la aplicación de la ley.
([208]) Artículo 8, apartados 5 y 7, de la LPPC. En esta notificación deben indicarse el objetivo, el objeto, el alcance, el período, el lugar de ejecución y el método de vigilancia, así como los motivos para no presentar una solicitud antes de adoptar la medida (artículo 8, apartado 6, de la LPPC).
([209]) Artículo 7, apartado 1, punto 2, de la LPPC.
([210]) Esto se refiere a actividades que amenazan la existencia y la seguridad de la nación, el orden democrático o la supervivencia y la libertad de la población.
([211]) Además, si una de las partes es una persona descrita en el artículo 7, apartado 1, punto 2, de la LPPC y la otra se desconoce o no puede especificarse, se aplicará el procedimiento establecido en el artículo 7, apartado 1, punto 2.
([212]) Artículo 8, apartado 1, del Decreto de Ejecución de la LPPC. El director del SNI es nombrado por el presidente previa confirmación del Parlamento (artículo 7 de la Ley SNI).
([213]) Artículo 8, apartado 2, del Decreto de Ejecución de la LPPC.
([214]) Artículo 8, apartado 3, del Decreto de Ejecución de la LPPC, en relación con el artículo 6, apartado 4, de la LPPC.

los detalles de la solicitud (es decir, los objetivos, la persona o las personas específicas, el alcance, el período efectivo de la recogida, así como la manera y el lugar en que se realizará la recogida). Cuando se soliciten varias autorizaciones al mismo tiempo, deberán indicarse la finalidad y los motivos ([215]).

En situaciones de emergencia ([216]), deberá obtenerse la autorización previa del ministro al que pertenezca la agencia de inteligencia competente. No obstante, en este caso, la agencia de inteligencia deberá solicitar la autorización del presidente inmediatamente después de que se hayan adoptado las medidas de emergencia. Si una agencia de inteligencia no obtiene la autorización en un plazo de treinta y seis horas a partir del momento en que se presenta la solicitud, la recogida deberá interrumpirse inmediatamente ([217]). En tales casos, la información recogida siempre se destruirá.

3.2.1.1.4. Limitaciones generales y salvaguardias

A la hora de solicitar la cooperación de entidades privadas, las agencias de inteligencia deberán facilitarles la orden judicial, la autorización presidencial o una copia de la portada de una declaración de censura de emergencia, que la entidad obligada deberá conservar en sus archivos ([218]). Las entidades a las que se solicite que divulguen información a las agencias de inteligencia sobre la base de la LPPC podrán negarse a hacerlo cuando la autorización o la declaración de censura de emergencia se refieran al identificador incorrecto (por ejemplo, un número de teléfono perteneciente a una persona distinta de la identificada). Además, en todos los casos, las contraseñas utilizadas para las comunicaciones no podrán divulgarse ([219]).

Las agencias de inteligencia podrán confiar la aplicación de medidas de restricción de la comunicación o la recogida de información de confirmación de la comunicación a una oficina de correos o a un proveedor de servicios de telecomunicaciones (según la definición de la Ley del sector de las telecomunicaciones) ([220]). Tanto la agencia de inteligencia correspondiente como el proveedor que reciba una solicitud de cooperación deberán mantener registros en los que se indique la finalidad de solicitar las medidas, la fecha de ejecución o cooperación y el objeto de las medidas (por ejemplo, correo, teléfono, correo electrónico) durante tres años ([221]). Los proveedores de servicios de telecomunicaciones que faciliten datos de confirmación de la comunicación deberán conservar información sobre la frecuencia de la recogida en sus archivos durante siete años e informar dos veces al año al Ministerio de Ciencia y TIC ([222]).

Las agencias de inteligencia deberán informar al director del SNI sobre la información que han recopilado y el resultado de la actividad de vigilancia ([223]). Por lo que se refiere a la recogida de datos de confirmación de la comunicación, deberán mantenerse registros de que se ha realizado una solicitud relativa a tales datos, así como de la propia solicitud escrita y de la institución que se ha amparado en ella ([224]).

La recogida tanto del contenido de las comunicaciones como de los datos de confirmación de la comunicación solo podrá durar un máximo de cuatro meses y, si el objetivo perseguido se alcanza entretanto, deberá interrumpirse de inmediato ([225]). Si persisten las condiciones de la autorización, el plazo podrá ampliarse hasta cuatro meses, con la autorización del órgano jurisdiccional o del presidente. La solicitud de autorización para prorrogar las medidas de vigilancia deberá presentarse por escrito, indicando los motivos por los que se solicita la prórroga y facilitando materiales de apoyo ([226]).

En función de la base jurídica para la recogida, suele notificarse a las personas cuando se recogen sus comunicaciones. En particular, independientemente de si la información recogida se refiere al contenido de las comunicaciones o a datos de confirmación de la comunicación, y con independencia de si la información se obtuvo mediante el procedimiento ordinario o en una situación de emergencia, el jefe de la agencia de inteligencia deberá informar por escrito a la persona afectada de la medida de vigilancia en un plazo de treinta días a partir de la fecha en que finalizó la vigilancia ([227]). La notificación debe incluir 1) el hecho de que se ha recogido la información, 2) el organismo de ejecución y 3) el período de ejecución. No obstante, si es probable que la notificación ponga en peligro la seguridad nacional o perjudique la vida

([215]) Artículo 8, apartado 3, y artículo 4 del Decreto de Ejecución de la LPPC.
([216]) Es decir, en los casos en que la medida esté destinada a un acto de conspiración que amenace la seguridad nacional, no haya tiempo suficiente para obtener la aprobación del presidente y la no adopción de medidas de emergencia pueda perjudicar a la seguridad nacional (artículo 8, apartado 8, de la LPPC).
([217]) Artículo 8, apartado 9, de la LPPC.
([218]) Artículo 9, apartado 2, de la LPPC y artículo 12 del Decreto de Ejecución de la LPPC.
([219]) Artículo 9, apartado 4, de la LPPC.
([220]) Artículo 13 del Decreto de Ejecución de la LPPC.
([221]) Artículo 9, apartado 3, de la LPPC y artículo 17, apartado 2, del Decreto de Ejecución de la LPPC. Este plazo no se aplica a los datos de confirmación de la comunicación (véase el artículo 39 del Decreto de Ejecución de la LPPC).
([222]) Artículo 13, apartado 7, de la LPPC y artículo 39 del Decreto de Ejecución de la LPPC.
([223]) Artículo 18, apartado 3, del Decreto de Ejecución de la LPPC.
([224]) Artículo 13, apartado 5, y artículo 13-4, apartado 3, de la LPPC.
([225]) Artículo 7, apartado 2, de la LPPC.
([226]) Artículo 7, apartado 2, de la LPPC y artículo 5 del Decreto de Ejecución de la LPPC.
([227]) Artículo 9-2, apartado 3, de la LPPC. De conformidad con el artículo 13-4 de la LPPC, esto se aplica tanto a la recogida del contenido de las comunicaciones como a los datos de confirmación de la comunicación.

y la seguridad física de las personas, la notificación podrá aplazarse ([228]). La notificación deberá realizarse en un plazo de treinta días una vez que dejen de existir los motivos para el aplazamiento ([229]).

Sin embargo, este requisito de notificación solo se aplicará a la recogida de información cuando al menos una de las partes sea un nacional coreano. Por consiguiente, solo se notificará a los nacionales no coreanos cuando se recojan sus comunicaciones con nacionales coreanos. Por lo tanto, no existe ningún requisito de notificación cuando se recogen comunicaciones exclusivamente entre nacionales no coreanos.

El contenido de cualquier comunicación y los datos de confirmación de la comunicación obtenidos a través de la vigilancia, sobre la base de la LPPC, solo podrán utilizarse 1) para la investigación, el enjuiciamiento o la prevención de determinados delitos, 2) para procedimientos disciplinarios, 3) para procedimientos judiciales cuando una parte relacionada con la comunicación se base en ellos para una reclamación por daños y perjuicios o 4) sobre la base de otras leyes ([230]).

3.2.1.2. Recogida de información sobre las comunicaciones por parte de la policía o los fiscales con fines de seguridad nacional

La policía o el fiscal podrán recoger información sobre las comunicaciones (tanto el contenido de las comunicaciones como los datos de confirmación de la comunicación) con fines de seguridad nacional en las mismas condiciones que se describen en la sección 3.2.1.1. Cuando se actúe en situaciones de emergencia ([231]), el procedimiento aplicable será el descrito anteriormente con respecto a la recogida del contenido de las comunicaciones a efectos de control de la aplicación de la ley en situaciones de emergencia (es decir, el artículo 8 de la LPPC).

3.2.2. *Recogida de información sobre sospechosos de terrorismo*

3.2.2.1. Base jurídica

La Ley antiterrorista faculta al director del SNI para recoger información sobre los sospechosos de terrorismo ([232]). El concepto de «sospechoso de terrorismo» se define como un miembro de un grupo terrorista ([233]), una persona que haya propagado un grupo terrorista (mediante la promoción y la difusión de ideas o tácticas de un grupo terrorista), recaudado o aportado fondos para el terrorismo ([234]) o participado en otras actividades de preparación, conspiración, propaganda o instigación del terrorismo, o una persona con respecto a la cual existan motivos fundados para sospechar que ha llevado a cabo tales actividades ([235]). Como regla general, todo funcionario público que aplique la Ley antiterrorista deberá respetar los derechos fundamentales consagrados en la Constitución coreana ([236]).

La Ley antiterrorista por sí sola no establece facultades, limitaciones y salvaguardias específicas para la recogida de información sobre los sospechosos de terrorismo, sino que hace referencia a los procedimientos establecidos en otras leyes. En primer lugar, sobre la base de la Ley antiterrorista, el director del SNI podrá recoger 1) información sobre la entrada en la República de Corea y la salida de esta, 2) información sobre transacciones financieras e 3) información sobre las comunicaciones. En función del tipo de información buscada, los requisitos procedimentales pertinentes se establecen en la Ley de inmigración, la Ley de aduanas, la LCUIETF o la LPPC, respectivamente ([237]). Para la recogida de información sobre la entrada y salida de Corea, la Ley antiterrorista hace referencia a los procedimientos establecidos en la Ley de inmigración y la Ley de aduanas. Sin embargo, actualmente estas leyes no prevén tales facultades. Para

([228]) Artículo 9-2, apartado 4, de la LPPC.
([229]) Artículo 13-4, apartado 2, y artículo 9-2, apartado 6, de la LPPC.
([230]) Artículo 5, apartados 1 y 2, y artículos 12 y 13-5 de la LPPC.
([231]) Es decir, cuando la medida esté destinada a un acto de conspiración que amenace la seguridad nacional y exista una emergencia que impida seguir el procedimiento de aprobación ordinario (artículo 8, apartado 1, de la LPPC).
([232]) Artículo 9 de la Ley antiterrorista.
([233]) El término «grupo terrorista» se define como un grupo de terroristas designado por las Naciones Unidas (artículo 2, apartado 2, de la Ley antiterrorista).
([234]) El término «terrorismo» se define en el artículo 2, apartado 1, de la Ley antiterrorista como una conducta llevada a cabo con el fin de impedir el ejercicio de la autoridad del Estado, de un Gobierno local o de un Gobierno extranjero (incluidos los Gobiernos locales y las organizaciones internacionales) o con el fin de hacer que realicen alguna actividad que no están obligados a realizar o de amenazar al público. Esto incluye a) matar a una persona o poner en riesgo la vida de una persona causando lesiones corporales o a través de la detención, el confinamiento, el secuestro o la toma de rehenes; b) determinados tipos de conducta dirigida a una aeronave (por ejemplo, chocar, secuestrar o dañar una aeronave en vuelo); c) determinados tipos de conducta relacionados con un buque (por ejemplo, incautar o destruir un buque o una estructura marina en funcionamiento o causar daños en los mismos en un grado tal que ponga en peligro su seguridad, incluidos los daños de la mercancía cargada en un buque o una estructura marina en funcionamiento); d) colocar, detonar o utilizar de cualquier otro modo armas o dispositivos bioquímicos, explosivos o incendiarios con la intención de causar la muerte, lesiones graves o daños materiales graves o tener tales efectos en determinados tipos de vehículos o instalaciones (por ejemplo, trenes, tranvías, vehículos de motor, parques y estaciones públicos, instalaciones de suministro de electricidad, gas y telecomunicaciones, etc.); e) determinados tipos de conducta relacionados con materiales nucleares o radiactivos o instalaciones nucleares (por ejemplo, atentar contra la vida humana, la integridad física o la propiedad individual, o perturbar de otro modo la seguridad pública destruyendo un reactor nuclear o manipulando indebidamente materiales radiactivos, etc.).
([235]) Artículo 2, apartado 3, de la Ley antiterrorista.
([236]) Artículo 3, apartado 3, de la Ley antiterrorista.
([237]) Artículo 9, apartado 1, de la Ley antiterrorista.

la recogida de información sobre las comunicaciones e información sobre transacciones financieras, la Ley antiterrorista hace referencia a las limitaciones y salvaguardias establecidas en la LPPC (que se detallan más adelante) y de la LCUIETF (que, como se explica en la sección 2.1, no es pertinente a efectos de la evaluación de la decisión de adecuación).

Además, el artículo 9, apartado 3, de la Ley antiterrorista especifica que el director del SNI podrá solicitar información personal o sobre la ubicación de un sospechoso de terrorismo a un responsable del tratamiento de información personal ([238]) o a un proveedor de información sobre la ubicación ([239]). Esta posibilidad se limita a las solicitudes de divulgación voluntaria, a las que los responsables del tratamiento de información personal y los proveedores de información sobre la ubicación no están obligados a responder y, en cualquier caso, solo pueden hacerlo de conformidad con la LPIP y la Ley de información sobre la ubicación (véase la sección 3.2.2.2).

3.2.2.2. Limitaciones y salvaguardias aplicables a la divulgación voluntaria en virtud de la LPIP y de la Ley de información sobre la ubicación

Las solicitudes de cooperación voluntaria en virtud de la Ley antiterrorista deberán limitarse a la información sobre los sospechosos de terrorismo (véase la sección 3.2.2.1). Cualquier solicitud de este tipo del SNI deberá cumplir los principios de licitud, necesidad y proporcionalidad que se derivan de la Constitución coreana (artículo 12, apartado 1, y artículo 37, apartado 2) ([240]), así como los requisitos de la LPIP para la recogida de información personal (artículo 3, apartado 1, de la LPIP, véase la sección 1.2). Además, la Ley SNI especifica que el SNI no podrá obligar a ninguna institución, organización o persona a hacer algo que no estén obligados a hacer ni obstruir el ejercicio de los derechos de ninguna persona, mediante el abuso de sus potestades públicas ([241]). Una infracción de esta prohibición podrá ser objeto de sanciones penales ([242]).

Los responsables del tratamiento de información personal y los proveedores de información sobre la ubicación que reciban solicitudes del SNI sobre la base de la Ley antiterrorista no estarán obligados a acceder a tales solicitudes. Podrán acceder de manera voluntaria, pero solo se les permitirá hacerlo de conformidad con la LPIP y la Ley de información sobre la ubicación. En lo que respecta al cumplimiento de la LPIP, el responsable del tratamiento deberá, en particular, tener en cuenta los intereses del interesado y no podrá divulgar la información si es probable que vulnere deslealmente los intereses de la persona o de un tercero ([243]). Además, de conformidad con la Nota n.º 2021-1 sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, la persona afectada deberá ser informada de la divulgación. En situaciones excepcionales, esta notificación podrá retrasarse, en particular siempre y cuando la notificación ponga en peligro una investigación penal en curso o pueda atentar contra la vida o la integridad física de un tercero, en el caso de que esos derechos o intereses sean manifiestamente superiores a los derechos del interesado ([244]).

3.2.2.3. Limitaciones y salvaguardias en virtud de la LPPC

Sobre la base de la Ley antiterrorista, las agencias de inteligencia solo podrán recoger información sobre las comunicaciones (tanto el contenido de las comunicaciones como los datos de confirmación de la comunicación) cuando sea necesario para actividades de lucha contra el terrorismo, es decir, actividades relacionadas con la prevención del terrorismo y contramedidas al respecto. Los procedimientos de la LPPC descritos en la sección 3.2.1 se aplicarán a la recogida de información sobre las comunicaciones con fines antiterroristas.

3.2.3. *Divulgación voluntaria por parte de los operadores de telecomunicaciones*

Sobre la base de la LST, los operadores de telecomunicaciones podrán acceder a una solicitud de divulgación de «datos de comunicaciones» de una agencia de inteligencia que tenga la intención de recoger la información para evitar una amenaza para la seguridad nacional ([245]). Cualquier solicitud de este tipo deberá cumplir los principios de licitud, necesidad y proporcionalidad que se derivan de la Constitución coreana (artículo 12, apartado 1, y artículo 37, apartado 2) ([246]), así como los requisitos de la LPIP para la recogida de información personal (artículo 3, apartado 1, de la LPIP, véase la sección 1.2). Además, se aplicarán las mismas limitaciones y salvaguardias que con respecto a la divulgación voluntaria a efectos de control de la aplicación de la ley (véase la sección 2.2.3) ([247]).

([238]) Tal como se define en el artículo 2 de la LPIP, es decir, una institución pública, una persona jurídica, una organización, un particular, etc. que trata información personal directa o indirectamente para gestionar ficheros información personal con fines oficiales o comerciales.

([239]) Tal como se define en el artículo 5 de la Ley sobre la protección, el uso, etc. de la información sobre la ubicación (en lo sucesivo, «Ley de información sobre la ubicación»), es decir, cualquier persona que haya obtenido autorización de la Comisión de Comunicaciones de Corea para participar en una empresa de información sobre la ubicación.

([240]) Véase también el artículo 3, apartados 2 y 3, de la Ley antiterrorista.

([241]) Artículo 11, apartado 1, de la Ley SNI.

([242]) Artículo 19 de la Ley SNI.

([243]) Artículo 18, apartado 2, de la LPIP.

([244]) Nota n.º 2021-1 de la CPIP sobre las normas complementarias para la interpretación y la aplicación de la Ley sobre la protección de la información personal, sección III, apartado 2, inciso iii).

([245]) Artículo 83, apartado 3, de la LST.

([246]) Véase también el artículo 3, apartados 2 y 3, de la Ley antiterrorista.

([247]) En particular, la solicitud deberá presentarse por escrito y exponer los motivos de la misma, así como el vínculo con el usuario de que se trate y el alcance de la información solicitada, y el proveedor de servicios de telecomunicaciones deberá mantener registros e informar al ministro de Ciencia y TIC dos veces al año.

Los operadores de telecomunicaciones no estarán obligados a acceder, pero podrán hacerlo de manera voluntaria y únicamente de conformidad con la LPIP. A este respecto, se aplicarán a los operadores de telecomunicaciones las mismas obligaciones, incluidas las relativas a la notificación de la persona, que cuando reciben solicitudes de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, como se explica con más detalle en la sección 2.2.3.

3.3. **Supervisión**

Diferentes organismos supervisan las actividades de las agencias de inteligencia coreanas. La supervisión del Comando de Apoyo a la Seguridad de la Defensa corre a cargo del Ministerio de Defensa Nacional, de conformidad con la Directiva sobre la ejecución de auditorías internas del Ministerio. El SNI está sujeto a la supervisión por parte del poder ejecutivo, la Asamblea Nacional y otros organismos independientes, como se explica con más detalle a continuación.

3.3.1. *El oficial de protección de los derechos humanos*

Cuando las agencias de inteligencia recogen información sobre sospechosos de terrorismo, la Ley antiterrorista prevé la supervisión por parte de la Comisión de Lucha contra el Terrorismo y del oficial de protección de los derechos humanos (en lo sucesivo, «OPDH») ([248]).

La Comisión de Lucha contra el Terrorismo, entre otras cosas, desarrolla políticas relativas a las actividades de lucha contra el terrorismo y supervisa la aplicación de medidas antiterroristas, así como las actividades de las distintas autoridades competentes en este ámbito ([249]). La Comisión está presidida por el primer ministro y está compuesta por varios ministros y jefes de organismos gubernamentales, incluidos los ministros de Asuntos Exteriores, de Justicia, de Defensa Nacional y del Interior y Seguridad, el director del SNI, el comisario general de la Agencia Nacional de Policía y el presidente de la Comisión de Servicios Financieros ([250]). Cuando se lleven a cabo investigaciones antiterroristas y se rastreen sospechosos de terrorismo para recabar la información o los materiales necesarios para las actividades de lucha contra el terrorismo, el director del SNI deberá informar al presidente de la Comisión de Lucha contra el Terrorismo (es decir, el primer ministro) ([251]).

Además, la Ley antiterrorista establece la figura del OPDH con el fin de proteger los derechos fundamentales de las personas contra las vulneraciones causadas por las actividades de lucha contra el terrorismo ([252]). El OPDH es nombrado por el presidente de la Comisión de Lucha contra el Terrorismo de entre las personas que reúnen las cualificaciones mencionadas en el Decreto de Ejecución de la Ley antiterrorista (es decir, cualquier persona cualificada como abogado con al menos diez años de experiencia laboral o con conocimientos especializados en el ámbito de los derechos humanos y que trabaje o haya trabajado, al menos, como profesor asociado durante al menos diez años o que haya ejercido como funcionario público de rango superior en agencias estatales o Gobiernos locales, o con al menos diez años de experiencia laboral en el ámbito de los derechos humanos, por ejemplo, en una organización no gubernamental) ([253]). El OPDH es nombrado por un período de dos años (con la posibilidad de renovar su mandato) y solo puede ser destituido por motivos específicos y limitados y por causa justificada, por ejemplo, cuando se le acuse en un proceso penal relacionado con sus funciones, cuando divulgue información confidencial o por incapacidad mental o física de larga duración ([254]).

En términos de competencias, el OPDH podrá formular recomendaciones para mejorar la protección de los derechos humanos por parte de las agencias que participen en actividades de lucha contra el terrorismo y tramitar peticiones civiles (véase la sección 3.4.3) ([255]). Cuando pueda establecerse razonablemente la existencia de una vulneración de los derechos humanos en el ejercicio de las funciones oficiales, el OPDH podrá recomendar al jefe de la agencia responsable que corrija dicha vulneración ([256]). A su vez, la agencia responsable deberá informar al OPDH de las medidas adoptadas para aplicar dicha recomendación ([257]). Si una agencia no aplicara una recomendación del OPDH, el asunto se elevaría a la Comisión, incluido su presidente, el primer ministro. Hasta la fecha, no ha habido casos en los que no se hayan aplicado las recomendaciones del OPDH.

3.3.2. *La Asamblea Nacional*

Como se describe en la sección 2.3.2, la Asamblea Nacional podrá investigar e inspeccionar a las autoridades públicas y, en ese contexto, solicitar la divulgación de documentos y exigir a la comparecencia de testigos. Con respecto a las cuestiones que son competencia del SNI, esta supervisión parlamentaria corre a cargo el Comité de Inteligencia de la Asamblea Nacional ([258]). El director del SNI, que supervisa el desempeño de las funciones

([248]) Artículo 7 de la Ley antiterrorista.
([249]) Artículo 5, apartado 3, de la Ley antiterrorista.
([250]) Artículo 3, apartado 1, del Decreto de Ejecución de la Ley antiterrorista.
([251]) Artículo 9, apartado 4, de la Ley antiterrorista.
([252]) Artículo 7 de la Ley antiterrorista.
([253]) Artículo 7, apartado 1, del Decreto de Ejecución de la Ley antiterrorista.
([254]) Artículo 7, apartado 3, del Decreto de Ejecución de la Ley antiterrorista.
([255]) Artículo 8, apartado 1, del Decreto de Ejecución de la Ley antiterrorista.
([256]) Artículo 9, apartado 1, del Decreto de Ejecución de la Ley antiterrorista. El OPDH decide de manera autónoma sobre la adopción de recomendaciones, pero debe informar de ellas al presidente de la Comisión de Lucha contra el Terrorismo.
([257]) Artículo 9, apartado 2, del Decreto de Ejecución de la Ley antiterrorista.
([258]) Artículo 36 y artículo 37, apartado 1, punto 16, de la Ley de la Asamblea Nacional.

de la agencia, informa al Comité de Inteligencia (así como al presidente) ([259]). El propio Comité de Inteligencia también podrá solicitar un informe sobre un asunto específico, y el director del SNI deberá responder sin demora ([260]). Solo podrá negarse a responder o testificar ante el Comité de Inteligencia con respecto a secretos de Estado relativos a cuestiones militares, diplomáticas o relacionadas con Corea del Norte, cuando el conocimiento público pueda tener graves consecuencias para el destino nacional ([261]). En este caso, el Comité de Inteligencia podrá solicitar una explicación al primer ministro. Si tal explicación no se presenta en el plazo de siete días a partir de la presentación de la solicitud, la respuesta o el testimonio ya no podrán denegarse.

Si la Asamblea Nacional comprueba que ha habido actividades ilícitas o inadecuadas, podrá solicitar a la autoridad pública correspondiente que adopte medidas correctoras, incluidas la concesión de indemnizaciones, la adopción de medidas disciplinarias y la mejora de sus procedimientos internos ([262]). A raíz de tal solicitud, la autoridad deberá actuar sin demora e informar del resultado a la Asamblea Nacional. Existen normas específicas relativas a la supervisión parlamentaria con respecto al uso de medidas de restricción de la comunicación (es decir, la recogida del contenido de las comunicaciones) con arreglo a la LPPC ([263]). Por lo que se refiere a esta última, la Asamblea Nacional podrá solicitar a los jefes de las agencias de inteligencia un informe sobre cualquier medida específica de restricción de la comunicación. Además, podrá llevar a cabo inspecciones *in situ* de los equipos de escuchas telefónicas. Por último, las agencias de inteligencia que hayan recogido y los operadores que hayan divulgado información sobre el contenido con fines de seguridad nacional deberán informar sobre dicha divulgación a petición de la Asamblea Nacional.

3.3.3. *La Comisión de Control e Inspección*

La CCI desempeña las mismas funciones de supervisión con respecto a las agencias de inteligencia que en el ámbito de la aplicación del Derecho penal (véase la sección 2.3.2) ([264]).

3.3.4. *La Comisión de Protección de la Información Personal*

Por lo que se refiere al tratamiento de datos con fines de seguridad nacional, incluida la fase de recogida, la CPIP llevará a cabo una supervisión adicional. Como se explica con más detalle en la sección 1.2, esto incluye los principios y obligaciones generales establecidos en los artículos 3 y 58, apartado 4, de la LPIP, así como el ejercicio de los derechos individuales garantizados por el artículo 4 de la LPIP. Además, según el artículo 7-8, apartados 3 y 4, y el artículo 7-9, apartado 5, de la LPIP, la supervisión de la CPIP también abarca las posibles infracciones de las normas contenidas en las leyes específicas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal, tales como la LPPC, la Ley antiterrorista y la LST. Habida cuenta de los requisitos establecidos en el artículo 3, apartado 1, de la LPIP para la recogida lícita y leal de información personal, toda infracción de dichas leyes constituye una violación de la LPIP. Por lo tanto, la CPIP tiene la facultad de investigar ([265]) las infracciones de las leyes que regulan el acceso a los datos con fines de seguridad nacional, así como de las normas de tratamiento establecidas en la LPIP, y de proporcionar asesoramiento para la mejora, imponer medidas correctoras, recomendar medidas disciplinarias y remitir posibles infracciones a las autoridades de investigación pertinentes ([266]).

3.3.5. *La Comisión Nacional de Derechos Humanos*

La supervisión por parte de la CNDH se aplica de la misma manera a las agencias de inteligencia que a otras autoridades gubernamentales (véase la sección 2.3.2).

3.4. **Reparación individual**

3.4.1. *Reparación ante el oficial de protección de los derechos humanos*

Por lo que se refiere a la recogida de información personal en el contexto de las actividades de lucha contra el terrorismo, el OPDH, establecido bajo los auspicios de la Comisión de Lucha contra el Terrorismo, ofrece una vía de recurso específica. El OPDH tramita las peticiones civiles relacionadas con la vulneración de los derechos humanos como consecuencia de las actividades de lucha contra el terrorismo ([267]). Podrá recomendar medidas correctoras y la agencia correspondiente deberá informar al Oficial de cualquier medida adoptada para aplicar dicha recomendación. No existe ningún requisito de legitimación para que los particulares presenten una reclamación ante el OPDH. En consecuencia, el OPDH tramitará una reclamación incluso cuando el particular de que se trate no pueda demostrar la existencia de un perjuicio en la fase de admisibilidad.

([259]) Artículo 18 de la Ley SNI.
([260]) Artículo 15, apartado 2, de la Ley SNI.
([261]) Artículo 17, apartado 2, de la Ley SNI. Los «secretos de Estado» se definen como «los hechos, bienes o conocimientos clasificados como secretos de Estado, cuyo acceso se permite a un número limitado de personas y que no se divulgarán a ningún otro país u organización, con el fin de evitar cualquier perjuicio grave para la seguridad nacional» (véase el artículo 13, apartado 4, de la Ley SNI).
([262]) Artículo 16, apartado 2, de la Ley de inspección e investigación de la administración del Estado.
([263]) Artículo 15 de la LPPC.
([264]) Al igual que en el caso del Comité de Inteligencia de la Asamblea Nacional, el director del SNI solo podrá negarse a responder a la CCI sobre cuestiones que constituyan secretos de Estado y si el conocimiento público pudiera tener graves consecuencias para la seguridad nacional (artículo 13, apartado 1, de la Ley SNI).
([265]) Artículo 63 de la LPIP.
([266]) Artículo 61, apartado 2; artículo 65, apartados 1 y 2, y artículo 64, apartado 4, de la LPIP.
([267]) Artículo 8, apartado 1, punto 2, del Decreto de Ejecución de la Ley antiterrorista.

3.4.2. *Mecanismos de reparación disponibles en virtud de la LPIP*

Los particulares podrán ejercer sus derechos de acceso, rectificación, supresión y suspensión en virtud de la LPIP con respecto a la información personal tratada con fines de seguridad nacional ([268]). Las solicitudes para ejercer estos derechos podrán presentarse directamente ante la agencia de inteligencia o de manera indirecta a través de la CPIP. La agencia de inteligencia podrá retrasar, limitar o denegar el ejercicio del derecho en la medida y durante el tiempo necesarios y proporcionados para proteger un objetivo importante de interés público (por ejemplo, en la medida y durante el tiempo que la concesión del derecho ponga en peligro una investigación en curso o amenace la seguridad nacional) o cuando la concesión del derecho pueda atentar contra la vida o la integridad de un tercero. En caso de denegación o restricción de la solicitud, el particular debe ser informada sin demora de los motivos.

Además, de conformidad con el artículo 58, apartado 4, de la LPIP (obligación de garantizar la tramitación adecuada de las reclamaciones individuales) y el artículo 4, apartado 5, de la LPIP (derecho a una reparación adecuada por cualquier daño o perjuicio derivado del tratamiento de información personal, mediante un procedimiento rápido y justo), los particulares tendrán derecho a obtener reparación. Esto incluye el derecho a denunciar una presunta infracción ante el Centro de atención telefónica sobre privacidad gestionado por la Agencia de Internet y Seguridad de Corea y a presentar una reclamación ante la CPIP ([269]). Estas vías de recurso están disponibles en caso de posibles infracciones tanto de las normas contenidas en las leyes específicas que establecen las limitaciones y salvaguardias con respecto a la recogida de información personal con fines de seguridad nacional como de la LPIP. Como se explica en la Nota n.º 2021-1, un ciudadano de la UE podrá presentar una reclamación ante la CPIP a través de su autoridad nacional de protección de datos. En este caso, la CPIP lo notificará a la persona a través de la autoridad nacional de protección de datos una vez finalizada la investigación (incluida, en su caso, la información sobre las medidas correctoras impuestas). Las decisiones o la inacción de la CPIP podrán ser recurridas ante los órganos jurisdiccionales coreanos en virtud de la Ley de lo contencioso-administrativo.

3.4.3. *Reparación ante la Comisión Nacional de Derechos Humanos*

La posibilidad de obtener una reparación individual ante la CNDH se aplicará de la misma manera a las agencias de inteligencia que a otras autoridades gubernamentales (véase la sección 2.4.2).

3.4.4. *Reparación judicial*

Al igual que en el caso de las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, los particulares podrán obtener reparación judicial contra las agencias de inteligencia con respecto a las infracciones de las limitaciones y salvaguardias antes mencionadas a través de distintas vías.

En primer lugar, los particulares podrán obtener una indemnización por daños y perjuicios con arreglo a la Ley de indemnización estatal. Por ejemplo, en un asunto, se concedió una indemnización en relación con la vigilancia ilícita por parte del Comando de Apoyo a la Defensa (predecesor del Comando de Apoyo a la Seguridad de la Defensa) ([270]).

En segundo lugar, la Ley de lo contencioso-administrativo permite a los particulares impugnar las disposiciones y omisiones de los organismos administrativos, incluidas las agencias de inteligencia ([271]).

Por último, los particulares podrán interponer un recurso de inconstitucionalidad ante el Tribunal Constitucional contra las medidas adoptadas por las agencias de inteligencia sobre la base de la Ley del Tribunal Constitucional.

([268]) Artículo 3, apartado 5, y artículo 4, apartados 1, 3 y 4, de la LPIP.
([269]) Artículos 62 y 63, apartado 2, de la LPIP.
([270]) Resolución n.º 96Da42789 del Tribunal Supremo, de 24 de julio de 1998.
([271]) Artículos 3 y 4 de la Ley de lo contencioso-administrativo.