Dictamen 15/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con la Directiva (UE) 2016/680 sobre el nivel de protección adecuado de los datos personales en el Reino Unido

Adoptado el 13 de abril de 2021

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

Historial de versiones

Versión 1.1	6 de julio de 2021	Cambio de formato
Versión 1.0	13 de abril de 2021	Adopción del Dictamen

ÍNDICE

El Comité Europeo de Protección de Datos

Visto el artículo 51, apartado 1, letra g), de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[1] (en lo sucesivo, la «Directiva sobre protección de datos en el ámbito penal»),

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1 RESUMEN

1. La Comisión Europea aprobó su proyecto de Decisión de Ejecución (en lo sucesivo, «proyecto de Decisión») sobre el nivel de protección adecuado de los datos personales por parte del Reino Unido en virtud de la Directiva sobre protección de datos en el ámbito penal el 19 de febrero de 2021[2]. A continuación, la Comisión Europea inició el procedimiento para su adopción formal.

2. En la misma fecha, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos (en lo sucesivo, «CEPD»)[3]. La evaluación por parte del CEPD sobre la adecuación del nivel de protección ofrecido en el Reino Unido se ha realizado basándose en el examen del propio proyecto de Decisión, así como sobre la base de un análisis de la documentación facilitada por la Comisión Europea.

3. El CEPD ha utilizado como referencia principal para este trabajo las referencias sobre adecuación de la Directiva sobre protección de datos en el ámbito penal[4] adoptadas el 2 de febrero de 2021, así como la jurisprudencia pertinente reflejada en sus Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia[5].

4. El principal objetivo del CEPD es emitir un dictamen para la Comisión Europea sobre la adecuación del nivel de protección ofrecido a las personas en el Reino Unido. Es importante reconocer que el CEPD no espera que el marco jurídico del Reino Unido reproduzca la legislación europea en materia de protección de datos.

5. Sin embargo, el CEPD recuerda que para considerar que proporciona un nivel adecuado de protección, el artículo 36 de la Directiva sobre protección de datos en el ámbito penal y la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «TJUE») exigen que la legislación del tercer

[1] DO L 119 de 4.5.2016, p. 89.
[2] Véase el comunicado de prensa de la Comisión Europea, Zona de prensa, Protección de datos: la Comisión Europea pone en marcha el procedimiento sobre los flujos de datos personales al Reino Unido, de 19 de febrero de 2021, https://ec.europa.eu/commission/presscorner/detail/es/ip_21_661.
[3] *Ibidem*.
[4] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, adoptadas el 2 de febrero de 2021, https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_es.pdf.
[5] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_es.pdf.

país se ajuste a la esencia de los principios fundamentales consagrados en dicha Directiva. En el ámbito de la protección de datos, el CEPD observa que existe un gran paralelismo entre el marco de la Directiva y el marco jurídico del Reino Unido sobre determinadas disposiciones básicas como, por ejemplo, conceptos, («datos personales», «tratamiento de datos personales», «responsable del tratamiento de datos»); fundamentos del tratamiento lícito y leal para fines legítimos; limitación de la finalidad; calidad y proporcionalidad de los datos; conservación de datos, seguridad y confidencialidad; transparencia; categorías especiales de datos; decisiones automatizadas y elaboración de perfiles.

6. El CEPD recomienda que la Comisión Europea complemente su análisis con información sobre la existencia de un mecanismo para informar a las autoridades competentes de los Estados miembros pertinentes del tratamiento o la divulgación ulteriores por parte de las autoridades del Reino Unido a las que transfirieron los datos personales y que determine su eficacia en el ordenamiento jurídico británico.

7. El CEPD considera que las disposiciones del capítulo 5 de la parte 3 de la *Data Protection Act 2018* (Ley de Protección de Datos de 2018) (en lo sucesivo, «DPA de 2018»), en principio, proporcionan un nivel de protección que es esencialmente equivalente al garantizado por el Derecho de la UE en lo que respecta a la transferencia de datos personales de una autoridad policial del Reino Unido a un tercer país.

8. Aunque el CEPD toma nota de la capacidad del Reino Unido, en virtud de su marco jurídico, para reconocer a los territorios que ofrecen un nivel adecuado de protección de datos a la luz del marco de protección de datos del Reino Unido, desea destacar que esto podría dar lugar a posibles riesgos para la protección proporcionada a los datos personales transferidos desde la UE, especialmente si en el futuro el marco de protección de datos del Reino Unido se desvía del acervo de la Unión. **Por lo tanto, para las situaciones mencionadas, la Comisión Europea debe cumplir su función de supervisión y, en caso de que no se mantenga el nivel de protección esencialmente equivalente de los datos personales transferidos desde la UE, la Comisión Europea debe considerar la posibilidad de modificar la decisión de adecuación a fin de introducir garantías específicas para los datos transferidos desde la UE, o suspender la decisión de adecuación.**

9. **Por último, en lo que respecta a los acuerdos internacionales celebrados entre el Reino Unido y terceros países,** se invita a la Comisión Europea a que examine la interacción entre el marco de protección de datos del Reino Unido y sus compromisos internacionales, en particular para garantizar la continuidad del nivel de protección cuando los datos personales se transfieren de la UE al Reino Unido sobre la base de la decisión de adecuación del Reino Unido, y posteriormente se transfieren a otros terceros países; y a que supervise de manera continua y adopte medidas, cuando sea necesario, en caso de que la celebración de acuerdos internacionales entre el Reino Unido y terceros países amenace con socavar el nivel de protección de los datos personales previsto en la UE.

10. A este respecto, el CEPD destaca que la entrada en vigor del Acuerdo entre el Reino Unido y los EE. UU. sobre el acceso a los datos electrónicos a efectos de la lucha contra la delincuencia grave [en lo sucesivo, «Acuerdo relativo a la *Clarifying Lawful Overseas Use of Data Act* (CLOUD, Ley estadounidense de aclaración del uso legal de datos en el extranjero), entre el Reino Unido y los EE. UU.»][6] puede afectar a las transferencias ulteriores de las autoridades policiales del Reino Unido,

[6] Véase el *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, Washington DC, EE. UU., 3 de octubre de 2019.

en particular en relación con la emisión y transmisión de órdenes con arreglo al artículo 5 del Acuerdo de la CLOUD Act entre el Reino Unido y los EE. UU.

11. El CEPD también recomienda que la Comisión Europea supervise de manera continua si la celebración de futuros acuerdos con terceros países con fines de cooperación policial, que proporcionen una base jurídica para la transferencia de datos personales a estos países, podría afectar a las condiciones del intercambio ulterior de la información recopilada, en particular si las disposiciones de estos acuerdos internacionales pueden afectar a la aplicación de la legislación de protección de datos del Reino Unido y establecer una mayor limitación o exención en relación con el uso y la divulgación ulteriores en el extranjero de la información recopilada a efectos de aplicación de la ley. El CEPD considera que dicha información y evaluación son esenciales para permitir una revisión exhaustiva del nivel de protección que ofrece el marco legislativo y las prácticas del Reino Unido en relación con la divulgación a otros terceros países.

2 INTRODUCCIÓN

2.1 Marco de protección de datos del Reino Unido

12. El marco de protección de datos del Reino Unido se basa en gran medida en el marco de protección de datos de la UE [en particular, la Directiva sobre protección de datos en el ámbito penal y el Reglamento (UE) 2016/679 el 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 (en lo sucesivo, «RGPD»)], lo que se deriva del hecho de que el Reino Unido fue un Estado miembro de la UE hasta el 31 de enero de 2020. Por otra parte, la DPA de 2018, que entró en vigor el 23 de mayo de 2018 y deroga la *UK Data Protection Act 1998* (Ley de Protección de Datos del Reino Unido de 1998), transpone la Directiva sobre protección de datos en el ámbito penal a través de su parte 3, además de especificar en mayor medida la aplicación del RGPD en el Derecho del Reino Unido y de otorgar poderes e imponer obligaciones a la autoridad nacional de supervisión de la protección de datos, la Oficina del Comisario de Información del Reino Unido (*Information Commissioner's Office*, «ICO»).

13. Como se menciona en el considerando 12 del proyecto de Decisión, el Gobierno del Reino Unido promulgó la *European Union (Withdrawal) Act 2018* (Ley de Retirada de la Unión Europea de 2018), que incorpora la legislación de la UE directamente aplicable al Derecho del Reino Unido. En virtud de esta Ley, los ministros del Reino Unido están facultados para introducir derecho derivado, por medio de instrumentos jurídicos, para realizar las modificaciones necesarias en el Derecho de la Unión conservado como consecuencia de la retirada del Reino Unido de la UE.

14. Por consiguiente, el marco jurídico pertinente aplicable en el Reino Unido una vez finalizado el período de transición[7] está compuesto por:

- El Reglamento General de Protección de Datos del Reino Unido (en lo sucesivo, «RGPD del Reino Unido»), incorporado al Derecho del Reino Unido en virtud de la *European Union (Withdrawal) Act* de 2018, modificado por la normativa *DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019* [Reglamento de 2019 en materia

[7] El periodo de transición se fijó para el 31 de diciembre de 2020, fecha a partir de la cual el Derecho de la Unión deja de aplicarse en el Reino Unido. El «periodo puente» está fijado para el 30 de junio de 2021, a más tardar y se refiere al periodo adicional durante el cual la transmisión de datos personales desde la UE al Reino Unido no se considera transferencia.

de protección de datos, intimidad y comunicaciones electrónicas (enmienda, etc.) (retirada de la UE)];

- la DPA de 2018, modificada por la normativa DPPEC de 2019, y la normativa *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020* [Reglamento de 2020 en materia de protección de datos, privacidad y comunicaciones electrónicas (enmiendas, etc.) (retirada de la UE)] de 2020; y
- la *Investigatory Powers Act* de 2016 (Ley de poderes de investigación, «IPA de 2016»).

(en su conjunto constituyen el «marco de protección de datos del Reino Unido»).

2.2 Alcance de la evaluación del CEPD

15. El proyecto de Decisión de la Comisión Europea es el resultado de una evaluación del marco de protección de datos del Reino Unido, a la que siguieron conversaciones con el Gobierno británico. De conformidad con el artículo 51, apartado 1, letra g), de la Directiva sobre protección de datos en el ámbito penal, el CEPD emitirá un dictamen independiente sobre las conclusiones de la Comisión Europea, identificará las insuficiencias del marco de adecuación, si las hubiera, y se esforzará por formular propuestas para resolverlas.

16. Tal como se menciona en las referencias sobre adecuación de la Directiva de protección de datos en el ámbito penal, «la información ofrecida por la Comisión Europea debe ser exhaustiva y colocar al CEPD en una posición que le permita realizar una evaluación propia con respecto al nivel de protección de datos en el tercer país»[8].

17. A este respecto, cabe señalar que el CEPD solo recibió a tiempo una parte de los documentos pertinentes para el examen del marco jurídico del Reino Unido. El CEPD recibió la mayor parte de la legislación británica mencionada en el proyecto de Decisión a través de los enlaces a los que se hace referencia en este último. La Comisión Europea no pudo proporcionar al CEPD explicaciones y compromisos por escrito del Reino Unido en relación con los intercambios entre las autoridades británicas y la Comisión Europea pertinentes para este ejercicio[9].

18. Teniendo en cuenta lo anterior y debido al limitado plazo (dos meses) de que dispone para adoptar el presente Dictamen, el CEPD ha optado por centrarse en algunos puntos específicos presentados en el proyecto de Decisión y ofrecer su análisis y dictamen al respecto. Al analizar la legislación y la práctica de un tercer país que ha sido Estado miembro de la UE hasta hace poco, es evidente que el CEPD ha reconocido muchos aspectos que son esencialmente equivalentes. En vista de su papel en el proceso

[8] Véanse las Recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartado 15, p. 5.

[9] Estos son los elementos en los que la Comisión Europea se refiere, en su proyecto de Decisión, a las explicaciones de las autoridades británicas sin proporcionar documentos escritos de dichas autoridades que las apoyen, como por ejemplo en lo que respecta a: los efectos de las disposiciones transitorias y la ausencia de una disposición de extinción (considerando 87); ejemplos de consentimiento como base adecuada para el tratamiento (nota a pie de página 68); el término «inexactos» como datos personales «incorrectos o engañosos» (nota a pie de página 79); el mandato del *Intelligence and Security Committee* (ISC) (nota a pie de página 245); el bajo umbral para presentar una denuncia ante el *Investigatory Powers Tribunal* (IPT) y el hecho de que no es inusual que el IPT determine que el denunciante, de hecho, nunca fue objeto de investigación por parte de una autoridad pública (nota a pie de página 263); la combinación de poderes derivados de la legislación y el *common law* (nota a pie de página 52); las prerrogativas ejercidas por el Gobierno (nota a pie de página 62); el hecho de que otras organizaciones pueden decidir libremente si se atienen a los principios del *Code of Practice on the Management of Police Information* (Código de práctica sobre la gestión de la información policial, Código de práctica MoPI) si lo desean (nota a pie de página 86).

de adopción de una decisión de adecuación y la abundancia de legislación y práctica que debe analizarse, el CEPD ha decidido centrar su atención en aquellos aspectos en los que ha considerado que es necesario profundizar.

19. El CEPD tuvo en cuenta el marco europeo de protección de datos aplicable, incluidos los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la «Carta de la UE»), que protegen, respectivamente, el respeto de la vida privada y familiar, el derecho a la protección de los datos de carácter personal y el derecho a la tutela judicial efectiva y a un juez imparcial; y el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, «CEDH») que protege el derecho a la vida privada y familiar. Además de lo anterior, el CEPD consideró los requisitos de la Directiva sobre protección de datos en el ámbito penal, así como la jurisprudencia pertinente.

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

2.3 Observaciones generales y preocupaciones

2.3.1 Compromisos internacionales contraídos por el Reino Unido

21. Con arreglo a lo dispuesto en el artículo 36, apartado 2, letra c), de la Directiva sobre protección de datos en el ámbito penal y las referencias sobre adecuación[12], al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, entre otras cosas, los compromisos internacionales asumidos por el tercer país, u otras obligaciones que deriven de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales, y el cumplimiento de las citadas obligaciones. Asimismo, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con

[10] Véase TJUE, asunto C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 de octubre de 2015, ECLI:EU:C:2015:650, (en lo sucesivo, «Schrems I»), apartados 73-74.
[11] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartado 14, p. 5.
[12] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartado 24, p. 7.

respecto al tratamiento automatizado de datos de carácter personal (en lo sucesivo, «el Convenio 108»)[13] y su Protocolo adicional[14].

22. **A este respecto, el CEPD celebra que el Reino Unido se haya adherido al CEDH y esté sometido a la jurisdicción del Tribunal Europeo de Derechos Humanos («TEDH»). Además, el Reino Unido también se ha adherido al Convenio 108 y a su Protocolo Adicional, firmó el Convenio 108+[15] en 2018 y está trabajando actualmente en su ratificación.**

2.3.2 Posible divergencia futura del marco de protección de datos del Reino Unido

23. Como se menciona en el considerando 171 del proyecto de Decisión, la Comisión Europea debe tener en cuenta que, al finalizar el período de transición previsto en el Acuerdo de Retirada[16], el Reino Unido administra, aplica y hace cumplir su propio régimen de protección de datos y, en cuanto deje de aplicarse la disposición puente[17] en virtud del artículo FINPROV.10A del Acuerdo de Comercio y Cooperación[18], esto puede implicar, en particular, modificaciones o cambios en el marco de protección de datos evaluado en el proyecto de Decisión, así como otras novedades pertinentes.

24. Por ello, la Comisión Europea ha decidido incluir una cláusula de extinción en su proyecto de Decisión[19] y ha fijado la fecha de expiración cuatro años después de su entrada en vigor.

25. Cabe tener en cuenta que la posibilidad de que los ministros y el Secretario de Estado del Reino Unido introduzcan derecho derivado tras el final del periodo puente puede traducirse en una divergencia significativa del marco de protección de datos del Reino Unido con respecto al de la UE en el futuro.

26. Por último, no solo desde el final del período de transición, el Reino Unido deja de estar sometido a la jurisprudencia del TJUE, sino que también las sentencias ya adoptadas del TJUE consideradas como jurisprudencia conservada en el marco jurídico del Reino Unido, podrían dejar de ser vinculantes para el Reino Unido, ya que en particular, el Reino Unido tiene la posibilidad de modificar el Derecho de la Unión conservado tras el final del período de transición y su Tribunal Supremo no está vinculado por ninguna jurisprudencia de la UE conservada[20].

27. **Teniendo en cuenta los riesgos relacionados con la posible desviación del marco de protección de datos del Reino Unido del acervo de la Unión una vez finalizado el «período puente», el CEPD acoge**

[13] Véase el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Convenio 108, de 28 de enero de 1981.
[14] Véase el Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, abierto a la firma el 8 de noviembre de 2001.
[15] Véase el Protocolo que modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en lo sucesivo, «Convenio 108+»), de 18 de mayo de 2018.
[16] Véase el Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica (DO L 029 de 31.1.2020, p. 7).
[17] El periodo de transición se fijó para el 31 de diciembre de 2020, fecha a partir de la cual el Derecho de la Unión deja de aplicarse en el Reino Unido. El «periodo puente» está fijado para el 30 de junio de 2021, a más tardar, y se refiere al periodo adicional durante el cual la transmisión de datos personales desde la UE al Reino Unido no se considera una transferencia.
[18] Véase el Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra (DO L 444 de 31.12.2020, p. 14).
[19] Véase el Véase el artículo 4 del proyecto de Decisión. Véase igualmente el considerando 172 del proyecto de Decisión.
[20] Véase la sección 6, apartados 3 a 6, de la *EU (Withdrawal) Act* de 2018.

con satisfacción la decisión de la Comisión Europea de introducir una cláusula de extinción de cuatro años para el proyecto de Decisión. Sin embargo, el CEPD quiere destacar aquí la importancia del papel de supervisión de la Comisión Europea[21]. De hecho, la Comisión Europea debe supervisar todos los cambios importantes en el Reino Unido que puedan afectar a la equivalencia esencial del nivel de protección de los datos personales transferidos en virtud de la decisión de adecuación del Reino Unido de forma continua y permanente desde su entrada en vigor. Además, la Comisión Europea debe tomar las medidas oportunas suspendiendo, modificando o derogando la decisión de adecuación en función de las circunstancias que se presenten si, después de la adopción de dicha decisión, la Comisión Europea tiene indicios de que ya no se garantiza un nivel de protección adecuado en el Reino Unido.

28. Por su parte, el CEPD hará todo lo posible para informar a la Comisión Europea sobre cualquier acción pertinente emprendida por las autoridades de control de la protección de datos de los Estados miembros (en lo sucesivo, «autoridades de control»), y en particular sobre las reclamaciones presentadas por los interesados en la UE en relación con la transferencia de datos personales de la UE al Reino Unido.

3 NORMAS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LAS AUTORIDADES COMPETENTES A EFECTOS DE CONTROL DE LA APLICACIÓN DEL DERECHO PENAL

3.1 Ámbito de aplicación material

29. En relación con los considerandos 24 y siguientes del proyecto de Decisión, el CEPD observa que el proyecto de decisión de adecuación no contiene muchos detalles sobre las actividades y el marco jurídico aplicable a los organismos distintos de la policía que tienen funciones policiales.

30. Por ejemplo, la sección F del *UK Explanatory Framework for Adequacy Discussions*: *Law Enforcement*[22], sugiere en la página 11 que **la *National Crime Agency*** (Agencia contra el Crimen, «NCA») podría ser un servicio policial de especial interés, que, entre otras cosas, tiene una función general de inteligencia criminal. La NCA describe su misión como la de reunir información de una serie de fuentes con el fin de maximizar el análisis, la evaluación y las oportunidades tácticas, incluida la interceptación técnica de las comunicaciones, los socios de las fuerzas de seguridad en el Reino Unido y en el extranjero, y las agencias de seguridad e inteligencia[23]. La NCA es también uno de los principales interlocutores para la colaboración policial internacional y desempeña un papel fundamental en el intercambio de información criminal[24].

[21] Véase el artículo 36, apartado 4, de la Directiva sobre protección de datos en el ámbito penal.

[22] Véase la sección F del *UK Government, Explanatory Framework for Adequacy Discussions*: Law Enforcement, de 13 de marzo de 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[23] Véase el sitio web de la National Crime Agency, *Intelligence: enhancing the picture of serious organised crime affecting the UK* (Inteligencia: mejorar el panorama de la delincuencia organizada grave que afecta al Reino Unido), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[24] Aunque no toda la información que trata la NCA son datos personales, una parte importante podría serlo y las actividades aquí descritas difieren de las tareas policiales clásicas, por lo que una evaluación del acceso a los

31. El CEPD también toma nota del hecho de que el *Government Communications Headquarters* (Centro Gubernamental de Comunicaciones, «GCHQ»), cuyas actividades suelen entrar en el ámbito de la parte 4 de la DPA de 2018, es decir, la seguridad nacional, asume también un papel activo en la reducción del daño social y financiero que la delincuencia grave y organizada causa al Reino Unido, y trabaja estrechamente con el Ministerio del Interior, la NCA, la Agencia Tributaria británica (*HM Revenue and Customs*, «HMRC»), y otros departamentos gubernamentales[25]. Sus actividades están relacionadas con la lucha contra los abusos sexuales de menores, el fraude, otros tipos de delitos económicos, incluido el blanqueo de capitales, el uso delictivo de la tecnología, la delincuencia informática, la inmigración ilegal organizada, incluido el tráfico de personas, estupefacientes y armas de fuego, así como otras actividades ilícitas de contrabando.

32. **El CEPD pide a la Comisión Europea que complemente su análisis con un análisis de las agencias activas en el ámbito de la aplicación de la ley que parecen haber hecho de la recopilación y el análisis de datos, incluidos los datos personales, un elemento central de sus operaciones cotidianas, en particular la NCA. Además, el CEPD invita a la Comisión a examinar más de cerca las agencias como el GCHQ, cuyas actividades entran en el ámbito de la aplicación de la ley y de la seguridad nacional, y el marco jurídico que les es aplicable para el tratamiento de datos personales.**

3.2 Salvaguardias, derechos y obligaciones

3.2.1 Tratamiento sobre la base del «consentimiento» del interesado

33. El CEPD toma nota de que la Comisión Europea afirma en los considerandos 37 y 38 del proyecto de Decisión que **ampararse en el consentimiento** no se considera pertinente en una situación de adecuación, ya que en las situaciones de transferencia los datos no los recoge directamente de un interesado una autoridad policial del Reino Unido sobre la base del consentimiento.

34. A este respecto, el CEPD recuerda que el artículo 36, apartado 2, letra a), de la Directiva sobre protección de datos en el ámbito penal exige evaluar una amplia gama de elementos que no se limitan a la situación de la transferencia, como «el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluidas [...] el Derecho penal».

35. El consentimiento en el contexto de la aplicación de las leyes puede ser pertinente como base jurídica para el tratamiento de datos, como garantía adicional o, de forma más general, como base para ejecutar los poderes de investigación que permiten obtener datos personales, por ejemplo, el consentimiento de un tercero para registrar sus instalaciones o para incautar la memoria de datos.

---

datos personales por parte de las fuerzas del orden en el Reino Unido estaría incompleta si no se evaluaran a fondo las actividades de la NCA. Parece razonable asegurarse de que a los principios de protección de datos se les otorgue el mismo significado en todos los servicios encargados de la ejecución de las leyes pertinentes, arrojando así luz sobre un organismo especialmente orientado a los datos como la NCA. Además, al «mirar hacia el futuro», la explicación continúa y añade que se buscan continuamente nuevas oportunidades para recopilar, desarrollar y mejorar las capacidades tradicionales con el fin de aumentar la cantidad y la calidad de la inteligencia disponible para explotar tanto en el Reino Unido como en el extranjero. «Como parte de ello, se está desarrollando la nueva Capacidad Nacional de Explotación de Datos, utilizando los poderes conferidos a la agencia por la Ley de Delitos y Tribunales (*Crime and Courts Act*), para enlazar los datos en poder de todos los niveles del Gobierno, acceder a ello y explotarlos». [...] «Todo esto aumentará la agilidad y flexibilidad para responder a las nuevas amenazas y operar de forma proactiva, para recopilar y analizar información e inteligencia sobre las amenazas emergentes, de modo que sea posible actuar antes de que las amenazas se hagan realidad».

[25] Véase el sitio web del GCHQ, *Mission, Serious and Organised Crime*, https://www.gchq.gov.uk/section/mission/serious-crime.

36. El CEPD observa, basándose también en la información proporcionada por la Comisión Europea en el considerando 38 del proyecto de Decisión, que el uso del consentimiento, tal como se enmarca en el régimen del Reino Unido, requeriría siempre una base jurídica en la que ampararse. Esto significa que, aunque la policía tenga poderes legales para tratar los datos a efectos de una investigación, en determinadas circunstancias específicas (por ejemplo, para recoger una muestra de ADN), la policía puede considerar apropiado pedir el consentimiento del interesado.

37. **El CEPD invita a la Comisión Europea a analizar, como norma, el posible uso del consentimiento en un contexto de aplicación de las leyes a la hora de evaluar la idoneidad de un tercer país en el marco de la Directiva.**

3.2.2 Derechos individuales

3.2.2.1 Certificados de seguridad nacional

38. Según la sección 79 de la DPA de 2018, los responsables del tratamiento pueden solicitar certificados de seguridad nacional emitidos por un ministro, un miembro del gabinete, el Fiscal General o el Abogado General de Escocia, que certifiquen que las limitaciones de las obligaciones y los derechos consagrados en los capítulos 3 y 4 de la parte 3 de la DPA de 2018 son una medida necesaria y proporcionada para la protección de la seguridad nacional.

39. Estos certificados tienen como objetivo ofrecer a los responsables del tratamiento una mayor seguridad jurídica y serán una prueba concluyente de que la seguridad nacional es un factor que se debe tener en cuenta a la hora de tratar datos personales. Sin embargo, cabe mencionar que estos certificados no son necesarios para acogerse a las restricciones de seguridad nacional, sino que constituyen una medida de transparencia[26].

40. El CEPD entiende, a partir del anexo 20 de la DPA de 2018, secciones 17 y 18, que un certificado de seguridad nacional emitido en virtud de la Ley de Protección de Datos de 1998 (en lo sucesivo, «antiguo certificado») surtía efecto de manera ampliada para el tratamiento de datos personales en virtud de la DPA de 2018 hasta el 25 de mayo de 2019. Hasta esta fecha, a menos que se hubieran sustituido o revocado, los antiguos certificados se trataban como si se hubieran emitido conforme a la DPA de 2018. Sin embargo, cuando en un certificado de seguridad nacional expedido en virtud de la Ley de Protección de Datos de 1998 no se indica una fecha de vencimiento expresa, el CEPD entiende que dicho certificado seguirá surtiendo efecto en relación con el tratamiento en virtud de dicha Ley, a menos que se revoque o anule[27]. Aunque la protección que ofrecen estos antiguos certificados se limita al tratamiento de datos personales en virtud de la Ley de Protección de Datos de 1998, el CEPD toma nota del hecho de que se pueden expedir nuevos certificados de seguridad nacional en virtud de dicha Ley para los datos personales que se trataron en virtud de la misma[28].

---

[26] Véase Ministerio del Interior del Reino Unido, *The Data Protection Act 2018, National Security Certificates Guidance* (La ley de protección de datos de 2018, orientación sobre los certificados de seguridad nacional), de agosto de 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, p. 4.

[27] Véase Ministerio del Interior del Reino Unido, *The Data Protection Act 2018, National Security Certificates Guidance* (La ley de protección de datos de 2018, orientación sobre los certificados de seguridad nacional), de agosto de 2020, p. 5.

[28] Véase Ministerio del Interior del Reino Unido, *The Data Protection Act 2018, National Security Certificates Guidance* (La ley de protección de datos de 2018, orientación sobre los certificados de seguridad nacional), de agosto de 2020, p. 5.

41. **En aras de la exhaustividad, el CEPD invita a la Comisión Europea a que aclare en su proyecto de decisión de adecuación que los certificados de seguridad nacional pueden seguir emitiéndose en virtud de la Ley de Protección de Datos de 1998. Además, el CEPD invita a la Comisión Europea a que describa en su proyecto de decisión de adecuación los mecanismos de recurso y supervisión en relación con los certificados expedidos en virtud de la Ley de Protección de Datos de 1998. Por último, el CEPD invita a la Comisión Europea a que incluya en su proyecto de decisión de adecuación el número de certificados existentes expedidos en virtud de la Ley de Protección de Datos de 1998, y a que supervise atentamente este aspecto.**

3.2.2.2 Mecanismo de decisión automatizado en virtud de la Directiva

42. El CEPD subraya que el artículo 11, apartado 3, de la Directiva sobre protección de datos en el ámbito penal prohíbe la elaboración de perfiles que dé lugar a discriminación de las personas físicas basándose en categorías especiales de datos personales. Sin embargo, el CEPD señala que la sección 50 de la DPA de 2018, que establece las normas específicas para las decisiones automatizadas, no prevé tal prohibición.

43. **Por lo tanto, el CEPD invita a la Comisión Europea a verificar este punto, y a exponer explícitamente sus conclusiones en su decisión de adecuación. Además, el CEPD invita a la Comisión Europea a seguir de cerca los casos relacionados con las decisiones automatizadas y la elaboración de perfiles.**

44. Según las referencias de adecuación de la Directiva de protección de datos en el ámbito penal, «[e]n cualquier caso, el Derecho del tercer país debe establecer las garantías necesarias para los derechos y libertades del interesado. A este respecto, también debe tenerse en cuenta la existencia de un mecanismo para informar a las autoridades competentes del Estado miembro correspondiente de cualquier tratamiento ulterior, como el uso de los datos transferidos para la elaboración de perfiles a gran escala»[29].

45. **El CEPD invita a la Comisión a evaluar este elemento a la luz de las orientaciones ofrecidas por el CEPD en sus referencias.**

3.2.3 Transferencias ulteriores

46. Según las referencias de adecuación de la Directiva de protección de datos en el ámbito penal, las transferencias ulteriores de datos personales por parte del destinatario inicial a otro tercer país u organización internacional no deben socavar el nivel de protección, previsto en la Unión, de las personas físicas cuyos datos se transfieren. Por lo tanto, estas transferencias de datos solo deben permitirse cuando se garantice la continuidad del nivel de protección que ofrece el Derecho de la UE. El CEPD considera que, como señala la Comisión Europea en su evaluación, las disposiciones del capítulo 5 de la parte 3 de la DPA de 2018, y en particular su sección 73, en principio proporcionan un nivel de protección que es esencialmente equivalente al garantizado por el Derecho de la UE por lo que respecta a la transferencia de datos personales de una autoridad policial del Reino Unido a un tercer país.

47. En primer lugar, la sección 73, apartado 1, letra b), de la DPA de 2018 establece, en particular, que un responsable del tratamiento no puede transferir datos personales a un tercer país o a una organización internacional salvo «en casos en los que los datos personales hayan sido transmitidos originalmente o puestos a disposición del responsable del tratamiento o de otra autoridad competente por un Estado miembro distinto del Reino Unido y ese Estado miembro, o cualquier persona con sede en ese Estado

[29] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartados 59-61.

miembro que sea una autoridad competente a efectos de la Directiva sobre protección de datos en el ámbito penal, haya autorizado la transferencia de conformidad con la legislación del Estado miembro». Estas disposiciones parecen estar en consonancia con las referencias de adecuación de la Directiva de protección de datos en el ámbito penal, que establece que también debe tenerse en cuenta la existencia de un mecanismo para informar a las autoridades competentes del Estado miembro en cuestión para que autoricen dicha transferencia ulterior de datos. El destinatario inicial de los datos transferidos desde la UE debe ser responsable y poder demostrar que la autoridad competente pertinente del Estado miembro ha autorizado la transferencia ulterior y que se ofrecen las garantías adecuadas para las transferencias ulteriores de datos en ausencia de una decisión de adecuación relativa al tercer país al que se transferirían los datos. «En este contexto, debe tenerse en cuenta la existencia de una obligación o un compromiso de aplicar los códigos de tratamiento pertinentes definidos por las autoridades de los Estados miembros que realizan la transferencia»[30].

48. **El CEPD invita a la Comisión a evaluar este elemento a la luz de las orientaciones ofrecidas por el CEPD en sus referencias de adecuación de la Directiva sobre protección de datos en el ámbito penal.**

49. En segundo lugar, como se explica en el considerando 81 del proyecto de Decisión, el Secretario de Estado del Reino Unido tiene la facultad de reconocer a un tercer país (o a un territorio o sector dentro de un tercer país), a una organización internacional o a una descripción de dicho país, territorio, sector u organización como garantía de un nivel adecuado de protección de los datos personales, previa consulta a la ICO[31]. Al evaluar la idoneidad del nivel de protección, el Secretario de Estado debe tener en cuenta los mismos elementos que la Comisión Europea debe evaluar con arreglo al artículo 36, apartado 2, letras a) a c), de la Directiva sobre protección de datos en el ámbito penal, interpretado junto con su recital 67 y la jurisprudencia de la Unión conservada. Esto significa que, al evaluar el nivel adecuado de protección de un tercer país, el criterio pertinente será si ese tercer país en cuestión garantiza un nivel de protección «esencialmente equivalente» al garantizado en el Reino Unido. Aunque el CEPD toma nota de la capacidad del Reino Unido, en virtud de la DPA de 2018, para reconocer a los territorios que ofrecen un nivel adecuado de protección a la luz del marco de protección de datos del Reino Unido, desea destacar que estos últimos territorios podrían no beneficiarse, hasta la fecha, de una decisión de adecuación emitida por la Comisión Europea que reconozca un nivel de protección «esencialmente equivalente» al garantizado en la UE. Esto podría dar lugar a posibles riesgos para la protección que se proporciona a los datos personales transferidos desde la UE, especialmente si el marco de protección de datos del Reino Unido se desviara del acervo de la Unión en el futuro. Cabe señalar que en julio de 2020, el asunto emblemático del TJUE, Schrems II[32], dio lugar a la invalidación de la decisión sobre el Escudo de la privacidad de los Estados Unidos ya que, según el TJUE, no se podía considerar que el marco jurídico estadounidense proporcionara un nivel de protección esencialmente equivalente en comparación con el de la UE. Sin embargo, las sentencias ya adoptadas del TJUE, consideradas como jurisprudencia conservada en el marco jurídico del Reino Unido, podrían dejar de ser vinculantes para el Reino Unido, ya que, en particular, el Reino Unido tiene la posibilidad de modificar el Derecho de la Unión conservado tras el final del período de transición y su Tribunal Supremo no está vinculado por ninguna jurisprudencia de la UE conservada[33].

[30] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartados 55-56.
[31] Véase la sección 182, apartado 2, de la DPA de 2018. Véase también el memorando de entendimiento sobre el papel de la ICO en relación con las nuevas evaluaciones de adecuación del Reino Unido, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[32] Véase el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, 16 de julio de 2020, ECLI:EU:C:2020:559, (en lo sucesivo, «Schrems II»).
[33] Véase la sección 6, apartados 3 a 6, de la *EU (Withdrawal) Act* de 2018.

50. **Por lo tanto, el CEPD invita a la Comisión Europea a supervisar de cerca el proceso y los criterios de evaluación de la adecuación por parte de las autoridades del Reino Unido con respecto a otros terceros países, en particular con respecto a terceros países no reconocidos por la UE como adecuados en virtud de la Directiva sobre protección de datos en el ámbito penal.**

51. En caso de que la Comisión Europea estimara que el tercer país considerado adecuado por el Reino Unido no garantiza un nivel de protección esencialmente equivalente al garantizado dentro de la UE, según el artículo 36 de la Directiva sobre protección de datos en el ámbito penal, **el CEPD invita a la Comisión Europea a tomar todas las medidas necesarias como, por ejemplo, modificar la decisión de adecuación del Reino Unido para introducir salvaguardias específicas para los datos personales procedentes de la UE, o considerar la suspensión de la decisión de adecuación del Reino Unido, cuando los datos personales transferidos desde la UE al Reino Unido sean objeto de transferencias ulteriores al tercer país en cuestión sobre la base de un reglamento de adecuación del Reino Unido**.

52. **Por último, en relación con los acuerdos internacionales celebrados, o que se celebren en el futuro, por el Reino Unido y el posible acceso por parte de las autoridades de terceros países que sean parte de dichos acuerdos a los datos personales de la UE, el CEPD recomienda que la Comisión Europea examine la interacción entre el marco de protección de datos del Reino Unido y sus compromisos internacionales, en particular para garantizar la continuidad del nivel de protección en caso de transferencias ulteriores a otros terceros países de datos personales transferidos de la UE al Reino Unido sobre la base de una decisión de adecuación del Reino Unido; y a que supervise de manera continua y adopte medidas, cuando sea necesario, con respecto a la celebración de acuerdos internacionales entre el Reino Unido y terceros países que amenacen con socavar el nivel de protección de los datos personales previsto en la UE**. Por ejemplo, mientras que la Comisión Europea se ha referido al hecho de que el Acuerdo sobre la Ley CLOUD entre el Reino Unido y los Estados Unidos[34] puede afectar a las transferencias ulteriores hacia los Estados Unidos desde proveedores de servicios en el Reino Unido, **el CEPD destaca que la entrada en vigor de este Acuerdo también puede afectar a las transferencias ulteriores desde las autoridades policiales en el Reino Unido, en particular en relación con la emisión y transmisión de órdenes según el artículo 5 del Acuerdo sobre la Ley CLOUD entre el Reino Unido y los Estados Unidos.**

53. El CEPD también considera que la celebración de futuros acuerdos con terceros países con fines de cooperación policial que proporcionen una base jurídica para la transferencia de datos personales a estos países también puede afectar significativamente a las condiciones de intercambio ulterior de la información recogida, ya que dichos acuerdos pueden afectar al marco jurídico de protección de datos del Reino Unido tal como se ha evaluado.

54. **Por lo tanto, el CEPD recomienda que la Comisión Europea supervise continuamente si la celebración de futuros acuerdos entre el Reino Unido y terceros países puede afectar a la aplicación de la legislación británica en materia de protección de datos, y prevea una mayor limitación o exención en relación con el intercambio ulterior y el uso y la divulgación ulteriores en el extranjero de la información recopilada a efectos de aplicación de la ley. El CEPD considera que dicha información y evaluación son esenciales para permitir una revisión exhaustiva del nivel de protección que ofrece el marco legislativo y las prácticas del Reino Unido en relación con la divulgación a otros terceros países.**

[34] Véase el *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, Washington DC, EE. UU., 3 de octubre de 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

55. Por último, el CEPD toma nota de que, de conformidad con la sección 76, apartado 4, letra b), de la DPA de 2018 (transferencias sobre la base de circunstancias especiales), las autoridades policiales del Reino Unido pueden transferir datos personales a un tercer país o a una organización internacional cuando la transferencia sea necesaria «para obtener asesoramiento jurídico en relación con cualquiera de los fines de aplicación de la ley». **El CEPD subraya que el artículo 38 de la Directiva sobre protección de datos en el ámbito penal no contiene una disposición correspondiente; por lo tanto, invita a la Comisión Europea a que aclare qué se entiende por asesoramiento jurídico y qué tipo de datos personales se intercambian en estos casos.**

3.2.4 Tratamiento ulterior, incluido el intercambio ulterior de datos por razones de seguridad nacional

56. En sus referencias de adecuación de la Directiva sobre protección de datos en el ámbito penal, el CEPD había señalado que, en cuanto al cuanto al tratamiento ulterior o la comunicación de los datos transferidos desde la UE con fines distintos a los de aplicación de la ley, por ejemplo, por razones de seguridad nacional, también deben estar previstos por la ley, ser necesarios y proporcionados. Tal y como evalúa la Comisión Europea en su proyecto de Decisión, el artículo 36, apartado 3, de la DPA de 2018, la *Digital Economy Act* (Ley de Economía Digital) de 2017, la *Crime and Courts Act* (Ley de Delitos y Tribunales) de 2013 y la *Serious Crime Act* (Ley de Delitos Graves) de 2017 sí contemplan un marco jurídico claro que permite el intercambio ulterior de datos, siempre y cuando dicho intercambio se ajuste a las normas establecidas en la DPA de 2018.

57. El CEPD observa que, en el contexto del tratamiento ulterior de los datos transferidos desde la UE con fines distintos a los de aplicación de la ley, la Comisión Europea no ha evaluado si existen mecanismos para que las autoridades policiales del Reino Unido informen a las autoridades competentes de los Estados miembros correspondientes de un posible tratamiento ulterior de los datos. Sin embargo, las referencias de adecuación de la Directiva sobre protección de datos en el ámbito penal lo consideran un elemento que se debe tener en cuenta[35]. Además, la existencia de dicho mecanismo para informar a las autoridades competentes de los Estados miembros pertinentes sobre el tratamiento de datos ulterior con fines de aplicación de la ley también se considera un elemento que debe tenerse en cuenta en el marco de las referencias de adecuación de la Directiva sobre protección de datos en el ámbito penal[36].

58. **El CEPD invita, por tanto, a la Comisión Europea a complementar su análisis con información sobre la existencia de mecanismos para que las autoridades policiales del Reino Unido notifiquen a las autoridades competentes de los Estados miembros pertinentes un posible tratamiento ulterior de los datos transferidos desde la UE.**

59. Asimismo, en relación al intercambio por razones de seguridad nacional de datos recogidos por parte de una autoridad policial con un servicio de inteligencia, la base jurídica que autoriza dicho intercambio es la *Counter Terrorism Act* (Ley de Lucha contra el Terrorismo) de 2008. A este respecto, el CEPD observa que el ámbito de aplicación y las disposiciones de la sección 19 de la *Counter Terrorism Act* de 2008 no se abordan plenamente en la evaluación de la Comisión Europea y puede implicar un uso más amplio, en particular en lo que respecta a la sección 19, apartado 2, de dicha Ley que establece que «la información obtenida por cualquiera de los servicios de inteligencia en relación con el ejercicio de cualquiera de sus funciones puede ser utilizada por dicho servicio en relación con el ejercicio de cualquiera de sus otras funciones». A este respecto, el CEPD subraya que, una vez han sido objeto de

[35] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartado 41 y nota a pie de página 39.
[36] Véanse las Recomendaciones 01/2021 del CEPD relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, apartado 40.

tratamiento ulterior o se han comunicado, los datos deben gozar del mismo nivel de protección que cuando fueron tratados inicialmente por la autoridad competente receptora.

3.3 Supervisión y control de la aplicación de la normativa

60. El CEPD señala que la supervisión de las autoridades policiales está garantizada por una combinación de diferentes comisarios (*Commissioners*), además de la ICO. El proyecto de decisión de adecuación menciona al *Investigatory Powers Commissioner* (Comisario de Poderes de Investigación, «IPC»), al *Commissioner for the Retention and Use of Biometric Material* (Comisario de Retención y Uso de Material Biométrico), así como al *Surveillance Camera Commissioner* (Comisario de Cámaras de Vigilancia). En este contexto, cabe señalar que el TJUE ha subrayado en repetidas ocasiones la necesidad de una supervisión independiente. El IPC reviste especial importancia en las cuestiones de acceso a los datos personales transferidos al Reino Unido. El CEPD entiende que el IPC constituye una especie de *judicial commissioner* («comisario judicial»), igual que otros comisarios judiciales, a los que hay que referirse en el contexto del capítulo de seguridad nacional, y que dichos comisarios judiciales gozan de la independencia de los jueces, también cuando actúan como comisarios. En cuanto a la oficina del IPC, la Comisión Europea explica en el considerando 245 del proyecto de Decisión que actúa de forma independiente como un denominado «organismo de libre competencia» (*arm's length body*), aunque está financiado por el Ministerio del Interior.

61. Además, el IPC también es competente para la supervisión *a posteriori* de las medidas de vigilancia. Sin embargo, parece que en esta función el cometido del IPC es formular recomendaciones en casos de incumplimiento, e informar al interesado, si el error es grave y es de interés público que la persona sea informada.

62. El CEPD no ha encontrado en el proyecto de decisión más indicaciones para evaluar la independencia del Comisario de Retención y Uso de Material Biométrico ni del Comisario de Cámaras de Vigilancia.

63. **Se invita a la Comisión Europea a que siga evaluando la independencia de los comisarios judiciales, también en los casos en que el comisario no ejerza (ya) como juez, así como a que evalúe la independencia del Comisario de Retención y Uso de Material Biométrico, y la del Comisario de Cámaras de Vigilancia.**