Dictamen 32/2021 sobre el Proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales en la República de Corea, conforme al Reglamento (UE) 2016/679

Versión 1.0

Adoptado el 24 de septiembre de 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

ÍNDICE

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra s), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (**«RGPD»**),

Visto el Acuerdo sobre el Espacio Económico Europeo (**«EEE»**) y, en particular, su anexo XI y su Protocolo 37, modificados por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. RESUMEN EJECUTIVO

1. El 16 de junio de 2021, la Comisión Europea inició el procedimiento oficial para la adopción del proyecto de decisión de ejecución (en lo sucesivo, **«proyecto de decisión»**) relativa a la adecuación de la protección de los datos personales en la República de Corea en virtud de la Ley sobre la protección de datos personales, de conformidad con el RGPD[2].

2. Ese mismo día, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos (**«CEPD»**)[3]. La evaluación por parte del CEPD de la adecuación del nivel de protección ofrecido en la República de Corea se ha realizado sobre la base del examen del propio proyecto de decisión y tras analizar la documentación facilitada[4] por la Comisión Europea.

3. El CEPD centró su evaluación tanto en los aspectos generales relacionados con el RGPD del proyecto de decisión como en el acceso de las autoridades públicas a los datos personales transferidos desde el EEE con fines policiales y de seguridad nacional, incluidas las vías de recurso disponibles para los ciudadanos del EEE. El CEPD también evaluó si se aplican y resultan eficaces las salvaguardias previstas en el marco jurídico coreano.

4. Como referencia principal para este trabajo, el CEPD utilizó sus criterios de referencia sobre la adecuación[5] en virtud del RGPD (en lo sucesivo, **«Referencias sobre adecuación»**), aprobadas en febrero de 2018, y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia[6].

[1] Las referencias a los **«Estados miembros»** realizadas en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».
[2] Véase el comunicado de prensa: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] *Ibid*.
[4] El CEPD basó su análisis en las traducciones oficiales preparadas por el gobierno coreano.
[5] WP 254, «Referencias sobre adecuación», de 6 de febrero de 2018 (aprobadas por el CEPD; véase: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020: https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Ámbitos de convergencia

5. El principal objetivo del CEPD es proporcionar a la Comisión Europea un dictamen acerca de la adecuación del nivel de protección conferido a las personas cuyos datos personales se transfieran a la República de Corea. Es importante reconocer que el CEPD no espera que el marco jurídico coreano en materia de protección de datos reproduzca la legislación europea en esta materia.

6. Sin embargo, el CEPD recuerda que, para considerar que la legislación de un tercer país proporciona un nivel adecuado de protección, el artículo 45 del RGPD y la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, **«TJUE»**) exigen que esta legislación se ajuste en esencia a los principios fundamentales consagrados en el RGPD. En este sentido, el marco jurídico coreano en materia de protección de datos presenta numerosas similitudes con el europeo, ya que cuenta con un instrumento legislativo principal que cubre tanto el sector público como el privado, al que completan actos legislativos específicos para distintos sectores.

7. En relación con el contenido, el CEPD observa determinadas áreas importantes del marco jurídico del RGPD y el marco jurídico coreano en materia de protección de datos en las que ciertas disposiciones fundamentales se encuentran armonizadas, como los conceptos (p. ej., «información personal», «tratamiento» o «interesado»); los motivos para el tratamiento lícito y leal con fines legítimos; la limitación de la finalidad; la calidad de los datos y la proporcionalidad; la conservación, la seguridad y la confidencialidad de los datos; la transparencia; y las categorías especiales de datos.

8. Asimismo, el CEPD acoge con satisfacción los esfuerzos realizados por la Comisión Europea y las autoridades coreanas con vistas a garantizar que la República de Corea proporcione un nivel de protección adecuado en los términos prescritos por el RGPD, mediante la adopción de notificaciones por la autoridad de control coreana (no solo aplicables a los datos personales transferidos desde el EEE hasta la República de Corea) con el fin de colmar las lagunas entre el RGPD y el marco jurídico coreano en materia de protección de datos. El CEPD desea subrayar la relevancia de estas notificaciones para la evaluación de la adecuación del nivel de protección en la República de Corea, teniendo en cuenta, por ejemplo, que ofrecen aclaraciones pertinentes sobre algunas salvaguardias importantes, relacionadas, entre otras cosas, con el alcance de la aplicación de las excepciones previstas en la Ley de protección de datos personales de Corea para el tratamiento de datos personales seudonimizados con fines científicos, de investigación y estadísticos , las transferencias ulteriores y las normas aplicables en el contexto del acceso a los datos por parte de las autoridades públicas.

1.2. Dificultades

9. Pese a que el CEPD ha identificado la equivalencia sustancial entre numerosos aspectos del marco jurídico coreano en materia de protección de datos y el marco europeo, también ha concluido que muchos otros aspectos pueden precisar de un examen más detenido y una aclaración. En concreto, el CEPD considera que los siguientes aspectos deben ser objeto de un examen más detallado y un control atento por parte de la Comisión Europea a fin de asegurar que se alcance un nivel de protección sustancialmente equivalente.

1.2.1. Consideraciones generales

10. El CEPD toma nota de que la notificación n.º 2021-1 *tiene naturaleza de norma administrativa con carácter jurídicamente vinculante para el responsable del tratamiento de datos personales, en el sentido de que cualquier incumplimiento de la notificación puede considerarse una vulneración de las correspondientes disposiciones de la Ley de Protección de Datos Personales de Corea*[7]. Sin embargo, teniendo en cuenta que la notificación no incluye en sí misma normas adicionales, sino únicamente

[7] Véase la sección I del anexo I del proyecto de decisión.

aclaraciones sobre el modo en que debería aplicarse la parte dispositiva de la Ley de Protección de Datos Personales de Corea, y en vista de su importancia general, en particular, en lo que se refiere a las disposiciones sobre seudonimización previstas en dicha ley, que, según entiende el CEPD, actualmente son objeto de varios procesos judiciales en curso, el CEPD insta a la Comisión Europea a que ofrezca más información sobre el carácter vinculante, la coercibilidad y la validez de la notificación n.º 2021-1 y recomienda que se controle con atención su observancia en la práctica, en particular, en lo referente a su aplicación no solo por la autoridad de control coreana, sino también por los órganos jurisdiccionales, especialmente cuando el nivel de protección equivalente que ofrezca el ordenamiento jurídico coreano se base en las aclaraciones proporcionadas en dicha notificación.

1.2.2. Aspectos generales relativos a la protección de datos

11. Por lo que respecta al alcance de la aplicación de la decisión de adecuación, el CEPD señala que abarcará las transferencias desde el territorio en que rija el marco jurídico del EEE a «responsables del tratamiento de datos personales», públicos y privados, que se encuentren incluidos en el ámbito de aplicación de la Ley de Protección de Datos Personales de Corea. El CEPD entiende que se incluyen en este término las entidades que actúan como encargados del tratamiento en el sentido del RGPD. Sin embargo, a fin de evitar malentendidos, insta a la Comisión Europea a que aclare que la decisión de adecuación también se aplica a las transferencias realizadas a «encargados del tratamiento» en Corea.

12. Un aspecto importante sobre el que desea llamar la atención el CEPD es el concepto de «datos seudonimizados» en el marco jurídico coreano en materia de protección de datos. El Derecho coreano prevé excepciones a la aplicación de diversas disposiciones pertinentes, incluidas las relativas a los derechos individuales de los interesados y la conservación de datos, en lo que se refiere al tratamiento de datos personales seudonimizados.,. Según la Comisión Europea, estas excepciones únicamente se aplican cuando los datos personales seudonimizados se tratan con fines estadísticos, de investigación científica o de archivo en beneficio de un interés público. Sin embargo, esta afirmación se apoya principalmente en la notificación n.º 2021-1 y, por tanto, resultan especialmente pertinentes en este sentido la mencionada necesidad de información adicional sobre esta notificación y el control de su carácter vinculante, coercibilidad y validez. Además, el CEPD insta a la Comisión Europea a que evalúe con más detalle el efecto de la seudonimización en el Derecho coreano y, sobre todo, cómo puede afectar a los derechos y las libertades fundamentales de los interesados cuyos datos personales se transfieran a la República de Corea con arreglo a la decisión de adecuación. En particular, el CEPD apela a la Comisión Europea a que examine de un modo más minucioso las excepciones contempladas en el artículo 28, apartado 7, de la Ley de Protección de Datos Personales de Corea y el artículo 40, apartado 3, de la Ley de Información Crediticia de Corea, y a que supervise atentamente su aplicación y la correspondiente jurisprudencia con el fin de garantizar que los derechos de los interesados no se limiten de manera indebida cuando los datos personales transferidos con arreglo a la decisión de adecuación se traten para los fines mencionados.

13. El CEPD también observa que la legislación coreana únicamente contempla el derecho a retirar el consentimiento en determinadas circunstancias y, en consecuencia, insta a la Comisión Europea a que evalúe con mayor grado de detalle los efectos de la ausencia de un derecho general a retirar el consentimiento y a que ofrezca más garantías de que se asegurará en todo momento un nivel de protección de datos básico, aclarando, cuando sea necesario, qué función cumple el derecho a la suspensión en virtud de la Ley de Protección de Datos Personales de Corea en ausencia de un derecho general a retirar el consentimiento.

14. Por lo que respecta a las transferencias ulteriores, el CEPD toma nota de que generalmente se utilizará el consentimiento informado del interesado como base para las transferencias de datos por responsables del tratamiento de datos personales establecidos en Corea a destinatarios establecidos en países terceros y que la notificación n.º 2021-1 prevé la obligación de informar a los interesados sobre el país tercero al que se enviarán sus datos. El CEPD invita, no obstante, a la Comisión Europea

a garantizar que la información que deba proporcionarse al interesado también incluya información sobre los posibles riesgos de las transferencias derivados de la ausencia de una protección adecuada en el país tercero y de la ausencia de unas salvaguardias adecuadas. Además, agradecería que en la decisión de adecuación se incluyeran garantías de que los responsables del tratamiento de datos personales establecidos en Corea no realizarán transferencias de datos personales a terceros países en aquellas situaciones en las que, con arreglo al RGPD, no pueda prestarse un consentimiento válido, p. ej., cuando exista un desequilibrio de poder.

15. En relación con el nombramiento de los miembros de la autoridad de control coreana, aunque el procedimiento formal estaría en consonancia con el RGPD y, en consecuencia, superaría el examen de la equivalencia con el marco jurídico del EEE, el CEPD agradecería que la Comisión Europea vigilara cualquier eventualidad que pudiera afectar a la independencia de los miembros de dicha autoridad de control.

16. Por lo que respecta al presupuesto, en la información facilitada por la Comisión Europea no se hace referencia a datos pormenorizados sobre el personal adscrito al Comité de Protección de Datos Personales de Corea ni a los recursos económicos de que dispone. En consecuencia, el CEPD agradecería cualquier información adicional sobre estos dos aspectos en el proyecto de decisión.

1.2.3. Acceso de las autoridades públicas a los datos transferidos a la República de Corea

17. El CEPD también ha analizado el marco jurídico coreano en lo referente al acceso del Gobierno, con fines policiales y de seguridad nacional, a los datos personales transferidos desde el EEE a la República de Corea. Pese a haber tomado nota de las declaraciones y garantías ofrecidas por el Gobierno coreano, según se recogen en el anexo II del proyecto de decisión, el CEPD ha identificado diversos aspectos que requieren una aclaración o resultan problemáticos.

18. El CEPD observa que las disposiciones de la Ley de Protección de Datos Personales de Corea se aplican sin restricciones en el ámbito policial. Constata también que el tratamiento de datos en el campo de la seguridad nacional se encuentra sujeto a un conjunto más reducido de disposiciones incluidas en dicha ley.

19. Por lo que respecta a la divulgación voluntaria de datos personales a los organismos nacionales de seguridad por proveedores de servicios de telecomunicaciones, preocupa al CEPD la falta de claridad en la relación entre la sección 3 del anexo I del proyecto de decisión, que especifica que, en principio, los proveedores deben notificar al interesado cuando respondan voluntariamente a una solicitud, y el artículo 58, apartado 1, punto 2, de la Ley de Protección de Datos Personales de Corea, es decir, la excepción parcial por motivos de seguridad nacional. Esto podría dejar sin efecto las obligaciones en materia de información, lo cual dificultaría considerablemente el ejercicio de los derechos de los interesados en materia de protección de datos, especialmente, de las acciones judiciales.

20. Pese a que el proyecto de decisión no lo menciona expresamente, el CEPD infiere, de las explicaciones facilitadas por la Comisión Europea, que el marco jurídico coreano no permite la interceptación masiva de datos de telecomunicaciones. Por tanto, la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (**«TEDH»**) sobre los regímenes de interceptación masiva no tendría una relevancia directa para la evaluación del nivel de protección de datos en Corea.

21. Por otra parte, el proyecto de decisión no contiene información alguna sobre el marco jurídico para las transferencias ulteriores en el ámbito de la seguridad nacional. Aunque el CEPD entiende que, en opinión de la Comisión Europea, las transferencias ulteriores con fines relacionados con la seguridad nacional se encuentran suficientemente reguladas en virtud de las salvaguardias y los principios generales dimanados del marco constitucional y la Ley de Protección de Datos Personales de Corea, también se pregunta si esto cumple los requisitos de precisión y claridad de la ley y consagra unas salvaguardias eficaces y aplicables. Las salvaguardias a que hace referencia la Comisión Europea tienen

un carácter muy general y no abordan, en el plano jurídico, las circunstancias y las condiciones específicas en las que pueden tener lugar las transferencias ulteriores por motivos de seguridad nacional. En este contexto, el CEPD también observa que la Comisión Europea no tuvo en cuenta la existencia de acuerdos internacionales suscritos entre la República de Corea y terceros países u organizaciones internacionales que puedan contener disposiciones específicas sobre la transferencia internacional de datos personales a terceros países por los servicios policiales o de inteligencia. El CEPD considera que la celebración de acuerdos bilaterales o multilaterales con terceros países con fines de cooperación policial o en materia de inteligencia puede afectar al marco jurídico coreano sobre protección de datos examinado.

22. El CEPD también constata que la supervisión de la aplicación del Derecho penal y de los organismos nacionales de seguridad se encuentra garantizada mediante una combinación de distintos organismos internos y externos, en particular, el Comité de Protección de Datos Personales de Corea, al que se ha dotado de unos poderes ejecutivos suficientes.

23. Para garantizar unos recursos y unos medios de reparación efectivos, los interesados deben poder dirigirse a un órgano competente que cumpla los requisitos del artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la **«Carta»**); esto es, que tenga competencia para determinar si se está llevando a cabo un tratamiento de datos personales y para verificar la licitud del tratamiento, y que cuente con poderes correctivos coercibles en caso de que el tratamiento de los datos sea ilícito. Teniendo en cuenta todo esto, el CEPD solicita a la Comisión Europea que aclare si las reclamaciones ante el Comité de Protección de Datos Personales de Corea o las acciones ante los órganos jurisdiccionales están sujetas a obligaciones sustantivas o de procedimiento, como la carga de la prueba, y si las personas físicas establecidas en el EEE podrían satisfacer este tipo de obligaciones.

1.3. Conclusión

24. En opinión del CEPD, esta decisión de adecuación es de la máxima importancia, puesto que, con la salvedad de las excepciones señaladas en el dictamen, cubrirá las transferencias tanto en el sector público como en el privado.

25. El CEPD acoge con satisfacción los esfuerzos realizados por la Comisión Europea y las autoridades coreanas con vistas a armonizar el marco jurídico coreano con el europeo. Las mejoras que pretende introducir la notificación n.º 2021-1 para salvar algunas de las diferencias entre los dos marcos son muy importantes y se consideran bien encaminadas. Sin embargo, el CEPD observa que persisten diversas cuestiones que son motivo de preocupación, algunas relacionadas con la notificación n.º 2021-1, además de la necesidad de aclarar determinados asuntos, y recomienda a la Comisión Europea que dé respuesta a estas preocupaciones y a las solicitudes de aclaraciones formuladas por el CEPD y ofrezca más información y explicaciones sobre las cuestiones planteadas en el presente dictamen.

2. INTRODUCCIÓN

2.1. Marco jurídico coreano en materia de protección de datos

26. El principal texto legislativo que rige la protección de datos en la República de Corea es la Ley de Protección de Datos Personales (Ley n.º 10465, de 29 de marzo de 2011, con las modificaciones introducidas por la Ley n.º 16930, de 4 de febrero de 2020; en lo sucesivo, **«LPDP»**). Complementa a esta un decreto de aplicación (Decreto Presidencial n.º 23169, de 29 de septiembre de 2011, con las modificaciones introducidas por el Decreto Presidencial n.º 30892, de 4 de agosto de 2020; en lo sucesivo, «decreto de aplicación de la LPDP»), que es jurídicamente vinculante y de obligado cumplimiento.

27. Además de la LPDP, el marco jurídico coreano en materia de protección de datos incluye «notificaciones» normativas emitidas por la autoridad de control coreana, el Comité de Protección de Datos Personales (en lo sucesivo, **«CPDP»**), en las que se proporcionan reglas adicionales sobre la interpretación y la aplicación de la LPDP. Recientemente, el CPDP adoptó la notificación n.º 2021-1, de 21 de enero de 2021, sobre la interpretación, la aplicación y el cumplimiento de determinadas disposiciones de la LPDP (en lo sucesivo, **«notificación n.º 2021-1»**), por la que se modificó la anterior notificación n.º 2020-10, de 1 de septiembre de 2020. Más concretamente, esta notificación fue el resultado de los debates sobre la adecuación mantenidos entre las autoridades coreanas y la Comisión Europea. Contiene aclaraciones sobre la aplicación de ciertas disposiciones de la LPDP, también en relación con el tratamiento de los datos personales transferidos a la República de Corea en virtud de la decisión de adecuación prevista[8], y *tiene naturaleza de norma administrativa con carácter jurídicamente vinculante para el responsable del tratamiento de datos personales, en el sentido de que cualquier incumplimiento de la notificación puede considerarse una vulneración de las correspondientes disposiciones de la LPDP*[9]. A este respecto, el CEPD desea señalar que, a pesar de que el proyecto de decisión hace referencia a esta como «normativa complementaria», la notificación no incluye en sí misma normas adicionales, sino únicamente explicaciones con las que se pretende aclarar el modo en que debería aplicarse la parte dispositiva de la LPDP, en particular, en lo que se refiere a los datos transferidos desde el EEE. Teniendo en cuenta todo esto, el CEPD recomienda que se supervise con atención la observancia de la notificación n.º 2021-1 en la práctica, en particular, en lo referente a su aplicación no solo por el CPDP, sino también por los órganos jurisdiccionales, especialmente cuando el nivel de protección equivalente que ofrezca el ordenamiento jurídico coreano se base en las aclaraciones proporcionadas en dicha notificación.

28. Otras leyes pertinentes del marco jurídico coreano en materia de protección de datos establecen normas sobre el tratamiento de datos personales en sectores específicos, como, por ejemplo:

- la Ley sobre el Uso y la Protección de Información Crediticia (en lo sucesivo, **«LIC»**), junto a su decreto de aplicación (en lo sucesivo, **«decreto de aplicación de la LIC»**), que establecen normas específicas aplicables a los operadores comerciales y a las entidades especializadas (por ejemplo, agencias de calificación crediticia e instituciones financieras) cuando tratan información crediticia personal que resulta necesaria para determinar la solvencia de las partes en operaciones financieras o comerciales;
- la Ley sobre la Promoción del Uso de la Red de Información y Comunicaciones y la Protección de Datos (en lo sucesivo, **«Ley sobre la Red»**); y
- la Ley para la Protección de la Privacidad de las Comunicaciones (en lo sucesivo, **«LPPC»**).

29. En el ámbito del acceso por el Gobierno, además de las disposiciones pertinentes recogidas en la LPDP y la LPPC, el CEPD ha tenido en cuenta otros textos legislativos: la Ley de Enjuiciamiento Criminal (en lo sucesivo, **«LEC»**), la Ley de Empresas de Telecomunicaciones (en lo sucesivo, **«LET»**), la Ley sobre la Notificación y el Uso de Información Específica sobre Transacciones Financieras (en lo sucesivo, **«LNUIETF»**) y la Ley sobre el Servicio Nacional de Inteligencia (en lo sucesivo, **«LSNI»**).

2.2. Alcance de la evaluación del CEPD

30. El proyecto de decisión de la Comisión Europea es el resultado de una evaluación del marco jurídico coreano en materia de protección de datos seguida por unas conversaciones mantenidas con el Gobierno coreano. De conformidad con lo dispuesto en el artículo 70, apartado 1, letra s), del RGPD, se espera que el CEPD emita un dictamen independiente sobre las conclusiones de la Comisión

[8] Véase la sección I del anexo I del proyecto de decisión.
[9] *Ibid*.

Europea, identifique las insuficiencias en el marco de adecuación, en su caso, y se esfuerce por realizar propuestas para abordarlas.

31. Al objeto de evitar las repeticiones, y con el fin de facilitar la evaluación del marco jurídico coreano, el CEPD ha decidido centrarse en determinados puntos concretos presentados en el proyecto de decisión y ofrecer su análisis y opinión sobre estos, absteniéndose de reproducir la mayoría de las constataciones factuales y las evaluaciones en aquellos casos en los que el CEPD no haya observado ningún indicio para asumir que el Derecho de la República de Corea no sea sustancialmente equivalente al del EEE. Además, en consonancia con la jurisprudencia del TJUE, una parte muy importante del análisis aborda el régimen jurídico del acceso de los organismos nacionales de seguridad a los datos personales transferidos a la República de Corea, así como las prácticas de su aparato de seguridad nacional.

32. En su evaluación, el CEPD tuvo en cuenta el marco jurídico europeo aplicable en materia de protección de datos, en particular, los artículos 7, 8 y 47 de la Carta, que protegen, respectivamente, el derecho al respeto de la vida privada y familiar, el derecho a la protección de los datos de carácter personal y el derecho a la tutela judicial efectiva y a un juez imparcial, y el artículo 8 del CEDH, que protege el derecho al respeto a la vida privada y familiar. Además de lo anterior, el CEPD consideró los requisitos del RGPD, así como la jurisprudencia pertinente.

33. El objetivo del presente examen es proporcionar a la Comisión Europea un dictamen acerca de la adecuación del nivel de protección en la República de Corea. Este concepto de «nivel de protección adecuado», que ya existía en la Directiva 95/46, ha sido ampliado por el TJUE. En este punto, conviene recordar la norma establecida por el TJUE en el asunto *Schrems I*, en particular, que, aunque el «nivel de protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la UE, *«los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la [UE]»*[10]. Por tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de la legislación objeto de examen. Se puede lograr la adecuación combinando los derechos de los interesados, las obligaciones de aquellos que realizan el tratamiento de los datos, o que ejercen control sobre dicho tratamiento, y la supervisión por parte de organismos independientes. No obstante, las normas de protección de datos solo resultan efectivas si son exigibles y se siguen en la práctica. Por tanto, se debe tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país u organización internacional, sino también el sistema existente para garantizar la efectividad de dichas normas. Unos mecanismos de aplicación eficientes son de vital importancia para la efectividad de las normas de protección de datos.[11]

2.3. Observaciones generales y motivos de preocupación

2.3.1. Compromisos internacionales asumidos por la República de Corea

34. De conformidad con el artículo 45, apartado 2, letra c), del RGPD y las Referencias sobre adecuación[12], al evaluar la adecuación del nivel de protección de un tercer país, la Comisión Europea tendrá en cuenta, entre otras cosas, los compromisos internacionales asumidos por el tercer país u otras obligaciones derivadas de la participación del tercer país en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, así como la aplicación de dichas obligaciones.

[10] C-362/14, *Maximilian Schrems contra Data Protection Commissioner*, 6 de octubre de 2015, ECLI:EU:C:2015:650, apartados 73-74.
[11] WP 254, p. 2.
[12] WP 254, p. 2.

35. Corea es parte en varios acuerdos internacionales que garantizan el derecho a la intimidad, 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, como miembro de la OCDE, Corea debe respetar el marco jurídico de la OCDE en materia de intimidad, en particular las directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.

36. El CEPD también toma nota de la participación de Corea, como Estado observador, en el trabajo del Comité Consultivo del Convenio n.º 108(+) del Consejo de Europa, aunque aún no ha decidido si se adherirá a este.

2.3.2. Alcance de la decisión de adecuación

37. Según se establece en el considerando 5 del proyecto de decisión, la Comisión Europea concluye que la República de Corea garantiza un nivel de protección adecuado para los datos personales transferidos desde responsables o encargados del tratamiento establecidos en la Unión a responsables del tratamiento de datos personales (p. ej., personas físicas o jurídicas, organizaciones o instituciones públicas) que se encuentren incluidos en el ámbito de aplicación de la LPDP, con la excepción del tratamiento de datos personales para la actividad misionera llevada a cabo por organizaciones religiosas y para el nombramiento de candidatos por partidos políticos[13], y del tratamiento de información crediticia de carácter personal con arreglo a la LIC por responsables del tratamiento que estén sujetos a la supervisión de la Comisión de Servicios Financieros de Corea.

38. El CEPD señala que la decisión de adecuación abarcará las transferencias desde el territorio en que rija el marco jurídico del EEE a «responsables del tratamiento de datos personales», públicos y privados, que se encuentren incluidos en el ámbito de aplicación de la LPDP. El CEPD entiende que también se incluyen en el término «responsable del tratamiento de datos personales» las entidades que actúan como encargados del tratamiento, en el sentido del RGPD, habida cuenta de que la LPDP se les aplica igualmente y de que resultan aplicables obligaciones específicas cuando un responsable del tratamiento de datos personales (el «subcontratante») contrata a un tercero para el tratamiento de dichos datos (el «subcontratista»). Sin embargo, a fin de evitar malentendidos, el CEPD insta a la Comisión Europea a que aclare que la decisión de adecuación también se aplica a las transferencias realizadas a «encargados del tratamiento» en Corea y que el nivel de protección de los datos personales transferidos desde el EEE tampoco se vulnerará en dichos casos.

39. Además, puesto que la decisión de adecuación también cubre las transferencias de datos personales entre organismos públicos, el CEPD entiende que también quedan cubiertas las que tienen lugar entre autoridades de control de la protección de datos. Por tanto, en aras de la claridad, invita a la Comisión Europea a abordar expresamente esta cuestión.

40. Por otro lado, por lo que respecta a las entidades excluidas del alcance de la decisión de adecuación, el CEPD desea hacer hincapié en la conveniencia de que se identifiquen más claramente en esta las «organizaciones comerciales» que se encuentran sujetas a la supervisión del CPDP (artículo 45, apartado 3, de la LIC), de modo que, antes de la transferencia de los datos a las entidades incluidas en el ámbito de aplicación de la LIC, los responsables y encargados del tratamiento establecidos en el EEE puedan evaluar fácilmente si se aplica al importador la decisión de adecuación o, al menos, puedan ser avisados de la necesidad de evaluar este aspecto.

41. Por lo que respecta al alcance de la decisión de adecuación, de las explicaciones adicionales facilitadas por la Comisión Europea, el CEPD ha entendido que la Unidad de Inteligencia Financiera de Corea (**«KoFIU»**), dependiente de la Comisión de Servicios Financieros y encargada de supervisar la

[13] En la sección 3.1.2 del presente dictamen se ofrece más información sobre el contexto.

prevención del blanqueo de capitales y la financiación del terrorismo con arreglo a la LNUIETF[14], también se encuentra excluida de su alcance, puesto que su competencia se limita a las instituciones financieras, que no están cubiertas por el proyecto de decisión. Sin embargo, el artículo 1, apartado 2, letra c), del proyecto de decisión únicamente excluye de su alcance a los responsables del tratamiento de datos personales que estén sujetos a la supervisión de la Comisión de Servicios Financieros de Corea y traten información crediticia de carácter personal con arreglo a la LIC. Teniendo en cuenta todo lo anterior, el CEPD solicita a la Comisión Europea que aclare si la KoFIU y las actividades de tratamiento de datos llevadas a cabo por esta se encuentran dentro del alcance del proyecto de decisión.

3. ASPECTOS GENERALES RELATIVOS A LA PROTECCIÓN DE DATOS

3.1. Principios relativos al contenido

42. El capítulo 3 de las Referencias sobre adecuación trata sobre los «principios relativos al contenido». El sistema de un tercer país debe incluirlos a fin de considerar que el nivel de protección ofrecido es sustancialmente equivalente al garantizado por la legislación de la UE.

43. Pese a que el derecho a la protección de los datos personales no se encuentra recogido expresamente en la Constitución coreana, se considera un derecho fundamental derivado de los derechos constitucionales a la dignidad humana y la búsqueda de la felicidad (artículo 10), la vida privada (artículo 17) y la confidencialidad de las comunicaciones (artículo 18). Tal como se indica en el proyecto de decisión de la Comisión Europea[15], esto ha sido confirmado por el Tribunal Supremo y el Tribunal Constitucional de dicho país. El CEPD toma nota de este reconocimiento, del cual se desprende, con arreglo al artículo 37 de la Constitución coreana, que la protección de los datos como derecho fundamental *«solo puede restringirse en virtud de una ley y cuando sea necesario por motivos de seguridad nacional, para el mantenimiento del orden público o para preservar el bienestar de los ciudadanos»* y que *«aun cuando se impongan tales limitaciones, estas no podrán afectar a la esencia de la libertad o el derecho»*.

44. Según la Comisión Europea[16], el Tribunal Constitucional coreano ha dictaminado que también son titulares de derechos fundamentales los extranjeros. Asimismo, en las declaraciones oficiales efectuadas por el Gobierno coreano[17] se indica que, aunque la jurisprudencia no ha abordado por ahora de manera expresa el derecho a la intimidad de los nacionales de países distintos de la República de Corea, se reconoce ampliamente en la doctrina que los artículos 12 a 22 de la Constitución consagran «derechos humanos». Además, se han promulgado en la República de Corea, en el campo de la protección de datos, una serie de leyes que ofrecen garantías para todas las personas con independencia de su nacionalidad, como la LPDP. Al respecto, el CEPD observa que el artículo 6, apartado 2, de la Constitución coreana prevé que el estatuto jurídico de los ciudadanos extranjeros quede garantizado según lo prescrito en el Derecho y los tratados internacionales, y también toma nota de la jurisprudencia mencionada en el proyecto de decisión, según la cual los «extranjeros» pueden ser titulares de «derechos fundamentales». Teniendo en cuenta la relevancia del reconocimiento del derecho de los «extranjeros» a la protección de datos, el CEPD señala a la Comisión Europea la necesidad de continuar revisando la jurisprudencia en la que se aborde la protección de datos como un derecho fundamental reconocido no solo a los ciudadanos coreanos, sino a todos los interesados, a fin de garantizar que el nivel de protección conferido a las personas

[14] Véase la sección 2.2.3.1 del anexo II.
[15] Véase el considerando 8 del proyecto de decisión y la jurisprudencia pertinente citada en la nota 10 a pie de página de dicho documento, de la que únicamente se encuentran disponibles resúmenes en inglés.
[16] Véase el considerando 9 del proyecto de decisión.
[17] Sección 1.1 del anexo II del proyecto de decisión.

físicas en el RGPD no se vulnere cuando se transfieran datos personales a Corea en virtud de la decisión de adecuación.

3.1.1. Conceptos

45. Según se establece en las Referencias sobre adecuación, debe existir una serie de conceptos o principios básicos sobre protección de datos en el marco jurídico del país tercero. Estos no deben imitar la terminología del RGPD, pero deben reflejar los conceptos consagrados en la legislación europea en materia de protección de datos y ser coherentes con ellos. A modo de ejemplo, el RGPD incluye los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «responsable del tratamiento», «encargado del tratamiento», «destinatario» y «datos sensibles».[18]

46. La LPDP incluye varias definiciones, entre otras, la de «datos personales», «tratamiento» e «interesado», que se parecen en gran medida a los correspondientes términos recogidos en el RGPD.

3.1.1.1. *Concepto de «datos seudonimizados»*

47. Entre las definiciones previstas en la LPDP, su artículo 2, apartado 1, define, en particular, los datos personales como cualquiera de los siguientes datos relativos a una persona física viva: a) la información que identifique a una persona física concreta a través de su nombre y apellidos, número de registro como residente, imagen, etc.; y b) la información que, aun no identificando por sí sola una persona física concreta, pueda combinarse fácilmente con otra información para identificarla. En este último caso, la facilidad de la posibilidad de combinación se determinará teniendo en cuenta de manera razonable el tiempo, el coste, la tecnología, etc., empleados para identificar a la persona, como, por ejemplo, la probabilidad de que pueda obtenerse el resto de la información.

48. Además, en virtud del artículo 2, apartado 1, letra c), de la LPDP, los «datos seudonimizados» también se consideran datos personales. Los datos seudonimizados se definen como los datos indicados en las letras a) o b) anteriores que se encuentran seudonimizados de conformidad con lo dispuesto en los párrafos 1 y 2, y, por tanto, no pueden utilizarse para identificar a una persona física concreta sin el empleo de datos o una combinación de datos que permitan el restablecimiento de los datos seudonimizados a su estado original. Los datos totalmente anonimizados quedan excluidos del ámbito de aplicación de la LPDP. Según lo dispuesto en el artículo 58, apartado 2, de la LPDP, esta ley no se aplica a información que ya no identifique a una persona física concreta incluso si se combina con otra información, teniendo en cuenta de manera razonable el tiempo, el coste, la tecnología, etc.

49. En el considerando 17 del proyecto de decisión, la Comisión Europea establece que esto se corresponde con el ámbito de aplicación material del RGPD y con las nociones de «datos personales», «seudonimización» e «información anónima» recogidos en este.

50. No obstante, con arreglo al artículo 28, apartado 7, de la LPDP, los artículos 20, 21 y 27, el artículo 34, apartado 1, los artículos 35 a 37, y el artículo 39, apartados 3, 4 y 6 a 8, no se aplican a los datos personales seudonimizados.

51. En su proyecto de decisión, la Comisión Europea señala que el artículo 28, apartado 7, de la LPDP solo resulta aplicable a los datos personales seudonimizados cuando estos se tratan con fines estadísticos, de investigación científica o de archivo en beneficio de un interés público.[19] Sin embargo, esto no se desprende directamente del tenor literal de la ley, sino de las explicaciones ofrecidas en la notificación n.º 2021-1.[20] Pese a que el CEPD reconoce que la estructura y el fundamento de la LPDP pueden llevar

[18] WP 254, p. 4.
[19] Véase, entre otros, el considerando 82 del proyecto de decisión.
[20] Sección 4 del anexo I del proyecto de decisión.

a argüir que el artículo 28, apartado 2, de esta ley debe entenderse e interpretarse lógicamente en el sentido de que también se aplica al artículo 28, apartado 7, de dicha ley, en vista de la importancia de la notificación n.º 2021-1 en la evaluación de la adecuación del nivel de protección de los datos personales en la República de Corea llevada a cabo por la Comisión Europea, y a fin de disipar cualquier duda, el CEPD insta a la Comisión Europea a que ofrezca más información sobre el carácter vinculante, la coercibilidad y la validez de la notificación n.º 2021-1 y a que supervise su aplicación en este contexto concreto.

52. En este contexto, el CEPD desea recordar que, en el RGPD, la seudonimización se entiende como una medida de seguridad recomendada. En otras palabras, con arreglo al RGPD, los datos seudonimizados son datos personales a los que se les aplica plenamente el RGPD. Teniendo en cuenta lo anterior, preocupa al CEPD que el nivel de protección que confiere el RGPD a los datos personales seudonimizados pueda menoscabarse cuando se transfieran datos personales a la República de Corea. Por tanto, el CEPD insta a la Comisión Europea a que evalúe con más detalle el efecto de la seudonimización en virtud de la LPDP y, sobre todo, cómo puede afectar a los derechos y las libertades fundamentales de los interesados cuyos datos personales se transfieran a la República de Corea con arreglo a la decisión de adecuación. En este sentido, el CEPD solicita a la Comisión Europea que ofrezca garantías de que el nivel de protección de los datos personales de los interesados establecidos en el EEE no se rebajará tras su transferencia a la República de Corea, incluso cuando dichos datos personales se encuentren seudonimizados.

3.1.1.2. *Concepto de responsable del tratamiento de datos personales*

53. El artículo 2, apartado 5, de la LPDP incluye una definición de «responsable del tratamiento de datos personales», por el que se entiende una institución pública, persona jurídica, organización, persona física, etc., que trata datos personales, directa o indirectamente, con el fin de utilizar los archivos con datos personales *«como parte de sus actividades»*. Sin embargo, en las salvaguardias adicionales establecidas en la notificación n.º 2021-1, este término se define como toda institución pública, persona jurídica, organización, persona física, etc., que trata datos personales, directa o indirectamente, con el fin de utilizar los archivos con datos personales *«con fines comerciales»*. Por otra parte, la nota 272 a pie de página del proyecto de decisión establece lo siguiente sobre la noción de «responsable del tratamiento de datos personales»: *«Tal como se define en el artículo 2 de la LPDP; esto es, una institución pública, persona jurídica, organización, persona física, etc., que trata datos personales, directa o indirectamente, con el fin de utilizar los archivos con datos personales "con fines oficiales o comerciales"»*.

54. El CEPD reconoce que estas discrepancias pueden deberse a las traducciones del texto original proporcionadas por las autoridades coreanas e insta a la Comisión Europea a que verifique con regularidad la calidad y exactitud de las traducciones. Aun así, el CEPD subraya que, para poder evaluar la equivalencia sustancial del nivel de protección de datos del marco jurídico coreano, es necesario conocer claramente qué fines del tratamiento se encuentran incluidos en el ámbito de aplicación material de la LPDP. Además, el CEPD observa al respecto que la LPDP no utiliza la misma terminología que el RGPD para las nociones de «responsable» y «encargado» del tratamiento e insta a la Comisión Europea a que aclare cuál es la definición correcta y el alcance del concepto de «responsable del tratamiento de datos personales» y a que señale en concreto si este término también incluye a los encargados del tratamiento en el sentido del RGPD, puesto que ello afectaría directamente al alcance de la decisión de adecuación.[21]

[21] Véase también el párr. 38 *supra*.

3.1.2. Excepciones parciales previstas en la LPDP

55. El artículo 58, apartado 1, de la LPDP excluye de la aplicación de determinadas partes de la LPDP (esto es, los artículos 15 a 57) a las cuatro categorías de tratamientos de datos personales descritas a continuación. En concreto, estas excepciones se refieren a las disposiciones de la LPDP relativas a motivos concretos para el tratamiento, ciertas obligaciones en materia de protección de datos, las normas específicas para el ejercicio de los derechos individuales y las normas que regulan la resolución de controversias. Sin embargo, el CEPD toma nota de que algunas disposiciones generales de la LPDP siguen siendo aplicables, como las relativas a los principios sobre protección de datos (artículo 3 de la LPDP) y los derechos individuales (artículo 4 de la LPDP). Además, el artículo 58, apartado 4, de esta ley establece obligaciones específicas relativas a las cuatro categorías de tratamientos de datos mencionadas.

56. En primer lugar, la excepción parcial cubre los datos personales recogidos en virtud de la Ley de Estadística coreana para su tratamiento por las instituciones públicas. En el considerando 27 de su proyecto de decisión, la Comisión Europea indica que el Gobierno coreano ha aclarado que el tratamiento de los datos personales en este contexto normalmente afecta a nacionales coreanos y solo en circunstancias excepcionales puede incluir información sobre extranjeros, en concreto, en el caso de las estadísticas sobre la entrada y salida del territorio o sobre la inversión extranjera. No obstante, según el proyecto de decisión, incluso en tales casos, estos datos normalmente no son transferidos por responsables o encargados del tratamiento establecidos en el EEE, sino que son recogidos directamente por autoridades públicas de Corea.

57. El CEPD toma nota del razonamiento de la Comisión Europea sobre la excepcionalidad de la aplicación de la Ley de Estadística coreana al tratamiento de datos personales transferidos en virtud de la decisión de adecuación. Sin embargo, agradecería un mayor información y garantías sobre las salvaguardias concretas que se aplicarían en caso de que se recogieran más datos personales transferidos desde el EEE con arreglo a dicha Ley de Estadística con el fin de que fueran tratados por las instituciones públicas, en particular, por lo que respecta al ejercicio de los derechos individuales por los interesados, en línea con lo dispuesto en el artículo 89, apartado 2, del RGPD, siempre que no sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines específicos y cuando tales excepciones no sean necesarias para alcanzar esos fines.

58. En este sentido, la aplicación del artículo 4 de la LPDP a este tipo de tratamiento parece ofrecer garantías, pero el CEPD agradecería que en la decisión de adecuación se incluyeran información adicional y aclaraciones sobre las obligaciones específicas impuestas en relación con dichas actividades de tratamiento con arreglo al artículo 58, apartado 4, de la LPDP, en concreto, por lo que respecta a la minimización de datos, los límites a la conservación de los datos, las medidas de seguridad y la tramitación de las reclamaciones.

59. En segundo lugar, la excepción parcial se aplica a los datos personales recogidos o solicitados con el fin de analizar información relacionada con la seguridad nacional. El CEPD es consciente de que, según ha reconocido el TEDH, los Estados disponen de un amplio margen de apreciación en cuestiones de seguridad nacional. También observa que, en virtud del artículo 37, apartado 2, de la Constitución coreana, ninguna limitación de los derechos y libertades, por ejemplo, cuando sea necesario para la protección de la seguridad nacional, puede quebrantar la esencia de dicha libertad o derecho. Por otra parte, toma nota de las salvaguardias previstas en la sección 6 de la notificación n.º 2021-1 relativas al tratamiento de los datos personales por motivos de seguridad nacional, incluida la investigación de las infracciones y la aplicación de las correspondientes medidas. Sin embargo, en este contexto, el CEPD insta a la Comisión Europea a que aclare el alcance de las excepciones, ya que se pregunta si todas las excepciones previstas en el artículo 58, apartado 1, punto 2, de la LPDP (capítulos III a VII) son relevantes para el trabajo de los servicios de inteligencia y si aseguran una equivalencia con los principios de necesidad y proporcionalidad. En particular, insta a la Comisión Europea a que aclare en

qué circunstancias podría un servicio de inteligencia invocar las excepciones. El CEPD considera necesario controlar con atención el efecto de estas limitaciones en la práctica, en especial, en el ejercicio efectivo y la observancia de los derechos de los interesados.

60. En tercer lugar, la excepción parcial se aplica a los *«datos personales tratados temporalmente cuando esto sea necesario y urgente por motivos de seguridad pública, salud pública, etc.»*. Según el considerando 29 del proyecto de decisión de la Comisión Europea, el CPDP realiza una interpretación restrictiva de esta categoría, que se aplica exclusivamente en situaciones de emergencia que requieran una actuación urgente, por ejemplo, para rastrear agentes infecciosos o rescatar y auxiliar a víctimas de catástrofes naturales.

61. El CEPD también hace hincapié en que cualquier excepción al nivel de protección de los datos personales debe interpretarse en sentido restrictivo. Al mismo tiempo, el CEPD observa que la disposición no se encuentra definida de un modo restrictivo y no proporciona una lista exhaustiva de ejemplos de situaciones en las que el tratamiento de datos personales pueda considerarse *«necesario y urgente»*. Por ejemplo, no queda claro al CEPD si las transferencias internacionales de datos relativos a la salud durante la actual pandemia de COVID-19 también quedarían incluidas en el alcance de esta excepción. En vista de lo anterior, el CEPD solicita a la Comisión Europea que ofrezca aclaraciones sobre el alcance de esta excepción y que supervise plenamente su aplicación y alcance para asegurarse de que no conlleve una rebaja del nivel de protección de los datos personales procedentes del EEE tras su transferencia a Corea en virtud de la decisión de adecuación.

62. Por último, la excepción parcial se aplica a los datos personales recogidos o empleados para fines informativos por la prensa, para la actividad misionera llevada a cabo por organizaciones religiosas y para el nombramiento de candidatos por los partidos políticos.[22] Por lo que respecta al tratamiento de datos personales por la prensa para actividades periodísticas, la Comisión Europea señala en el considerando 31 de su proyecto de decisión que el equilibrio entre libertad de expresión y otros derechos, incluido el derecho a la intimidad, se encuentra recogido en la Ley coreana sobre Arbitraje y Acciones, etc., por Perjuicios Provocados por la Información Periodística (en lo sucesivo, la **«Ley de Prensa»**); y presenta una serie de salvaguardias específicas derivadas de esta ley. Sin embargo, el CEPD solicita que la Comisión Europea examine minuciosamente esta excepción y la jurisprudencia pertinente a fin de asegurar que en el marco jurídico coreano también se garantice en la práctica un nivel de protección de datos equivalente.

3.1.3. Motivos para el tratamiento lícito y leal con fines legítimos

63. De acuerdo con las Referencias sobre adecuación, y en consonancia con lo dispuesto en el RGPD, el tratamiento de los datos debe ser lícito, leal y legítimo. La base jurídica según la cual el tratamiento de los datos personales puede ser lícito, leal y legítimo debe establecerse de manera clara. El marco europeo reconoce varios de estos motivos legítimos, incluyendo, por ejemplo, disposiciones en el Derecho nacional, el consentimiento del interesado, la ejecución de un contrato o los intereses legítimos del responsable del tratamiento o de una tercera parte que no invaliden los intereses del interesado.

64. Siguiendo una estructura similar a la del RGPD, la LPDP introduce primero el principio de licitud, lealtad y transparencia (artículo 3, apartados 1 y 2, de la LPDP) y, posteriormente, recoge las normas concretas para su aplicación (artículos 15 a 19 de la LPDP). En concreto, el artículo 15 de esta ley incluye un catálogo de causas legales en las que los responsables del tratamiento de datos personales pueden fundamentar la recogida de datos personales y con arreglo a las cuales pueden usarlos dentro

[22] Por consiguiente, el tratamiento de los datos personales por organizaciones religiosas con motivo de su actividad misionera y el tratamiento de los datos personales por partidos políticos en el contexto del nombramiento de candidatos también se encuentran excluidos del alcance de la decisión de adecuación. Véase también el párr. 37 *supra*, en la sección 2.3.2.

de los fines para los que se recogieron. Estas causas legales son 1) el consentimiento informado del interesado; 2) la autorización prevista en la normativa o la necesidad de cumplir una obligación legal; 3) la necesidad para el desempeño de las funciones de una institución pública; 4) la necesidad para la ejecución o el cumplimiento de un contrato celebrado con un interesado; 5) la necesidad para la protección de la vida, la integridad física o la propiedad del interesado o un tercero frente a un peligro inminente (siempre que no pueda obtenerse el consentimiento previo); y 6) la necesidad de perseguir un interés justificable del responsable del tratamiento de datos personales que sea superior al del interesado.

65. Además, el artículo 17 de la LPDP incluye una lista con las causas legales que justifican la divulgación de datos personales a un tercero: 1) el consentimiento informado del interesado; 2) la autorización prevista en la normativa o la necesidad de cumplir una obligación legal; 3) la necesidad para el desempeño de las funciones de una institución pública y 4) la necesidad para la protección de la vida, la integridad física o la propiedad del interesado o un tercero frente a un peligro inminente (siempre que no pueda obtenerse el consentimiento previo). Incluso en ausencia del consentimiento del interesado, se permite la divulgación de datos personales cuando esta tenga lugar dentro de un ámbito que se encuentre razonablemente relacionado con los fines para los que se recogieron inicialmente dichos datos (artículo 17, apartado 4, de la LPDP).

66. El artículo 18 de la LPDP establece unas normas específicas que autorizan el uso y la divulgación de datos personales fuera del alcance del fin original de la recogida o el suministro de los datos. Nuevamente, el consentimiento es, entre otros, uno de los motivos contemplados en dichas normas.

67. Pese a reconocer la sustancial similitud entre el Derecho coreano y el RGPD en lo referente al principio de licitud y la existencia de un derecho general a la suspensión (artículo 37 de la LPDP), que también puede invocarse cuando los datos personales se traten sobre la base de un consentimiento, el CEPD desea poner de relieve la ausencia de un derecho general a retirar el consentimiento en la LPDP.[23] En vista de la importancia del consentimiento como causa legal en todos los casos descritos, y teniendo en cuenta la función de los derechos individuales en los sistemas jurídicos de protección de datos con el fin de salvaguardar los derechos y libertades fundamentales de los interesados, el CEDP insta a la Comisión Europea a que evalúe con mayor grado de detalle los efectos de la ausencia de un derecho general a retirar el consentimiento en el Derecho coreano y a que ofrezca más garantías de que se asegurará en todo momento un nivel de protección de datos básico similar al previsto en el RGPD, aclarando, cuando sea necesario, la función del derecho a la suspensión en este contexto concreto.

3.1.4. Principio de limitación de la finalidad

68. Las Referencias sobre adecuación establecen, en consonancia con lo dispuesto en el RGPD, que los datos personales deben ser tratados para un fin específico y utilizados posteriormente solo en la medida en que esto no sea incompatible con el fin del tratamiento.

[23] Aunque los interesados pueden negar el consentimiento en determinadas circunstancias: véase, por ejemplo, el artículo 18, apartado 3, punto 5, de la LPDP. En cambio, el derecho a retirar el consentimiento solo parece existir en ciertos casos concretos: con arreglo al artículo 27, apartado 1, punto 2, de la LPDP, los interesados tienen derecho a retirar el consentimiento cuando no deseen que sus datos personales se transfieran a un tercero como consecuencia de la transferencia, total o parcial, del negocio del responsable del tratamiento de datos personales, de una fusión, etc.; con arreglo al artículo 39, apartado 7, de la LPDP, los usuarios pueden retirar en todo momento el consentimiento a la recogida, el uso y el suministro de datos personales por parte del proveedor de servicios de información y comunicaciones, etc.; y, con arreglo al artículo 37 de la LIC, el titular de la información crediticia puede revocar el consentimiento prestado a un proveedor o usuario de información crediticia.

69. De conformidad con lo establecido en el artículo 3, apartados 1 y 2, de la LPDP, los responsables del tratamiento de datos personales precisarán de manera explícita cuáles son los fines del tratamiento y se asegurarán de que este sea compatible con dichos fines. Pese a que este principio se confirma en otras disposiciones (el artículo 15, apartado 1, el artículo 18, apartado 1, y el artículo 19, apartado 1, de la LPDP), en determinadas circunstancias se permite el tratamiento para fines «razonablemente relacionados» (véase el artículo 17, apartado 4, de la LPDP)[24], así como el uso y el suministro de datos personales para fines distintos de los precisados (véanse los artículos 18 y 19 de la LPDP)[25].

70. El CEPD entiende que, en el caso de las transferencias de datos personales a la República de Corea desde el EEE en virtud de la decisión de adecuación, el fin por el que los responsables del tratamiento establecidos en el EEE hubieran recogido los datos personales constituirá la finalidad para la que se transfieren los datos a los efectos de su tratamiento por el destinatario responsable establecido en Corea. Solo se permitirá que el responsable establecido en Corea modifique la finalidad en las circunstancias previstas en el artículo 18, apartado 2, puntos 1 a 3, de la LPDP, *«a menos que, previsiblemente, ello pudiera vulnerar de manera injusta el interés de un interesado o un tercero»*[26]. En este sentido, el CEPD toma nota de lo indicado por la Comisión Europea en el considerando 55 del proyecto de decisión: cuando la normativa autorice modificaciones en la finalidad, dichas normas deberán respetar el derecho fundamental a la intimidad y la protección de datos. El CEPD observa, sin embargo, que no se ha proporcionado ninguna información concreta que respalde este enunciado. Por ejemplo, no se ha hecho referencia al artículo 37 de la Constitución coreana. Por tanto, el CEPD insta a la Comisión Europea a que ofrezca más garantías en el proyecto de decisión con el fin de asegurar que cualquier norma que autorice una modificación del fin del tratamiento también deba respetar los derechos y libertades fundamentales a la intimidad y la protección de datos de los interesados.

3.1.5. Principio de calidad de los datos y proporcionalidad

71. Las Referencias sobre adecuación establecen que los datos deberán ser precisos y, en caso necesario, se mantendrán actualizados. Los datos deberán ser adecuados, pertinentes y no excesivos con respecto a los fines para los que se traten.

72. En virtud de la LPDP, los responsables del tratamiento de datos personales deben velar por que estos datos sean precisos, estén completos y se encuentren actualizados en la medida en que sea necesario para los fines para los que se traten (artículo 3, apartado 3, de la LPDP). Los responsables del tratamiento de datos personales deben recoger, exclusivamente, los datos personales imprescindibles para alcanzar el fin concreto perseguido. Al respecto, deberán asumir, además, la carga de la prueba (artículo 16, apartado 1, de la LPDP).

73. Teniendo en cuenta todo lo anterior, el CEPD comparte la evaluación realizada en este sentido por la Comisión Europea en lo referente a la equivalencia sustancial entre el nivel de protección de la LPDP y el ofrecido por el RGPD.

3.1.6. Principio de retención de datos

74. Según lo dispuesto en las Referencias sobre adecuación, por regla general, los datos deben almacenarse durante un período no superior al necesario para los fines para los que se traten. Como se observa en el artículo 21, apartado 1, de la LPDP, este principio también existe en el Derecho coreano. En virtud de la LPDP, los responsables del tratamiento de datos personales deben destruir estos datos sin demora una vez que devengan innecesarios como consecuencia de la expiración del

[24] En cuyo caso, deberá haberse determinado previamente la compatibilidad de los fines sobre la base de los criterios establecidos en el artículo 14, apartado 2, del decreto de aplicación de la LPDP.
[25] Véase también lo dispuesto en el párr. 66 *supra*.
[26] Artículo 18, apartado 2, de la LPDP.

plazo de conservación o por haberse alcanzado el fin previsto para el tratamiento, salvo que resulte aplicable un plazo de conservación establecido en la normativa.

75. Preocupa, sin embargo, al CEPD el hecho de que el citado artículo 21, apartado 1, de la LPDP no resulte aplicable a los datos personales seudonimizados. El CEPD toma nota de que, con arreglo a lo dispuesto en la sección 4, inciso iii, de la notificación n.º 2021-1, *«[c]uando un responsable del tratamiento de datos personales trate datos seudonimizados para fines de elaboración de estadísticas, investigación científica, llevanza de registros públicos, etc., y siempre que los datos seudonimizados no hayan sido destruidos una vez satisfecho el fin específico del tratamiento en consonancia con lo dispuesto en el artículo 37 de la Constitución y el artículo 3 ("principios para la protección de datos personales") de la Ley, procederá a hacer anónimos los datos con vistas a garantizar que ya no puedan identificar a una persona concreta, por sí mismos o en combinación con otros datos, teniendo en cuenta de un modo razonable el tiempo, el coste, la tecnología, etc., con arreglo al artículo 58, apartado 2, de la LPDP»*. Teniendo en cuenta nuevamente la importancia de la notificación n.º 2021-1 y con vistas a disponer de certeza jurídica de la equivalencia del nivel de protección de los datos personales transferidos a la República de Corea en virtud de la decisión de adecuación, el CEPD reitera su llamamiento a la Comisión Europea para que ofrezca más información específica sobre el modo en que la notificación n.º 2021-1 resulta vinculante y en que se garantizan su coercibilidad y validez[27].

3.1.7. Principio de seguridad y confidencialidad

76. Tal como se describe en las Referencias sobre adecuación, el principio de seguridad y confidencialidad requiere que las entidades que traten los datos personales se aseguren de que estos sean tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas. El nivel de seguridad debe tener en cuenta el estado de la técnica y los costes relacionados.

77. La Comisión Europea ha identificado un principio similar sobre la seguridad de los datos en el artículo 3, apartado 4, de la LPDP, que se detalla en el artículo 29 de esta ley. Además, resultan aplicables disposiciones relativas a la seguridad de los datos personales en aquellos casos en los que el responsable del tratamiento contrate un «subcontratista». La seguridad del tratamiento debe garantizarse mediante unas salvaguardias técnicas y organizativas, que también deben incorporarse al acuerdo vinculante sobre el tratamiento de los datos (artículo 26 de la LPDP y artículo 28 del decreto de aplicación de la LPDP). Además, la LPDP establece unas obligaciones específicas en caso de violación de la seguridad de los datos, incluida la obligación de notificar dicha violación a los interesados afectados, así como a la autoridad de control cuando el número de interesados afectados supere el número previsto (artículo 34 de la LPDP, en relación con el artículo 39 del decreto de aplicación de la LPDP), salvo que los datos en cuestión sean datos personales seudonimizados tratados para fines estadísticos, de investigación científica o de archivo en beneficio de un interés público (artículo 28, apartado 7, de la LPDP). Preocupan nuevamente[28] al CEPD las amplias excepciones relativas a los datos seudonimizados y, por tanto, el CEPD reitera su llamamiento a la Comisión Europea para que esta evalúe con mayor grado de detalle este aspecto a fin de asegurarse de que el Derecho coreano prevea un nivel de protección sustancialmente equivalente[29].

[27] Véanse también el párr. 51 *supra* incluido en la sección 3.1.1.1 del presente dictamen y el párr. 52, donde se exponen las preocupaciones generales del CEPD en relación con los efectos de la seudonimización en el Derecho coreano.
[28] Tal como se ha indicado previamente en los párrafos 51-52 *supra* y en la sección 3.1.1.1 del presente dictamen.
[29] Véanse también las secciones 3.1.6 y 3.1.10 del presente dictamen.

78. No obstante lo anterior, el CEPD está satisfecho en general con la evaluación y la conclusión de la Comisión Europea relativas a la equivalencia sustancial del Derecho coreano por lo que se refiere al principio de seguridad y confidencialidad.

3.1.8. Principio de transparencia

79. Tal como se recoge en el artículo 5, apartado 1, letra a), del RGPD, la transparencia es un principio fundamental del sistema de protección de datos de la UE. El considerando 39 del RGPD subraya la función crucial de este principio, cuando afirma que *«[p]ara las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. [...] Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento»*.

80. Las Referencias sobre adecuación mencionan expresamente la «transparencia» como uno de los principios relativos al contenido que debe tenerse en cuenta al evaluar si el nivel de protección ofrecido por un tercer país es sustancialmente equivalente. En concreto, establecen que *«[t]odos [sic] las personas deben ser informadas acerca de los elementos principales del tratamiento de sus datos personales en forma clara, de fácil acceso, concisa, transparente e inteligible. Dicha información debe incluir los fines del tratamiento, la identidad del responsable, los derechos a su disposición y otra información en la medida en que esto sea necesario para garantizar la lealtad. En determinadas condiciones, pueden existir ciertas excepciones a este derecho de información, como, por ejemplo, salvaguardar investigaciones penales, la seguridad del Estado, la independencia judicial y los procedimientos judiciales u otros objetivos importantes de interés público general, como en el caso del artículo 23 del RGPD»*.

81. Al igual que el RGPD, la LPDP contiene un principio general de transparencia que obliga a los responsables del tratamiento de datos personales a hacer públicas sus políticas de privacidad y otras cuestiones relacionadas con el tratamiento de los datos personales (artículo 3, apartado 5, de la LPDP). Se aplican unas obligaciones de información específicas cuando los responsables del tratamiento de datos personales pretenden recabar el consentimiento de los interesados a la recogida y el tratamiento de datos personales (artículo 15, apartado 2, de la LPDP), al intercambio de datos personales con un tercero (artículo 17, apartado 2, de la LPDP) y al tratamiento para fines distintos de los precisados (artículo 18, apartado 3, de la LPDP). Cabe señalar que estas obligaciones de información también se aplican *mutatis mutandis* al subcontratista (artículo 26, apartado 7, de la LPDP).

82. El CEPD valora y acoge de buen grado las salvaguardias adicionales previstas en la sección 3, incisos i) y ii), de la notificación n.º 2021-1[30] en relación con la información que se debe proporcionar a los interesados cuando sus datos sean transferidos por una entidad establecida en el EEE, teniendo en cuenta que, con arreglo al artículo 20, apartado 1, de la LPDP, cuando los datos no se hayan obtenido del interesado, solo se informará a estos previa solicitud, mientras que el derecho general a ser informado solo se reconoce en el artículo 20, apartado 2, de la LPDP cuando determinadas operaciones de tratamiento superen los límites previstos en el decreto de aplicación de la LPDP (artículo 15, apartado 2).

83. En general, el CEPD estima que el nivel de protección ofrecido por el Derecho coreano en lo referente al principio de transparencia es sustancialmente equivalente al proporcionado por el RGPD.

[30] Anexo I del proyecto de decisión.

3.1.9. Categorías especiales de datos personales

84. Para que se reconozca que el sistema de protección de datos de un país tercero ofrece un nivel de protección de los datos personales sustancialmente equivalente al del RGPD, deben existir unas salvaguardias específicas para aquellas situaciones que afecten a las categorías especiales de datos personales contempladas en los artículos 9 y 10 del RGPD.

85. En virtud de la LPDP, se aplican unas disposiciones específicas al tratamiento de los datos denominados «sensibles», que comprenden los datos personales que revelen la ideología, las creencias, la adhesión a un sindicato o partido político o la desvinculación de estos, las opiniones políticas, la salud, la vida sexual y otra información personal que previsiblemente amenace de manera considerable la intimidad de cualquier interesado; así como, con arreglo al decreto de aplicación de la LPDP, la información relativa al ADN obtenida con pruebas genéticas, los datos que muestren los antecedentes penales, la información personal derivada del tratamiento técnico concreto de los datos relativos a las características físicas, fisiológicas o conductuales de una persona para el fin de identificar unívocamente a dicha persona, y los datos personales que revelen el origen racial o étnico.

86. Al igual que el RGPD, el Derecho coreano en materia de protección de datos prohíbe el tratamiento de datos sensibles a menos que: 1) se informe de ello al interesado y se obtenga su consentimiento expreso; o 2) existan disposiciones legales que autoricen el tratamiento (artículo 23, apartado 2, de la LPDP).

87. Teniendo en cuenta lo anterior, el CEPD comparte en principio la conclusión de la Comisión Europea según la cual el Derecho coreano es sustancialmente equivalente en lo referente al tratamiento de las categorías especiales de datos personales. Sin embargo, el CEPD desea señalar que no se le han facilitado el manual sobre la LPDP ni aclaraciones del CPDP sobre la interpretación del término «vida sexual» en un sentido inclusivo de la orientación o las preferencias sexuales, que no se han incluido en la notificación n.º 2021-1. En consecuencia, el CEPD solicita a la Comisión Europea que proporcione esta información para que pueda evaluarla de manera independiente. También insta a la Comisión Europea a que cite expresamente los documentos en los que pueda encontrarse la información sobre este tema a la que hace referencia.

3.1.10. Derechos de acceso, rectificación, supresión y oposición

88. En el marco jurídico coreano, los derechos de los interesados se reconocen en el artículo 3, apartado 5, de la LPDP, en virtud del cual el responsable del tratamiento de datos personales garantizará los derechos de los interesados indicados en el artículo 4 de la LPDP y desarrollados en los artículos 35 a 37 y 39, y el artículo 39, apartado 2, de la LPDP, y, por lo que respecta a la «información crediticia de carácter personal» (esto es, la información necesaria para determinar la solvencia de las partes en operaciones financieras o comerciales, tal como se explica en el considerando 3 del proyecto de decisión), en los artículos 37 y 38, y el artículo 38, apartado 3, de la LIC.

89. El CEPD observa que el derecho de acceso (y de rectificación y supresión, que puede ejercer un *«interesado que haya accedido a sus datos personales con arreglo al artículo 35»* de la LPDP) puede ser limitado o negado *«cuando el acceso esté prohibido o restringido en virtud de la legislación»*, *«cuando el acceso pueda poner en riesgo la vida o la integridad física de un tercero o vulnerar de manera injustificada el derecho de propiedad u otros intereses de cualquier otra persona»* y, adicionalmente en el caso de las instituciones públicas, cuando la concesión del acceso *«dificulte gravemente»* el desempeño de ciertas funciones que se especifican en el artículo 35, apartado 4, de

la LPDP[31]. El artículo 37 de la LPDP contiene disposiciones similares relacionadas con el derecho de suspensión del tratamiento de datos personales.

90. El artículo 23 del RGPD permite que el Derecho de la Unión o de los Estados miembros limite los derechos individuales cuando dicha limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, entre otras cosas, la protección del interesado o de los derechos y libertades de otros y *«una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g)»* de ese mismo artículo.

91. Teniendo en cuenta todo lo anterior, el CEPD acogería de buen grado unas garantías generales en el proyecto de decisión en relación con la necesidad de que toda norma o ley que limite los derechos de los interesados cumpla los requisitos establecidos en la Constitución coreana, según los cuales los derechos fundamentales únicamente podrán limitarse cuando esto sea necesario por motivos de seguridad nacional o para el mantenimiento del orden público y esta limitación no podrá afectar a la esencia de la libertad o del derecho de que se trate (artículo 37, apartado 2, de la Constitución coreana).

92. Por otra parte, por lo que respecta a la excepción como resultado de *«vulnerar de manera injustificada el derecho de propiedad u otros intereses de cualquier otra persona»*, el CEPD toma nota de que esto *«implica que debe encontrarse un equilibrio entre, de un lado, los derechos y libertades reconocidos por la Constitución al interesado y, de otro, los reconocidos a las demás personas»*[32]. Sin embargo, solicita a la Comisión Europea que examine minuciosamente la aplicación de esta excepción y la jurisprudencia pertinente a fin de asegurar que en el marco jurídico coreano también se garantice en la práctica un nivel de protección equivalente de los derechos de los interesados.

93. En esta misma línea, el CEPD agradecería una atenta supervisión de la aplicación de la excepción a los organismos públicos, en particular, en aquellos casos en los que se considere que la concesión del acceso *«dificulte gravemente»* el desempeño de sus funciones, teniendo en cuenta que esta expresión parece ser más amplia que la empleada en otras disposiciones de la LPDP, p. ej., en el artículo 18, apartado 2, punto 5[33], y debe interpretarse de manera restrictiva a fin de evitar las limitaciones indebidas en los derechos de los interesados.

94. Por otra parte, no queda claro al CEPD si las excepciones en virtud de las cuales las disposiciones relativas a la transparencia previa solicitud (artículo 20 de la LPDP) y los derechos individuales (artículos 35 a 37 de la LPDP) —además de las disposiciones similares relacionadas con los requisitos para los proveedores de servicios de información y comunicaciones (artículo 39, apartado 2 y apartados 6 a 8, de la LPDP) y las recogidas en la LIC (véanse las excepciones contempladas en el artículo 40, apartado 3, de la LIC)— no resultan aplicables a los datos seudonimizados cuando estos se tratan con fines estadísticos, de investigación científica o de archivo en beneficio de un interés público (artículo 28, apartado 7, de la LPDP) están en consonancia con las garantías previstas en el marco jurídico europeo.

95. Estas disposiciones parecen introducir una excepción general para este tipo de tratamiento. Por contra, el RGPD prevé que, cuando los datos personales (incluidos los datos personales

[31] Las mismas condiciones y excepciones previstas en la LPDP en relación con los derechos de acceso y rectificación también se aplican al derecho de acceso y rectificación previsto en la LIC para la información crediticia de carácter personal (nota 135 a pie de página del proyecto de decisión).

[32] Considerando 76 del proyecto de decisión.

[33] Por lo que respecta a las excepciones a la limitación al uso y el suministro de datos personales para fines distintos de los precisados, el artículo 18, apartado 2, punto 5, de la LPDP hace referencia a situaciones en las que, *«resulta imposible»* para las instituciones públicas desempeñar sus funciones.

seudonimizados) se traten con fines de investigación científica o histórica o estadísticos, el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos del interesado, pero *«siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines»*, siendo la seudonimización meramente una de las medidas técnicas y organizativas que pueden adoptarse para garantizar el respeto del principio de minimización de datos (artículo 89, apartado 1, del RGPD).

96. La Comisión Europea considera que la excepción contemplada en el artículo 28, apartado 7, de la LPDP también se encuentra justificada en vista del artículo 28, apartado 5, de dicha ley, en virtud del cual se prohíbe expresamente al responsable del tratamiento de datos personales tratar los datos seudonimizados con el fin de identificar a una persona concreta, y desea hacer referencia en este sentido al enfoque del artículo 11, apartado 2, del RGPD (en relación con el considerando 57 del RGPD) sobre el tratamiento que no requiere la identificación del interesado[34].

97. De hecho, con arreglo a lo dispuesto en el artículo 11 del RGPD, no podrá obligarse al responsable del tratamiento a *«mantener, obtener o tratar información adicional con vistas a identificar al interesado»* con la única finalidad de cumplir el RGPD si, para los fines previstos, puede tratar datos personales que no requieren o ya no requieren la identificación de un interesado. En tales casos, cuando el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, no se aplicarán los derechos de este. Tal como señala la Comisión Europea[35], el RGPD requiere, por tanto, en tales casos una imposibilidad «práctica» para el responsable del tratamiento y, con arreglo al principio de minimización de datos, reconoce que no necesitan tratarse datos adicionales «debido al» RGPD.

98. Sin embargo, el CEPD estima que esta situación es diferente a aquella en la que un responsable del tratamiento se encuentra en la práctica en condiciones de identificar al interesado, pero se lo impide alguna disposición legal, como la incluida en el artículo 28, apartado 5, de la LPDP. El CEPD agradece al respecto las aclaraciones introducidas por el CPDP en la notificación n.º 2021-1[36], donde se confirma que la sección 3 de la LPDP (que incluye el artículo 28, apartado 7) y la excepción prevista en el artículo 40, apartado 3, de la LIC solo resultan aplicables cuando los datos seudonimizados se tratan con fines estadísticos, de investigación científica o de archivo en beneficio de un interés público. No obstante, y además de las preocupaciones ya mencionadas acerca de la naturaleza vinculante de la notificación n.º 2021-1[37], el CEPD aún se pregunta si las excepciones previstas en el artículo 28, apartado 7, de la LPDP y el artículo 40, apartado 3, de la LIC pueden considerarse necesarias y proporcionadas en una sociedad democrática, en la medida en que limitan los derechos del interesado en todos los casos en los que los datos seudonimizados se traten para dichos fines, es decir, incluso cuando el responsable del tratamiento de los datos personales se encuentre en la práctica en condiciones de identificar al interesado y no sea probable que los derechos imposibiliten u obstaculicen gravemente el logro de los fines en cuestión.

99. En particular, el CEPD considera que estas excepciones pueden no estar justificadas y precisarían de un análisis más minucioso, especialmente cuando las aplique el responsable del tratamiento de datos personales que seudonimice los datos *«con fines estadísticos, de investigación científica y de archivo*

[34] Debe tenerse en cuenta que este mismo razonamiento no podría aplicarse tal cual a la excepción prevista en el artículo 40, apartado 3, de la LIC en relación con el tratamiento de información crediticia seudonimizada, puesto que el artículo 40, apartado 2, punto 6, estipula que *«las sociedades de información crediticia, etc., no tratarán datos seudonimizados de modo tal que pueda identificarse a una persona concreta con un fin lucrativo o desleal»* y, por tanto, podría permitir la reidentificación para un fin legítimo, como dar respuesta a la solicitud de un interesado.

[35] Véase el considerando 82 del proyecto de decisión.

[36] Sección 4 del anexo I del proyecto de decisión.

[37] Véase la sección 3.1.1.1 *supra*.

en beneficio de un interés público, etc.», de conformidad con lo dispuesto en el artículo 28, apartado 2, de la LPDP, *«sin el consentimiento de los interesados»* (y sin proporcionar la información prevista en el artículo 20 de la LPDP)[38], en aquellos casos en que este responsable conserve los datos que permitan la reidentificación. Con arreglo al RGPD, cualquier interesado debe poder ejercer sus derechos en relación con cualquier dato que pueda identificarlo o singularizarlo, incluso cuando los datos se encuentren «seudonimizados», salvo que resulte aplicable el citado artículo 11 del RGPD. Al respecto, el CEPD observa que únicamente cuando estos datos se proporcionen a un tercero para dichos fines estadísticos, de investigación científica y de archivo, no deberían incluirse los datos que puedan utilizarse para identificar a una persona concreta y, por tanto, solo el responsable del tratamiento de datos personales al que se proporcionen los datos seudonimizados en virtud del artículo 28, apartado 2, punto 2, de la LPDP probablemente no esté «en la práctica» en condiciones de identificar al interesado si no dispone de datos adicionales.

100. En resumen, teniendo en cuenta que, tal como reconoce la Comisión Europea, *«en lugar de contar con la seudonimización como posible salvaguardia, la LPDP la impone como condición previa para llevar a cabo determinadas actividades de tratamiento con fines estadísticos, de investigación científica y archivo en beneficio de un interés público (como poder tratar los datos sin consentimiento o combinar diferentes conjuntos de datos)»*[39], pero prevé para tales casos importantes limitaciones en los derechos del interesado, el CEPD insta a la Comisión Europea a que examine con más detalle las excepciones contempladas en el artículo 28, apartado 7, de la LPDP y el artículo 40, apartado 3, de la LIC, y a que supervise atentamente su aplicación y la correspondiente jurisprudencia[40] con el fin de garantizar que los derechos de los interesados no se limiten de manera indebida cuando los datos personales transferidos con arreglo a la decisión de adecuación se traten para estos fines, teniendo en cuenta que, en muchos casos, estos derechos también ayudan al responsable del tratamiento a garantizar la calidad de los datos tratados.

3.1.11. Limitaciones en materia de transferencias ulteriores

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

102. Por lo que respecta a las transferencias ulteriores a subcontratistas (esto es, los «encargados del tratamiento») establecidos en países terceros, el CEPD observa que el marco jurídico coreano no contiene normas especiales que regulen estos casos y que, tal como ha valorado la Comisión Europea[41], los responsables del tratamiento de datos personales establecidos en corea deben garantizar el cumplimiento de las disposiciones sobre subcontratación previstas en la LPDP (artículo 26 de la LPDP) mediante un instrumento jurídicamente vinculante y responderán por los datos personales objeto de subcontratación (artículo 26 de la LPDP).

---

[38] Véase el artículo 28, apartado 7, de la LPDP, tal como se explica en la notificación n.º 2021-1, con arreglo al cual determinadas salvaguardias incluidas en la LPDP, esto es los *«artículos 20, 21 y 27, el artículo 34, apartado 1, los artículos 35 a 37 y el artículo 39, apartados 3, 4 y 6 a 8»* no se aplicarán a los datos seudonimizados tratados con fines de elaboración de estadísticas, investigación científica, llevanza de registros públicos, etc.

[39] Considerando 42 del proyecto de decisión.

[40] Véanse, por ejemplo, los recursos de inconstitucionalidad publicados en OpenNet (información disponible, únicamente en coreano, en https://opennet.or.kr/19909).

[41] Considerando 87 del proyecto de decisión.

103. Por cuanto hace a las transferencia ulteriores a terceros (esto es, otros responsables del tratamiento de datos personales), el artículo 17, apartado 3, de la LPDP obliga al responsable del tratamiento de datos personales coreano a notificar a los interesados las transferencias al extranjero y a obtener su consentimiento a dichas transferencias, y establece que dicho responsable *«no celebrará ningún contrato con el fin de realizar una transferencia transfronteriza de datos personales contraviniendo la LPDP»*. En opinión del CEPD, esta última disposición garantizará, tal como ha valorado la Comisión Europea[42], que ningún contrato en virtud del cual pretendan realizarse transferencias transfronterizas pueda contener obligaciones que contravengan los requisitos impuestos por la LPDP al responsable del tratamiento de los datos personales y podría, por tanto, considerarse una salvaguardia. Sin embargo, no impone obligación alguna de establecer salvaguardias con el fin de garantizar que el destinatario ofrezca el mismo nivel de protección que confiere la LPDP. Por tanto, el CEPD toma nota de que generalmente se utilizará el consentimiento informado del interesado como base para las transferencias de datos por responsables del tratamiento de datos personales establecidos en Corea a destinatarios establecidos en países terceros.

104. Al respecto, se agradecen las aclaraciones adicionales introducidas por el CPDP en la notificación n.º 2021-1 en relación con la obligación de informar a las personas acerca del tercer país al que vayan a enviarse los datos[43], ya que, tal como ha subrayado la Comisión Europea[44], esto ayudaría a los interesados establecidos en el EEE a tomar una decisión informada sobre su consentimiento o no a la transferencia al extranjero.

105. Sin embargo, tal como también se estimó en el Dictamen 28/2018 sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón, debe subrayarse que, en virtud del RGPD, debe informarse explícitamente a los interesados, antes del consentimiento, sobre los posibles riesgos de tales transferencias derivados de la ausencia de una protección adecuada en el tercer país y la ausencia de salvaguardias apropiadas. Dicha notificación debería incluir, por ejemplo, información sobre la posibilidad de que en el tercer país pudiera no haber una autoridad de supervisión o que los principios de tratamiento de datos o los derechos de los interesados pudieran no estar previstos en el tercer país[45]. Para el CEPD, el suministro de esta información es esencial para permitir que el interesado preste su consentimiento informado con pleno conocimiento de estos hechos concretos de la transferencia[46]. Por tanto, el CEPD tiene ciertas reservas sobre las conclusiones alcanzadas por la Comisión Europea en el proyecto de decisión de adecuación en relación con este tipo concreto de transferencias. Por lo general, los interesados desconocen el marco jurídico de los terceros países en materia de protección de datos. En consecuencia, no cabe concluir que el interesado pueda evaluar el riesgo de la transferencia sobre la base del mero conocimiento del país de destino: es necesario en este sentido que, antes de prestar su consentimiento, disponga de información clara sobre los riesgos concretos de dicha transferencia de datos personales a un país que se encuentre fuera del territorio de la República de Corea.

106. Por tanto, el CEPD invita a la Comisión Europea a garantizar que la información que deba proporcionarse al interesado *«sobre las circunstancias específicas de la transferencia»* incluya información sobre los posibles riesgos de las transferencias derivados de la ausencia de una protección adecuada en el país tercero y de la ausencia de unas salvaguardias adecuadas. Esto es importante para que el CEPD pueda evaluar si los requisitos relativos al consentimiento son sustancialmente equivalentes a los previstos en el RGPD.

[42] Considerando 88 del proyecto de decisión.
[43] *Ibid*.
[44] *Ibid*.
[45] Directrices 2/2018 del CEPD sobre las excepciones a lo dispuesto en el artículo 49 del Reglamento (UE) 2016/679, de 25 de mayo de 2018, p. 8.
[46] Directrices 2/2018 del CEPD sobre las excepciones a lo dispuesto en el artículo 49 del Reglamento (UE) 2016/679, de 25 de mayo de 2018, p. 7.

107. Además, agradecería que en la decisión de adecuación se incluyeran garantías de que los responsables del tratamiento de datos personales establecidos en Corea no realizarán transferencias de datos personales a terceros países en aquellas situaciones en las que, con arreglo al RGPD, no pueda prestarse un consentimiento válido, p. ej., cuando exista un desequilibrio de poder.

108. En relación con aquellos casos en los que el responsable del tratamiento de datos personales pueda suministrar datos personales a un tercero que se encuentre en el extranjero sin el consentimiento del interesado; esto es, 1) si los datos personales se suministran dentro de un ámbito que se encuentre razonablemente relacionado con los fines iniciales por los que se recogieron, con arreglo al artículo 17, apartado 4, de la LPDP; y 2) si los datos personales pueden suministrarse a un tercero en los casos excepcionales mencionados en el artículo 18, apartado 2, de la LPDP; el CEPD toma nota de las aclaraciones ofrecidas por el CPDP en la sección 2 de la notificación n.º 2021-1 (y agradece el deber, impuesto al responsable del tratamiento establecido en Corea y al destinatario extranjero, de garantizar, por medio de un instrumento jurídicamente vinculante, como un contrato, un nivel de protección equivalente al ofrecido por la LPDP, también en relación con los derechos de los interesados).

3.1.12. Mercadotecnia directa

109. De conformidad con el artículo 21, apartados 2 y 3, del RGPD y las Referencias sobre adecuación, el interesado siempre debe poder oponerse, sin coste alguno, al tratamiento de datos con fines de elaboración de perfiles y mercadotecnia directa.

110. Por lo que respecta al derecho a la suspensión previsto en el artículo 37 de la LPDP, el CEPD observa que la Comisión Europea considera que este derecho también resulta aplicable cuando los datos se usan con fines de mercadotecnia directa[47]. Sin embargo, el CEPD agradecería una información y unas aclaraciones adicionales en el proyecto de decisión en relación con esta valoración y, en particular, con la aplicación práctica del derecho a la suspensión en el contexto de la mercadotecnia directa (p. ej., mediante referencias a la jurisprudencia pertinente, etc.). Al respecto, el CEPD también desea poner de relieve que el derecho a solicitar a un proveedor o usuario de información crediticia que deje de ponerse en contacto con el interesado con el fin de presentar productos o servicios, o animar a la compra de productos o servicios, se establece expresamente en la LIC (artículo 37, apartado 2).

111. Además, tal como lo reconoce la Comisión Europea[48], en el marco jurídico coreano, dicho tratamiento requiere por lo general el consentimiento específico (adicional) del interesado (véanse el artículo 15, apartado 1, punto 1, y el artículo 17, apartado 2, punto 1 de la LPDP).

112. Puesto que no puede descartarse que los datos personales transferidos desde el EEE puedan tratarse en Corea con dichos fines, el CEPD también agradecería que en la decisión de adecuación se introdujeran aclaraciones sobre la existencia del derecho del interesado a retirar el consentimiento[49] y sobre el derecho a que se borren sus datos personales y dejen de tratarse cuando el tratamiento tenga por base jurídica el consentimiento (como ocurre en el caso del tratamiento realizado con fines de mercadotecnia) y el interesado lo haya retirado.

[47] Considerando 79 del proyecto de decisión.
[48] *Ibid*.
[49] Véase también lo dispuesto en el párr. 67 *supra*. Pese a que la posibilidad de revocar el consentimiento se contempla de manera clara en el artículo 37, apartado 1, de la LIC, este derecho únicamente se menciona en dos ocasiones en la LPDP para las circunstancias específicas indicadas en el artículo 27, apartado 1, punto 2, y el artículo 39, apartado 7.

3.1.13. Decisiones automatizadas y elaboración de perfiles

113. Tal como lo reconoce la Comisión Europea en su proyecto de decisión[50], la LPDP y su decreto de aplicación no contienen disposiciones generales que aborden la cuestión de las decisiones que afecten a los interesados y se basen exclusivamente en el tratamiento automatizado de datos personales. Aun así, el ordenamiento jurídico coreano prevé este derecho en la LIC, que contiene normas relativas a las decisiones automatizadas (artículo 36, apartado 2), pese a que su aplicación parece estar excluida del alcance de la supervisión del CPDP (y, por tanto, del alcance del presente proyecto de decisión: véase la sección 2.3.2 *supra* sobre el alcance del proyecto de decisión).

114. Como ya estimaron el Grupo de Trabajo del Artículo 29[51] en su Dictamen 01/2016 sobre el Escudo de la Privacidad y el CEPD en su dictamen previo sobre la decisión de adecuación relativa a Japón[52], la creciente importancia de la toma de decisiones automatizada, la elaboración de perfiles y la inteligencia artificial sugieren la necesidad de adoptar un enfoque más proteccionista al respecto. En contra de lo que argumenta la Comisión Europea[53], según la cual es poco probable que la ausencia de normas específicas en la LPDP sobre la toma automatizada de decisiones pueda afectar al nivel de protección de los datos personales recogidos en la UE (puesto que toda decisión basada en el tratamiento automatizado normalmente sería adoptada por el responsable del tratamiento de la UE que tenga una relación directa con el interesado de que se trate), el CEPD considera que no puede descartarse que un responsable del tratamiento de datos personales establecido en Corea pueda recurrir a la toma de decisiones automatizada para los datos transferidos en virtud de la decisión de adecuación (por ejemplo, en el contexto del empleo, para evaluar el rendimiento laboral, la integridad, la conducta, etc.).

115. El desarrollo de nuevas tecnologías permite a las empresas adoptar más fácilmente o considerar la adopción de sistemas automatizados de toma de decisiones, que pueden debilitar la posición de los interesados. Cuando las decisiones tomadas exclusivamente por dichos sistemas automatizados repercuten en la situación jurídica de los interesados o les afectan significativamente (por ejemplo, mediante su inclusión en listas negras y, por tanto, privando a las personas de sus derechos), resulta fundamental ofrecer unas garantías suficientes, incluido el derecho a ser informado sobre las razones específicas que sustentan la decisión y la lógica aplicada, a corregir información inexacta o incompleta, y a impugnar la decisión cuando esta haya sido adoptada sobre unos hechos incorrectos.[54]

116. En este contexto, preocupa al CEPD la falta de disposiciones legales en la LPDP sobre la toma de decisiones automatizada y, por tanto, el CEPD insta a la Comisión Europea a que aborde esta cuestión y siga observando el desarrollo del marco legislativo coreano al respecto.

3.1.14. Responsabilidad proactiva

117. El marco jurídico coreano contiene varias disposiciones con las que se pretende garantizar que los responsables del tratamiento de datos personales adopten unas medidas técnicas y organizativas adecuadas que les permitan cumplir efectivamente sus obligaciones en materia de protección de datos y demostrar dicho cumplimiento, entre otros, ante la autoridad de control competente. El CEPD celebra en particular la existencia de disposiciones que prevén la adopción de un plan de gestión

[50] Véase el considerando 81 del proyecto de decisión.
[51] Este grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Fue un órgano consultivo europeo independiente en materia de protección de datos y privacidad. Su cometido se describe en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. El Grupo de Trabajo del Artículo 29 se ha convertido ahora en el CEPD.
[52] Dictamen 28/2018 sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón, adoptado el 5 de diciembre de 2018.
[53] Considerando 81 del proyecto de decisión.
[54] WP 254, p. 7.

interna (artículo 29 de la LPDP), la obligación de realizar una «evaluación de impacto sobre la intimidad» (en lo sucesivo, **«EII»**) en aquellos casos en los que el tratamiento presente un mayor riesgo de posibles vulneraciones de la intimidad (artículo 33, apartado 1, de la LPDP y artículo 35 del decreto de aplicación de la LPDP), normas sobre la formación y supervisión del personal (artículo 28 de la LPDP) y la obligación de nombrar un delegado de protección de la intimidad (artículo 31 de la LPDP en relación con el artículo 32 del decreto de aplicación de la LPDP).

118. El CEPD comparte la opinión de la Comisión Europea en relación con la protección sustancialmente equivalente que ofrecen ambos marcos jurídicos, incluso en casos en que las normas parezcan divergir relativamente con respecto a las previstas en el RGPD —p. ej., no existe ninguna disposición que establezca la necesidad de que el delegado de protección de la intimidad sea independiente, aunque se establece claramente que debe rendir cuentas ante el director del responsable del tratamiento de datos personales (artículo 31, apartado 4, de la LPDP) y que no debe sufrir perjuicios injustificados como consecuencia del desempeño de estas funciones (artículo 31, apartado 5, de la LPDP)—, y sugiere que, al revisar la decisión de adecuación, la Comisión Europea examine la aplicación de estas disposiciones en la práctica a fin de evaluar su correcto cumplimiento.

3.2. Mecanismos relativos al procedimiento y la ejecución

119. Sobre la base de los criterios establecidos en las Referencias sobre adecuación, el CEPD ha analizado los siguientes aspectos del marco jurídico coreano en materia de protección de datos cubiertos por el proyecto de decisión: la existencia y el funcionamiento efectivo de una autoridad de control independiente, la existencia de un sistema que garantice un buen nivel de cumplimiento y un sistema de acceso a mecanismos de recurso adecuados que doten a los ciudadanos del EEE de los medios para ejercer sus derechos y solicitar reparación sin encontrar obstáculos engorrosos a los recursos administrativos y judiciales.

120. De conformidad con lo dispuesto en el capítulo VI del RGPD y el capítulo 3 de las Referencias sobre adecuación, deben existir una o más autoridades de control independientes, que se encargarán de supervisar, garantizar y hacer cumplir las disposiciones en materia de protección de datos e intimidad en el país tercero con el fin de asegurar un nivel de protección equivalente al del EEE.

121. En este contexto, la autoridad de control del país tercero deberá actuar con una independencia y una imparcialidad absolutas en el cumplimiento de sus obligaciones y el ejercicio de sus facultades, y, al hacerlo, no solicitará ni aceptará instrucciones. Además, dispondrá de todas las facultades y misiones necesarias y disponibles para garantizar el cumplimiento de los derechos en materia de protección de datos y fomentar la sensibilización. Asimismo, se deberá tener en cuenta el personal y el presupuesto de la autoridad de control. Esta también podrá llevar a cabo investigaciones por iniciativa propia.

3.2.1. Autoridad de control competente independiente

122. En la República de Corea, la autoridad independiente encargada de supervisar y hacer cumplir la LPDP es el CPDP. Este consta de un presidente, un vicepresidente y siete comisarios. El presidente y el vicepresidente del CPDP son nombrados por el presidente de la República de Corea a propuesta del primer ministro. De los comisarios, dos son nombrados a propuesta del presidente del CPDP, dos, a propuesta de representantes del partido político al que pertenezca el presidente de la República, y los tres restantes, a propuesta de representantes de otros partidos políticos (artículo 7, apartado 2, punto 2, de la LPDP). El CPDP es asistido por una Secretaría (artículo 7, apartado 13) y puede establecer subcomisiones (compuestas por tres comisarios) para abordar infracciones leves y cuestiones recurrentes (artículo 7, apartado 12, de la LPDP).

123. Al respecto, el CEPD observa que, a pesar de su reciente reorganización, que modificó en gran medida su estatuto y sus competencias, el CEPD ha realizado un esfuerzo considerable por crear la infraestructura necesaria para facilitar la aplicación de la LPDP y de sus modificaciones más recientes. Entre estos esfuerzos, cabe hacer referencia a la elaboración del reglamento del CPDP, la creación de

unas directrices que orienten la interpretación de la LPDP, y la implantación de un servicio telefónico para ofrecer asesoramiento a empresarios y particulares acerca de las disposiciones en materia de protección de datos, además de un servicio de mediación para la tramitación de reclamaciones. En particular, las tareas del CPDP incluyen asesorar sobre leyes y reglamentos relacionados con la protección de datos, elaborar políticas y directrices en materia de protección de datos, investigar vulneraciones de derechos individuales, tramitar reclamaciones, mediar en conflictos, hacer cumplir la LPDP, garantizar la educación y la promoción en el campo de la protección de datos e intercambiar información y cooperar con las autoridades encargadas de la protección de datos en terceros países.[55]

124. El nombramiento y la composición del CPDP se establecen en el artículo 7, apartado 2, de la LPDP. Pese a que el CPDP es dependiente del primer ministro (y el presidente y el vicepresidente del CPDP son nombrados por el presidente de la República a propuesta del primer ministro), el marco jurídico aplicable obliga a los comisarios a desempeñar sus funciones con plena independencia, con arreglo a la legislación y según su conciencia. El CEPD toma nota de las garantías institucionales y procedimentales incluidas en la LPDP, en particular, en el artículo 7, apartados 4 a 7. Aun así, agradecería que la Comisión Europea vigilara cualquier eventualidad que pudiera afectar a la independencia de los miembros de la autoridad de control surcoreana.

125. Por otra parte, el proyecto de decisión no incluye aún un análisis del presupuesto del CPDP, incluidas las fuentes de financiación y la transparencia presupuestaria. El CEPD considera que este aspecto, que se menciona tanto en el artículo 56, apartado 1, del RGPD como en los principios y mecanismos relativos al procedimiento y la coerción en materia de protección de datos que, según las Referencias sobre adecuación, deben considerarse al evaluar el sistema de un país o una organización internacional, debe tenerse plenamente en cuenta, puesto que se trata de un indicador de los recursos económicos y humanos de que dispone la autoridad de control para cumplir con independencia con sus atribuciones y obligaciones legales en materia de protección de datos, y, en consecuencia, aconseja a la Comisión Europea que lo tenga en cuenta con mayor grado de detalle en el proyecto de decisión.

3.2.2. Existencia de un sistema de protección de datos que garantice un buen nivel de cumplimiento

126. En el campo de la coerción, el CEPD constata el conjunto de poderes coercitivos y sanciones de que dispone el CPDP, tal como se contempla en la LPDP y la LIC, y toma nota de las aclaraciones incluidas en la notificación n.º 2021-1, según la cual, las condiciones a que hacen referencia el artículo 64, apartado 1, de la LPDP y el artículo 45, apartado 4, de la LIC[56] serán de aplicación cuando se vulnere cualquiera de los principios, derechos y obligaciones previstos en la ley con el fin de proteger datos personales. Sin embargo, recomienda a la Comisión Europea que supervise con atención la aplicación práctica de las facultades del CPDP con el fin de obligar al infractor a adoptar las medidas que considere pertinentes de entre las previstas en el artículo 64, apartado 1, o el artículo 45, apartado 4, de la LIC.

127. Por otra parte, por lo que respecta a las medidas correctoras previstas en el artículo 64, apartado 1, de la LPDP, en caso de incumplimiento de una de dichas medidas, el CPDP puede imponer una multa por un importe máximo de 50 millones de wones surcoreanos (artículo 75, apartado 2, punto 13, de la LPDP). Este importe equivale a 36 564 euros. El CEPD considera y teme que, en contra de lo que pretende la ley, unas sanciones pecuniarias de un importe tan reducido puedan no tener en los

[55] Las atribuciones y facultades del CPDP se contemplan principalmente en el artículo 7, apartados 8 y 9, y en los artículos 61 a 66 de la LPDP.

[56] Esto es, *«se considere que el incumplimiento de la ley presumiblemente suponga una vulneración de los derechos y las libertades de las personas en materia de datos personales y la falta de adopción de medidas presumiblemente ocasione un daño difícil de reparar»*.

infractores un efecto disuasorio especialmente fuerte que garantice la aplicación de las normas en materia de protección de datos, puesto que no parecen suficientes para conseguir tal efecto, especialmente en el caso de las organizaciones o empresas de gran tamaño que cuenten con grandes recursos económicos.

128. Por lo que respecta a la posibilidad de que el CPDP pueda requerir que el responsable de un organismo administrativo central investigue al responsable del tratamiento de datos personales o participe en una investigación sobre vulneraciones de la LPDP e incluso imponga medidas correctoras a los responsables del tratamiento de datos personales sobre los que tenga competencia (artículo 63, apartados 4 y 5, de la LPDP), el CEPD observa que, a pesar de haberse proporcionado cierta información en el considerando 122 del proyecto de decisión, quedan poco claras en general la naturaleza de estos otros organismos y su relación jurídica con el CPDP. Además, el artículo 68, apartado 1, de la LPDP hace referencia a numerosas entidades en las que puede delegarse la autoridad del CPDP. A pesar de que, según parece, esta disposición solo se ha aplicado en relación con la Agencia Coreana de Internet y Seguridad[57], el CEPD apreciaría cualquier aclaración sobre la naturaleza de las posibles interacciones entre estas entidades, así como una atenta supervisión de la aplicación de esta disposición en el futuro con el fin de garantizar la independencia de las entidades a las que se encomiende la aplicación de las normas en materia de protección de datos.

129. Por lo que respecta a las sanciones, el sistema coreano parece combinar distintos tipos de sanciones, desde medidas correctoras y multas administrativas hasta sanciones penales, que pueden tener un efecto disuasorio fuerte, y las autoridades coreanas han presentado varios ejemplos de multas impuestas recientemente por el CPDP, entre otras, una de 6 700 millones de wones surcoreanos impuesta en diciembre de 2020 a una empresa por infringir diversas disposiciones de la LPDP y otra de 103,3 millones de wones surcoreanos impuesta el 28 de abril de 2021 a una empresa dedicada a la inteligencia artificial por vulnerar las normas sobre licitud del tratamiento, en particular, el consentimiento, y sobre el tratamiento de datos seudonimizados.

130. A pesar de que las cantidades citadas pueden tener un efecto disuasorio, el CEPD agradecería cualquier información adicional sobre el método empleado por el CPDP para calcular la cuantía de las multas administrativas, por ejemplo, por lo que respecta a las multas por el incumplimiento de una medida correctora impuesta con arreglo al artículo 64, apartado 1, de la LPDP (véase el artículo 75, apartado 2, punto 13, de la LPDP). Esto resulta especialmente pertinente en relación con las sanciones penales y la aplicación del Código Penal coreano.

3.2.3. El sistema de protección de datos debe proporcionar apoyo y ayuda a los interesados en el ejercicio de sus derechos y mecanismos de recurso adecuados

131. Por lo que respecta al resarcimiento, el sistema coreano ofrece diversos procedimientos para garantizar la protección adecuada y, en particular, el respeto de los derechos individuales a través de unas vías de recurso administrativas y judiciales eficaces que incluyen la indemnización por daños y perjuicios.

132. Por otra parte, además de los procedimientos administrativos y judiciales, ofrece mecanismos alternativos a los que pueden recurrir las personas para obtener una reparación, tal como se explica en los considerandos 132 y 133 del proyecto de decisión en relación, respectivamente, con el Centro de Atención Telefónica sobre el Derecho a la Intimidad y con el Comité para la Mediación en Conflictos. Al tratarse de medios de reparación adicionales, el CEDP agradecería unas explicaciones más detalladas sobre el modo en que complementan las posibilidades de recurso ante el CPDP y los órganos jurisdiccionales con las que cuentan los interesados cuyos datos personales se transfieran a la República de Corea en virtud de la decisión de adecuación.

[57] Véanse el considerando 117 del proyecto de decisión y el artículo 62 del decreto de aplicación.

4. ACCESO A LOS DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA Y USO DE ESTOS POR LAS AUTORIDADES PÚBLICAS SURCOREANAS

133. En relación con la evaluación del nivel de protección de los datos en los ámbitos policial y de la seguridad nacional, la Comisión Europea ha ofrecido una información detallada al respecto en su proyecto de decisión y en los anexos facilitados. Por lo tanto, el CEPD se abstiene de reproducir la mayoría de las constataciones factuales y las evaluaciones en el presente dictamen.

134. La Comisión Europea concluye que, en estos ámbitos citados, existe un nivel de protección de los datos que cumple los requisitos establecidos por el TJUE en su jurisprudencia y puede, en consecuencia, considerarse que dicha protección es sustancialmente equivalente a la conferida en la UE.

135. Como observación general, el CEPD desea hacer hincapié en que, incluso en aquellos casos en los que parezca, o la Comisión Europea alegue, que los datos transferidos desde la UE a la República de Corea no vayan a verse afectados previsiblemente por la legislación coreana pertinente, debe plantearse esta posibilidad a la hora de evaluar la adecuación del nivel de protección de los datos en la República Corea en tales casos. Su relevancia también se pone de manifiesto por el hecho de que la propia Comisión Europea los haya tenido en cuenta en el proyecto de decisión.

4.1. Marco jurídico general en materia de protección de datos en el contexto del acceso a estos por el Gobierno

136. En relación con el acceso a los datos personales por las autoridades públicas, deben tenerse en cuenta varias normas coreanas con el fin de evaluar el nivel de protección del derecho a la intimidad y la protección de los datos. En primer lugar, el CEPD observa que la LPDP, al ser una ley fundamental en materia de protección de datos, alega tener un ámbito de aplicación amplio. Sin embargo, pese a que esta ley resulta plenamente aplicable en el ámbito de la actuación policial, su aplicación al tratamiento de datos por motivos de seguridad nacional es limitada. Con arreglo a lo dispuesto en el artículo 58, apartado 1, punto 2, de la LPDP, los capítulos III a VII no resultan aplicables al tratamiento de datos personales por motivos de seguridad nacional. Sí se aplican en este ámbito los capítulos I, II, IX y X. Por tanto, los principios esenciales de la LPDP, así como las garantías fundamentales para los derechos de los interesados y las disposiciones relativas a la supervisión, la aplicación y los recursos se aplican al acceso a los datos personales y a su uso por los organismos nacionales de seguridad.

137. La Constitución surcoreana también consagra principios esenciales en materia de protección de datos, en concreto, los principios de legalidad, necesidad y proporcionalidad. Estos principios también se aplican al acceso a los datos personales por las autoridades públicas surcoreanas en los ámbitos policial y de la seguridad nacional.[58]

138. En el campo de la actuación policial, la policía, la fiscalía, los órganos jurisdiccionales y otros organismos públicos pueden recoger datos personales al amparo de ciertas leyes: por ejemplo, la Ley de Enjuiciamiento Criminal (**«LEC»**), la Ley para la Protección de la Privacidad de las Comunicaciones (**«LPPC»**), la Ley de Empresas de Telecomunicaciones (**«LET»**) y la Ley sobre la Notificación y el Uso de Información Específica sobre Transacciones Financieras (**«LNUIETF»**), que se aplica al enjuiciamiento y la prevención del blanqueo de capitales y la financiación del terrorismo. Estas leyes concretas prevén unas limitaciones, garantías y excepciones adicionales.

[58] Véase el considerando 145 del proyecto de decisión.

139. En el campo de la seguridad nacional, el Servicio Nacional de Inteligencia (**«SNI»**) puede recoger datos personales e interceptar comunicaciones al amparo de la Ley sobre el Servicio Nacional de Inteligencia **«LSNI»**) y otras «leyes relativas a la seguridad nacional»[59]. El CEPD entiende que, al hacer uso de sus facultades, el SNI debe cumplir las citadas disposiciones legales, además de la LPDP.

140. El CEPD desea que la Comisión aclare si, además del SNI, existen otras autoridades en la República de Corea que sean responsables de la seguridad nacional, ya que, en la sección 6 del anexo I, la Comisión Europea parece aludir al SNI como ejemplo de organismo encargado de la seguridad nacional.

4.2. Protección y salvaguardias en relación con los datos de confirmación de las comunicaciones en el contexto del acceso del Gobierno con fines policiales

141. En virtud de la ley aplicable, esto es, la LPPC, las autoridades policiales pueden adoptar dos tipos de medidas para acceder a los datos sobre las comunicaciones. La LPPC distingue entre medidas limitadoras de las comunicaciones, que abarcan tanto la recogida de los datos del contenido del correo ordinario como la interceptación directa del contenido de las telecomunicaciones[60], y la recogida de los conocidos como «datos de confirmación de las comunicaciones». Estos últimos incluyen la fecha de las telecomunicaciones, su hora de inicio y finalización, el número de llamadas realizadas y recibidas, así como el número de abonado de la otra parte, la frecuencia de uso, los archivos del registro del uso de los servicios de telecomunicaciones y la información relativa a la ubicación[61].

142. El CEPD desea indicar que no parecen aplicarse a los datos de confirmación de las comunicaciones las mismas garantías que a los datos recogidos con las medidas limitadoras de las comunicaciones, esto es, los datos sobre el contenido. De hecho, el CEPD observa que la recogida de datos sobre el contenido con fines policiales se encuentra protegida por más garantías que la recogida los datos de confirmación de las comunicaciones. En primer lugar, al contrario que en la recogida de datos sobre el contenido, la recogida de datos de confirmación de las comunicaciones no se limita a la investigación de determinados delitos graves, sino que puede llevarse a cabo siempre que se considere necesario para realizar «cualquier investigación o aplicar cualquier sanción» (artículo 13, apartado 1, de la LPPC). En segundo lugar, la recogida de datos de confirmación de las comunicaciones no se estructura en principio como último recurso que únicamente deba utilizarse cuando resulte difícil de otro modo evitar la comisión de un delito, arrestar un delincuente u obtener pruebas.[62] Los datos de confirmación de las comunicaciones se pueden recoger siempre que un fiscal o agente de la policía judicial «lo considere necesario» para investigar un delito o aplicar una sanción. Sin embargo, el artículo 13, apartado 2, de la LPPC introduce una excepción en el caso de los datos de seguimiento en tiempo real y los datos de confirmación de las comunicaciones relativos a una estación base concreta. En tercer lugar, las fuerzas del orden que recojan datos sobre el contenido de las comunicaciones deben dejar de hacerlo de inmediato en cuanto deje de considerarse necesario el acceso ininterrumpido a dichos datos.[63] Por lo que respecta a los datos de confirmación de las comunicaciones, esto no se estipula expresamente en la LPPC ni en su decreto de aplicación.

143. El CEPD toma nota de que la recogida de datos de confirmación de las comunicaciones solo puede tener lugar cuando se haya dictado una orden judicial en ese sentido. La LPPC también exige que se

[59] Las leyes relativas a la seguridad nacional incluyen, por ejemplo, la Ley para la Protección de la Privacidad de las Comunicaciones, la Ley sobre Política Antiterrorista para la Protección de los Ciudadanos y la Seguridad Ciudadana, y la Ley de Empresas de Telecomunicaciones.
[60] Artículo 3, apartado 2, y artículo 2, apartados 6 y 7, de la LPPC.
[61] Artículo 2, apartado 11, de la LPPC.
[62] Este es el caso de los datos sobre el contenido contemplados en el artículo 3, apartado 2, y el artículo 5, apartado 1, de la LPPC.
[63] Artículo 2 del decreto de aplicación de la LPPC.

proporcione una información detallada tanto en la petición de la orden como en la propia orden.[64] Dicha autorización judicial previa sirve para limitar la discrecionalidad de las autoridades policiales a la hora de aplicar la normativa y para comprobar si, en el caso concreto de que se trate, existen motivos suficientes para recoger los datos de confirmación de las comunicaciones. El CEPD también reconoce que el Derecho de la República de Corea no parece prever una conservación general e indiscriminada de dichos datos. Por tanto, el acceso del Gobierno a estos datos siempre se refiere a datos que se conservan con fines de facturación y prestación de los propios servicios de comunicación.

144. Sin embargo, el CEPD subraya que el TJUE ha cuestionado la idea de que los datos de tráfico sean menos sensibles que otros, en particular, que los datos sobre el contenido.[65] Habida cuenta de que, en varios aspectos, se confiere a los datos de confirmación de las comunicaciones un menor nivel de protección que a los datos sobre el contenido, el CEPD insta a la Comisión Europea a que examine minuciosamente si las garantías previstas en el Derecho coreano para dichas categorías de datos personales aseguran un nivel de protección sustancialmente equivalente al previsto en la UE, en particular, en lo referente a la proporcionalidad y la previsión de la ley aplicable.

4.3. Acceso a los datos sobre las comunicaciones por las autoridades públicas coreanas por motivos de seguridad nacional

145. Por lo que respecta al marco jurídico para el acceso de los organismos nacionales de seguridad a los datos sobre las comunicaciones transferidos desde el EEE a la República de Corea, el CEPD ha identificado dos motivos de preocupación, ambos relativos al régimen de acceso a las comunicaciones entabladas entre nacionales de países distintos de la República de Corea que entren dentro de un conjunto específico de casos de uso (véase el párrafo 29). En dichos casos, no se aplican determinadas salvaguardias previstas ni a los datos de confirmación de las comunicaciones ni a los datos sobre el contenido. En otras palabras, en estos casos concretos, estos datos no están protegidos por las mismas garantías que los datos comunicados cuando participa en la comunicación al menos un ciudadano coreano.

4.3.1. Ausencia de obligación de notificar a los interesados el acceso del Gobierno a las comunicaciones entre extranjeros

146. En la situación descrita previamente, esto es, cuando ninguna de las partes en una comunicación sea nacional de la República de Corea, los organismos nacionales de seguridad no estarán obligados a notificar a los interesados la recogida y el tratamiento de sus datos. El CEPD reconoce que esta cuestión solo afecta a determinados casos. En primer lugar, como ya se ha señalado previamente, cuando al menos un ciudadano coreano participe en una comunicación, las obligaciones de notificación previstas en la LPPC se aplican a todas las partes en la comunicación, con independencia de su nacionalidad.[66] En segundo lugar, la recogida de datos personales que sean producto de las comunicaciones entabladas exclusivamente entre extranjeros se encuentra limitada a un conjunto

[64] Véase el considerando 156 del proyecto de decisión.

[65] Véase: TJUE, C-623/17, *Privacy International*, 6 de octubre de 2020, ECLI:EU:C:2020:790, apartado 71: *«La injerencia que supone la transmisión de los datos de tráfico y de localización a las agencias de seguridad e inteligencia en el derecho consagrado en el artículo 7 de la Carta debe considerarse especialmente grave, habida cuenta, en particular, del carácter sensible de la información que pueden proporcionar esos datos y, en particular, de la posibilidad de determinar a partir de ellos el perfil de las personas afectadas, ya que tal información es tan sensible como el propio contenido de las comunicaciones. Además, puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante (véanse, por analogía, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C‑293/12 y C‑594/12, EU:C:2014:238, apartados 27 y 37, y de 21 de diciembre de 2016, Tele2, C‑203/15 y C‑698/15, EU:C:2016:970, apartados 99 y 100)»*.

[66] Véase el considerando 192 del proyecto de decisión.

específico de casos de uso. En particular, el derecho de acceso en tales casos se aplica a las comunicaciones de a) países hostiles a la República de Corea, b) organismos, grupos o ciudadanos extranjeros sospechosos de participar en actividades anticoreanas[67] o c) miembros de grupos que operen en la Península de Corea, pero no se encuentren sujetos a la jurisdicción de la República de Corea, así como sus grupos coordinadores establecidos en terceros países. Por tanto, los datos de las comunicaciones entre ciudadanos de la UE transferidas a la República de Corea desde el EEE solo pueden recogerse por motivos de seguridad nacional si dichas comunicaciones se encuentran incluidas en alguna de las tres categorías mencionadas.[68] Además de las limitaciones anteriores, el CEPD ha entendido, tras examinar las explicaciones facilitadas por la Comisión Europea, que el marco jurídico aplicable no prevé la interceptación de datos en tránsito fuera de la República de Corea.

147. En consecuencia, puede considerarse que la posible crítica de la ausencia de la obligación de notificación tiene un efecto limitado en la práctica. Sin embargo, el CEPD subraya la importancia de la notificación (posterior) del acceso por el Gobierno, en particular, para garantizar la posibilidad efectiva de recurrir. Tal como ha dictaminado el TJUE, la notificación es *«necesaria para que dichas personas puedan ejercer su derecho, resultante de los artículos 7 y 8 de la Carta, a solicitar el acceso a sus datos de carácter personal objeto de dichas medidas y, en su caso, su rectificación o supresión, así como a interponer, con arreglo al artículo 47, párrafo primero, de la Carta, un recurso efectivo ante un tribunal»*[69]. El acceso del Gobierno por motivos de seguridad nacional incluye a menudo medidas secretas de vigilancia, de modo que los objetos de dicha vigilancia, es decir, los interesados, no están al corriente del tratamiento de sus datos. Por tanto, *«en principio, el interesado tiene escaso margen para el recurso judicial, a menos que se le informe de las medidas tomadas sin su conocimiento y de tal suerte pueda oponerse a su legalidad de manera retrospectiva o, como alternativa, a menos que cualquier persona que sospeche que sus comunicaciones están siendo o han sido interceptadas pueda recurrir a los órganos jurisdiccionales, para que la competencia de los tribunales no dependa de la notificación al interesado de la interceptación de sus comunicaciones»*[70]. En este contexto, y en consonancia con lo mencionado en el presente dictamen, el CEPD ha expresado en numerosas ocasiones su preocupación por que no se garanticen unos recursos efectivos en los casos de vigilancia. El CEPD desea hacer hincapié en que el carácter secreto de las medidas adoptadas por el Gobierno no debe traducirse en la imposibilidad de recurrirlas. Teniendo en cuenta todo lo anterior, para determinar si la ausencia de la obligación de notificación para las comunicaciones entre extranjeros repercute en el nivel de protección de los datos que se evalúa en el proyecto de decisión, debe valorarse esta circunstancia dentro de una evaluación global que tenga en cuenta especialmente los mecanismos de supervisión y reparación previstos en el Derecho coreano (véanse las secciones 4.7 y 4.8).

148. El CEPD también constata en este contexto que la ley hace referencia a términos muy amplios, como «actividades anticoreanas» o «antinacionales»[71], y que resulta difícil adivinar cómo se interpretan

[67] Véase la nota 244 a pie de página del anexo II, según la cual, la noción de actividades anticoreanas hace referencia a actividades que amenazan la existencia y la seguridad de la nación, el orden democrático o la supervivencia y la libertad de las personas.

[68] Véase el considerando 187 del proyecto de decisión.

[69] TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, *La Quadrature du Net y otros*, 6 de octubre de 2020, ECLI:EU:C:2020:791, apartado 190.

[70] TEDH, *Big Brother Watch y otros contra Reino Unido*, 25 de mayo de 2021, ECLI:CE:ECHR:2021:0525JUD005817013, apartado 337; y TEDH, *Roman Zakharov contra Rusia*, 4 de diciembre de 2015, ECLI:CE:ECHR:2015:1204JUD004714306, apartado 234.

[71] La Comisión Europea ha aclarado que, según las explicaciones proporcionadas por el Gobierno coreano, estos términos hacen referencia a «actividades que amenazan la existencia y la seguridad de la nación, el orden democrático o la supervivencia y la libertad de las personas». Véase también al respecto la nota 319 a pie de página del proyecto de decisión de adecuación.

estos conceptos en el Derecho coreano. Por tanto, insta a la Comisión Europea a que examine cómo se precisan estos términos en el Derecho coreano y si su aplicación práctica satisface los requisitos de proporcionalidad previstos en el Derecho de la Unión.

4.3.2. Ausencia de autorización independiente previa a la recogida de datos de las comunicaciones entre extranjeros

149. En aquellos casos en que los datos personales procedentes del EEE y derivados de comunicaciones entre nacionales de países distintos de la República de Corea (siempre que se incluyan en alguno de los casos de uso previamente citados) deban tratarse en Corea por motivos de seguridad nacional, la recogida de dichos datos no estará sujeta a la autorización previa por un organismo independiente (al contrario de lo que sucede cuando, al menos, una de las partes en las comunicaciones sea un ciudadano coreano).[72]

150. Teniendo en cuenta, especialmente, los fallos recientes del Tribunal Europeo de Derechos Humanos (**«TEDH»**) en los asuntos *Big Brother Watch y otros contra Reino Unido* y *Centrum för Rättvisa contra Suecia*, el CEPD considera necesario examinar si esto supone una carencia importante del marco jurídico coreano en materia de protección de datos. Al respecto, y tal como puso de relieve en sus recomendaciones actualizadas sobre las garantías esenciales europeas para medidas de vigilancia[73], el CEPD recuerda que el artículo 6, apartado 3, del Tratado de la Unión Europea establece que los derechos fundamentales consagrados en el CEDH constituyen principios generales del Derecho de la Unión. Sin embargo, como el TJUE recuerda en su jurisprudencia, dicho Convenio no constituye, en la medida en que la Unión Europea no lo haya suscrito, un instrumento jurídico incorporado formalmente al Derecho de la Unión[74]. De tal manera, el nivel de protección de los derechos fundamentales exigido por el artículo 45, del RGPD debe determinarse en función de las disposiciones de dicho Reglamento, leído a la luz de los derechos fundamentales consagrados en la Carta. Dicho esto, de acuerdo con el artículo 52, apartado 3, de la Carta, los derechos en ella plasmados que se corresponden con derechos garantizados por el CEDH deben tener el mismo significado y alcance que los dispuestos por dicho Convenio y, en consecuencia, la jurisprudencia del TEDH sobre derechos también previstos en la Carta se ha de tener en cuenta como umbral mínimo de protección para interpretar los derechos correspondientes de la Carta; es decir, en la medida en que la Carta, en la interpretación que de esta haga el TJUE, no prevea un nivel de protección mayor.[75]

151. El CEPD constata que, aunque la autorización (independiente) previa a la adopción de las medidas de vigilancia se considera una importante garantía contra la arbitrariedad, dicha autorización no puede derivarse de la jurisprudencia del TJUE como requisito absoluto para la proporcionalidad de las medidas de vigilancia. No obstante, el TEDH ha establecido expresamente el requisito de la autorización independiente previa para la interceptación masiva.[76] Pese a que el proyecto de decisión no lo menciona expresamente, el CEPD entiende que el marco jurídico de la República de Corea no

[72] Véase el considerando 190 del proyecto de decisión.
[73] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, párrafos. 10 y 11.
[74] Véase: TJUE, C-311/18, *Data Protection Commissioner contra Facebook Ireland Ltd. y Maximilian Schrems*, 16 de julio de 2020, ECLI:EU:C:2020:559 (en lo sucesivo, *«Schrems II»*), apartado 98.
[75] Véase: TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, *La Quadrature du Net y otros*, 6 de octubre de 2020, ECLI:EU:C:2020:791, apartado 124.
[76] Véase: TEDH, *Big Brother Watch y otros contra Reino Unido*, 25 de mayo de 2021, ECLI:CE:ECHR:2021:0525JUD005817013, apartado 351: «La interceptación masiva debe ser objeto de una autorización independiente previa»; «la interceptación masiva debe ser autorizada por un organismo independiente; es decir, un organismo que no dependa del ejecutivo».

prevé la interceptación masiva, sino solo la interceptación selectiva de las telecomunicaciones.[77] La Comisión Europea ha confirmado esta interpretación.

152. Dicho esto, los citados fallos del TEDH, junto a la jurisprudencia del TJUE[78] y la jurisprudencia previa del TEDH[79], muestran una vez más la importancia de una supervisión exhaustiva a cargo de autoridades de control independientes. El CEPD hace hincapié en que la supervisión independiente en todas las etapas del proceso de acceso del Gobierno a los datos con fines policiales y de seguridad nacional representa una garantía importante contra las medidas de vigilancia arbitrarias y, por tanto, para evaluar si el nivel de protección de datos es adecuado. La garantía de la independencia de las autoridades de control en el sentido del artículo 8, apartado 3, de la Carta tiene por fin asegurar un control efectivo y fiable del cumplimiento de las normas sobre la protección de los interesados en el ámbito del tratamiento de datos personales. Esto resulta aplicable, en particular, en aquellas circunstancias en las que, debido al carácter secreto de la vigilancia, el interesado no pueda solicitar la revisión ni participar directamente en ningún procedimiento de revisión antes de la implantación de la medida de vigilancia o durante esta.

153. La ausencia de una autorización independiente previa no puede considerarse por sí sola una carencia sustancial del Derecho coreano por lo que respecta a la evaluación de un nivel de protección de los datos sustancialmente equivalente. Cabe recordar que la evaluación de la adecuación depende de todas las circunstancias del caso, en particular, de la eficacia de la supervisión *ex post* y de las posibilidades de reparación previstas en el ordenamiento jurídico coreano (véanse las secciones 4.7 y 4.8).

4.4. Divulgación voluntaria

154. De conformidad con lo dispuesto en el artículo 83, apartado 3, de la LET, los proveedores de servicios de telecomunicaciones podrán entregar voluntariamente, previa solicitud, los conocidos como «datos de abonado»[80] a las autoridades encargadas de la seguridad nacional y policiales. Pese a que el CEPD reconoce el carácter previsiblemente excepcional de los casos que afecten a datos personales transferidos a la República de Corea desde el EEE, como ya se ha mencionado previamente, estos deben analizarse para evaluar el nivel de protección de los datos.

155. El CEPD entiende que, en estos casos, resultan aplicables las garantías en materia de protección de datos previstas en la LPDP, y las autoridades públicas, así como los proveedores de servicios de telecomunicaciones, deben cumplir las correspondientes obligaciones[81], de modo que puede exigirse responsabilidad a ambos por las vulneraciones de los derechos y libertades de los interesados afectados[82]. El CEPD también entiende que los proveedores de servicios de telecomunicaciones no están obligados a responder a las citadas solicitudes.

---

[77] Solo la sección 3.2 del anexo II contiene una declaración expresa relativa a los fines de seguridad nacional, cuando especifica que las limitaciones y salvaguardias *«aseguran que la recogida y el tratamiento de los datos se limiten a lo estrictamente necesario para alcanzar un objetivo legítimo Esto excluye cualquier recogida masiva e indiscriminada de datos personales con fines de seguridad nacional»*.

[78] Véase, por ejemplo: TJUE, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB y otros*, ECLI:EU:C:2016:970.

[79] Véase, por ejemplo: TEDH, *Roman Zakharov contra Rusia*, 4 de diciembre de 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Los conjuntos de datos serían los siguientes: el nombre, el número de registro como residente, la dirección y el número de teléfono de los usuarios, las fechas en las que los usuarios suscriban el servicio o cancelen su suscripción, así como los códigos de identificación de los usuarios (utilizados para identificar al usuario legítimo de los sistemas informáticos o las redes de comunicaciones).

[81] Véanse los considerandos 164 y 194 del proyecto de decisión.

[82] Véase el considerando 166 del proyecto de decisión.

156. No obstante, por lo que respecta al concepto de acceso a los datos de abonado por las autoridades nacionales con fines policiales y, en particular, por motivos de seguridad nacional a través de la «divulgación voluntaria» realizada por los operadores de telecomunicaciones, preocupa el mayor riesgo que supone en los derechos y las libertades de los interesados, en especial, en su derecho a ser informados.

157. De conformidad con el artículo 58, apartado 1, punto 2, de la LPDP, lo dispuesto en los capítulos III a VII no se aplicará a los datos personales solicitados que deban proporcionarse por motivos de seguridad nacional. Al respecto, debe señalarse, por ejemplo, que el artículo 18 (limitación al uso y el suministro de datos personales para fines distintos de los precisados) y el artículo 20 (notificación de fuentes, etc., de los datos personales recogidos de terceros) de la LPDP no se aplican a estas solicitudes. En aquellos casos en los que un organismo nacional de seguridad realice una solicitud, cabe preguntarse, por un lado, si el artículo 58, apartado 1, punto 2, también excluye de la aplicación de la LPDP a los proveedores de telecomunicaciones. Por otro lado, se plantea la cuestión de si la exclusión de la aplicación del artículo 20 de la LPDP en tales casos también se aplica a la disposición correspondiente de la sección 3 del anexo I [notificación al interesado cuando los datos personales no se hayan obtenido de este (artículo 20 de esta ley)]. Si este es el caso y el artículo 58, apartado 1, punto 2, también se aplica a los proveedores de servicios de telecomunicaciones, puede deducirse de la información presentada que existe un riesgo de que no haya obligación legal alguna de informar a los interesados acerca de la divulgación voluntaria.

158. Por tanto, preocupa al CEPD que las obligaciones en materia de información queden sin efecto, dificultando considerablemente el ejercicio de los derechos de los interesados en materia de protección de datos, especialmente, el ejercicio de las acciones judiciales. En este sentido, el CEPD insta a la Comisión Europea a que aclare el alcance de las disposiciones pertinentes.

4.5. Uso posterior de los datos

159. El principio de limitación de la finalidad es un requisito legal básico en materia de protección de datos. Requiere que los datos personales solo se recojan para fines específicos, explícitos y legítimos, y que no se traten posteriormente en un modo incompatible con dichos fines. Además, el Derecho de la Unión permite a las autoridades públicas tratar datos personales para fines de prevención, investigación y enjuiciamiento de infracciones penales, incluso cuando tales datos se hayan obtenido inicialmente para fines distintos, cuando dichas autoridades cuenten con una base jurídica para tratar los datos en virtud de la legislación aplicable y cuando el tratamiento posterior no resulte desproporcionado.[83]

160. Teniendo esto en cuenta, el CEPD observa que el marco jurídico coreano en materia de protección de datos contiene unas garantías y unas limitaciones similares a las previstas en el Derecho de la Unión en relación con el uso posterior de los datos recogidos con fines policiales y de seguridad nacional (p. ej., el artículo 3, apartados 1 y 2, de la LPDP en relación con el principio de limitación de la finalidad).

4.6. Transferencias ulteriores y puesta en común de datos de inteligencia

161. El artículo 44 del RGPD establece que las transferencias y las transferencias ulteriores de datos personales solo podrán tener lugar cuando el nivel de protección garantizado por el RGPD no se vea menoscabado. Por tanto, el nivel de protección conferido a los datos personales transferidos a la República de Corea desde el EEE no debe verse menoscabado por la transferencia ulterior a destinatarios de un país tercero; es decir, solo se permitirán las transferencias ulteriores cuando se garantice un nivel de protección ininterrumpido sustancialmente equivalente al conferido por el

[83] Véase el artículo 4, apartado 2, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

Derecho de la Unión. En consecuencia, al evaluar si un país tercero garantiza un nivel de protección de datos adecuado, debe tenerse en cuenta el marco jurídico de dicho país aplicable a las transferencias ulteriores. Este razonamiento resulta indiscutible y está en consonancia con la postura adoptada al respecto tanto por la Comisión Europea[84] como por el CEPD.

162. En este contexto, el CEPD toma nota de que el TEDH, en sus recientes fallos en los asuntos *Big Brother Watch y otros contra Reino Unido* y *Centrum för Rättvisa contra Suecia* ha introducido orientaciones[85] sobre las precauciones en materia de protección de datos que deben observar los Estados signatarios al comunicar datos personales a otras partes con fines policiales y de seguridad nacional en casos de recogida masiva: *«En primer lugar, el Derecho interno debe establecer claramente las circunstancias en las que puede tener lugar dicha transferencia. En segundo lugar, el Estado que realice la transferencia debe asegurarse de que el Estado destinatario cuente con unas salvaguardias capaces de evitar los abusos y las interferencias desproporcionadas en el tratamiento de los datos. En particular, el Estado destinatario debe garantizar el almacenamiento seguro del material y limitar su divulgación ulterior. […] En tercer lugar, resultarán necesarias unas salvaguardias reforzadas cuando sea evidente que se transfiere material que requiera una confidencialidad especial, como el material periodístico confidencial»*[86].

163. En relación con la aplicación de estas normas, el TEDH concluyó en el asunto *Centrum för Rättvisa contra Suecia* que la ausencia de requisitos legales expresos en el régimen de interceptación con vistas a valorar la necesidad y proporcionalidad de la puesta en común de datos de inteligencia para conocer su posible repercusión en el derecho a la intimidad constituye una vulneración del artículo 8 del CEDH. El TEDH criticó que, debido al grado de indefinición de la norma, el material interceptado podía enviarse en general al extranjero siempre que se considerara que ello redundaría en beneficio del interés nacional, con independencia de que el destinatario extranjero ofreciera o no un nivel mínimo aceptable de garantías.[87]

164. Aun reconociendo que el marco jurídico surcoreano no permite la interceptación masiva, en vista de las implicaciones de la jurisprudencia del TEDH mencionadas, el CEPD considera que, además de los requisitos derivados del Derecho de la Unión, según los interpreta el TJUE, también es necesario tener en cuenta la línea argumental del TEDH a la hora de evaluar si el marco jurídico para las transferencias ulteriores a un país tercero ofrece un nivel de protección de los datos adecuado.

4.6.1. Marco jurídico aplicable a las transferencias ulteriores por las autoridades policiales

165. Por lo que respecta las transferencias ulteriores por las autoridades competentes con fines policiales, el CEPD, tras examinar las explicaciones ofrecidas por la Comisión Europea, entiende que resulta aplicable la sección 2 del anexo I del proyecto de decisión, relativa a la limitación de las transferencias ulteriores, también cuando la transferencia se realice al amparo de alguna ley distinta de la LPDP. Según esta regla, *«si se proporcionan datos personales a un tercero en el extranjero, es posible que estos datos no disfruten del nivel de protección garantizado por la Ley de Protección de Datos Personales de Corea debido a las divergencias entre los sistemas de protección de datos personales de*

[84] Véanse el considerando 84 y siguientes del proyecto de decisión.

[85] Los elementos que se citan a continuación se establecieron con ocasión de los asuntos *Big Brother Watch* y *Centrum för Rättvisa*, relativos a los regímenes de interceptación masiva. El requisito relativo a las precauciones que deben observarse al comunicar material a terceros ya formaba parte de los criterios elaborados por el TEDH en el contexto de la interceptación selectiva y no había sido pormenorizado por este tribunal (véase el asunto *Big Brother Watch y otros contra Reino Unido*, apartados 335 y 362).

[86] TEDH, *Big Brother Watch y otros contra Reino Unido*, 25 de mayo de 2021, ECLI:CE:ECHR:2021:0525JUD005817013, apartado 362.

[87] Véase: TEDH, *Centrum för Rättvisa contra Suecia*, 25 de mayo de 2021, ECLI:CE:ECHR:2021:0525JUD003525208, apartado 326.

los distintos países. En consecuencia, tales casos se considerarán "casos en los que pueden causarse perjuicios al interesado", tal como se contemplan en el artículo 17, párrafo 4, de la Ley, o "casos en los que el interés del interesado o de un tercero se vulneran de manera injusta", según se contemplan en el artículo 18, párrafo 2, de la Ley y en el artículo 14, apartado 2, del decreto de aplicación de esta misma ley. A fin de cumplir los requisitos de estas disposiciones, el responsable del tratamiento de datos personales y el tercero deben, por tanto, garantizar de manera explícita un nivel de protección equivalente al de la Ley, incluida la garantía, por medio de documentos jurídicamente vinculantes, como contratos, de que se permitirá al interesado ejercer sus derechos, incluso después de que los datos personales se hayan transferido al extranjero»[88].

166. El CEPD agradece esta disposición, que, siempre que el nivel de protección de los datos en la República de Corea con este fin sea adecuado, garantiza la continuidad de un nivel de protección sustancialmente equivalente al conferido en virtud del Derecho de la Unión para las transferencias ulteriores. La Comisión ha confirmado que la interpretación del CEPD es correcta, es decir, que esta sección del anexo I se aplica a todas las transferencias ulteriores realizadas por las autoridades competentes con fines policiales. Sin embargo, el CEPD considera que debe garantizarse que esta norma ofrezca un nivel de protección ininterrumpido en la práctica, ya que puede existir incertidumbre sobre qué salvaguardias y obligaciones contractuales u otros mecanismos similares pueden emplearse para lograr dicho nivel de protección en caso de que los datos se traten con fines policiales. Al respecto, debe añadirse, por ejemplo, que los datos personales solo se pueden compartir con las correspondientes autoridades competentes del país tercero.

167. A la espera de que se aclare si el proyecto de decisión abarca también la KoFIU, el CEPD constata que en la declaración oficial sobre el acceso por el Gobierno[89] se explica que el artículo 8, apartado 1, de la LNUIETF prevé que el comisario de la KoFIU pueda proporcionar a las unidades de inteligencia financiera extranjeras determinada información sobre las transacciones financieras, si ello se considera necesario para lograr el objetivo de la LNUIETF[90]. El artículo 8 de la LNUIETF no prevé en sí mismo la obligación de determinar si el país tercero ofrece unas salvaguardias adecuadas en materia de protección de datos ni de asegurar que las ofrezca. El anexo II no hace referencia en este sentido a la nueva sección del anexo I. Por tanto, el CEPD insta a la Comisión Europea a que aclare la interrelación entre la sección pertinente del anexo I relativa a la limitación de las transferencias ulteriores y la base jurídica para estas transferencias con arreglo a la LNUIETF.

4.6.2. Marco jurídico aplicable a las transferencias ulteriores por motivos de seguridad nacional

168. El proyecto de decisión no contiene información alguna sobre el marco jurídico para las transferencias ulteriores en el ámbito de la seguridad nacional. En este sentido, el CEPD entiende que, al contrario que en el caso de las transferencias con fines policiales, la sección 2 del anexo I no resulta aplicable a las transferencias ulteriores por motivos de seguridad nacional. Los artículos 17 y 18 de la LPDP, a los que se aplica esta sección del anexo I, se encuentran incluidos en el capítulo III de la LPDP, que a su vez no se aplica al tratamiento de datos personales por motivos de seguridad nacional (artículo 58, apartado 1, de la LPDP).

[88] Anexo I del proyecto de decisión, p. 7.
[89] Véase el anexo II del proyecto de decisión.
[90] Véase la sección 2.2.3.2 del anexo II del proyecto de decisión. Aunque dicha divulgación de información solo puede tener lugar con la condición de que la unidad extranjera no utilice la información con fines distintos del fin original por el que se divulgó, y, en particular, para fines de investigación y enjuiciamiento penales (artículo 8, apartado 2, de la LNUIETF), el comisario de la KoFIU puede, a petición de un país tercero, prestar su consentimiento al uso de dichos datos en investigaciones penales o enjuiciamientos de delitos previo consentimiento del ministro de Justicia (artículo 8, apartado 3, de la LNUIETF).

169. Sin embargo, el CEPD presume que la República de Corea puede verse en la necesidad de transmitir y, de hecho, transmite datos personales a unidades de inteligencia extranjeras por motivos de seguridad nacional: por ejemplo, para colaborar en la lucha contra las amenazas transfronterizas para la seguridad nacional, para advertir a Gobiernos extranjeros sobre dichas amenazas o para solicitar la ayuda de estos con el fin de identificarlas.

170. El CEPD entiende que, en opinión de la Comisión Europea, las transferencias ulteriores se encuentran suficientemente reguladas en el Derecho coreano mediante las salvaguardias dimanadas del marco constitucional general, en particular, a través de los principios de necesidad y proporcionalidad, así como los principios básicos en materia de protección de datos contenidos en la LPDP, como la licitud y lealtad del tratamiento, la limitación de la finalidad, la minimización de datos, la seguridad y las obligaciones generales de prevención del abuso o el uso indebido de los datos personales.

171. El CEPD reconoce y constata la aplicación general de estos principios esenciales (en materia de protección de datos), pero teme que estas salvaguardias sean de una naturaleza excesivamente general y no hagan referencia expresamente, en el plano jurídico, a las circunstancias y condiciones específicas de las transferencias ulteriores de los datos transferidos desde el EEE por motivos de seguridad nacional ni aborden dichas circunstancias y condiciones. Pese al extenso ámbito de aplicación de estos principios generales, el CEPD se pregunta si cumplen los criterios relativos a unas normas claras y precisas y si consagran de manera suficiente unas salvaguardias eficaces y aplicables. En este sentido, es esencial contar con unas normas claras y detalladas, en especial, cuando el acceso por el Gobierno y el tratamiento de datos personales se realicen en secreto y las conclusiones que pudieran inferirse de los datos sean especialmente graves. La legislación debe indicar, de manera suficientemente clara, el alance de cualquier potestad discrecional conferida a las autoridades competentes y el modo de ejercerla, a fin de ofrecer suficiente protección al interesado. En la sentencia *Schrems II*, el TJUE recuerda que cualquier base legal que permita la injerencia en los derechos fundamentales debe definir en ella misma el alcance de la limitación del ejercicio del derecho de que se trate, a fin de cumplir los principios de necesidad y proporcionalidad, y establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas.[91] Por tanto, el CEPD teme que no sea suficiente con que dichas garantías se consagren de manera general en una ley jerárquicamente superior sin que se incluya expresamente, p. ej., la noción de proporcionalidad en la respectiva base legal.

172. Estas preocupaciones se sustentan también en el citado fallo del TEDH, en el que este tribunal dictaminó que las normas generales que no incluyan ninguna obligación expresa de evaluar la necesidad y la proporcionalidad o de tener en cuenta los aspectos relativos a la intimidad no resultan compatibles con el derecho a la intimidad contemplado en el artículo 8 del CEDH. Al respecto, el CEPD observa que, en el Derecho aplicable al caso en cuestión, esto es, en virtud de la Carta y a través de la adhesión al CEDH, así como en el Derecho coreano, existen unos principios generales de necesidad y proporcionalidad (garantizados por la Constitución, en el caso de Corea).

173. El CEPD insta a la Comisión Europea a que aclare en virtud de qué base jurídica, cómo, en qué medida y en qué condiciones concretas están obligadas las agencias de servicios de inteligencia a tener en cuenta cuestiones relativas a la intimidad y las salvaguardias en materia de protección de datos antes de divulgar datos personales a sus homólogos extranjeros por motivos de seguridad nacional. En caso de que dicha obligación derive directamente de principios constitucionales, la Comisión Europea debe evaluar también los requisitos de precisión y claridad de la ley aplicable y confirmar que se aplican correctamente los principios constitucionales generales y los relativos a la protección de datos.

[91] Véase *Schrems II*, apartados 175 y 180.

4.6.3. Acuerdos internacionales

174. El CEPD observa que la Comisión Europea no consideró en la evaluación de la adecuación la existencia de acuerdos internacionales suscritos entre la República de Corea y terceros países u organizaciones internacionales que puedan contener disposiciones específicas sobre la transferencia internacional de datos personales a terceros países por los servicios policiales o de inteligencia. El CEPD considera que la celebración de acuerdos bilaterales o multilaterales con terceros países con fines de cooperación policial o en materia de inteligencia puede afectar al marco jurídico coreano sobre protección de datos examinado.

175. En consecuencia, insta a la Comisión Europea a que aclare si existen estos acuerdos y en qué condiciones pueden celebrarse, y a que evalúe si lo dispuesto en los acuerdos internacionales puede afectar al nivel de protección que confieren a los datos personales transferidos a la República de Corea desde el EEE el marco legislativo y las prácticas relativas a las divulgaciones transfronterizas para fines policiales y de seguridad nacional.

4.7. Supervisión

176. El CEPD también constata que la supervisión de la aplicación del Derecho penal y de los organismos nacionales de seguridad se encuentra garantizada mediante una combinación de distintos organismos internos y externos.

177. En este contexto, debe tenerse en cuenta que el TJUE ha subrayado en repetidas ocasiones que una supervisión independiente es un componente esencial de la protección de las personas físicas en el ámbito del tratamiento de sus datos personales. El concepto de independencia engloba la autonomía institucional, la no sujeción a instrucciones y la independencia material. A fin de garantizar un control y una aplicación sistemáticos de la legislación en materia de protección de datos, las autoridades de control deben contar con una potestad real que incluya facultades correctivas y reparadoras.

178. El CEPD comparte la conclusión alcanzada por la Comisión Europea según la cual puede considerarse en general que la República de Corea cuenta con un sistema de control independiente y eficaz, pese a que varios organismos de su sistema de control no cumplan por sí mismos los requisitos mencionados previamente. Por ejemplo, la mayoría de estos no cuenta con poderes ejecutivos y únicamente puede formular recomendaciones. Este es el caso, p. ej., de la Comisión Nacional de Derechos Humanos o de la Junta de Auditoría e Inspección. Además, la mayoría de los respectivos organismos públicos no son instituciones dedicadas en exclusiva a la protección de datos, sino que suelen tener asignados otros cometidos en el área de la protección de los derechos fundamentales.

179. Sin embargo, tras leer las explicaciones presentadas por la Comisión Europea, el CEPD constata que el CPDP garantiza un control integral y sin excepciones de las autoridades policiales. En virtud de la LPDP y otras leyes en materia de protección de datos (p. ej., la LPPC), el CPDP posee facultades de investigación, reparación y coercitivas en todo el campo del acceso a los datos personales por autoridades policiales y encargadas de la seguridad nacional.

180. En este contexto, el CEPD desea reiterar que, para poder hacer uso de sus atribuciones y facultades, las autoridades de control deben contar con unos recursos humanos, técnicos y financieros suficientes. Por desgracia, no se ha aportado ninguna información en este sentido sobre los organismos de control designados, en particular, el CPDP. Por tanto, el CEPD vuelve a solicitar a la Comisión Europea que proporcione más información sobre este aspecto.

181. En general, el CEPD desea señalar que el proyecto de decisión apenas contiene ninguna mención, ejemplo o cifra sobre las actividades de control y la exigencia de la aplicación de la legislación en materia de protección de datos por los organismos de control en el ámbito policial y de la seguridad nacional. Este tipo de información resultaría útil para evaluar la eficacia de los organismos de control.

1.8. Recursos judiciales y medios de reparación

182. El CEPD recuerda que, para garantizar un nivel de protección de los datos adecuado, resulta esencial que los interesados dispongan de un amplio abanico de recursos y medios de reparación contra el acceso no autorizado a los datos o el tratamiento no autorizado de estos. Estas vías de recurso deben ser suficientes para que los interesados puedan acceder a sus datos que se encuentren almacenados y solicitar su rectificación o supresión.

183. En las sentencias del TJUE en los asuntos *Schrems I* y *Schrems II*, se aclara que, además del derecho a dirigirse a las autoridades competentes, la tutela judicial efectiva, en el sentido del artículo 47, apartado 1, de la Carta, es de una importancia fundamental para presumir la adecuación del Derecho de un país tercero.

184. El CEPD reconoce que la República de Corea ha previsto varios procedimientos para el ejercicio de los derechos de acceso, conservación, supresión y suspensión previstos en la LPDP. Estos derechos pueden ejercerse contra el propio responsable del tratamiento o a través de una reclamación presentada ante el CPDP u otros organismos de control, como la Comisión Nacional de Derechos Humanos. Además, el CEPD reconoce la posibilidad de impugnar la decisión de los responsables del tratamiento o las autoridades públicas en respuesta a su solicitud, tal como se prevé en la Ley sobre Litigios Administrativos de la República de Corea.

185. El CEPD entiende asimismo, tal como se deduce de las explicaciones ofrecidas por la Comisión Europea, que los interesados pueden interponer acciones contra la actuación de las autoridades policiales y encargadas de la seguridad nacional ante los órganos jurisdiccionales en virtud de la Ley sobre Litigios Administrativos y la Ley sobre el Tribunal Constitucional de la República de Corea, y pueden solicitar una indemnización por daños y perjuicios al amparo de la Ley sobre Indemnizaciones del Estado de dicho país.[92]

186. En este contexto, preocupa, no obstante, al CEPD la reparación efectiva a los interesados de la UE en casos relativos a la seguridad nacional en los que no participe ningún ciudadano coreano. Tal como se ha indicado en los párrafos 33 y siguientes, los organismos nacionales de seguridad no están obligados a notificar a los interesados la recogida y el tratamiento de sus datos personales. Puesto que resulta considerablemente más difícil obtener una protección legal efectiva en estos casos, el CEPD considera que, en estas situaciones, son necesarias determinadas garantías jurídicas cuando se transfieran datos desde el EEE. Estas garantías deben permitir a los interesados emprender acciones contra el tratamiento ilícito de datos de un modo seguro desde el punto de vista jurídico sin que se lo impidan unos requisitos procesales excesivamente gravosos, como la imposición de una carga de la prueba que no pueden asumir sin conocer el tratamiento. Además, los interesados deben poder dirigirse a un órgano competente que cumpla los requisitos del artículo 47 de la Carta, es decir, que tenga competencia para determinar si se está llevando a cabo un tratamiento de datos personales y para verificar la licitud del tratamiento, y que cuente con poderes correctivos ejecutables en caso de que el tratamiento de los datos sea ilícito. Teniendo en cuenta todo esto, no sería suficiente, por ejemplo, el mero derecho a reclamar ante la Comisión Nacional de Derechos Humanos. En consecuencia, el CEPD insta a la Comisión a que explique con mayor grado de detalle cómo se cumplen estos requisitos tanto en el ámbito procesal como en el ámbito material: p. ej., si es posible que los interesados se dirijan al CPDP y a un órgano jurisdiccional sin tener que probar el tratamiento de datos en cuestión.

187. Además, el CEPD observa que el proyecto de decisión contempla un mecanismo de derivación de reclamaciones en virtud del cual los ciudadanos de la UE pueden presentar una reclamación ante el CPDP a través de la autoridad de protección de datos de su país o el CEPD. El CPDP realizará la correspondiente notificación al interesado a través de ese mismo canal una vez que haya concluido la

[92] Véase la sección 3.2.4 del anexo II, en relación con la sección 2.4.3.

investigación.[93] El CEPD agradece este esfuerzo destinado a facilitar el acceso a los recursos contra los organismos nacionales de seguridad coreanos. Al mismo tiempo, aboga por que dicho mecanismo de derivación se canalice a través de las autoridades nacionales europeas encargadas de la protección de datos y no a través del CEPD, ya que las primeras cuentan con la competencia pertinente para la tramitación de las distintas reclamaciones y, por tanto, tienen un contacto directo con estas.

188. Además, el CEPD observa una posible contradicción en lo referente a la divulgación voluntaria. Por un lado, el proyecto de decisión establece que los interesados pueden obtener una reparación en caso de que sus datos se divulguen de manera ilícita como respuesta a una solicitud de divulgación voluntaria, pudiendo dirigirse incluso contra la autoridad policial que realice la solicitud.[94] Sin embargo, por otro, el proyecto de decisión hace referencia al requisito del efecto directo en relación con el derecho del interesado a impugnar la actuación de las autoridades públicas, pero incluye (exclusivamente) solicitudes de divulgación obligatoria como ejemplo de caso en que se considera que la actuación de la Administración afecta directamente al derecho a la confidencialidad.[95] Tras examinar las explicaciones ofrecidas por la Comisión Europea, el CEPD entiende que no existe ninguna limitación a las posibilidades de reparación contra las solicitudes de divulgación voluntaria y, en consecuencia, solicita a la Comisión Europea que aclare este aspecto en la decisión, tanto en los ámbitos de la actuación policial como de la seguridad nacional (al contrario que en la sección sobre el ámbito policial, la sección sobre la divulgación voluntaria por motivos de seguridad nacional no contiene ninguna declaración expresa sobre la reparación en este contexto).

[93] Véanse el considerando 205 y la página 19 del anexo I del proyecto de decisión.
[94] Véase el considerando 166 del proyecto de decisión.
[95] Véanse el considerando 181 (actuación policial) y los considerandos 208 y 181 (seguridad nacional) del proyecto de decisión.