Dictamen del Comité (art. 70.1.s)

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

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) n.º 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, el «RGPD»),

Visto el Acuerdo EEE y, en particular, su anexo XI y su Protocolo 37, en su versión modificada por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018,

Vistos el artículo 12 y el artículo 22 de su reglamento interno, de 25 de mayo de 2018,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1 RESUMEN EJECUTIVO

1. La Comisión Europea aprobó su proyecto de Decisión de Ejecución sobre la protección adecuada de los datos personales por parte de Japón de conformidad con el Reglamento general de protección de datos (en lo sucesivo, «RGPD»)[1] el 5 de septiembre de 2018[2]. A continuación, la Comisión Europea inició el procedimiento para su adopción formal.

2. El 25 de septiembre de 2018, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos (en lo sucesivo, «CEPD»)[3]. Se pidió a la Comisión que facilitara al CEPD toda la documentación necesaria sobre este país, incluida cualquier correspondencia pertinente con el Gobierno de Japón.

3. A la luz de los debates mantenidos con el CEPD, la Comisión Europea modificó dos veces su proyecto de decisión de adecuación y envió su última versión el 13 de noviembre de 2018[4] El CEPD ha basado su presente dictamen en la última versión del proyecto de Decisión de Ejecución (en lo sucesivo, «el proyecto de decisión de adecuación»).

4. La evaluación por parte del CEPD del nivel de protección garantizado por la decisión de adecuación de la Comisión se ha realizado sobre el examen de la propia decisión, así como sobre la base de un análisis de la documentación facilitada[5] por la Comisión[6].

5. El CEPD se centró tanto en la evaluación de los aspectos comerciales del proyecto de decisión de adecuación como en el acceso del Gobierno a los datos personales transferidos desde la UE con fines

[1] Reglamento (UE) n.º 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
[2] Véase el comunicado de prensa http://http://europa.eu/rapid/press-release_IP-18-5433_es.htm
[3] De conformidad con el artículo 70, apartado 1, letra s), del RGPD.
[4] Véase el anexo I del dictamen del CEPD sobre la versión actualizada del proyecto de Decisión de Ejecución de la Comisión Europea.
[5] El CEPD basó su análisis en las traducciones facilitadas por las autoridades japonesas verificadas por la Comisión Europea.
[6] Véase el anexo II del dictamen del CEPD para la lista de documentos no facilitados por la Comisión Europea al CEPD.

policiales y de seguridad nacional, incluidas las vías de recurso disponibles para los ciudadanos de la UE. El CEPD también evaluó si hay salvaguardias previstas en el marco jurídico japonés y si son eficaces.

6. El CEPD ha utilizado como referencia principal para este trabajo sus referencias sobre adecuación[7] adoptadas en febrero de 2018.

1.1 Ámbitos de convergencia

7. El principal objetivo del CEPD ha sido emitir un dictamen para la Comisión Europea sobre el nivel de protección de las personas en el marco japonés. Es importante reconocer que el CEPD no espera que el marco jurídico japonés reproduzca la legislación europea en materia de protección de datos.

8. Sin embargo, el CEPD recuerda que para considerar que proporciona un nivel adecuado de protección, la jurisprudencia del TJUE y el artículo 45 del RGPD exigen que la legislación del tercer país se ajuste a la esencia de los principios fundamentales consagrados en el RGPD. En los ámbitos de la protección de datos, el CEPD señala, además, que existen ámbitos clave de armonización entre el marco del RGPD y el marco japonés sobre determinadas disposiciones básicas, como la precisión y la minimización de los datos, la limitación del almacenamiento, la seguridad de los datos, la limitación de la finalidad y una autoridad de supervisión independiente, la Comisión de Protección de la Información Personal (Personal Información Protection Commission, PPC).

9. Además de lo anterior, el CEPD acoge con satisfacción los esfuerzos realizados por la Comisión Europea y las autoridades japonesas para garantizar que Japón proporcione un nivel de protección adecuado al del RGPD, en particular colmando las lagunas entre el RGPD y el marco de protección de datos de Japón mediante la adopción de normas suplementarias por parte de la PPC aplicables únicamente a los datos personales transferidos de la UE a Japón (en lo sucesivo, las «normas suplementarias»). Por ejemplo, el CEPD señala que la PPC acordó tratar más categorías de datos como datos sensibles (en virtud de la legislación japonesa, los datos sensibles no incluyen la orientación sexual ni la afiliación sindical). Además, las normas suplementarias garantizan que los derechos de los interesados se apliquen a todos los datos personales transferidos desde la UE, con independencia de su periodo de conservación (mientras que el ordenamiento jurídico japonés establece que los derechos de los interesados no se aplican a los datos personales que deben suprimirse en un plazo de seis meses).

10. El CEPD también toma nota de los esfuerzos de la Comisión Europea por reforzar la decisión de adecuación en respuesta a las preocupaciones planteadas por el CEPD.

1.2 Retos generales

11. No obstante, siguen existiendo retos y el CEPD sugiere las siguientes como las principales áreas que deben reforzarse y ser objeto de un estrecho seguimiento en el sistema japonés.

12. El primer reto se refiere al seguimiento de esta nueva arquitectura de adecuación, que combina un marco jurídico existente con normas suplementarias específicas, para garantizar que será un sistema sostenible y fiable que no planteará **problemas prácticos en relación con el cumplimiento concreto y eficiente** por parte de las entidades japonesas y la ejecución por parte de la PPC.

13. En segundo lugar, el CEPD toma nota de los reiterados compromisos y garantías de la Comisión Europea y de las autoridades japonesas en relación con el carácter vinculante y aplicable de las normas suplementarias, al tiempo que invita a la Comisión Europea a **supervisar continuamente su carácter vinculante y su aplicación efectiva en Japón**, ya que su valor jurídico es un elemento absolutamente esencial de la adecuación entre la UE y Japón. Con respecto a las directrices de la PPC, el CEPD desearía

[7] WP 254, referencias sobre adecuación, 6 de febrero de 2018.

recibir aclaraciones en el proyecto de decisión de adecuación en relación con **su carácter vinculante y pide a la Comisión que siga atentamente este aspecto**[8].

1.3 Aspectos comerciales específicos

14. En el ámbito de los aspectos comerciales del proyecto de decisión de adecuación entre la UE y Japón, el CEPD tiene algunas inquietudes específicas y desearía solicitar aclaraciones sobre algunos asuntos importantes.

1.3.1 Preocupaciones del CEPD en relación con los principios clave de la protección de datos

15. El CEPD acoge con satisfacción que las normas suplementarias excluyan que los datos personales transferidos desde la UE se transfieran posteriormente a un tercer país sobre la base de las normas transfronterizas de protección de la privacidad aplicable a la cooperación económica Asia-Pacífico (APEC CBPR). Además, el CEPD reconoce que en su nuevo proyecto de decisión de adecuación, la Comisión Europea se comprometió a suspender la decisión de adecuación cuando las transferencias ulteriores ya no garanticen la continuidad de la protección.

16. Con arreglo a la legislación japonesa, una de las bases jurídicas para las transferencias ulteriores es el reconocimiento de que un tercer país proporciona un nivel de protección adecuado al de Japón. Sin embargo, la evaluación de la adecuación de un tercer país por Japón no parece incluir las «normas suplementarias» específicas negociadas entre la Comisión Europea y la PPC, que solo son aplicables a los datos personales de la UE con el fin de establecer un nivel de protección esencialmente equivalente a las normas del RGPD. De ello se deduce que los datos personales de la UE que se transfieren de Japón a otro tercer país no reconocido con un marco de protección de datos esencialmente equivalente al RGPD sobre la base de una adecuación japonesa ya no se beneficiarán necesariamente de la protección específica de los datos personales de la UE.

17. **No obstante, hay que tener en cuenta que pueden darse transferencias ulteriores de datos personales a terceros países que pasen a ser objeto de una posible decisión de adecuación japonesa posterior. Es posible que estos terceros países no hayan sido objeto de una evaluación anterior o de una constatación de adecuación de la UE. En este punto, la Comisión debería asumir su función de supervisión y garantizar el nivel de protección de los datos de la UE, o considerar la suspensión de esta decisión de adecuación.**

18. Además, el CEPD tiene dudas en cuanto a las **obligaciones de consentimiento y transparencia** de los responsables del tratamiento de datos (Personal Information Handling Business Operator, PIHBO). El CEPD realizó una cuidadosa verificación de estos elementos por la razón de que, a diferencia de la legislación europea en materia de protección de datos, el uso del consentimiento como base para el tratamiento y para las transferencias desempeña un papel central en el ordenamiento jurídico japonés. Por ejemplo, el CEPD tiene dudas sobre el concepto de consentimiento, que no se define en aras de incluir el derecho de desistimiento, un elemento esencial de la legislación de la UE para garantizar el verdadero control del interesado sobre sus datos personales. En cuanto a las obligaciones de transparencia de un PIHBO, existen dudas sobre si se facilita información proactiva a los interesados.

19. El CEPD expresa su preocupación por el hecho de que el **sistema de recurso japonés** pueda no ser de fácil acceso a los particulares de la UE que necesiten ayuda o que deseen presentar una reclamación a la luz del hecho de que la asistencia de la PPC está disponible únicamente a través de un servicio de atención telefónica y en japonés. La misma cuestión se da con el servicio de mediación prestado por la PPC, ya que el sistema no está publicado en la versión inglesa del sitio web de la PPC, mientras que

[8] Para más información, véase la sección 1.3.4 del presente dictamen.

documentos informativos importantes, como las preguntas frecuentes sobre la ley japonesa sobre la protección de la información personal APPI (Act on Protection of Personal Information, APPI), también están disponibles solo en japonés. A este respecto, el CEPD acogería con satisfacción la posibilidad de que la Comisión debatiera con la PPC la posibilidad de crear un servicio en línea, al menos en inglés, destinado a prestar apoyo y gestionar las reclamaciones de particulares en la UE, similar al previsto en el anexo II de esta decisión de adecuación. La Comisión Europea también deberá supervisar de cerca la eficacia de las sanciones y de las soluciones pertinentes.

1.3.2 Necesidad de aclaración

20. El CEPD daría la bienvenida a garantías en relación con algunos aspectos del proyecto de decisión de adecuación que siguen requiriendo mayores aclaraciones.

21. Se trata, por ejemplo, de algunos conceptos clave de la legislación japonesa. Más concretamente, hay una falta de claridad en torno al **estatuto del denominado «administrador»**, un término que se asemeja al del encargado del tratamiento en virtud del RGPD, pero cuya capacidad para determinar y modificar las finalidades y los medios del tratamiento de datos personales sigue siendo ambigua.

22. El CEPD también necesitaría garantías debido a la falta de los documentos pertinentes, sobre si las **restricciones a los derechos de las personas** (en particular, los derechos de acceso, rectificación y oposición) son necesarias y proporcionadas en una sociedad democrática y respetan la esencia de los derechos fundamentales.

23. El CEPD también espera que la Comisión Europea siga de cerca la protección efectiva de los **datos personales transferidos de la UE a Japón, sobre la base del proyecto de decisión de adecuación, a lo largo de todo su ciclo de vida**, a pesar de que la legislación japonesa impone una obligación de conservar el origen de los datos durante un máximo de tres años.

1.4 Sobre el acceso de las autoridades públicas a los datos transferidos a Japón

24. El CEPD también ha analizado el marco jurídico de las entidades gubernamentales japonesas a la hora de acceder a los datos personales transferidos de la UE a Japón con fines policiales o de seguridad nacional. Si bien reconoce las garantías proporcionadas por el Gobierno japonés, como el anexo II del proyecto de decisión de adecuación, el CEPD ha identificado una serie de aspectos para aclaraciones y de interés, de los que cabe destacar los siguientes.

25. En el ámbito de la aplicación de la ley, el CEPD observa que los principios jurídicos aplicables a los datos de acceso a menudo parecen ser similares a las normas de la UE, en la medida en que están disponibles. La falta de traducciones disponibles de varios textos jurídicos y de la jurisprudencia pertinente dificulta, sin embargo, llegar a la conclusión de que todos los procedimientos de acceso a los datos son necesarios y proporcionados y que la aplicación de estos principios se efectúa de manera «sustancialmente equivalente» a la legislación de la UE.

26. En el ámbito de la seguridad nacional, el CEPD reconoce que el Gobierno japonés ha reiterado que la información solo puede obtenerse a partir de fuentes de libre acceso o de divulgación voluntaria por parte de las empresas, y que no recoge información sobre el público en general. Es consciente, sin embargo, de las preocupaciones expresadas por los expertos y los medios de comunicación, y acogería con satisfacción nuevas aclaraciones sobre las medidas de vigilancia de las entidades gubernamentales japonesas.

27. En cuanto a las vías de recurso de los ciudadanos de la UE, en el ámbito de la aplicación de la ley y de la seguridad nacional, el CEPD saluda que la Comisión Europea y el Gobierno japonés hayan negociado un mecanismo adicional para que los ciudadanos de la UE dispongan de una vía de recurso adicional,

ampliando así las competencias de la autoridad japonesa de protección de datos. Sin embargo, un punto de preocupación sigue siendo que este nuevo mecanismo no compensa totalmente las deficiencias de la supervisión y las vías de recurso de la legislación japonesa. Por tanto, el CEPD busca nuevas clarificaciones con el fin de garantizar que este nuevo mecanismo compensa plenamente estas deficiencias.

1.5 Conclusión

28. El CEPD considera que esta decisión de adecuación es de vital importancia. Como primera decisión de adecuación desde la entrada en vigor del RGPD, constituirá **un precedente para las futuras solicitudes de adecuación, así como para la revisión de las decisiones de adecuación adoptadas en virtud de la Directiva 95/46[9].** También es importante subrayar que las personas son cada vez más conscientes del impacto de la globalización en su privacidad y se dirigen a las autoridades de supervisión para asegurarse de que existen las garantías adecuadas cuando sus datos personales se transfieren al extranjero. A la luz de estas implicaciones, el CEPD considera que la Comisión Europea debe garantizar que no existen deficiencias en la protección que ofrece la adecuación entre la UE y Japón y que este tipo específico de adecuación se ajusta a los requisitos del artículo 45 del RGPD.

29. El CEPD acoge con satisfacción los esfuerzos realizados por la Comisión Europea y la PPC japonesa para adaptar todo lo posible el marco jurídico japonés al europeo. **Las mejoras** introducidas por las normas suplementarias para salvar algunas de las diferencias entre los dos marcos son muy importantes y bien recibidas.

30. Sin embargo, tras un minucioso análisis del proyecto de decisión de adecuación de la Comisión, así como del marco japonés de protección de datos, el CEPD señala que sigue existiendo **una serie de preocupaciones, junto con la necesidad de aclaraciones adicionales**. Además, este tipo específico de adecuación, que combina un marco nacional existente con normas específicas adicionales, también plantea dudas sobre su aplicación operativa. En vista de lo anterior, el CEPD recomienda a la Comisión Europea que aborde las inquietudes y las solicitudes de aclaración planteadas por el CEPD y aporte más pruebas y explicaciones sobre las cuestiones planteadas. El CEPD también invita a la Comisión Europea a revisar este nivel de adecuación (como mínimo) cada dos años y no cada cuatro años, como se sugiere en el actual proyecto de decisión de adecuación.

2 INTRODUCCIÓN

2.1 Marco de protección de datos de Japón

31. El marco de protección de datos de Japón se modernizó muy recientemente, en 2017. Este marco comprende varios pilares, que giran en torno a una ley general, la Ley de protección de datos personales (Act on Protection of Personal Information, APPI). Otro acto legislativo importante es la Orden ministerial para la entrada en vigor de la APPI (en la sucesivo, la «Orden ministerial»), que especifica algunos principios fundamentales de dicha Ley.

32. Sobre la base de una decisión del Consejo de Ministros, adoptada el 12 de junio de 2018[10] y del artículo 6 de la APPI, se otorgó a la PPC la facultad de «a*doptar las medidas necesarias para salvar las*

[9] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[10] El CEPD observa que, según el proyecto de decisión de adecuación, esta Decisión del Consejo de Ministros se adoptó el 12 de junio de 2018. Sin embargo, el CEPD solo contó con el proyecto de la Decisión del Consejo de Ministros, con fecha de abril de 2018.

diferencias entre los sistemas y las operaciones entre Japón y el país extranjero afectado, con el fin de garantizar un tratamiento adecuado de la información de carácter personal recibida de cada país»[11]. La decisión del Consejo de Ministros también sugiere que las normas adoptadas por la PPC que completen o vayan más allá de las establecidas en la APPI serían vinculantes y aplicables a los operadores de empresas japoneses[12].

33. En consecuencia, la PPC inició negociaciones con la Comisión Europea y adoptó, en junio de 2018, normas más estrictas a las de la APPI y la Orden ministerial aplicables a los datos transferidos desde la UE. Estas son las normas suplementarias con arreglo a la Ley sobre la protección de la información personal para el tratamiento de datos personales transferidos desde la UE sobre la base de una decisión de adecuación (en lo sucesivo las «normas suplementarias»[13]). Estas normas suplementarias se adjuntan asimismo al proyecto de Decisión de Ejecución de la Comisión publicado en julio de 2018.

34. Es importante señalar que las normas suplementarias solo son aplicables a los datos personales transferidos desde la Unión Europea a Japón sobre la base de la decisión de adecuación y que tienen por objeto mejorar la protección aplicable a esos datos. Así, no se aplican a los datos personales de personas de Japón o procedentes de países distintos de los del EEE.

35. Por otra parte, el CEPD desea llamar la atención sobre el hecho de que la APPI modificada entró en vigor el 30 de mayo de 2017 y de que la PPC se estableció en su forma actual en 2016. Por añadidura, las normas suplementarias negociadas por la PPC con la Comisión Europea aún no han entrado en vigor, ya que ello dependerá del reconocimiento por parte de la Comisión Europea de Japón como una jurisdicción adecuada a la de la UE.

2.2 Alcance de la evaluación del CEPD

36. El proyecto de decisión de adecuación de la Comisión Europea es el resultado de una evaluación de las normas japonesas de protección de datos, seguida de negociaciones con las autoridades japonesas. El resultado de estas negociaciones se refleja, en particular, en los dos anexos adjuntos al proyecto de decisión de adecuación: el primero prevé medidas de protección adicionales que los operadores de empresas japoneses tendrán que aplicar al tratamiento de datos personales transferidos desde la UE, mientras que el segundo contiene garantías y compromisos del Gobierno japonés en relación con el acceso de las autoridades públicas a los datos.

37. El CEPD examinó el marco japonés de protección de datos, las normas suplementarias negociadas por la Comisión Europea y las garantías y compromisos del Gobierno japonés. Se espera que el CEPD emita un dictamen independiente sobre las conclusiones de la Comisión Europea, identifique las insuficiencias en el marco de adecuación, en su caso, y se esfuerce por proponer modificaciones o enmiendas para abordarlas.

38. Como se indica en las referencias sobre adecuación del CEPD, «*la información facilitada por la Comisión Europea debe ser exhaustiva y poner al CEPD en posición de realizar su propia evaluación sobre el nivel de protección de datos en el tercer país*»[14].

39. No obstante, el CEPD recibió la mayor parte de los documentos en traducciones al inglés, referenciados en el proyecto de decisión de adecuación, que constituyen una parte esencial del ordenamiento

[11] Decisión del Consejo de Ministros de 25 de abril de 2018.
[12] Para más información, véase la sección 1.3.4 siguiente.
[13] Normas suplementarias, anexo I de la Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, enviadas al CEPD en septiembre de 2018.
[14] WP 254, p. 3.

jurídico japonés. El CEPD, por lo tanto, emite el presente dictamen sobre la base del análisis de los documentos disponibles en inglés. El CEPD tuvo en cuenta el marco de protección de datos aplicable en la Unión Europea, incluido el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, el «CEDH»), que protege el derecho a la vida privada y familiar, así como los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la «Carta») que protegen, respectivamente, el derecho a 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. Además de lo anterior, el CEPD consideró los requisitos del RGPD y consideró la jurisprudencia pertinente.

40. El objetivo de este ejercicio es garantizar que el marco de protección de datos japonés sea sustancialmente equivalente al de la Unión Europea. El Tribunal de Justicia de la Unión Europea ha seguido desarrollando el concepto de «nivel adecuado de protección», que ya existía en virtud de la Directiva 95/46. Es importante recordar la norma establecida por el TJUE en el asunto Schrems, a saber, que, si bien el «nivel de protección» en el tercer país debe ser «esencialmente 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]»[15]. Por lo tanto, el objetivo no es reproducir punto por punto la legislación europea, sino establecer los requisitos principales y esenciales de la legislación sometida a examen. La adecuación puede lograrse combinando los derechos de los interesados y las obligaciones de aquellos que tratan los datos o que ejercen el control sobre dicho tratamiento y supervisión por organismos independientes. Sin embargo, las normas de protección de datos solo son eficaces si son aplicables y se aplican en la práctica. Por consiguiente, es necesario tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país o una organización internacional, sino también el sistema establecido para garantizar la eficacia de dichas normas. Unos mecanismos de aplicación eficientes son de vital importancia para la eficacia de las normas de protección de datos[16].

2.3 Observaciones generales y preocupaciones

2.3.1 Características específicas de este tipo de decisión de adecuación

41. La adecuación entre la UE y Japón es la primera que se ha de examinar en relación con el nuevo fundamento jurídico del RGPD. Esto hace que el trabajo del CEPD sea tanto más importante a la luz de los efectos de este proyecto de decisión de adecuación para las futuras solicitudes de adecuación.

42. La adecuación entre la UE y Japón sería también la primera mutua. Cuando la UE reconozca que Japón posee un nivel de protección esencialmente equivalente al del RGPD, Japón también emitirá su propia decisión de adecuación con arreglo al artículo 24 de la APPI, reconociendo que la UE ofrece un nivel adecuado de protección con arreglo al marco de protección de datos japonés. Así pues, esta adecuación prevista entre Japón y la UE es de una naturaleza particular que el CEPD ha tenido en cuenta en su evaluación. Como se ha mencionado anteriormente, la PPC japonesa ha negociado normas específicas y más estrictas con la Comisión Europea, aplicables únicamente a los datos personales transferidos desde la UE. Estas normas más estrictas son vinculantes y aplicables con arreglo a la Orden ministerial y deben ser respetadas por todos los operadores comerciales de manipulación de información personal (en lo sucesivo, «PIHBO») en Japón cuando traten datos personales procedentes de la UE en virtud de este proyecto de decisión de adecuación.

43. Por consiguiente, la Comisión Europea ha basado su análisis de adecuación no solo en el actual marco general de protección de datos de Japón, sino también en estas normas específicas. El hecho de que

[15] Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 de octubre de 2015 (apartados 73 y 74).
[16] WP 254, p. 2.

se exigieran normas suplementarias para completar la APPI es un indicio de que la Comisión Europea reconoce que la legislación japonesa en materia de protección de datos no es, en sí misma, esencialmente equivalente al RGPD.

44. **A la luz de las cuestiones mencionadas anteriormente, el CEPD invita a la Comisión Europea a garantizar que esta nueva arquitectura de la adecuación, la primera que se va a adoptar en el marco del RGPD, basada en las normas suplementarias, será un sistema sostenible y fiable que no planteará problemas prácticos en relación con el cumplimiento concreto y eficiente por parte de las entidades japonesas y la ejecución por parte de la PPC.**

2.3.2 Seguridad de las traducciones

45. Al igual que la Comisión Europea, el CEPD ha trabajado sobre la base de las traducciones al inglés proporcionadas por las autoridades japonesas[17]. El CEPD pide a la Comisión Europea que aclare que ha basado su proyecto de decisión de adecuación en las traducciones al inglés recibidas y que verifique regularmente la calidad y la seguridad de las mismas.

2.3.3 Adecuación sectorial

46. La comprobación de la adecuación de este proyecto de decisión de adecuación se limita a la protección de la información personal por parte de los PIHBO en el sentido de la APPI. Esto significa que la adecuación es sectorial, ya que solo se refiere al sector privado, excluyendo de su ámbito de aplicación las transferencias de datos personales entre autoridades públicas y organismos. En la actualidad, la Comisión Europea menciona brevemente esta especificidad del alcance de la adecuación en el considerando 10 del proyecto de decisión de adecuación.

47. **El CEPD invita a la Comisión Europea a mencionar explícitamente el carácter sectorial de esta constatación de adecuación en el título de la Decisión de Ejecución, así como en su artículo 1, de conformidad con el artículo 45, apartado 3, del RGPD.**

2.3.4 Carácter vinculante de las normas suplementarias y de las directrices de la PPC

48. El artículo 6 de la APPI menciona que «el Gobierno [...] adoptará las medidas legislativas y de otra índole necesarias para poder llevar a cabo una acción discreta para proteger la información personal que requiera, en particular, garantizar la estricta aplicación de su correcta manipulación con el fin de reforzar la protección de los derechos e intereses de las personas, y tomará las medidas necesarias, en colaboración con los Gobiernos de otros países, para construir un sistema de información personal que pueda adaptarse internacionalmente mediante el fomento de la cooperación con una organización internacional y otro marco internacional». Aunque en este artículo de la APPI se identifica claramente que el Gobierno es competente para emprender tal acción judicial, no se refiere directamente a la PPC como el organismo competente para adoptar normas específicas[18]. Debido a limitaciones de tiempo, el CEPD no pudo recabar, revisar y examinar las pruebas existentes al respecto.

49. **A la luz de la importancia de esta cuestión, el CEPD toma nota de los reiterados compromisos y garantías de la Comisión Europea y las autoridades japonesas en relación con el carácter vinculante y aplicable de las normas suplementarias. El CEPD invita a la Comisión Europea a supervisar continuamente su carácter vinculante y su aplicación efectiva en Japón, ya que su valor jurídico es un elemento esencial de la adecuación entre la UE y Japón.**

[17] La Comisión Europea ha verificado estas traducciones.

[18] Según un artículo publicado en julio de 2018, cuando las normas suplementarias estaban en proyecto, era probable que su carácter jurídicamente vinculante fuese objeto de debate interno en el país. Véase Fujiwara S.: «Comparison between the EU and Japan's Data Protection Legal Frameworks», *Jurist*, vol. 1521 (julio de 2018), p. 19.

50. Por otra parte, la Comisión Europea hace referencia en varias secciones de su proyecto de decisión de adecuación a las directrices de la PPC (en lo sucesivo, las «Directrices»).

51. Aunque la Comisión Europea aclara que las Directrices proporcionan una interpretación preceptiva de la APPI en el considerando 16 de su proyecto de decisión de adecuación, en el mismo considerando se hace referencia al carácter vinculante de las presentes Directrices: «Según la información recibida de la PPC, estas Directrices se consideran normas vinculantes que forman parte integrante del marco jurídico, que deben leerse conjuntamente con el texto de la APPI, la Orden Ministerial, las normas de la PPC y un conjunto de preguntas y respuestas preparado por la PPC».[19]

52. Sin embargo, la perspectiva del CEPD, basada en la misma información facilitada por la PPC, es que las Directrices no son jurídicamente vinculantes, sino que proporcionan una «interpretación preceptiva» de la ley. La PPC sostiene que, en la práctica, las Directrices son seguidas por los PIHBO, que la PPC las utiliza para hacer cumplir la ley contra los PIHBO y que son utilizadas por los órganos jurisdiccionales a la hora de dictar sentencia. Sin embargo, estos elementos no constituyen pruebas suficientes de que las Directrices sean normas jurídicamente vinculantes.

53. **El CEPD desearía recibir aclaraciones en la decisión de adecuación en relación con el carácter vinculante de las Directrices de la PPC y pide a la Comisión Europea que vigile atentamente este aspecto.**

54. Según la PPC, las Directrices se siguen en la práctica, aunque se trata de usos locales. La PPC menciona que los tribunales japoneses utilizan las Directrices de la PPC para emitir sus sentencias al aplicar las normas de la APPI. La Comisión Europea hace referencia a una sentencia judicial[20] que data de 2006 para demostrar que los tribunales japoneses se basan en las Directrices para sus conclusiones. A pesar de que no se proporcionó dicha sentencia al CEPD, este agradecería que la Comisión Europea pudiera proporcionar, si se dispone de ella, una sentencia más reciente, bien en el ámbito de la protección de datos, bien en otro sector en el que los tribunales japoneses hayan utilizado las Directrices de la PPC u otras directrices similares como base para su decisión.

2.3.5 Revisión periódica de la constatación de la adecuación

55. El artículo 45, apartado 3, del RGPD establece que debe efectuarse una revisión periódica al menos cada cuatro años. De acuerdo con las referencias sobre adecuación del CEPD[21], se trata de un plazo general que debe ajustarse a cada tercer país u organización internacional con una decisión de adecuación. Dependiendo de las circunstancias particulares de que se trate, podría justificarse un ciclo de revisión más breve. Asimismo, los incidentes, otra información o cambios en el marco jurídico en el tercer país o la organización internacional de que se trate podrían dar lugar a la necesidad de una revisión antes de la fecha prevista. También parece apropiado proceder con menor dilación a una primera revisión de una decisión de adecuación totalmente nueva e ir ajustando gradualmente el ciclo de revisión en función de los resultados.

56. Teniendo en cuenta una serie de factores, entre ellos el hecho de que la APPI entró en vigor en 2017, que la PPC se creó en 2016 y que aún no se dispone de información ni pruebas sobre la aplicación

[19] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, remitida al CEPD el 13 de noviembre de 2018, considerando 16.

[20] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, enviada al CEPD el 13 de noviembre de 2018, página 5, nota a pie de página n.º 16, Tribunal de Distrito de Osaka, Decisión de 19 de mayo de 2006, Hanrei Jiho, Vol. 1948, p. 122.

[21] WP 254, p. 3.

práctica de las normas suplementarias, **el CEPD invita a la Comisión Europea a revisar esta constatación de adecuación (como mínimo) cada dos años y no cada cuatro años, como se sugiere en el actual proyecto de decisión de adecuación.**

2.3.6 Compromisos internacionales contraídos por Japón

57. De conformidad con el artículo 45, apartado 2, letra c), del RGPD y las referencias sobre adecuación[22], al evaluar la adecuación del nivel de protección de un tercer país, la Comisión Europea tendrá en cuenta, entre otras cosas, los compromisos internacionales suscritos 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 datos personales, así como la aplicación de dichas obligaciones. Además, debe tenerse en cuenta la adhesión del tercer país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal («Convenio 108 +»[23]) y su Protocolo adicional.

58. **A este respecto, el CEPD observa que Japón es un observador del Comité Consultivo del Convenio 108 +.**

2.3.7 Poderes de las autoridades de protección de datos[24] para interponer acciones relativas a la validez de una decisión de adecuación ante un órgano jurisdiccional

59. El CEPD subraya que, si bien el considerando 179 del proyecto de decisión de adecuación solo menciona casos en los que una autoridad de protección de datos ha recibido una reclamación que cuestiona la compatibilidad de una decisión de adecuación con los derechos fundamentales de la persona a la intimidad y la protección de datos, esta afirmación debe entenderse como un ejemplo de situaciones en las que una autoridad de protección de datos puede someter el asunto a un órgano jurisdiccional nacional, lo que también podría ser posible en ausencia de una reclamación, en lugar de como una restricción a las facultades conferidas a las APD en virtud del RGPD y de las legislaciones nacionales de los Estados miembros a este respecto. En efecto, las disposiciones del RGPD incluyen tanto la facultad de suspender las transferencias de datos incluso cuando se basan en una decisión de adecuación como la de interponer una acción relativa a la validez de una decisión de adecuación, y no se limitan a los casos en los que han recibido una reclamación, en caso de que su legislación nacional les conceda la competencia para hacerlo de forma más amplia y con independencia de una reclamación, de conformidad con las disposiciones pertinentes del RGPD.

60. **El CEPD pide a la Comisión Europea que aclare en su proyecto de decisión de adecuación que la facultad de las autoridades de supervisión de interponer una acción contra la validez de una decisión de adecuación a raíz de una reclamación es solo un ejemplo de los poderes más amplios de las APD derivados del RGPD, que incluyen la facultad de suspender las transferencias y de interponer una acción sobre la validez de una decisión de adecuación en ausencia de reclamación en caso de que su legislación nacional así lo disponga.**

[22] WP 254, p. 2.
[23] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Convenio 108 +, de 18 de mayo de 2018.
[24] Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 de octubre de 2015.

3 ASPECTOS COMERCIALES

3.1 Principios relativos al contenido

61. El capítulo 3 de las referencias sobre adecuación se dedica a los «principios relativos al contenido». El sistema de un tercer país o de una organización internacional debe incluirlos a fin de considerar que el nivel de protección ofrecido es esencialmente equivalente al garantizado por la legislación de la UE. El CEPD reconoce el hecho de que el ordenamiento jurídico japonés persigue un enfoque diferente del RGPD con el fin de dar efecto al derecho a la intimidad. Aunque el derecho a la intimidad no está consagrado en la Constitución japonesa *per se*, ha sido reconocido como un derecho constitucional a través de la jurisprudencia, como también se menciona en la Decisión de la Comisión Europea[25].

62. Debido, en particular, al hecho de que el enfoque japonés difiere notablemente del europeo, es preciso observar cuidadosamente si, no solo los aspectos individuales, sino el sistema en su conjunto proporciona, en última instancia, un nivel de protección «esencialmente equivalente». Esto significa que las posibles «deficiencias» concernientes a un principio relativo al contenido podrían verse compensadas por otros aspectos que proporcionan un sistema de contrapoderes adecuado.

3.1.1 Conceptos

63. Sobre la base de las referencias sobre adecuación, deben existir conceptos o principios básicos de protección de datos en el marco jurídico del tercer país. Aunque no tienen que copiar la terminología del RGPD, deben reflejar y ser coherentes con los conceptos consagrados en la legislación europea en materia de protección de datos. Por ejemplo, el RGPD incluye los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «responsable del tratamiento», «encargado del tratamiento», «destinatario» y «datos sensibles»[26].

64. La APPI también incluye una serie de definiciones como, entre otras, las de «información personal», «datos personales», «operador comercial de manipulación de información personal». **Sin embargo, parece que la APPI no incluye una definición del término «manipulación de datos personales», que es similar al término «tratamiento de datos personales».**

65. En cuanto a la definición del término «manipulación de datos personales», la PPC ha respondido por escrito a la pregunta del CEPD sobre esta definición. La Comisión Europea citó esta respuesta al proyecto de Decisión de la Comisión: «*Aunque la APPI no utiliza el término "tratamiento", se basa en el concepto equivalente de "manipulación", que, según la información recibida por la PPC, abarca "todo acto sobre datos personales" incluida la adquisición, introducción, acumulación, organización, almacenamiento, edición/tratamiento, renovación, producción, seguridad, producción [Sic.], utilización o suministro de información personal*»[27].

66. Sin embargo, dado que no se ha facilitado el texto de referencia para esta definición, el CEPD invita a **la Comisión Europea a supervisar de cerca que la definición del concepto mencionado anteriormente, tal como ha sido facilitada por la PPC, se siga efectivamente en la práctica.**

---

[25] El CEPD no ha recibido la traducción al inglés de esta decisión judicial. Véase la Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, enviado al CEPD el 13 de noviembre de 2018, nota a pie de página 9.

[26] WP 254, p. 4.

[27] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, enviado al CEPD el 13 de noviembre de 2018, considerando 17.

3.1.1.1 Concepto de encargado del tratamiento de datos y obligaciones de un «administrador»

67. Como se ha mencionado anteriormente, las referencias sobre adecuación exigen que en el marco jurídico del tercer país existan conceptos o principios básicos de protección de datos.

68. La APPI incluye una definición de «operador comercial de manipulación de información personal» que, según la Comisión Europea, comprende tanto los términos de un responsable del tratamiento como de un encargado del tratamiento, según lo dispuesto por el RGPD, y no distingue entre ambos[28]. Sin embargo, la APPI incluye también el término «administrador» en su artículo 22, que se parece, de alguna manera, al término de un encargado del tratamiento de datos de conformidad con el RGPD.

69. Como explicó la PPC en sus respuestas proporcionadas al CEPD, y también incluidas en el proyecto de decisión de adecuación de la Comisión Europea, se considera que un administrador es el equivalente de un encargado del tratamiento de datos en virtud del RGPD —ya que un PIHBO le confía la manipulación de los datos personales—. Este administrador tiene las mismas obligaciones y derechos que los PIHBO, incluidos los de las normas suplementarias para los datos personales transferidos desde la UE. El PIHBO que confíe la manipulación de datos personales a un administrador está obligado a «ejercer la supervisión necesaria y adecuada»[29] sobre el mismo.

70. **El CEPD invita a la Comisión Europea a explicar el estatuto y las obligaciones del administrador cuando este cambia las finalidades y los medios del tratamiento y aclarar si el consentimiento del interesado sigue siendo una condición necesaria para tal cambio de finalidad o de determinación de los medios[30].**

3.1.1.2 Concepto de datos personales conservados

71. La APPI contiene el concepto de «datos personales conservados», que se considera una subcategoría de los datos personales. Según la APPI, las disposiciones relativas a los derechos del interesado[31] solo se aplican a los datos personales conservados. La definición de datos personales conservados se incluye en el artículo 2, apartado 7, de la APPI.

72. Los datos personales conservados son los datos personales distintos de los que i) deben suprimirse en un periodo no superior a 6 meses[32] o ii) están incluidos en las excepciones del artículo 4 de la Orden Ministerial y que pueden perjudicar al público o a otros intereses si se conocen su presencia o ausencia.

73. La norma suplementaria (2) establece que «*los datos personales recibidos de la UE basados en una decisión de adecuación deben ser tratados como datos personales conservados, independientemente del periodo en el que se fije su supresión*».

74. Sin embargo, los datos personales que entran en el ámbito de aplicación de las excepciones del artículo 4 de la Orden Ministerial no tendrán que tratarse como datos personales conservados y no se aplicarán los correspondientes derechos de los interesados.

---

[28] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, enviado al CEPD el 13 de noviembre de 2018, considerando 35.

[29] Artículo 22 de la Ley modificada sobre la protección de la información personal (APPI), que entró en vigor el 30 de mayo de 2017.

[30] Artículo 23, apartado 5, inciso i), de la APPI. Véase también la sección sobre el principio de transparencia que figura más adelante.

[31] Artículos 27-30 de la APPI.

[32] Modificación de la Orden Ministerial para aplicar la Ley sobre la protección de la información personal (Orden Ministerial), que entró en vigor el 30 de mayo de 2017, artículo 5.

75. El artículo 23 del RGPD establece que, al igual que el artículo 4 de la Orden Ministerial, la legislación de la Unión o de los Estados miembros a la que esté sujeto el responsable o el encargado del tratamiento puede restringir el alcance de las obligaciones que le son aplicables y los derechos de que dispone el interesado. Esto puede hacerse mediante una medida legislativa. Estas restricciones deben respetar la esencia de los derechos y las libertades fundamentales y son una medida necesaria y proporcionada en una sociedad democrática.

76. En cuanto al fondo de las excepciones previstas en el artículo 4 de la Orden Ministerial, el CEPD no dispone de documentación suficiente sobre estas limitaciones o elementos adicionales para aclarar el alcance de estas disposiciones[33]. El CEPD no está en condiciones de evaluar si estas limitaciones a los derechos de los interesados se limitan a lo que se consideraría estrictamente necesario y proporcionado en virtud de la legislación de la UE y, por tanto, si serían esencialmente equivalentes a los derechos facilitados a los interesados de la UE.

77. **Debido a la falta de algunos documentos pertinentes, el CEPD también acogerá con satisfacción garantías de la Comisión Europea si las restricciones a los derechos de las personas (en particular, los derechos de acceso, rectificación y oposición) son necesarias y proporcionadas en una sociedad democrática y respetan la esencia de los derechos fundamentales.**

78. Un requisito esencial de conformidad con el RGPD es que los datos personales estén protegidos durante todo su «ciclo de vida».

79. Teniendo en cuenta el hecho de que las normas suplementarias solo se aplican a los datos personales transferidos desde la UE, el CEPD desearía recibir más información sobre la aplicación práctica de estas normas por parte de los PIHBO, especialmente cuando estos datos se comunican posteriormente a otro PIHBO después de su primera transmisión a Japón.

80. La Comisión Europea ha aclarado en el considerando 15 de su proyecto de decisión de adecuación que los PIHBO que reciban o traten datos personales de la UE tendrán la obligación legal de cumplir las normas suplementarias y que, para ello, deberán garantizar que pueden identificar tales datos personales a lo largo de su «ciclo de vida».

81. En sus respuestas, la PPC[34] ha explicado que esta identificación se realizará utilizando métodos técnicos (marcado) o métodos de organización (almacenar los datos procedentes de la UE en una base de datos específica).

82. En la nota a pie de página 14 de su proyecto de decisión de adecuación, la Comisión Europea explica que los PIHBO deben registrar la información sobre el origen de los datos de la UE durante el tiempo que sea necesario para poder ajustarse a las normas suplementarias. Esto también está consagrado en el artículo 26, apartados 1, 3 y 4 de la APPI, que establece que un PIHBO tiene la obligación de confirmar y registrar la fuente de estos datos y todas las circunstancias que rodean a la adquisición de los mismos.

83. Sin embargo, el CEPD señala que el artículo 18 de las normas de la PPC[35] especifica que las obligaciones de conservación de registros de los PIHBO están limitadas a un máximo de tres años para los casos que no están incluidos en los métodos específicos de conservación de registros descritos en el artículo 16

[33] El CEPD no ha recibido las decisiones del Tribunal Supremo mencionadas en el considerando 53 del proyecto de decisión de adecuación.
[34] Anexo III del presente dictamen.
[35] Normas de aplicación de la Ley sobre la protección de la información personal (normas de la PPC), entradas en vigor el 30 de mayo de 2017, artículo 16.

de dichas normas de la PPC (mediante un documento escrito, un registro electromagnético o un microfilm). Esto también lo declara la Comisión Europea en el considerando 71 de su proyecto de decisión de adecuación: «*Como se especifica en el artículo 18 de las normas de la PPC, estos registros deben conservarse durante un periodo de uno a tres años, en función de las circunstancias*».

84. Aunque, como indica la Comisión Europea en la nota a pie de página 14 de su proyecto de decisión de adecuación, los PIHBO no tienen prohibido mantener registros sobre el origen de los datos durante más de tres años, con el fin de poder cumplir con sus obligaciones en virtud de la norma suplementaria (2), esto no se refleja claramente en la legislación japonesa ni en las normas suplementarias. El CEPD considera que existe el riesgo de que los PIHBO cumplan, de hecho, el artículo 18 de las normas de la PPC, aun cuando traten datos procedentes de la UE. Esto se debe principalmente a que actualmente, según entiende el CEPD y sobre la base de los documentos disponibles, no hay ninguna disposición que ponga a los PIHBO bajo dicha obligación de cumplimiento de las normas suplementarias. Esto daría lugar a que los datos transferidos desde la UE dejaran de estar protegidos por las salvaguardias adicionales incluidas en las normas suplementarias.

85. **El CEPD pide a la Comisión Europea que supervise de cerca la protección efectiva de los datos personales transferidos desde la UE a Japón sobre la base del proyecto de decisión de adecuación a lo largo de todo su ciclo de vida, a pesar de que la legislación japonesa imponga una obligación de mantener registros sobre el origen de los datos durante un máximo de tres años.**

3.1.2 Motivos para el tratamiento lícito y leal con fines legítimos

86. De acuerdo con las referencias sobre adecuación, en consonancia con el RGPD, los datos deben tratarse de manera lícita, leal y legítima.[36] La base jurídica en virtud de la cual los datos personales pueden tratarse legal, leal y legítimamente debe establecerse de manera suficientemente clara. El marco europeo reconoce varios de estos motivos legítimos, incluidas, por ejemplo, las disposiciones de la legislación nacional, el consentimiento del interesado, la ejecución de un contrato o que el interés legítimo del responsable del tratamiento o de un tercero no prevalezca sobre los intereses de la persona.

87. En virtud de la APPI, el consentimiento desempeña un papel central en el sistema jurídico de protección de datos de Japón. El consentimiento es la base jurídica central para el tratamiento de datos personales en Japón, así como una de las principales bases jurídicas para las transferencias de datos personales de Japón a un tercer país. Además, se requiere el consentimiento para una modificación de la finalidad del tratamiento.

88. De conformidad con la norma suplementaria (3), la base jurídica para el tratamiento de los datos personales transferidos desde la UE a Japón será la base jurídica sobre la que los datos se transfieren a Japón. Si el PIHBO desea tratar posteriormente estos datos para una finalidad distinta, deberá obtener previamente el consentimiento del interesado.

89. El CEPD considera que la calidad del consentimiento, especialmente debido a su papel central en el marco jurídico japonés, debe cumplir los requisitos fundamentales del concepto de consentimiento, es decir, con arreglo a la legislación de la UE, una «*manifestación de voluntad libre, específica, informada e inequívoca* [del] *interesado...*». El interesado puede retirar dicho consentimiento como una salvaguardia esencial para garantizar su libre voluntad a lo largo del tiempo[37]. El derecho de retirar el consentimiento, como elemento obligatorio del mismo, parece faltar en el marco jurídico japonés.

[36] WP 254, p. 4.

[37] RGPD, artículo 4, apartado 11. Para más información, véanse también las directrices pertinentes del CEPD sobre el consentimiento, WP 259, de 10 de abril de 2018.

De hecho, según las directrices de la PPC[38], la retirada del consentimiento es simplemente «deseable» y está supeditada a las «características, el tamaño y la situación de las actividades empresariales».

3.1.3 El principio de transparencia

90. Sobre la base del artículo 5 del RGPD, la transparencia es un principio fundamental del sistema de protección de datos de la UE[39]. Las referencias sobre adecuación designan explícitamente la «transparencia» como uno de los principios relativos al contenido que debe tenerse en cuenta al evaluar el nivel de protección esencialmente equivalente proporcionado por un tercer país. El principio de transparencia y lealtad estriba en garantizar que el interesado tiene el control sobre sus datos y, con este fin, como norma se le facilitará información de manera proactiva. En el caso del Escudo de la privacidad, el Grupo de Trabajo del Artículo 29[40], en su dictamen 1/2016, hizo referencia al apartado II 1 b del anexo II del acuerdo sobre el Escudo de la privacidad (notificación al interesado) y declaró que, si los datos no se recogen directamente, una organización debe notificar al interesado «en el momento en que los datos sean registrados por la entidad afiliada» (apartado 2.2.1.a). El hecho de que la política de privacidad esté públicamente disponible es un criterio adicional (véase el apartado 2.2.1.b). Por lo tanto, ya en virtud de la Directiva 95/46/CE, se consideró necesario informar directamente al interesado.

91. Se plantea una primera preocupación en relación con la modalidad de información facilitada al interesado en el marco de la APPI. De conformidad con el artículo 27, apartado 1, de la APPI, un PIHBO está obligado a facilitar la información descrita en el artículo 27, apartado 1, de la APPI exponiéndola «en un estado en el que un titular pueda conocer». Sin embargo, esta formulación no aclara en qué medida el PIHBO debe tomar medidas positivas para informar realmente al interesado.

92. **El CEPD invita a la Comisión a aclarar el significado de la expresión «pueda conocer» y si la APPI establece como norma la obligación de informar realmente a los interesados.**

93. Por otra parte, de acuerdo con las referencias sobre adecuación, pueden existir restricciones a la información que debe facilitarse al interesado, similares a las del artículo 23 del RGPD. En el mismo sentido, el artículo 14, apartado 5, del RGPD establece una excepción al derecho a ser informado cuando la información pueda imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento. Sin embargo, incluso en este caso, el responsable del tratamiento facilitará algún tipo de información, por ejemplo haciendo pública la información «generalizada». Además, cuando el riesgo deje de existir, se notificará al interesado[41]. Estos aspectos son importantes para garantizar el principio fundamental de la lealtad.

---

[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC): *An assessment of the level of protection of personal data provided under Japanese law*, p. 46: «Además, desde el punto de vista de la protección de los derechos e intereses de un titular, como los consumidores, es deseable, en caso de recibir una petición de un titular relativa a los datos personales conservados, responder mejor a la petición del titular de tal manera que se ponga fin a las actividades, etc., de correo directo o se ejecute voluntariamente un cese de uso, etc., teniendo en cuenta las características, el tamaño y la situación de las actividades empresariales».

[39] WP 254, capítulo 3, apartado 7, p. 5; véase también el considerando 39 del RGPD.

[40] 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. Sus tareas se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE. El Grupo de Trabajo del Artículo 29 se ha convertido ahora en el CEPD.

[41] Tele2, asuntos acumulados C-203/15 y C-698/15, sentencia del Tribunal de Justicia (Gran Sala) de 21 de diciembre de 2016, rec. 121 y Digital Rights Ireland, asuntos acumulados C-293/12 y C-594/12, Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, rec. 54-62.

94. De conformidad con el artículo 23 de la APPI, un PIHBO ha de ofrecer, en general, información previa al interesado sobre la transmisión de sus datos a un tercero, ya sea implícitamente en el momento de obtener su consentimiento o explícitamente mediante una notificación de exclusión voluntaria. El CEPD entiende que no hay ninguna notificación al interesado que le informe del hecho de que sus datos no son datos personales conservados en el marco de APPI porque entran en las excepciones del artículo 4 de la Orden Ministerial. En consecuencia, no podrán beneficiarse plenamente de sus derechos. Los interesados no están informados tampoco en los casos del artículo 18, apartado 4, de la APPI.

95. **El CEPD reconoce que los derechos pueden verse limitados por objetivos legítimos perseguidos por el PIHBO y las autoridades estatales. Al mismo tiempo, el CEPD considera que debe existir al menos una información general inicial sobre la posibilidad de restringir los derechos para los objetivos a que se refiere la ley y que debe notificarse al interesado cuando dejen de existir los riesgos por los que se restringe la información.**

96. Por último, a continuación se exponen con mayor detalle otros aspectos de la transparencia. Estos se refieren a los riesgos que entraña la transferencia a un tercer país[42] y a la información sobre la lógica del tratamiento en el contexto de la toma de decisiones automatizada, incluida la elaboración de perfiles.[43]

3.1.4 Restricciones de las transferencias ulteriores

97. El CEPD acoge con satisfacción los esfuerzos realizados por las autoridades japonesas y la Comisión Europea para mejorar el nivel de protección de las transferencias ulteriores en la norma suplementaria (4), que excluye que los datos personales transferidos desde la UE se transfieran posteriormente a un tercer país sobre la base las normas transfronterizas de privacidad del APEC. Además, el CEPD reconoce que en los considerandos 177 y 184 de su nuevo proyecto de decisión de adecuación, la Comisión Europea se comprometió a suspender la decisión de adecuación cuando las transferencias ulteriores ya no garanticen la continuidad de la protección. Sin embargo, el CEPD desea plantear dos cuestiones relativas a estas transferencias de datos personales de la UE desde Japón a terceros países.

98. **El uso del consentimiento como base para las transferencias de datos desde Japón a un tercer país en el ordenamiento jurídico japonés suscita preocupación, ya que el CEPD considera que la información facilitada al interesado de la UE antes de dar su consentimiento no parece exhaustiva.**

99. El artículo 24 de la APPI prohíbe la transferencia de datos personales a terceros fuera del territorio de Japón sin el consentimiento previo de la persona afectada. La norma suplementaria (4) dispone que los interesados de la UE deben recibir la información sobre las circunstancias relacionadas con la transferencia necesaria para tomar una decisión sobre su consentimiento.

100. La Comisión Europea concluye en su proyecto de decisión de adecuación que la norma suplementaria (4) garantiza un consentimiento bien informado concreto del interesado de la UE[44], ya que se le informará de que los datos se transferirán al extranjero y del país de destino específico. Esto permitiría al interesado evaluar el riesgo para la privacidad que acarrea la transferencia.

101. En virtud del principio de transparencia de las referencias sobre adecuación, deberá garantizarse un cierto grado de lealtad a la hora de informar a las personas. En el contexto de las transferencias

[42] Véase el apartado 2.1.4.
[43] Véase el apartado 2.1.6.
[44] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, remitido al CEPD el 13 de noviembre, considerando 76.

ulteriores basadas en el consentimiento, el CEPD opina que, para garantizar dicho grado adecuado de lealtad, 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 garantías apropiadas. Dicha notificación debería incluir, por ejemplo, la información de que en el tercer país podría no haber una autoridad de supervisión o que los principios de tratamiento de datos o los derechos de los interesados podrían no estar previstos en el tercer país[45]. Por lo que se refiere al CEPD, el suministro de esta información es esencial para permitir que el interesado preste su consentimiento con pleno conocimiento de estos hechos concretos de la transferencia[46].

102. El consentimiento informado también es importante en relación con las exclusiones sectoriales. La decisión de adecuación no abarca ciertos tipos de tratamiento por parte de determinados organismos, como las universidades para el tratamiento de datos personales con finalidades académicas. La preocupación del CEPD en este caso se refiere al supuesto específico de cuando los datos transferidos desde la UE en virtud de la decisión de adecuación —por ejemplo, los datos concernientes a los recursos humanos de los estudiantes Erasmus en Japón— se utilizan luego para un propósito diferente que no entra en el ámbito de la decisión de adecuación (por ejemplo, finalidades de investigación) con el consentimiento del interesado, y, por lo tanto, ya no están cubiertos por la protección adicional prevista por las normas suplementarias.

103. La Comisión Europea afirma en el considerando 38 de su proyecto de decisión de adecuación que tal escenario entrará en el contexto de las transferencias ulteriores y que, en estos casos, el PIHBO debe facilitar al interesado toda la información necesaria antes de obtener su consentimiento, incluido el hecho de que la información personal no entraría en el ámbito de la protección de las normas de la APPI.

104. La norma suplementaria (4) solo exige que el PIHBO obtenga el consentimiento del interesado después de haber recibido la información sobre las circunstancias que rodean la transferencia necesaria para que el titular tome una decisión sobre su consentimiento.

105. **El CEPD invita a la Comisión Europea a garantizar que la información que debe facilitarse al interesado «sobre las circunstancias que rodean la transferencia» debe incluir la información sobre los posibles riesgos de las transferencias derivados de la falta de una protección adecuada en el tercer país y la ausencia de salvaguardias adecuadas, o en el caso de las exclusiones sectoriales, de la falta de protección de las normas suplementarias y de la APPI.**

106. **Las transferencias ulteriores de datos personales pueden tener lugar a terceros países, que pasan a estar sujetos a una posible decisión de adecuación japonesa posterior.**

107. Sin perjuicio de las excepciones establecidas en el apartado 1 del artículo 23 de la APPI, los datos transferidos inicialmente desde la UE a Japón podrán transferirse posteriormente de Japón a un tercer país sin consentimiento en dos supuestos:

- Si el PIHBO y el tercero receptor han aplicado conjuntamente medidas que proporcionan un nivel de protección equivalente al de la APPI, leída en relación con las normas suplementarias

[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.

mediante un contrato, otras formas de acuerdos vinculantes o acuerdos vinculantes dentro de un grupo de empresas[47].

- Si la PPC, de conformidad con el artículo 24 de la APPI y el artículo 11 de las normas de la PPC[48], ha reconocido que el tercer país ofrece un nivel de protección equivalente al garantizado en Japón.

108. El CEPD valora el artículo 24 de la APPI como la norma más específica, que contiene una excepción a la norma general contemplada en el artículo 23 de la APPI. Por lo tanto, el CEPD no comparte la valoración de la Comisión Europea en la nueva última frase del considerando 78 del proyecto de decisión de adecuación, que establece que, incluso en esos casos, la transferencia al tercero sigue estando sujeta al requisito de obtener el consentimiento de conformidad con el artículo 23, apartado 1, de la APPI.

109. De conformidad con el artículo 11, apartado 1, de las normas de la PPC, una decisión de adecuación por parte de la PPC exige unas normas materiales equivalentes a la APPI cuya aplicación esté garantizada en el tercer país y que sean supervisadas eficazmente por una autoridad de ejecución independiente. Además, la PPC puede imponer las condiciones necesarias para proteger los derechos e intereses de las personas en Japón, de conformidad con el artículo 11, apartado 2, de las normas de la PPC.

110. La norma suplementaria (4) establece que los datos personales de la UE pueden transferirse a un tercer país con arreglo a una decisión de adecuación japonesa sin más restricciones. Sin embargo, el artículo 44 del RGPD regula que toda transferencia de datos personales a un tercer país debe cumplir las condiciones establecidas en el capítulo V del RGPD, incluidas las transferencias ulteriores desde el tercer país a otro tercer país. El nivel de protección de las personas físicas cuyos datos se transfieren no debe verse socavado por la transferencia [49]. Aunque, en principio, esta interpretación también es compartida por la Comisión Europea en su proyecto de decisión de adecuación[50], no parece que se siga por completo. La Comisión Europea ha negociado la prohibición de transferir datos procedentes de la UE a un tercer país sobre la base del sistema de normas transfronterizas de protección de la privacidad aplicable a la cooperación económica Asia-Pacífico (APEC CBPR). A la luz de la herramienta comparativa desarrollada en 2014 en el marco de la Directiva de la UE entre las normas corporativas vinculantes (binding corporate rules, BCR) y las normas CBPR, en la que se muestran los requisitos de ambos sistemas, sus convergencias y diferencias (dictamen 02/2014 del Grupo de Trabajo del Artículo 29), el CEPD tiene dudas sobre el uso de las CBPR como instrumento de transferencia ulterior para los datos personales transferidos desde la UE a países fuera de Japón.

111. En cambio, las transferencias ulteriores de datos personales transferidos desde la UE a Japón sobre la base de una decisión de adecuación japonesa parecen ser aceptadas por la Comisión Europea, sin posibilidad de que la PPC imponga las normas suplementarias como condiciones para proteger los derechos e intereses de los ciudadanos de la UE, en caso necesario. El CEPD deduce del artículo 44 del RGPD que la mayor protección de los datos transferidos desde la UE a Japón prevista en las normas

[47] Norma suplementaria (4), apartado (ii).
[48] Normas de aplicación de la Ley sobre la protección de la información personal, de 30 de mayo de 2017. La traducción al inglés del nuevo artículo 11 fue comunicada por la Comisión Europea al CEPD, pero este artículo aún no se ha publicado.
[49] WP 254, p. 5.
[50] Decisión de Ejecución de la Comisión, de XXXX, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por parte de Japón, remitido al CEPD el 13 de noviembre, considerando 75.

suplementarias siempre debe ampliarse cuando los datos personales transferidos desde la UE a Japón se transfieren posteriormente a un tercer país, si el marco de protección de datos en ese país no se reconoce como esencialmente equivalente al RGPD.

112. **Por lo tanto, el CEPD invita a la Comisión Europea a asumir su función de supervisión y a garantizar el mantenimiento del nivel de protección de los datos de la UE o a considerar la suspensión de esta decisión de adecuación si los datos personales transferidos desde la UE a Japón se transfieren más adelante a terceros países sujetos a una posible decisión de adecuación de Japón posterior, cuando estos terceros países no hayan sido objeto de una evaluación anterior o una constatación de la adecuación de la UE.**

3.1.5 Mercadotecnia directa

113. De conformidad con la norma suplementaria (3), se prohíbe a un PIHBO tratar los datos con la finalidad de mercadotecnia directa si han sido transferidos desde la Unión Europea con otro fin y el interesado de la UE no ha prestado su consentimiento para dicho cambio de finalidad.

114. De acuerdo con las referencias sobre adecuación, cuando los datos se tratan con fines de mercadotecnia directa, el interesado debe poder oponerse gratuitamente a que sus datos se traten con tales finalidades en cualquier momento. De conformidad con el artículo 16 de la APPI, solo se permite al PIHBO el tratamiento de información personal si el interesado da su consentimiento. La retirada del consentimiento podría proporcionar el mismo resultado que el derecho privilegiado a oponerse a la mercadotecnia directa.

115. El marco de protección de datos de Japón no ofrece un derecho de oposición privilegiado y, como se ha explicado anteriormente en el apartado sobre consentimiento, la retirada del consentimiento con arreglo a las directrices de la PPC es simplemente deseable y condicional y, por tanto, no puede considerarse que equivale a un derecho de oposición en cualquier momento, tal y como se requiere en las referencias sobre adecuación. **El CEPD invita a la Comisión Europea a ofrecer garantías sobre el derecho a retirar el consentimiento y supervisar los casos de mercadotecnia directa.**

3.1.6 Toma de decisiones automatizada y elaboración de perfiles

116. Según las referencias sobre adecuación, las decisiones basadas únicamente en el tratamiento automatizado (toma de decisiones individual automatizada), incluida la elaboración de perfiles, que producen efectos jurídicos o afectan significativamente al interesado, solo pueden tener lugar en determinadas condiciones establecidas en el marco jurídico del tercer país. Por lo tanto, cada vez que se realice una toma de decisiones automatizada y una elaboración de perfiles en las circunstancias mencionadas, debe existir un fundamento jurídico para ello.

117. En el marco europeo, las condiciones para la toma de decisiones automatizada incluyen, por ejemplo, la necesidad de obtener el consentimiento expreso[51] del interesado o la necesidad de dicha decisión para la celebración de un contrato. Si la decisión no se ajusta a las condiciones establecidas en el marco jurídico del tercer país, el interesado debe tener derecho a no ser sometido a ella. Además, en cualquier caso, la legislación del tercer país debe prever las salvaguardias necesarias, incluido el derecho a ser informado sobre los motivos específicos subyacentes a la decisión y la lógica aplicada para corregir la información inexacta o incompleta y para impugnar la decisión cuando se haya adoptado sobre una base fáctica incorrecta.

[51] Para las observaciones críticas al concepto de consentimiento en el marco jurídico de protección de datos japonés, véase: 2.1. Aspectos generales y 2.2.8. Mercadotecnia directa.

118. La Decisión de la Comisión solo se refiere al sector bancario, en el que se aplicarían las normas sectoriales[52] relativas a las decisiones automatizadas. Las directrices generales para la supervisión de los principales bancos mencionadas en el considerando 93 del proyecto de decisión de adecuación indican que deben facilitarse a la persona afectada explicaciones específicas sobre los motivos por los que se ha rechazado una solicitud para estipular un contrato de préstamo.

119. Las argumentaciones de la Comisión Europea relativas al proyecto de decisión de adecuación (considerando 94), sobre que es improbable que la ausencia de normas específicas sobre la toma de decisiones automatizada en el marco de la APPI afecte al nivel de protección parecen (por ejemplo) no tener en cuenta el caso en el que otro responsable del tratamiento japonés (distinto del importador de datos japonés original) trate los datos personales transferidos por la UE.

120. Por lo tanto, parece que no existen normas generales aplicables a todos los sectores de Japón que regulan la toma de decisiones automatizadas y la elaboración de perfiles.

121. **El CEPD invita a la Comisión Europea a supervisar los casos relacionados con la toma de decisiones automatizadas y la elaboración de perfiles.**

3.2 Mecanismos de procedimiento y ejecución

122. Sobre la base de los criterios establecidos en las referencia sobre adecuación, el CEPD ha analizado los siguientes aspectos de la protección de datos y el marco jurídico japoneses cubiertos por el proyecto de decisión de adecuación: la existencia y el funcionamiento efectivo de una autoridad de supervisión 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 de la UE de los medios para ejercer sus derechos y solicitar reparación sin encontrar obstáculos engorrosos para los recursos administrativos y judiciales.

123. Sobre la base de los parámetros establecidos por el TJUE en el asunto Schrems[53] y los descritos en el considerando 104 y en el artículo 45 del RGPD, el CEPD considera que, aunque existe en Japón un sistema coherente con el europeo, este puede ser de difícil acceso en la práctica a los ciudadanos de la UE cuyos datos se transferirán en virtud de esta decisión de adecuación, a la luz de la existencia de barreras lingüísticas e institucionales.

124. Los apartados que figuran a continuación examinarán los aspectos anteriormente mencionados del marco japonés antes de poner de relieve algunas recomendaciones para la Comisión.

3.2.1 Autoridad de supervisión independiente competente

125. La PPC se creó el 1 de enero de 2016 tras las enmiendas de la APPI de 2015, en sustitución de su antecesora, la Comisión específica para la protección de la información personal (creada en 2013 en el marco de la «*My Number Act*»). Aunque es una organización joven, desde su creación, la PPC ha realizado esfuerzos considerables para construir la infraestructura necesaria para dar cabida a la aplicación de la APPI modificada. Entre ellos se destacan el establecimiento de las normas de la PPC, las directrices de la PPC para orientar a los PIHBO en la interpretación de la APPI, la publicación de un documento de preguntas y respuestas de la PPC[54] y la creación de un servicio de asistencia telefónica

[52] Estas normas sectoriales no se proporcionaron al CEPD.

[53] Asunto C-362/14 (2015), Maximillian Schrems/Data Protection Commissioner (apartados 73 y 74).

[54] La Comisión Europea no ha facilitado este documento al CEPD en inglés.

para asesorar a los operadores comerciales y a los ciudadanos sobre las disposiciones en materia de protección de datos, así como de un servicio de mediación para tramitar las reclamaciones.

126. El establecimiento y el funcionamiento de la PPC se regulan en el capítulo V de la APPI. Aunque la PPC entra dentro de la jurisdicción del Primer Ministro, el artículo 62 establece que la PPC ejerce su función de forma independiente. El CEPD saluda la aclaración realizada por la Comisión Europea en el proyecto modificado de la decisión de adecuación distribuido el 13 de noviembre de 2018 para describir en mayor medida el grado en que la PPC está libre de influencias internas y externas.

3.2.2 El sistema de protección de datos debe garantizar un buen nivel de cumplimiento

127. El proyecto de decisión de adecuación lleva a cabo un examen exhaustivo de los poderes de los que la PPC está dotada de conformidad con los artículos 40, 41 y 42 de la APPI para garantizar la supervisión y la aplicación de la legislación. El artículo 40 faculta a la PPC para solicitar a los PIHBO la presentación de informes y documentación relativa a las operaciones de tratamiento, así como la realización de inspecciones *in situ*. Con arreglo al artículo 42, la PPC tiene la facultad —cuando reconozca que es necesario para proteger derechos individuales o cuando constate la violación de las disposiciones de la ley— de emitir recomendaciones y, en su defecto, órdenes a los PIHBO para que cesen el acto de incumplimiento o adopten las medidas necesarias para subsanar la infracción.

128. En octubre de 2018, la PPC adoptó una de sus primeras acciones en virtud del artículo 41 de la APPI modificada y emitió una «orientación» a un PIHBO, aconsejando a la empresa que reforzara sus medidas de seguridad y supervisara de forma eficaz a los proveedores de aplicaciones, ofreciendo al mismo tiempo claras y fáciles explicaciones a los usuarios sobre cómo se utiliza su información personal, y que obtuviera el consentimiento previo cuando la información se fuera a compartir con un tercero, así como que respondiera adecuadamente a las solicitudes de los usuarios de supresión de su información. En las respuestas facilitadas al CEPD[55], los funcionarios de la PPC comunicaron que la empresa ha anunciado que cooperará y que, si no lo hace, le emitirá una «recomendación» de conformidad con el artículo 42, apartado 1, de la APPI.

129. La investigación realizada por la PPC sobre el mencionado PIHBO es un indicador muy positivo de los esfuerzos de la autoridad de supervisión japonesa para garantizar un buen nivel de cumplimiento en el país.

130. Aunque se han producido mejoras en relación con el marco existente antes de las enmiendas de 2015, el CEPD observa que la PPC tiene menos competencias que las autoridades europeas de protección de datos en virtud del RGPD, especialmente en lo que se refiere a la **ejecución**. Las multas administrativas[56], por ejemplo, son bastante leves. En el considerando 108 de la decisión de la Comisión Europea se hace hincapié en que, en los casos de incumplimiento o algunas infracciones de la APPI, existen sanciones penales y que el presidente de la PPC puede remitir los casos a la fiscalía. Sin embargo, la decisión de la Comisión Europea no tiene en cuenta el hecho de que la acusación pública en Japón es discrecional y a veces puede ser objeto de largos procesos de revisión[57]. Además, la pena de prisión (con o sin trabajos) asociada a las infracciones de la APPI con arreglo a las disposiciones del

[55] Anexo III.

[56] Estas figuran en el capítulo VII de la APPI. La pena máxima es la prevista en el art. 83 (provisión o utilización furtivas de una base de datos de información personal con ánimo de lucro ilegal propio o de un tercero) y equivale a una pena de prisión de un año con trabajos o a una multa que no exceda de 500 000 yenes (unos 3 900 EUR). Según las explicaciones facilitadas por la Comisión, las multas son acumulativas por infracción. Aunque este puede ser el caso, el CEPD observa que, aunque se apliquen sanciones acumulativas, es probable que el importe total siga siendo considerablemente bajo en comparación con las normas europeas.

[65] Oda H.: *Japanese Law*, Oxford University Press (III edición), 2009, pp. 439 y 440.

capítulo VII puede ser difícil de ejecutar debido a que se dirige a personas físicas y, en cualquier caso, no castigan al PIHBO como persona jurídica que ha incumplido sus obligaciones de rendición de cuentas.

131. **En vista de lo anterior, el CEPD invita a la Comisión Europea a supervisar estrechamente la eficacia de las sanciones y las soluciones pertinentes en el sistema de protección de datos de Japón.**

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

132. La PPC proporciona una amplia información y orientaciones en su sitio web para sensibilizar a los PIHBO en relación con sus obligaciones y responsabilidades con arreglo al marco de protección de datos, así como un servicio de asistencia telefónica para proporcionar información y apoyo a los ciudadanos japoneses en relación con sus derechos individuales en virtud de la APPI. El sitio web tiene también una sección denominada el «Cuarto de los niños», dirigida explícitamente a un público infantil y joven. El CEPD observa que esta información, junto con el servicio de asistencia telefónica, la orientación y la documentación sobre preguntas y respuestas, está disponible en japonés[58]. Por lo tanto, el CEPD cree firmemente que sería beneficioso que la PPC pudiera proporcionar una página específica sobre la versión inglesa de su sitio web con el fin de ofrecer información sobre sus derechos individuales en virtud del marco de protección de datos japonés y de las normas suplementarias a los ciudadanos de la UE cuyos datos se transferirán a Japón en el marco de la decisión de adecuación de la Comisión Europea.

133. El CEPD acoge con satisfacción la aclaración realizada por la Comisión Europea en el considerando 104 del proyecto modificado de decisión de adecuación distribuido el 13 de noviembre de 2018 en relación con el servicio de mediación gestionado por la PPC de conformidad con el artículo 61, inciso ii), de la APPI. Sin embargo, el CEPD desea plantear tres cuestiones en este sentido. En primer lugar, el servicio de mediación no está publicado en la versión inglesa del sitio web de la PPC. En segundo lugar, el servicio solo es accesible por teléfono y únicamente está disponible en japonés. Por último, la mediación es simplemente un proceso facilitador que no da lugar a un acuerdo vinculante entre las partes que tenga implicaciones para la eficacia de las opciones de recurso de que disponen los interesados[59].

134. Por último, el CEPD señala que el proyecto de decisión de adecuación hace hincapié en los recursos disponibles en Derecho civil, así como en los procesos penales, pero no reconoce la existencia de **obstáculos institucionales a los litigios** en Japón, como los costes jurídicos (las costas judiciales se dividen a partes iguales entre el demandante y el demandado, independientemente de cuál sea la parte que gana el procedimiento[60]), la escasez de abogados en el país[61], el hecho de que los abogados extranjeros no están autorizados a ejercer conforme al Derecho nacional y el requisito de la carga de la prueba en virtud del derecho de responsabilidad civil. El CEPD teme que estos factores puedan, en

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima, T.: *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; y Menkel-Meadow, C.: *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).

[60] Wagatsuma (2012): «Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure», en Reimann (ed.), «Cost and Fee Allocation in Civil Procedure – Ius Gentium»; *Comparative Perspectives on Law and Justice*, vol. 11, pp. 195-200.

[61] Según las últimas cifras, el número de abogados en Japón es de 38 980 (aproximadamente 290 abogados por cada millón de personas [Federación de Colegios de Abogados de Japón] (2017), *White Paper on Attorneys*: pp. 8-9.

la práctica, obstaculizar el acceso de las personas a la justicia y poner en peligro su derecho a emprender vías de recurso de forma rápida y sin tener que soportar costes prohibitivos.

135. A la luz de lo anterior, **el CEPD manifiesta su preocupación por el riesgo de que los ciudadanos de la UE tengan dificultades para acceder a recursos administrativos y judiciales** y, por tanto, acogería con satisfacción que la Comisión Europea pudiera debatir con la PPC la posibilidad de crear un servicio en línea, al menos en inglés, **destinado a prestar apoyo y gestionar las reclamaciones de los ciudadanos de la UE**[62]. Además, el CEPD agradecería la posibilidad de permitir que las autoridades de protección de datos (data protection authorities, DPA) de la UE actuaran como intermediarios en las reclamaciones de interesados de la UE a las organizaciones que operan en Japón y la PPC.

4 SOBRE EL ACCESO DE LAS AUTORIDADES PÚBLICAS A LOS DATOS TRANSFERIDOS A JAPÓN

136. La intención de la Comisión es reconocer, a través de la decisión de adecuación, que «Japón garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a los operadores comerciales de manipulación de información personal en Japón», tal como se establece en el artículo 1 del proyecto de decisión de adecuación. De conformidad con el artículo 45, apartado 2, del RGPD, la Comisión ha analizado también las limitaciones y salvaguardias en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. El presente capítulo se centra en la evaluación del acceso a los datos personales por parte de las autoridades policiales y de otras entidades públicas a efectos de la seguridad nacional. El análisis del CEPD se basa en el proyecto de decisión de adecuación, en su anexo II, en el que el Gobierno japonés proporciona una visión general del marco jurídico pertinente, y en los textos jurídicos japoneses, en la medida en que fueron facilitados por la Comisión. Por lo tanto, en el contexto específico de esta evaluación, el CEPD ha tenido en cuenta los elementos relativos a la legislación japonesa que no forman parte de las conclusiones de la Comisión Europea, pero que son pertinentes para evaluar las condiciones y las salvaguardias en virtud de las cuales las autoridades públicas japonesas pueden acceder a los datos personales transferidos desde la Unión Europea.

4.1 Acceso de los cuerpos policiales a los datos

4.1.1 Procedimientos de acceso a los datos en el ámbito del Derecho penal

137. El proyecto de decisión de adecuación presenta tres formas previstas de conformidad con la legislación japonesa para que las autoridades policiales puedan acceder a los datos en Japón:

4.1.1.1 Solicitudes de acceso con una orden judicial

138. El proyecto de decisión de adecuación establece que, para el acceso del Gobierno de Japón, y especialmente para que las autoridades policiales soliciten acceso a pruebas electrónicas en el contexto de las investigaciones penales, deberán contar siempre con una orden judicial, a menos que utilicen el procedimiento de divulgación voluntaria (véase más adelante).

4.1.1.1.1 Requisito de «causa suficiente», necesidad y proporcionalidad de las órdenes judiciales

139. El CEPD reconoce que, en virtud de la Constitución japonesa, toda recogida de datos personales por medios coercitivos debe basarse en una orden judicial. Más concretamente, el proyecto de decisión de adecuación indica que, en todos los casos de «registros e incautaciones», debe emitirse una orden judicial por una «causa suficiente», que el Tribunal Supremo solo considera que existe cuando se

[62] Similar al previsto en el anexo II de esta decisión de adecuación para las reclamaciones de los residentes de la UE relativas al acceso a sus datos por parte de las autoridades públicas japonesas.

considera que el interesado (sospechoso o acusado) ha cometido un delito y que el registro y la incautación son necesarios para la investigación penal. La Comisión remite a la sentencia del Tribunal Supremo de 18 de marzo de 1969 en el asunto n.º 100 (1968(Shi)). El CEPD recuerda que, en virtud de la jurisprudencia del TJUE[63], solo un tribunal, y no los fiscales, por ejemplo, pueden autorizar, en particular, la recogida de datos de tráfico y de localización.

140. También a la luz de la jurisprudencia del TJUE, según la cual el acceso a los datos puede estar sujeto a una orden judicial, como en Tele2, el CEPD lamenta que no se facilitara información adicional para evaluar la forma en que los criterios para valorar la necesidad de una orden judicial —la gravedad del delito y cómo se cometió; el valor y la importancia de los materiales incautados como elementos de prueba; el alcance de los perjuicios causados por una incautación; otras condiciones relacionadas— y el concepto de «causa suficiente» derivado de la Constitución se aplican en la práctica. Por consiguiente, el CEPD invita a la Comisión a vigilar si la emisión de órdenes judiciales cumple los criterios establecidos por el TJUE en la práctica.

4.1.1.1.2 Tipos de delitos para los que se pueden emitir órdenes judiciales

141. El procedimiento de la orden judicial solo se aplica cuando se lleva a cabo una «investigación obligatoria». En principio, estas órdenes solo pueden emitirse en los casos en que se haya producido una violación de la ley. A este respecto, el CEPD toma nota de la recientemente adoptada «Ley sobre la sanción de los delitos organizados y el control de los productos del delito» el 15 de junio de 2017 en el contexto de la adhesión de Japón a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (CNUDOT)[64]. A falta de una versión inglesa disponible de esta legislación, y teniendo en cuenta el requisito establecido por la legislación de la UE de que algunos datos se recojan únicamente en el contexto de la investigación, la detección o el enjuiciamiento de delitos graves[65], así como las preocupaciones expresadas por varios comentaristas, incluido el Relator Especial de las Naciones Unidas Joseph Cansataci[66], sobre el amplio ámbito de aplicación, y que se basan en una definición de «grupo delictivo organizado» supuestamente poco clara y demasiado amplia, el CEPD no está en condiciones de concluir que el acceso a las pruebas electrónicas en virtud de la legislación japonesa pertinente está limitado a los umbrales establecidos por la legislación de la UE.

142. También hay que señalar que para algunos tipos de delitos, la Policía de prefectura es competente y que tienen sus ordenanzas policiales específicas. Las normas internas aplicables a la Policía de prefectura no estuvieron a disposición del CEPD.

143. Según el proyecto de decisión de adecuación, la recogida de información electrónica en el ámbito de la aplicación del Derecho penal es responsabilidad de la Policía de prefectura.

4.1.1.2 Órdenes judiciales para escuchas telefónicas

144. El anexo II del proyecto de medidas de adecuación indica que la Ley sobre escuchas telefónicas para investigaciones penales dispone medidas específicas para la interceptación de las comunicaciones. Esta legislación se proporcionó muy tarde, lo que no permitió un análisis en profundidad. Por lo tanto, aunque en este marco jurídico parece haber muchas salvaguardias, el CEPD no está en posición de evaluar si las condiciones previstas en este acto legislativo están provistas de garantías

[63] Véanse los asuntos 203/15, C-293/12 y C-594/12 del TJUE.
[64] Véase: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[65] Véanse los asuntos acumulados C-293/12 y C-594/12 y el asunto C-203/15.
[66] Relator especial de las Naciones Unidas sobre el derecho a la privacidad, así como Graham Greenleaf, investigador de la facultad de Derecho de la Universidad de Nueva Gales del Sur.

sustancialmente equivalentes a las exigidas en la UE tanto por la Carta, de acuerdo con la interpretación del TJUE, como por el CEDH, según la interpretación del Tribunal de Estrasburgo.

4.1.1.3 El procedimiento de «divulgación voluntaria» basado en un boletín de investigación

145. Esta forma de cooperación no obligatoria permite a las autoridades públicas pedir a los responsables del tratamiento (excepto a los operadores de telecomunicaciones) que les proporcionen datos que obran en su poder. No puede exigirse el cumplimiento de la solicitud. Sigue sin estar claro qué autoridades pueden utilizar este tipo de procedimiento, pero parece que se limita a las que investigan delitos.

4.1.1.3.1 Condiciones para emitir «boletines de investigación»

146. El CEPD reconoce que el Tribunal Supremo japonés, en referencia a la Constitución, ha formulado limitaciones sobre el uso de la «divulgación voluntaria»[67]. Del proyecto de decisión de adecuación se desprende que, en concreto, las autoridades competentes solo pueden pedir una «divulgación voluntaria» mediante la emisión de un «boletín de investigación». El envío de tal «boletín de investigación» solo se admite como parte de una investigación penal y, por lo tanto, siempre supone una sospecha concreta de un delito ya cometido. Estas investigaciones suelen ser llevadas a cabo por la Policía de prefectura, donde se aplican las limitaciones del artículo 2, apartado 2, de la Ley sobre la Policía, lo que significa que debe ser pertinente para las actividades policiales. Sin embargo, el CEPD desea más aclaraciones en cuanto al relieve concreto de los criterios que permiten emitir un boletín de investigación (como la jurisprudencia que ilustra la aplicación de dichos criterios) y la relación entre el procedimiento de divulgación voluntaria y la incautación de datos sobre la base de una orden judicial. De hecho, parece que, incluso cuando los datos no pudieran obtenerse a través del procedimiento voluntario, podrían seguir obteniéndose con una orden judicial si resultan indispensables para las autoridades encargadas de la investigación[68].

4.1.1.3.2 Jurisprudencia disponible sobre las limitaciones del uso de la divulgación voluntaria

147. Los casos citados en el proyecto de decisión de adecuación[69] para ilustrar las limitaciones del uso de los procedimientos de divulgación voluntaria se refieren a casos en los que la persona acusada ha sido fotografiada o filmada en el espacio público por la Policía directamente y, por tanto, ofrecen indicaciones limitadas sobre las situaciones en las que las autoridades competentes pueden pedir a un responsable del tratamiento que divulgue datos, en particular con respecto a los criterios enumerados en el anexo II en relación con la «idoneidad de los métodos», que parece referirse a la evaluación de si la investigación voluntaria es «apropiada» o razonable para lograr el propósito de la investigación. Lo mismo puede decirse de los criterios generales de «si puede considerarse razonable de conformidad con las convenciones socialmente aceptadas» para evaluar la legalidad de las investigaciones voluntarias. Además, la Agencia Nacional de Policía (ANP), que es la autoridad federal encargada de todas las cuestiones relativas a la policía criminal, dio instrucciones a la Policía de prefectura sobre «la correcta utilización de las actuaciones escritas en materia de investigación». Entre otras cosas, el investigador jefe debe recibir la aprobación interna de un oficial de alto rango. El CEPD no dispone de ninguna información sobre si estas instrucciones son vinculantes. No obstante, el CEPD establece que la utilización de este procedimiento ha de ser proporcionada o necesaria.

[67] Véase la página 8 del anexo II.
[68] Véase la página 7 del anexo II.
[69] Véase la página 8 del anexo II: dos resoluciones del Tribunal Supremo de 24 de diciembre de 1969 (1965 (A) n.º 1187) y de 15 de abril de 2008 (2007 (A) n.º 839).

4.1.1.3.3 Derechos y obligaciones de los responsables del tratamiento en el contexto de la divulgación voluntaria

148. Además, corresponde a los responsables del tratamiento dar su consentimiento para facilitar datos (pero no parece haber obligación alguna sobre ellos de solicitar el consentimiento de los interesados o de informarles), cuando estas solicitudes no entren en conflicto con otras obligaciones legales (como las obligaciones de confidencialidad). El informe facilitado por la Comisión parece indicar que, tras un alto nivel de cumplimiento, los responsables del tratamiento han empezado a tener en cuenta la protección de datos de sus clientes y, así, han empezado a responder menos a estas solicitudes.

149. Tampoco queda claro si los responsables del tratamiento tienen algún incentivo para cumplir con las solicitudes (por ejemplo, si tienen una ventaja a la hora de cumplir con las mismas, o si están exentos de enjuiciamiento, etc.). En particular, no se menciona ningún principio como el «principio de no autoinculpación».

150. El CEPD desearía recibir información adicional, si se dispone de ella, sobre el número y el tipo de solicitudes, así como sobre las respuestas facilitadas por los responsables del tratamiento solicitados. A falta de jurisprudencia y cifras, el CEPD invita a la Comisión a supervisar la eficiencia y la aplicación concreta de este procedimiento en la práctica.

151. Sin embargo, el CEPD carece de jurisprudencia y de cifras sobre este procedimiento para establecer estos elementos. Por consiguiente, el CEPD no está en condiciones de proporcionar una evaluación sobre la eficiencia y la aplicación concreta de este procedimiento sin más elementos relativos a la práctica.

4.1.1.4 Conclusión sobre los procedimientos de acceso a los datos a efectos de aplicación de la ley

152. Como conclusión, el CEPD reconoce que el principio según el cual las autoridades competentes solo pueden acceder de manera coercitiva a los datos personales solo cuando sea necesario y proporcionado al propósito, y sobre la base de una orden judicial, corresponde a las principales garantías esenciales previstas en la legislación de la UE y del CEDH. A raíz de las conclusiones anteriores, el CEPD pide a la Comisión que supervise el alcance de estas medidas, el alcance del procedimiento de divulgación voluntaria y la aplicación de este principio por parte de la Policía de prefectura y los tribunales en la jurisprudencia pertinente y que controle también si el marco jurídico japonés proporciona las garantías esenciales establecidas por el TJUE sobre la base de la Carta y el TEDH con arreglo al Convenio.

4.1.2 Supervisión en el ámbito del Derecho penal

153. El proyecto de decisión de adecuación, así como el anexo II, presentan cuatro tipos de supervisiones dirigidas a la Policía, los ministerios y los organismos públicos.

4.1.2.1 Supervisión judicial

4.1.2.1.1 En los casos en que la información electrónica se recoja por medios coercitivos (registro e incautación).

154. Según el proyecto de decisión de adecuación, en todos los casos en que la información electrónica se recoja por medios coercitivos (registro e incautación), la Policía debe obtener una orden judicial previa. No obstante, existe una excepción a esta norma[70]. De hecho, el artículo 220, apartado 1, de la Ley de enjuiciamiento criminal permite a un fiscal, a su asistente o a un agente de la Policía judicial, al detener a un sospechoso, registrar o incautarse de información electrónica en el momento de la detención. En esta situación existe la posibilidad de que dicha información sea excluida como prueba por un juez.

[70] Véase el anexo II.

155. El CEPD es consciente de que también existen excepciones similares en la legislación de la UE. Observa que no siempre existe control judicial en los casos en que la información electrónica se recoge por medios coercitivos, como se estipula en el proyecto de decisión de adecuación. En este contexto, el CEPD recuerda la jurisprudencia del TEDH sobre los controles judiciales a posteriori[71].

4.1.2.1.2 En el caso de las solicitudes de divulgación voluntaria

156. Según el proyecto de decisión de adecuación, en el caso de las solicitudes de divulgación voluntaria, no existe un control previo por parte de un juez. En tal caso, la Policía de prefectura actúa bajo la supervisión del ministerio fiscal. El proyecto de decisión de adecuación menciona los artículos 192, apartado 1, y 246 sobre la cooperación mutua y la coordinación de los fiscales, la Comisión de Seguridad Pública de la Prefectura y los Agentes de Policía Judicial y el intercambio de información entre ellos. También hace referencia al artículo 193, apartado 1, según el cual el fiscal puede dar las instrucciones necesarias a la Policía judicial y establecer normas para una investigación imparcial. Por último, menciona el artículo 194 sobre las medidas disciplinarias contra la Policía judicial por no haber respetado a la fiscalía, tomadas por la Comisión de Seguridad Pública Nacional o de la Prefectura.

157. El CEPD reconoce el establecimiento de las medidas anteriores y la supervisión llevada a cabo por la Comisión de Seguridad Pública Nacional y de la Prefectura sobre la Policía judicial (véase más adelante).

4.1.2.2 Supervisión de la Policía por parte de las Comisiones de Seguridad Pública

158. Según el anexo II del proyecto de decisión de adecuación, dos tipos de comisiones ejercen una supervisión de la Policía. Ambas están destinadas a garantizar la gestión democrática y la neutralidad política de la administración policial.

4.1.2.2.1 Supervisión por parte de la Comisión de Seguridad Pública Nacional

159. El anexo II del proyecto de decisión de adecuación menciona la supervisión llevada a cabo por la Comisión de Seguridad Pública Nacional sobre la ANP. La Ley sobre la Policía contiene una lista de las funciones de la Comisión de la que emanan sus poderes de supervisión (véase el artículo 5).

160. De conformidad con el artículo 4 de la Ley sobre la Policía, la Comisión de Seguridad Pública Nacional se crea bajo la jurisdicción del Primer Ministro y está compuesta por un presidente y cinco miembros. El artículo 7 establece algunas limitaciones al nombramiento de los miembros de la Comisión. El mandato de los miembros de la Comisión es de cinco años y solo puede renovarse una vez, según establece el artículo 8. Por otra parte, la Dieta parece tener un fuerte poder sobre el nombramiento y el cese de los miembros de la Comisión, lo que garantiza la independencia de la Comisión de Seguridad Pública Nacional.

161. Estas disposiciones jurídicas refuerzan la neutralidad política de la Comisión de Seguridad Pública Nacional.

4.1.2.2.2 Supervisión por parte de las Comisiones de Seguridad Pública de la Prefectura

162. La Policía de Prefectura está sujeta a la supervisión de las Comisiones de Seguridad Pública establecidas en cada prefectura. De conformidad con los artículos 2 y 36, apartado 2, de la Ley sobre la Policía, las Comisiones de Seguridad Pública de la Prefectura son responsables de «la protección de los derechos y la libertad de las personas». El artículo 38, así como el artículo 42 de la Ley sobre la Policía, enumeran las funciones de la Comisión de Seguridad Pública de la Prefectura. El objetivo de estas comisiones también es garantizar la gestión democrática y la neutralidad política de la administración policial, tal como se establece en el artículo 43, apartado 2, emitiendo a la Policía de Prefectura casos individuales

[71] TEDH, Modestou contra Grecia, n.º 51693/13.

cuando lo consideren necesario en el contexto de una inspección de las actividades de la Policía de prefectura o de faltas graves de su personal.

163. Sin embargo, no está claro si estas Comisiones tienen otras competencias que la inspección del comportamiento de la Policía. El CEPD se pregunta si el término «falta grave» incluye el acceso ilegal a los datos y, en tal caso, si dichas Comisiones pueden ordenar la supresión de datos o no.

164. En lo que respecta a la neutralidad y a la independencia de las Comisiones, tal como se recoge en el proyecto de decisión de adecuación[72], las Comisiones de Seguridad Pública de la Prefectura se establecen bajo la jurisdicción del gobernador de la prefectura, que tiene que nombrar a los miembros de la Comisión con el consentimiento de la asamblea de la prefectura. Los miembros de la Comisión de Seguridad Pública de la Prefectura tienen un mandato de tres años y pueden ser renovados en su cargo hasta dos veces. El artículo 39 de la Ley sobre la Policía establece limitaciones relativas al nombramiento de los miembros. El proyecto de decisión de adecuación también menciona la supervisión de la Policía de prefectura por parte de la asamblea local, haciendo referencia al artículo 100 de la Ley de autonomía local. Sin embargo, dicha Ley no se proporcionó al CEPD[73].

165. Además, de conformidad con el artículo 42, apartados 2 y 3, de la Ley sobre la Policía, «ningún miembro de la Comisión podrá ser simultáneamente miembro de la asamblea y del personal a tiempo completo de las entidades públicas locales o participar en el servicio a tiempo parcial prescrito en el párrafo 1 del artículo 28, apartado 5, de la Ley de servicios públicos locales».

166. Según los elementos expuestos anteriormente y considerando la colaboración entre las Comisiones de Seguridad Pública de la Prefectura y la Comisión de Seguridad Pública Nacional, el CEPD está de acuerdo con el proyecto de decisión de adecuación y acoge con satisfacción la neutralidad y la independencia de los miembros de las Comisiones de Seguridad Pública de la Prefectura. El CEPD entiende que las Comisiones de Seguridad de la Prefectura solo tienen competencias para investigar el comportamiento de la Policía y no tienen otros poderes de supervisión, incluida la supresión de los datos recogidos por la Policía de prefectura. Por lo tanto, parece necesario aclarar más si la supervisión llevada a cabo por las Comisiones de Seguridad Pública de la Prefectura es suficiente con arreglo a las normas establecidas en la legislación de la UE.

4.1.2.2.3 Supervisión por parte de la Dieta

167. El proyecto de decisión de adecuación[74] y el anexo II[75] proporcionan cierta información sobre la supervisión llevada a cabo por la Dieta en relación con el Gobierno, también con respecto a la legalidad de la recogida de información y datos por parte de la Policía. De hecho, ambos mencionan el artículo 62 de la Constitución, según el cual la Dieta podrá solicitar la presentación de documentos y el testimonio de testigos. Ambos mencionan asimismo las disposiciones legales de la Ley sobre la Dieta, especialmente el artículo 104, relativo a las competencias de la Dieta, así como el artículo 74, concerniente a la presentación de las investigaciones escritas, que deben ser respondidas por el Consejo de Ministros por escrito en el plazo de siete días, como establece el artículo 75. El proyecto de decisión de adecuación también añade «el papel de la Dieta en la supervisión del Ejecutivo está respaldado por obligaciones de información, por ejemplo, de conformidad con el artículo 29 de la Ley de escuchas telefónicas».

[72] Véase el proyecto de decisión de adecuación, p. 31.
[73] Véase el proyecto de decisión de adecuación, p. 33.
[74] Véase el proyecto de decisión de adecuación, p. 30.
[75] Véase el anexo II, p. 12.

168. El CEPD reconoce la implicación de la Dieta en la supervisión del Gobierno y de la Policía con respecto a la legalidad de la recogida de datos.

4.1.2.2.4 Supervisión llevada a cabo por Ejecutivo

169. Según el anexo II del proyecto de adecuación, por una parte, el Ministro o Jefe de cada ministerio u organismo tiene la autoridad de supervisión y ejecución sobre la base de la APPIHAO (Ley japonesa sobre la protección de la información personal conservada por organismos administrativos, por sus siglas en inglés)[76]. Por otra parte, el Ministro del Interior y de Comunicaciones (MIC, por su acrónimo en inglés) tiene una competencia de investigación relativa a la ejecución de la APPIHAO por parte de todos los demás ministerios, incluido el Ministro de Justicia para la Policía, tal como se menciona en el proyecto de decisión de adecuación[77].

170. El Ministro podrá solicitar al jefe de un organismo administrativo que presente materiales y explicaciones sobre el tratamiento de información personal por parte del organismo de que se trate sobre la base del artículo 50 de la APPIHAO. Podrá solicitar una revisión de las medidas cuando se sospeche que se ha producido una infracción o un funcionamiento inadecuado de la Ley, así como emitir dictámenes sobre el tratamiento de información personal por el organismo administrativo en cuestión, de conformidad con los artículos 50 y 51 de la APPIHAO.

171. El proyecto de decisión de adecuación y el anexo II también mencionan la creación de 51 centros de información exhaustiva que «garantizan la correcta aplicación de esta Ley», de conformidad con el artículo 47 de la Constitución. El CEPD señala que el APPIHAO no explica en mayor medida la función y las competencias de dichos centros de información, pero el proyecto de decisión de adecuación proporciona algunas precisiones.

172. Por lo tanto, el CEPD saluda el hecho de que exista un control ejecutivo del cumplimiento de la APPIHAO en los ministerios y los organismos administrativos por parte del MIC.

173. Como conclusión, la legislación de la UE y el CEDH, en la jurisprudencia de sus respectivos tribunales, están estableciendo normas y garantías con arreglo a las cuales la supervisión debe ser completa, neutral e independiente. El CEPD señala que la PPC no tiene competencias de supervisión en asuntos relacionados con la aplicación de la ley. Además, aunque la supervisión llevada a cabo por la Dieta, la Comisión de Seguridad Nacional y las Comisiones de Seguridad de la Prefectura parece ser neutral e independiente, se requieren más aclaraciones sobre las competencias de supervisión de las Comisiones de Seguridad Pública de la Prefectura.

4.1.3 Recurso en el ámbito del Derecho penal

174. El proyecto de decisión de adecuación, complementado por el anexo II, presenta varias vías a través de las cuales las personas pueden presentar sus reclamaciones, tanto ante autoridades independientes como ante los jueces.

175. Estas vías y los elementos centrales de estos procedimientos derivados de la documentación disponible se presentan a continuación, tras un breve resumen de los derechos disponibles para aclarar qué pueden esperar los interesados de las autoridades públicas en el contexto del tratamiento de datos en el ámbito de los procedimientos penales.

[76] Véase el anexo II, p. 10.
[77] Véase el anexo II, p. 11.

4.1.3.1 Derechos disponibles de los interesados en el contexto de los procedimientos penales

176. A fin de obtener una reparación, los interesados deben tener derechos en virtud de la ley, para poder alegar que no se han respetado. Por lo tanto, el CEPD también evaluó los derechos disponibles en el contexto de los procedimientos penales presentados en el proyecto de decisión de adecuación.

4.1.3.1.1 Limitaciones generales a los derechos de los interesados en el marco del APPIHAO

177. En su proyecto de decisión de adecuación, la Comisión se refiere y se basa en los principios generales de protección de datos que las autoridades públicas deben respetar, una vez los hayan recogido. Estos principios también se describen con más detalle en el anexo II, de manera que el CEPD ha decidido formular también sus observaciones al respecto.

178. Por lo que se refiere a los derechos disponibles, el CEPD observa que, de conformidad con el anexo II del proyecto de decisión de adecuación, algunos de los derechos generales proporcionados a los interesados en el contexto de los datos tratados por los organismos administrativos siguen estando disponibles también en el contexto de investigaciones penales. Sin embargo, de la propia APPIHAO también se desprenden limitaciones adicionales con respecto a la recogida y el posterior tratamiento de la información personal en este contexto.

179. Estas limitaciones, que también parecen aplicarse tanto en el contexto de los datos recogidos sobre la base de una orden judicial como de un boletín de investigación en el contexto de una divulgación voluntaria, plantean cuestiones relativas a varios aspectos.

180. En cuanto al principio de limitación de la finalidad, aunque en principio se exige que los organismos administrativos especifiquen el propósito para el que conservan los datos personales y que no los retengan más allá del alcance necesario para alcanzar la finalidad de uso especificada, pueden cambiar dicha finalidad si es «lo que puede considerarse razonablemente pertinente para la finalidad original».

181. La APPIHAO también establece el principio de no divulgación, según el cual un empleado no divulgará la información personal obtenida a otra persona sin un motivo justificado ni utilizará dicha información para una finalidad injusta. Sin embargo, no se facilita información adicional sobre la interpretación de lo que podría representar un «motivo justificado» o una «finalidad injusta», por lo que sería necesaria una mayor aclaración para la evaluación.

182. El artículo 8, apartado 1, de la APPIHAO establece también la prohibición de utilizar o divulgar datos «salvo disposición en contrario de las leyes y los reglamentos». No obstante, aunque esta disposición no es en principio contraria al nivel de protección que ofrece la legislación de la UE, el CEPD carece de elementos adicionales sobre la medida en que se ejerce una supervisión o un control cuando la divulgación se efectúa en virtud de disposiciones legales o reglamentarias. Además, de conformidad con el artículo 8, apartado 2, se aplican excepciones adicionales a esta norma cuando «no es probable que tal divulgación excepcional cause un perjuicio injusto a los derechos e intereses del interesado o de un tercero». Sin más elementos a este respecto, esta excepción, que se basa en la ambigua noción de perjuicio «injusto», requiere una mayor clarificación, si es lo suficientemente restringida.

183. Por último, el artículo 9 de la APPIHAO establece restricciones adicionales sobre la finalidad o el método de utilización o cualquier otra restricción que debe imponer el jefe de un organismo administrativo en el que se facilita información personal conservada a un tercero. Como los conceptos de «cualquier otra restricción necesaria» y «facilitada a un tercero» son muy amplios, estas restricciones adicionales a los derechos de los interesados plantean dudas sin más aclaraciones sobre el ámbito de aplicación de esta disposición.

184. Si bien el CEPD es plenamente consciente de que los derechos de acceso y otros principios de protección de datos también están limitados en los procesos penales en virtud del Derecho de la UE, se proporcionan salvaguardias adicionales cuando se prevén tales limitaciones, también en lo que se refiere a la supervisión, la vigilancia y las vías de recurso. A falta de una suficiente jurisprudencia sobre estas limitaciones o elementos adicionales para aclarar el alcance de estas disposiciones, el CEPD no está en condiciones de evaluar si estas limitaciones a los derechos de los interesados se circunscriben a lo que se consideraría estrictamente necesario y proporcionado en virtud de la legislación de la UE y, por tanto, serían esencialmente equivalentes a los derechos ofrecidos a los interesados de la UE.

4.1.3.1.2 Limitaciones adicionales a los derechos de la APPIHAO derivadas de la Ley de enjuiciamiento criminal y de las ordenanzas de la Policía de prefectura

185. El CEPD señala que, si bien la APPIHAO parece ser aplicable a todo tratamiento por parte de los organismos administrativos de Japón, de legislaciones específicas se derivan algunas limitaciones importantes a los derechos de los interesados. En particular, el artículo 53, apartado 2, de la Ley de enjuiciamiento criminal[78] establece que «la información personal registrada en los documentos relativos a los juicios y a los artículos incautados» queda excluida del ámbito de aplicación de los derechos individuales plasmados en el capítulo IV de la APPIHAO. En concreto, el CEPD entiende, por lo tanto, que, en el contexto de los procedimientos penales, los interesados no se benefician de los derechos de información, acceso, rectificación o supresión de los datos personales registrados en documentos relativos a juicios y artículos incautados.

186. Por lo que se refiere a estas limitaciones, el CEPD entiende que se aplican en el contexto de los datos recopilados sobre la base de órdenes judiciales, así como en el ámbito de los datos recogidos con arreglo a una comunicación voluntaria a través de boletines de investigación (véase más adelante). En efecto, al figurar la base jurídica de los dos procedimientos de acceso a los datos (mediante una orden judicial y a través de un boletín de investigación) en la Ley de enjuiciamiento criminal, su artículo 53-2 parece aplicarse a los dos tipos de recogida. Sin embargo, como el artículo 53-2 se refiere a los artículos «incautados», podría aclararse si las limitaciones a los derechos previstos en esta disposición se aplican también en el contexto de la divulgación voluntaria.

187. El CEPD lamenta que no se le hayan proporcionado las ordenanzas de la Policía de prefectura, que dicen proteger información personal, derechos y obligaciones equivalentes a los de la APPIHAO. Teniendo en cuenta la falta de claridad relativa a la interpretación de la APPIHAO y la no disponibilidad de las ordenanzas de la Policía de prefectura, el CEPD se pregunta si los derechos concedidos a los ciudadanos en este contexto y los mecanismos adicionales de supervisión o recurso son suficientes para compensar la ausencia de derechos.

4.1.3.2 Recurso a través de autoridades independientes

4.1.3.2.1 Recurso administrativo

188. El CEPD señala que los organismos administrativos que recogen datos, como la Policía de prefectura, son competentes para tratar las solicitudes procedentes de ciudadanos relativas a sus —limitados— derechos, en lo que respecta a sus datos recogidos en el marco de investigaciones penales (véanse más arriba los derechos disponibles), que parecen incluir la recogida de datos sobre la base tanto de una orden de detención como de los boletines de investigación. En concreto, estos derechos parecen limitarse a principios generales, como la necesidad de conservación de datos, en relación con la finalidad (véase el artículo 3, apartado 1, de la APPIHAO), el principio de limitación de la finalidad (artículo 4) o la exactitud de los datos (artículo 5), mientras que los derechos individuales, como el

[78] Disponible en http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 y citado en el anexo II del proyecto de decisión de adecuación, nota a pie de página 25.

derecho a la información, el acceso, la rectificación o la supresión, quedan excluidos en el caso de los datos personales registrados en documentos relativos a juicios y artículos incautados[79]. Aunque estos organismos no pueden considerarse independientes y, por tanto, susceptibles de ofrecer un recurso o una supervisión independientes, el CEPD acoge con satisfacción esta vía. Sin embargo, hace hincapié en que las reclamaciones presentadas en este contexto siguen estando limitadas a muy pocos derechos de los interesados, habida cuenta de las limitaciones de los derechos dispuestas por la APPIHAO.

189. Además, dado que «la información personal registrada en los documentos relativos a juicios y artículos incautados» está excluida del ámbito de aplicación de los derechos individuales recogidos en el capítulo IV de la APPIHAO, de conformidad con el artículo 53-2 de la Ley de enjuiciamiento criminal, las posibilidades de solicitar el acceso a la información personal también se limitan a los procedimientos previstos en otras disposiciones de dicha Ley. Parece que solo las víctimas, los sospechosos o los acusados pueden actuar en este contexto, y, aun así, dependiendo de la fase del procedimiento penal. Por lo tanto, el CEPD manifiesta su preocupación por el hecho de que no se disponga de ningún derecho general de acceso, rectificación o supresión de la información en virtud de la legislación japonesa en el marco del procedimiento penal, y de que todas las vías de recurso disponibles implican ser una víctima (en cuyo caso es probable que la persona sepa que se han recogido sus datos), un sospechoso o un acusado, o la demostración de un perjuicio, mientras que los interesados también deberían tener derecho a acceder a sus datos y, en su caso, a que sus datos se rectificaran o suprimieran a pesar de no haber sufrido ningún daño (aunque fuera posible que sí) o cuando no sean víctimas, sospechosos o acusados, sino testigos, por ejemplo.

4.1.3.2.2 Recurso administrativo a través de las Comisiones de Seguridad Pública de la Prefectura

190. Además, las Comisiones de Seguridad Pública de la Prefectura parecen ser competentes para tramitar las reclamaciones. Sobre la base del artículo 79 de la Ley sobre la Policía a que se hace referencia en el proyecto de decisión de adecuación, los particulares pueden reclamar contra cualquier conducta ilegal o indebida de un agente en el ejercicio de sus funciones.

191. El CEPD busca aclaraciones sobre si el tratamiento «ilícito» de datos personales puede constituir un «comportamiento ilegal o incorrecto de un agente» y sobre la demostración de un perjuicio, que parece exigirse al interesado. De hecho, la notificación emitida por la NPA a la Policía y a las Comisiones de Seguridad Pública de la Prefectura sobre la correcta tramitación de las reclamaciones relativas a la ejecución de sus funciones por parte de los agentes de Policía limitan dichas reclamaciones a demandas concretas relativas a «la corrección de cualquier perjuicio específico que se haya causado como resultado de un comportamiento ilegal o inadecuado, o de la omisión de efectuar una acción necesaria, por parte de un agente de Policía en el ejercicio de sus funciones» y la posibilidad de «presentar una queja por el modo inadecuado de ejecución de sus funciones por parte de un agente de Policía». Se aclara expresamente que «se excluirán las reclamaciones relativas al incumplimiento de un agente de Policía en relación con cualquier asunto que no se considere que entra dentro de sus funciones, así como a las que expresen una opinión general o una propuesta, que no afecten directamente a la propia parte reclamante».

192. En cuanto a los requisitos de procedimiento para presentar una reclamación, aunque deben presentarse por escrito, el CEPD señala que la legislación japonesa prevé la asistencia para la redacción de la reclamación en este contexto, incluido para los extranjeros. Además, el Gobierno japonés parece

[79] Véase arriba, en relación con las limitaciones a la APPIHAO y, en particular, el artículo 53-2 de la Ley de enjuiciamiento criminal (no facilitada pero citada en el anexo II del proyecto de decisión de adecuación, nota a pie de página 25).

haber confiado también a la PPC la obligación de prestar asistencia a los interesados de la UE para tramitar y resolver las reclamaciones en este ámbito, extremo que el CEPD acoge con satisfacción. El CEPD subraya que, en este contexto, la PPC solo actuará como punto de contacto entre los interesados de la UE y las autoridades competentes de Japón.

193. Los resultados de la Comisión de Seguridad Pública de la Prefectura a raíz de una reclamación no se notificarán en los casos enumerados en el artículo 79-2 de la Ley sobre la Policía, que incluyen el caso en que «se desconoce la actual residencia del reclamante». El CEPD reconoce que la referencia al residente no implica que en todos los casos los interesados de la UE quedarían excluidos, por tanto, de la notificación de los resultados de sus reclamaciones en razón de que no residen en Japón.

4.1.3.2.3 Mecanismo *ad hoc* de la PPC

194. A la vista de las conclusiones descritas en lo que antecede, el CEPD saluda que el Gobierno japonés y la Comisión Europea hayan acordado un mecanismo de recurso adicional que proporcione a los ciudadanos de la UE una vía de recurso añadida en Japón a través de la cual los particulares también pueden recurrir contra investigaciones ilegales o indebidas por parte de las autoridades públicas. El CEPD también observa y acoge con satisfacción que las solicitudes puedan presentarse a la PPC, en lugar de a otro funcionario del Gobierno, ampliando así el ámbito de competencias de al PPC al área de la aplicación de la ley y la seguridad nacional.

195. El objetivo del CEPD, a la hora de analizar el nuevo mecanismo, ha sido comprender las competencias de la PPC en este contexto.

196. Aunque la formulación no es del todo clara, el CEPD entiende que el mecanismo de recurso adicional no requiere «legitimación», en el sentido de que no se requiere que el solicitante demuestre que es probable que sus datos personales hayan sido sometidos a vigilancia por parte de una autoridad japonesa. El CEPD desearía de todas maneras solicitar una confirmación al respecto por parte de la Comisión.

197. En consonancia con su evaluación del mecanismo del Defensor del Pueblo, creado en virtud del Escudo de la privacidad, el CEPD hace hincapié en la necesidad de que el destinatario de la solicitud, en este caso la PPC, tenga poderes efectivos, a fin de considerar el mecanismo de recurso como esencialmente equivalente a una tutela judicial efectiva en el sentido del artículo 47 de la Carta de los Derechos Fundamentales.

198. Al explicar el mecanismo de recurso, el Gobierno japonés remite al artículo 6, al artículo 61, inciso ii), y al artículo 80 de la APPI y establece estas competencias en el anexo II. El CEPD entiende que el procedimiento descrito en el anexo II especifica o amplía las competencias de la PPC, ya que la formulación del artículo 6, el artículo 61, inciso ii), y el artículo 80 es bastante vaga y general. En la medida en que el anexo II especifica o amplía las competencias de la PPC, el CEPD desearía solicitar la aclaración de que los demás organismos del Gobierno japonés están obligados por la misma.

199. Sobre la base del procedimiento del anexo II, el CEPD observa que las autoridades públicas competentes de Japón están obligadas a cooperar con la PPC, «entre otras cosas, proporcionándole la información necesaria y el material pertinente, de modo que la PPC pueda evaluar si la recogida o el uso posterior de información personal ha tenido lugar de conformidad con las normas aplicables». Para la evaluación de la eficacia del sistema, es importante, por tanto, volver a remitirse a los poderes que tienen dichas autoridades competentes, con las que coopera la PPC. El CEPD entiende que estas competencias no se ampliarán en virtud de las garantías que figuran en el anexo II.

200. El CEPD también señala que, si se ha detectado una infracción de las normas, «la cooperación de las autoridades públicas competentes con la PPC incluye la obligación de subsanar la infracción», lo que incluye expresamente la supresión de los datos recogidos en violación de las normas aplicables. El CEPD entiende que las obligaciones de la autoridad competente se derivan de la «cooperación con la PPC», y no de una decisión de la PPC.

201. Por último, la PPC informará al solicitante del «resultado de la evaluación, incluida cualquier medida correctora adoptada, llegado el caso». Por añadidura, la PPC informará al solicitante de la «posibilidad de pedir una confirmación de los resultados a la autoridad pública competente y sobre la autoridad a la que se presentará dicha solicitud de confirmación».

202. Además, la PPC se ha comprometido a ayudar al solicitante a interponer acciones adicionales en virtud de la legislación japonesa, si dicho solicitante no está satisfecho con el resultado del procedimiento.

203. En vista de la necesidad de disponer de un mecanismo de recurso eficaz, esencialmente equivalente a las normas de la UE, el CEPD se pregunta no obstante si la PPC tiene competencias específicas distintas de evaluar si la recogida o el uso posterior de datos personales ha tenido lugar de conformidad con las normas aplicables y solicitar a las autoridades competentes que hagan uso de sus competencias respectivas y que se ocupen de las reclamaciones que les haya transmitido la PPC. En caso de que la PPC solo actúe como punto de contacto para los ciudadanos de la UE, el CEPD consideraría que esto es insuficiente para ofrecer un mecanismo de recurso eficaz y esencialmente equivalente a las normas de la UE. El CEPD, por lo tanto, pide a la Comisión que aclare los puntos mencionados en este subcapítulo, en particular sobre si y cómo el mecanismo amplía las obligaciones de las autoridades competentes, su carácter vinculante y cómo puede garantizar la PPC el cumplimiento efectivo, sin limitarse a actuar como punto de contacto para los ciudadanos de la UE.

4.1.3.3 Recurso judicial

4.1.3.3.1 Mecanismo de cuasidemanda

204. El denominado procedimiento de «cuasidemanda» permite actuar contra la recogida coercitiva de información sobre la base de una orden judicial para la anulación o la modificación de una confiscación ilegal.

205. Esta vía implica que la persona es consciente de la incautación de los datos. Sin embargo, el CEPD entiende que el procedimiento para la recogida de datos sobre la base de una orden judicial no se notifica al interesado. Asimismo, entiende que la divulgación voluntaria no implica que las empresas a las que se solicita tengan la obligación de informar a los interesados sobre las solicitudes recibidas y cumplidas. Por lo tanto, aunque en el anexo II se hace hincapié en que «esta impugnación puede llevarse a cabo sin que la persona tenga que esperar a la conclusión del caso», en la práctica, aparte de las órdenes judiciales de autorización de escuchas telefónicas, para las que se indica que la Ley prevé una obligación de notificación[80], esta vía solo parece estar efectivamente disponible una vez que el interesado haya tenido conocimiento de la recogida mediante un procedimiento contra el mismo.

4.1.3.3.2 Medidas cautelares

206. Además, con el fin de obtener la supresión de los datos recogidos mediante un procedimiento penal (las denominadas «medidas cautelares»), o para obtener una indemnización por daños y perjuicios, las personas también pueden interponer acciones civiles ante un juez.

[80] El artículo 23 de la Ley de escuchas telefónicas se menciona en la página 33 del proyecto de decisión de adecuación, si bien el CEPD no recibió este texto y, por tanto, no puede evaluar en qué medida se aplica esta obligación de notificación y en qué casos podría estar limitada.

207. Por lo que se refiere a la compensación, el CEPD observa que el procedimiento parece limitarse a las situaciones en las que un funcionario público en el ejercicio de sus funciones, ilegalmente y con culpa (de forma deliberada o por negligencia), inflige daños a la persona en cuestión. A juicio del CEPD, los daños y perjuicios parecen incluir los daños morales. Sin embargo, no se especifica con más detalle qué debe demostrar la persona que sufrió un daño. El CEPD no estuvo en posición de evaluar la jurisprudencia relativa a la concesión de indemnizaciones y, por lo tanto, no puede evaluar si esta vía ofrece una tutela judicial efectiva en caso de daños.

208. Por lo que se refiere a las «medidas cautelares», el CEPD también señala que, para presentar una solicitud, la persona debe saber en primer lugar que sus datos se recogieron y que siguen conservándose. Por lo tanto, habida cuenta de los derechos limitados de información y de acceso de las personas en el contexto de las investigaciones y los procedimientos penales, la eficiencia del procedimiento también parece bastante limitada.

4.1.3.4 Evaluación general de las vías de recurso

209. Tras la evaluación de todas las vías de recurso disponibles para los particulares con arreglo a la legislación japonesa, así como para los interesados de la UE ante la PPC, el CEPD acoge con satisfacción el mecanismo de resolución de litigios *ad hoc* en el que participa la PPC. Tiene un valor añadido para los interesados de la UE, en particular porque les permite entender qué vías tienen disponibles para obtener una reparación o una compensación, así como presentar sus solicitudes con arreglo a los requisitos de procedimiento aplicables según la legislación japonesa. Sin embargo, son necesarias más aclaraciones, en particular sobre si el mecanismo amplía las obligaciones de las autoridades competentes, el modo en que están vinculadas por él y cómo puede la PPC garantizar eficazmente su cumplimiento, con el fin de garantizar que este nuevo mecanismo prevea una reparación efectiva.

210. Esta evaluación pone de manifiesto que ningún mecanismo de recurso de la legislación japonesa parece permitir el acceso, la rectificación o la supresión de datos a los interesados que no son víctimas, sospechosos o acusados en el contexto de un procedimiento penal, por ejemplo, para poner remedio a la recogida o conservación ilícitas de sus datos. También muestra que todos los mecanismos y procedimientos de recurso e indemnización disponibles en virtud del Derecho japonés para las víctimas, los sospechosos o los acusados implican el conocimiento de la recogida de datos, que parece estar limitado en la práctica, ya que los derechos de acceso e información proporcionados son limitados. Además, parece necesaria una mayor clarificación sobre la demostración de un comportamiento ilegal por parte de las autoridades, en particular si dicho comportamiento incluye el tratamiento ilegal de datos personales, o de un daño sufrido por la persona.

211. Por consiguiente, sin más documentación y sin otros elementos, el CEPD está preocupado por si la reparación en virtud de la legislación japonesa y el proyecto de decisión de adecuación es suficientemente eficaz en comparación con las normas de la legislación de la UE.

4.2 Acceso con fines de seguridad nacional

4.2.1 Ámbito de la vigilancia

212. En el proyecto de decisión de adecuación, el capítulo sobre «Acceso y uso por parte de las autoridades públicas japonesas con fines de seguridad nacional» se introduce mediante una declaración general, en consonancia con la garantía proporcionada por el Gobierno japonés en el anexo II, según la cual ninguna legislación japonesa permitirá la presentación de «solicitudes obligatorias de información o "escuchas administrativas" fuera de las investigaciones penales». Como conclusión, se dice que «por motivos de seguridad nacional, la información solo puede obtenerse a partir de una fuente de información que pueda ser accesible libremente por cualquier persona o mediante divulgación voluntaria. Esto excluye cualquier actividad de vigilancia encubierta en este ámbito. Los operadores

comerciales que reciban una solicitud de cooperación voluntaria (en forma de divulgación de información electrónica) no están obligados en Derecho a facilitar dicha información».[81]

213. Dentro de estas limitaciones, se enumeran cuatro entidades gubernamentales que tienen la facultad de recabar información electrónica de los operadores comerciales japoneses por motivos de seguridad nacional. Por lo que se refiere al Ministerio de Defensa, como una de esas cuatro entidades, se dice que «solo tiene autoridad para recoger información (electrónica) a través de la divulgación voluntaria».[82]

214. Para evaluar la configuración general de la recogida de datos a efectos de la seguridad nacional, el CEPD desea recordar la primera de las cuatro «garantías esenciales», según la cual «el tratamiento debe basarse en normas claras, precisas y accesibles»[83]. Más concretamente, el TEDH ha dejado muy claro que los programas de vigilancia solo son «conformes a la ley» si las medidas de vigilancia «se fundamentan en alguna legislación nacional». El Tribunal ha aclarado que la compatibilidad con el Estado de Derecho exige que la ley por la que se autoriza la medida sea accesible y previsible en cuanto a sus efectos. Haciendo referencia al riesgo de arbitrariedad, el Tribunal ha exigido «normas claras y detalladas sobre medidas de vigilancia secreta»; «suficientemente claras para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades públicas están facultadas para recurrir a tal medida».[84]

215. Para la aplicación de estas garantías esenciales al ordenamiento jurídico de Japón, el CEPD es consciente no solo del hecho de que, en materia de seguridad nacional, los Estados disponen de un amplio margen de apreciación, reconocido por el Tribunal Europeo de Derechos Humanos, sino también de que los poderes nacionales en materia de seguridad reflejan la experiencia histórica de cada país. El CEPD entiende, por tanto, que, como destacó el Gobierno japonés, tras la Segunda Guerra Mundial, las agencias nacionales japonesas de inteligencia cuentan con unas competencias más limitadas que en otros Estados.

216. En la lectura del CEPD, el proyecto de decisión de adecuación, en consonancia con la garantía del Gobierno japonés, sugiere que las entidades públicas japonesas no gestionan programas que supervisen estratégicamente o vigilen en sentido amplio las comunicaciones (por internet). Como se ha dicho anteriormente, el Gobierno japonés ha dado garantías, en una carta firmada por el Ministro de Justicia, de que «por motivos de seguridad nacional solo puede obtenerse información procedente de una fuente de información que pueda ser accesible libremente por cualquier persona o mediante su divulgación voluntaria».

217. En cuanto a la base jurídica del Ministerio de Defensa, el CEPD señala que el proyecto de decisión de adecuación incluye información general sobre sus competencias y cita su misión «para llevar a cabo estos asuntos en la medida en que sean relevantes a fin de garantizar la paz y la independencia nacionales y la seguridad de la nación». Sin embargo, el CEPD no ha recibido una traducción al inglés de la base jurídica.

218. Al mismo tiempo, el CEPD está al corriente de los informes publicados en diferentes medios de comunicación, que sugieren que los programas de vigilancia están gestionados por la Dirección de

[81] Decisión de adecuación, apartado 151.
[82] Decisión de adecuación, apartado 153.
[83] Grupo de Trabajo del Artículo 29, WP 237: Documento de trabajo 01/2016 sobre la justificación de las interferencias con los derechos fundamentales a la intimidad y a la protección de datos a través de medidas de vigilancia al transferir datos personales (garantías esenciales europeas).
[84] Véase, por ejemplo, Big Brother Watch y otros contra el Reino Unido, apartado 305.

Inteligencia de Señales del Ministerio de Defensa de Japón[85]. En el informe también se afirma que el Ministerio de Defensa de Japón, aunque se negó a debatir detalles del informe, «reconoció que Japón tiene "oficinas en todo el país" que interceptan comunicaciones» y que «se centrarían en actividades militares y en "ciberamenazas" y no recogerían la información del público en general». Esta última declaración (que el Ministerio de Defensa no recoge información sobre el público en general) forma parte de la reafirmación del Gobierno japonés.

219. El Gobierno de Japón ha reiterado, en una carta firmada por el Ministro de Justicia, que el Ministerio de Defensa no recoge información sobre el público en general.

220. No es tarea del CEPD realizar una evaluación general de las posibles capacidades de vigilancia del Gobierno japonés. Estas actividades solo son importantes para su evaluación si son pertinentes para la transferencia de datos personales entre la UE y Japón. En este contexto, el CEPD desea reafirmar su enfoque ya adoptado por su predecesor al pedírsele su opinión sobre el Escudo de la privacidad UE-EE. UU. Al emitir un dictamen sobre el Escudo de la privacidad, el Grupo de Trabajo del Artículo 29 incluyó en su análisis las competencias y los límites de EE. UU. para llevar a cabo la vigilancia de datos «durante su transferencia» a Estados Unidos[86]. Aplicando el mismo rasero para la decisión de adecuación sobre Japón, el CEPD adopta la opinión de que la información sobre las capacidades de las autoridades japonesas para vigilar datos «durante su transferencia» a Japón son relevantes. En caso de que estas facultades de vigilancia existieran, también la decisión del TEDH en el asunto Big Brother Watch parece sugerir que las mismas tendrían que ser reguladas de conformidad con las normas establecidas por el CEDH.

221. Como consecuencia de ello, si las interceptaciones se limitaran a la «asistencia a la acción militar», bien podrían no ser pertinentes para la evaluación de la decisión de adecuación. Por lo tanto, el interés del CEPD estriba en recibir aclaraciones sobre las medidas de vigilancia de las entidades gubernamentales japonesas. A este respecto, esta aclaración sería bienvenida para determinar si los datos objeto de transferencia en virtud de este marco de adecuación podrían ser objeto de acceso con fines de seguridad nacional por las autoridades competentes japonesas en este ámbito.

4.2.2 Comunicación voluntaria en caso de seguridad nacional

222. El proyecto de decisión de adecuación establece que las cuatro entidades públicas solo tienen autoridad para recoger información (electrónica) mediante su divulgación voluntaria. Según el proyecto de decisión y el anexo II, existen algunas limitaciones por razones legales, lo que significa que la recogida de datos se limita a lo necesario para la ejecución de las tareas por parte de las entidades.

223. En el ámbito del Derecho penal, tal como se menciona en la sección sobre la aplicación de la ley, la divulgación voluntaria solo es admisible como parte de una investigación penal y, por lo tanto, presupone una sospecha concreta de un delito ya cometido. Las investigaciones en materia de seguridad nacional difieren de las investigaciones en el ámbito de la aplicación de la ley. El CEPD reconoce que, de conformidad con el anexo II, los principios centrales de «necesidad de investigación»

[85] En mayo de 2018, la publicación de noticias en línea «*The Intercept*» publicó un informe titulado «La historia no contada de la agencia de espionaje secreto de Japón».

[86] Véase el WP 255, «Escudo de la privacidad UE-EE. UU. — Primera revisión anual conjunta», adoptado el 28 de noviembre de 2017, p. 16: «El Grupo de Trabajo del Artículo 29 considera que el análisis de la legislación del tercer país para el que se considera la adecuación no debe limitarse a la legislación y a las prácticas que permiten la vigilancia dentro de las fronteras físicas de ese país, sino que también debe incluir un análisis de los fundamentos jurídicos de la legislación de dicho tercer país que le permitan llevar a cabo la vigilancia fuera de su territorio en lo que respecta a los datos de la UE. Como ya se ha subrayado en su anterior dictamen, «debe quedar claro que los principios del Escudo de la privacidad se aplicarán desde el momento en que tiene lugar la transferencia de datos, lo que implica incluir los datos "durante su transferencia" hacia dicho país».

e «idoneidad del método» se aplican igualmente en el ámbito de la seguridad nacional y deben respetarse teniendo debidamente en cuenta las circunstancias específicas de cada caso[87]. Lamenta que la solicitud no se aclare en mayor medida, en particular mediante una referencia adicional a la jurisprudencia. No obstante, el CEPD establece que la utilización de este procedimiento ha de ser proporcionada o necesaria.

224. Según el proyecto de decisión, cuando se ha recogido («obtenido») información personal, su tratamiento está regido por la APPIHAO, excepto para la Policía de prefectura[88]. En el anexo II se indica que el tratamiento de la información personal por parte de la Policía de prefectura se rige por órdenes prefectorales que establecen principios para la protección de la información personal, derechos y obligaciones equivalentes a los que figuran en la APPIHAO[89]. Dado que no existen traducciones al inglés de estas ordenanzas, el CEPD no está en condiciones de evaluar si los principios son equivalentes a los de la APPIHAO.

225. En cuanto a los demás comentarios sobre la comunicación voluntaria, se hace referencia al apartado sobre la aplicación de la ley.

4.2.3 Supervisión

4.2.3.1 Aspectos generales

226. Las cuatro entidades gubernamentales facultadas para recoger información electrónica de los operadores comerciales japoneses por motivos de seguridad nacional son: (i) la Oficina de Inteligencia e Investigaciones del Consejo de Ministros (CIRO, por sus siglas en inglés); (ii) el Ministerio de Defensa; (iii) la Policía [tanto la Agencia Nacional de Policía (NPA)[90] como la Policía de prefectura); y (iv) la Agencia de Inteligencia de Seguridad Pública (Public Security Intelligence Agency, PSIA).

227. Según el proyecto de decisión de adecuación, estas entidades gubernamentales están sujetas a varios niveles de supervisión de tres ramas del Gobierno[91]. El CEPD observa que existen mecanismos de supervisión en el marco de la rama legislativa (Dieta japonesa) y del poder ejecutivo [Oficina de Cumplimiento Legal del Inspector General (Inspector General's Office, IGO), las Comisiones de Seguridad Pública de la Prefectura y la Comisión de Examen de Seguridad Pública). El CEPD hace hincapié en que la Comisión debería aclarar la supervisión judicial (de oficio/garantía C del WP 237; en cuanto a la reparación, hay un capítulo aparte en el proyecto de decisión y una garantía adicional en el WP 237) de los organismos gubernamentales antes mencionados, ya que no está claro si existe una supervisión judicial en el ámbito de la recogida de información personal con fines de seguridad nacional sin medios coercitivos.

4.2.3.2 Supervisión por parte de la Dieta japonesa

228. El CEPD observa que la Dieta japonesa puede llevar a cabo investigaciones en relación con las actividades de las autoridades públicas y, por lo tanto, también para todos los entes gubernamentales anteriormente mencionados. Además, la Dieta también puede solicitar la presentación de documentos y el testimonio de testigos (*artículo 62 de la Constitución japonesa, artículo 104 de la Ley sobre la Dieta*). El CEPD también señala que, con arreglo a los *artículos 74 y 75 de la Ley sobre la Dieta*, los miembros de la Dieta pueden formular preguntas escritas al Consejo de Ministros que pueden acabar

[87] Véase el anexo II, p. 23.
[88] Decisión de adecuación, apartados 118 y 157.
[89] Véase el anexo II, p. 3.
[90] Sin embargo, según la información recibida, el principal papel de la NPA es coordinar las investigaciones de los diversos departamentos de la Policía de prefectura y sus actividades de recogida de información se limitan a intercambios con autoridades extranjeras.
[91] Véase el anexo II, p. 39.

en una respuesta por parte de este (*artículo 75 de la Ley sobre la Dieta*). Por último, también hay que indicar que existen obligaciones específicas de información para, por ejemplo, la Agencia de Inteligencia de Seguridad Pública (PSIA) (artículo 36 de la SAPA/artículo 31 de la ACO), mediante un informe anual a la Dieta. Este informe no se transmitió al CEPD.

4.2.3.3 Supervisión por parte de la Oficina de Cumplimiento Legal (OIG) del Inspector General

229. El CEPD observa que existe un organismo de supervisión del Ministerio de Defensa, denominado OIG. Al CEPD no se le facilitó a la Ley de establecimiento del Ministerio de Defensa, sino solo las manifestaciones que figuran en el anexo II del proyecto de decisión. Con arreglo al anexo II, la OIG es una oficina independiente dentro del Ministerio de Defensa, bajo la supervisión directa del Ministerio de Defensa de conformidad con el artículo 29 de la Ley de establecimiento del Ministerio de Defensa. La OIG tiene la facultad de llevar a cabo inspecciones del cumplimiento de las leyes y los reglamentos por parte de los funcionarios del Ministerio de Defensa (denominadas «Inspecciones de Defensa») en todo el ministerio, incluidas las Fuerzas de Autodefensa.

230. De conformidad con el anexo II, la OIG realiza sus funciones con independencia de los departamentos operativos del Ministerio de Defensa. El CEPD observa que la OIG es un organismo de supervisión *interno*.

231. Las inspecciones dan lugar a conclusiones y, con la intención de garantizar el cumplimiento, a medidas notificadas directamente al Ministro de Defensa. Sobre la base del informe de la OIG, el Ministro de Defensa puede dictar órdenes para aplicar las medidas necesarias para subsanar la situación. El Viceministro de Defensa Adjunto es responsable de la implementación de estas medidas y debe informar al Ministro de Defensa sobre la situación al respecto.

232. Analizando el anexo II, sin haber recibido las disposiciones legales (Ley de establecimiento del Ministerio de Defensa) para estas consideraciones, el CEPD acoge con satisfacción la posibilidad de ordenar las necesarias medidas de cumplimiento para remediar la situación. Sin embargo, el CEPD plantea dudas en cuanto a la independencia de la OIG, ya que se trata de una oficina dentro del Ministerio de Defensa y está bajo la supervisión directa del Ministro de Defensa de conformidad con el anexo II (con arreglo al WP 237 «*la independencia funcional no es suficiente por sí misma para proteger a dicha autoridad de supervisión de toda influencia exterior*»).

233. En consonancia con la jurisprudencia del TEDH y del *WP 237*, respectivamente, a raíz de las consideraciones del anexo II, el Inspector General puede solicitar informes a la oficina en cuestión (documentos, lugares, explicaciones). Al CEPD le parece necesario aclarar si las oficinas concernidas están obligadas a responder a estas solicitudes o no y si los documentos solicitados incluyen materiales reservados, como se menciona en el *WP 237*, o no.

234. Aunque el CEPD acoge con satisfacción que expertos jurídicos de muy alto nivel (ex-Fiscal Jefe) dirijan la OIG, parece necesaria una aclaración sobre la forma de proceder al nombramiento de este organismo de supervisión.

4.2.3.4 Supervisión por parte de la Comisión de Examen de Seguridad Pública

235. Según el anexo II (página 25), la PSIA lleva a cabo inspecciones periódicas y especiales sobre las operaciones de sus delegaciones y oficinas individuales (Oficina de Inteligencia de Seguridad Pública, Delegaciones y Subdelegaciones de Inteligencia de Seguridad Pública, etc.). A efectos de la inspección periódica, se designa como inspectores a un Director General Adjunto o a un Director. Tales inspecciones también deben referirse a la gestión de la información personal.

236. De conformidad con el considerando 163 del proyecto de decisión, la Comisión de *Examen de Seguridad Pública* actúa como un organismo independiente de supervisión *ex ante* para la PSIA, con relación a cuestiones de la ACO[92] y la SAPA[93]. El CEPD celebra tal extremo.

237. Aunque en el sitio web del Ministerio de Justicia japonés facilita cierta información[94], el CEPD no está en posición de evaluar cuidadosamente y en mayor medida la independencia de la Comisión de Examen de Seguridad Pública, ya que no se le proporcionó la Ley de establecimiento de la Comisión de Examen de Seguridad Pública[95] ni el Reglamento de la Comisión de Examen de Seguridad Pública[96].

4.2.3.5 Supervisión por parte de la Comisión de Seguridad Pública Nacional, las Comisiones de Seguridad Pública de la Prefectura y la APPIHAO (Ejecutivo)

238. Véase 3.1.2.2.1 (Comisión de Seguridad Pública Nacional), 3.1.2.2.2. (Comisiones de Seguridad Pública de la Prefectura) y 3.1.2.2.4. (Ejecutivo).

4.2.3.6 Supervisión por parte de la PPC

239. El CEPD invita a la Comisión a que mencione en el considerando 164 que la PPC no es un organismo de supervisión de las citadas entidades públicas y que solo es competente para el recurso de las personas o que traslade el pasaje del considerando 164 acerca de la PPC a al apartado «recurso individual».

4.2.4 Mecanismo de recurso

240. Para el análisis del mecanismo de recurso negociado recientemente se hace referencia al apartado sobre la aplicación de la ley.

241. Además, cabe señalar que la legislación japonesa prevé una vía de recurso específica disponible en el ámbito de la seguridad nacional. El CEPD entiende que todas las personas, incluidos los ciudadanos de la UE, pueden solicitar, en general, la divulgación, la corrección (incluida la supresión) o la suspensión del uso de los datos a los órganos administrativos, incluso si se tratan a efectos de seguridad nacional. En caso de que una solicitud de este tipo se «deniegue por considerar que la información de que se trata se considera no divulgable», podrá interponerse un recurso de revisión y deberá consultarse al Comité de Revisión de Protección de la Información Personal. Este Comité está compuesto por miembros designados por el Primer Ministro con el consentimiento de ambas Cámaras, está dotado de poderes de investigación, y concluye con un informe escrito para la persona interesada, que no es jurídicamente vinculante, pero que casi siempre se sigue[97]. Según el anexo II, solo en dos de 2000 casos la autoridad administrativa adoptó una decisión que difería de la conclusión del Comité.[98]

242. Parece desprenderse de la explicación facilitada que la revisión no está disponible si la información puede ser «divulgada», pero la persona no está satisfecha con el resultado. El CEPD reconoce esta vía

---

[92] Ley relativa al control de organizaciones que han cometido actos de asesinato indiscriminado masivo (Ley n.º 147, de 7 de diciembre de 1999).

[93] Ley de prevención de actividades subversivas (Ley n.º 240 de 21 de julio de 1952).

[94] Véase http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (septiembre de 2018): el órgano extraministerial «*está formado por un presidente y seis miembros. Se seleccionan de entre personas de buena conducta que son capaces de emitir un juicio justo sobre el control de las organizaciones y que poseen amplios conocimientos y experiencia tanto sobre la legislación como sobre la sociedad. Son nombrados por el Primer Ministro y deben ser aprobados por ambas cámaras de la Dieta. Por lo que se refiere a la aplicación de la legislación previamente mencionada (SAPA/ACO), los miembros desempeñan sus funciones con bastante independencia, libres de cualquier dirección o supervisión del Primer Ministro o del Ministro de Justicia*.»

[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (septiembre de 2018).

[96] Artículo 28 de la ACO.

[97] Anexo II, pp. 25 y 26. Ley de establecimiento de la Comisión de Revisión de Protección de la Información Personal y de Divulgación de Información, artículos 4, 9 y 11.

[98] Anexo II, nota a pie de página 35.

de recurso, pero desea obtener más aclaraciones sobre este último aspecto, que limitaría significativamente su ámbito de aplicación.

En nombre del Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)