Dictamen 14/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con el Reglamento (UE) 2016/679 sobre el nivel de protección adecuado de los datos personales en el Reino Unido

Adoptado el 13 de abril de 2021

ÍNDICE

El Comité Europeo de Protección de Datos

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

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

Vistos los artículos 12 y 22 de su Reglamento interno,

HA APROBADO 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 del RGPD 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 se centró en la evaluación tanto de los aspectos generales relativos al RGPD del proyecto de Decisión como en el acceso, por parte de las autoridades públicas, a los datos personales transferidos desde el EEE con fines de aplicación de las leyes y de seguridad nacional, y en particular los recursos legales disponibles para las personas dentro del EEE. El CEPD también analizó si las salvaguardias previstas en el marco jurídico de Reino Unido han sido implantadas y son efectivas.

[1] Las referencias a los «Estados miembros» en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».
[2] Véase el comunicado de prensa de la Comisión Europea, «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] Véase la nota 2.

4. El CEPD ha utilizado como referencia principal para este trabajo el documento relativo a las referencias sobre adecuación con arreglo al RGPD[4] adoptado en febrero de 2018, así como las Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia[5].

[4] Véase Grupo de trabajo del artículo 29, «Referencias sobre adecuación», aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, WP254 rev.01 (adoptado por el CEPD, véase https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (en lo sucesivo, «documento relativo a las referencias sobre adecuación con arreglo al RGPD»).

[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/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_es.

1.1. Ámbitos de convergencia

5. 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.

6. Sin embargo, el CEPD recuerda que, para considerar que se proporciona un nivel adecuado de protección, el artículo 45 del RGPD y la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «TJUE») exigen que la legislación del tercer país se ajuste a la esencia de los principios fundamentales consagrados en dicho Reglamento. El marco de protección de datos de Reino Unido se basa en gran medida en el de la Unión [y particularmente, en el RGPD y en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, en lo sucesivo, «Directiva sobre protección de datos en el ámbito penal»], lo cual se debe a que Reino Unido fue un Estado miembro de la UE hasta el 31 de enero de 2020. Por otra parte, la *Data Protection Act 2018* (Ley de protección de datos de 2018) de Reino Unido, que entró en vigor el 23 de mayo de 2018 y deroga la *Data Protection Act 1998* (Ley de protección de datos de 1998), especifica en mayor medida la aplicación del RGPD en el Derecho del Reino Unido, además de transponer la Directiva sobre protección de datos en el ámbito penal, y otorga poderes e impone obligaciones a la autoridad nacional de supervisión de la protección de datos, la UK Information Commissioner's Office (Oficina del Comisario de Información del Reino Unido, en lo sucesivo «ICO», por sus siglas en inglés). Por tanto, el CEPD reconoce que el marco de protección de datos de Reino Unido es, mayoritariamente, un reflejo del RGPD.

7. **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 sustancialmente equivalentes.**

8. En el ámbito de la protección de datos, el CEPD observa que existe un gran paralelismo entre el marco del RGPD y el marco jurídico del Reino Unido respecto a determinadas disposiciones básicas como, por ejemplo, conceptos («datos personales», «tratamiento de datos personales», «responsable del tratamiento»); motivos para el tratamiento lícito y equitativo para fines legítimos; limitación de la finalidad; calidad de los datos y proporcionalidad; conservación de datos, seguridad y confidencialidad; transparencia; categorías especiales de datos; mercadotecnia directa; decisiones automatizadas y elaboración de perfiles.

1.2. Desafíos

9. El Reino Unido fue, hasta hace poco, un Estado miembro de la UE; por tanto, al analizar la legislación y la práctica, el CEPD ha constatado que muchos aspectos son sustancialmente equivalentes. Al mismo tiempo, habida cuenta de su papel en el proceso de la decisión de adecuación, así como de las limitaciones temporales, el CEPD ha resuelto centrar su atención en los aspectos en los que considera que es necesario un examen más profundo y detallado.

10. Sin embargo, sigue habiendo desafíos, y el CEPD considera que los siguientes aspectos deben estudiarse en mayor detalle para garantizar el cumplimiento de un nivel de protección sustancialmente equivalente, y deben ser supervisados con atención en el Reino Unido por parte de la Comisión.

1.2.1. Aspectos generales

11. El primer desafío, de carácter general, tiene que ver con el seguimiento de la evolución de todo el sistema jurídico del Reino Unido en materia de protección de datos. De hecho, el Gobierno de Reino Unido ha señalado su intención de desarrollar políticas separadas e independientes a este respecto, y es posible que pretenda apartarse de la legislación de protección de datos de la Unión. Estas declaraciones políticas todavía no se han materializado en el marco jurídico del país. Sin embargo, esta posible **divergencia futura puede crear riesgos para el mantenimiento del nivel de protección que se ofrece a los datos personales transferidos desde la UE. En vista de esto, se invita a la Comisión Europea a realizar un estrecho seguimiento de la situación desde la entrada en vigor de su decisión de adecuación, así como a tomar las medidas necesarias, incluidas la modificación o suspensión de la decisión si fuese necesario.**

1.2.2. Aspectos generales de protección de datos

12. En primer lugar, la denominada «**exención para el control de la inmigración**», establecida en el **anexo 2 de la *Data Protection Act 2018*, parte 1**, apartado 4, **está formulada de forma muy «amplia»**. Concretamente, esta exención se aplica también cuando los datos personales no fueron recogidos por parte del responsable del tratamiento con fines de control de la inmigración, pero este responsable los pone a disposición de otro que los trata con tales fines.

13. El CEPD invita a la Comisión Europea a verificar el estado actual del asunto *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* y, dado que la sentencia no es firme (*res iudicata*), comprobar si la instancia superior la confirma o la reexamina, teniendo en cuenta cualquier actualización en este sentido y especificándola en la decisión. **El CEPD también insta a la Comisión Europea a que aporte, en su decisión de adecuación, información adicional sobre la exención para el control de la inmigración[6], particularmente en lo relativo a la necesidad y proporcionalidad de una exención tan amplia en el Derecho de Reino Unido, en especial teniendo en cuenta el gran ámbito de aplicación *ratione personae*.** Al mismo tiempo, el CEPD invita a la Comisión a seguir estudiando si existen o se pueden esperar salvaguardias adicionales en el marco jurídico del Reino Unido, por ejemplo, a través de instrumentos jurídicamente vinculantes que complementen la exención para el control de la inmigración mejorando su previsibilidad y las salvaguardias para los interesados, además de permitir una evaluación y seguimiento más idóneos y oportunos de los requisitos de necesidad y proporcionalidad.

14. En segundo lugar, aunque reconoce que el marco de protección de datos del Reino Unido recoge la mayoría del capítulo V del RGPD, el CEPD ha detectado algunos aspectos del marco jurídico del país **respecto a las transferencias ulteriores** que podrían menoscabar el nivel de protección de los datos personales transferidos desde el EEE.

[6] También como resultado de la revisión en curso sobre el uso de la exención para el control de la inmigración mencionada en la página 5 del *Explanatory Framework for Adequacy Discussions* (Marco explicativo para las discusiones de adecuación) del Gobierno de Reino Unido, sección E3: Restricciones del anexo 2, 13 de marzo de 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

15. De hecho, el artículo 44 del RGPD[7] establece que solo se realizarán transferencias de datos personales, incluidas las transferencias ulteriores, cuando estas no menoscaben el nivel de protección de las personas físicas garantizado por el RGPD. **Esto no solo quiere decir que la legislación de Reino Unido será «sustancialmente equivalente» a la de la Unión en lo relativo al tratamiento de los datos personales transferidos al Reino Unido en virtud de la futura decisión de adecuación, sino también que las normas aplicables en el Reino Unido respecto a la transferencia ulterior de dichos datos a países terceros deberán garantizar el mantenimiento de un nivel de protección sustancialmente equivalente.**

16. Aunque el CEPD reconoce la capacidad del Reino Unido, en virtud de su marco jurídico, para identificar 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 «sustancialmente equivalente» al garantizado en el EEE. Esto podría dar lugar a posibles riesgos para la protección que se proporciona a los datos personales transferidos desde el EEE, especialmente si, en el futuro, el marco de protección de datos del Reino Unido se desvía del acervo de la Unión. Además, el Reino Unido ya ha reconocido la adecuación de terceros países que cuentan con una decisión de adecuación de la Comisión Europea en virtud de la Directiva 95/46/CE[8], mientras que la Comisión revisara próximamente estas conclusiones, sin que se conozcan todavía las conclusiones de dicha revisión.

17. **Respecto a las situaciones mencionadas, la Comisión Europea debe cumplir su función de supervisión y, en caso de que no se mantenga el nivel de protección sustancialmente equivalente de los datos personales transferidos desde el EEE, considerar la posibilidad de modificar la decisión de adecuación a fin de introducir salvaguardias específicas para los datos transferidos desde el EEE o suspender la decisión de adecuación.**

18. **Por 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 más allá del acuerdo sobre el acceso a los datos electrónicos con fines de lucha contra la delincuencia grave celebrado con los Estados Unidos [*Agreement on access to electronic data for the purpose of countering serious crime*, en lo sucesivo, «*UK-US CLOUD Act Agreement*» (Acuerdo sobre la Ley CLOUD entre el Reino Unido y los Estados Unidos)][9], en particular para garantizar la continuidad del nivel de protección cuando los datos

[7] «Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado».

[8] 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 (DO L 281 de 23.11.1995, p. 31).

[9] 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* (Acuerdo entre el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte y el Gobierno de los Estados Unidos de América relativo al acceso a datos electrónicos con fines de lucha contra la delincuencia grave), 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.

personales se transfieran de la UE al Reino Unido sobre la base de la decisión de adecuación del Reino Unido, y posteriormente se transfieran 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 menoscabar el nivel de protección de los datos personales previsto en la UE.

19. Además, se invita a la Comisión Europea a supervisar el *UK-US CLOUD Act Agreement* respecto a si garantiza salvaguardias adicionales adecuadas, teniendo cuenta el nivel de sensibilidad de las categorías de datos afectadas y los requisitos exclusivos de transferencia de pruebas electrónicas directamente por proveedores de servicios en lugar de entre autoridades, analizando también en qué circunstancias podrían establecerse salvaguardias mediante una aplicación adecuada de la adaptación del Acuerdo marco UE-EE. UU.[10].

20. Además, el CEPD señala que las transferencias ulteriores también pueden realizarse desde el Reino Unido a otros países terceros a partir de las **herramientas de transferencia en virtud de la legislación de protección de datos aplicable en Reino Unido**[11]. Tras el asunto *Schrems II*[12], el CEPD invita a la Comisión Europea a introducir, en la decisión de adecuación, garantías relativas al establecimiento efectivo de las salvaguardias necesarias, teniendo también en cuenta la legislación del país tercero destinatario.

21. Respecto a la ausencia, en la legislación del Reino Unido, de las **protecciones previstas en el artículo 48 del RGPD**, el CEPD invita a la Comisión Europea a que aporte garantías adicionales y referencias específicas a la legislación del Reino Unido que garanticen que el nivel de protección en el marco jurídico del Reino Unido es sustancialmente equivalente al que se garantiza en el EEE.

22. Respecto a los **mecanismos procedimentales y de cumplimiento**, el CEPD señala que la existencia y 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 dota a los particulares del EEE de los medios para hacer valer sus derechos y buscar reparación sin encontrarse gravosas barreras para los recursos administrativos y judiciales son elementos fundamentales que deben caracterizar un marco de protección de datos que sea coherente con el europeo.

23. El CEPD reconoce que el Reino Unido ha replicado la mayoría de las disposiciones pertinentes del RGPD en el *UK Data Protection Regulation* (Reglamento de protección de datos del Reino Unido, en lo sucesivo, «*UK GDPR*») y en la *Data Protection Act 2018*; no obstante, se invita a la Comisión Europea a realizar un seguimiento continuo de cualquier novedad en el marco jurídico y la práctica del Reino Unido que pueda ocasionar efectos perjudiciales en tales ámbitos.

1.2.3. Sobre el acceso, por parte de las autoridades públicas, a los datos transferidos al Reino Unido

24. El CEPD señala los significativos cambios del marco jurídico del Reino Unido aplicables a las agencias de seguridad e inteligencia, especialmente en lo relativo a la interceptación y obtención de datos de

[10] Véase el Acuerdo entre los Estados Unidos y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, de diciembre de 2016 (en lo sucesivo, «Acuerdo marco UE-EE. UU.), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A3104_8.
[11] Véanse los artículos 46 y 47 del RGPD de Reino Unido.
[12] Véase Schrems II.

comunicaciones. El CEPD comprende que estos cambios son, entre otras cosas, una respuesta a los procedimientos incoados ante el TJUE y el Tribunal Europeo de Derechos Humanos (TEDH) y sus sentencias recientes en este contexto.

25. En particular, el CEPD celebra que el Reino Unido haya instaurado el Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación, en lo sucesivo, «IPT», por sus siglas in inglés). El IPT no solo es competente para ver causas sobre el uso de poderes de investigación por parte de las fuerzas o cuerpos de seguridad, sino también por los servicios de inteligencia. Por tanto, el CEPD entiende que el IPT funciona como un órgano judicial en el sentido el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la «Carta de la UE»).

26. Además, celebra la introducción de «comisarios judiciales» en la *Investigatory Powers Act* 2016 (Ley sobre facultades de investigación de 2016, en lo sucesivo, «IPA 2016», por sus siglas en inglés) como una mejora significativa. Comprende que una función importante de los comisarios judiciales es la aprobación *ex ante* de medidas de vigilancia, incluida la interceptación específica y la obtención en bloque de datos de comunicaciones (el denominado «procedimiento de doble llave») en casos individuales.

27. Sin embargo, a fin de evaluar la eficacia de este nivel adicional de supervisión, el CEPD considera que se necesitan aclaraciones adicionales sobre las situaciones en las que resulta posible una interceptación lícita sin la aprobación del Comisario de Facultades de Investigación («IPC», por sus siglas en inglés) o los comisarios judiciales, e invita a la Comisión Europea a profundizar su evaluación y demostrar que, incluso en casos en los que no se aplica el procedimiento de doble llave, el marco jurídico del Reino Unido ofrece salvaguardias adecuadas, particularmente a través de la supervisión *ex post* eficaz y las opciones de recurso de que disponen los particulares, garantizando un nivel de protección sustancialmente equivalente al de la Unión.

28. Además, el CEPD invita a la Comisión Europea a que evalúe más detenidamente las condiciones en las que se puede invocar la urgencia y que aclare las posibles vías para el ejercicio de los derechos de los interesados, así como las posibles vías de recurso que se les ofrecen en el marco de operaciones de interferencia de equipos, especialmente en el caso de excepciones al procedimiento de doble llave.

29. El CEPD considera también que es necesario aclarar y evaluar en mayor profundidad las interceptaciones en bloque de datos, en particular en lo que respecta a la selección y aplicación de selectores, a fin de aclarar en qué medida el acceso a los datos personales cumple el umbral establecido por el TJUE, así como qué salvaguardias existen para proteger los derechos fundamentales de las personas cuyos datos son interceptados en este contexto, incluidos los períodos de retención de los datos. Resultaría especialmente útil una evaluación independiente de las autoridades de supervisión competentes del Reino Unido. El CEPD señala, además, que es aún más crítico que, en el caso de las «comunicaciones relacionadas con el extranjero» que están dentro del alcance de las prácticas de interceptación en bloque de datos, parece implicarse que el Reino Unido podría interceptar y recoger grandes volúmenes de datos directamente dentro de la UE, así como datos en tránsito entre la UE y el Reino Unido, que entrarían en el alcance del proyecto de Decisión. Dada la importancia de este aspecto, el CEPD insta a la Comisión a que siga atentamente la evolución de este asunto.

30. También en relación con la interceptación en bloque de datos, el CEPD destaca la apreciación reiterada del TEDH y del TJUE, y recuerda las preocupaciones manifestadas en relación con los datos secundarios, que deberían gozar de salvaguardias específicas debido a su sensibilidad. Por

consiguiente, el CEPD pide a la Comisión Europea que analice cuidadosamente si las salvaguardias previstas en la legislación del Reino Unido para dicha categoría de datos personales garantizan un nivel de protección sustancialmente equivalente al que se garantiza en el EEE.

31. A este respecto, el CEPD es consciente de que el informe del Intelligence and Security Committee de 2016 (Comisión de Inteligencia y Seguridad del Parlamento de Reino Unido) respecto al uso de facultades relativas a grandes volúmenes de datos [13]se refiere a prácticas efectuadas en virtud del marco jurídico anterior, que fue sustituido por la *IPA 2016*. No obstante, considera necesario que las autoridades de control competentes del Reino Unido lleven a cabo una evaluación y supervisión independientes sobre el uso de herramientas de tratamiento automatizado, y pide a la Comisión Europea que evalúe más detenidamente este problema y las garantías que se reconocerían o que podrían reconocerse, en este contexto, a los interesados del EEE.

32. El CEPD comparte la postura manifestada por el IPC de que se necesita un examen más profundo y un mayor seguimiento para garantizar que las salvaguardias aplicadas en la práctica por las autoridades competentes del ámbito de la seguridad nacional y la inteligencia para resolver incumplimientos en la aplicación de la legislación pertinente se mantengan y se sigan mejorando. El CEPD también celebra el hecho de que, como consecuencia, el IPC revisara su método para la inspección de interceptaciones en bloque en 2019, «incluyendo una cuidadosa revisión de las formas, técnicamente complejas, en las que se efectúan en la realidad las interceptaciones en bloque», y se comprometió a incluir «un examen detallado de los selectores y criterios de búsqueda a los que aludía anteriormente el TEDH» en las inspecciones de las interceptaciones en bloque a partir de 2020. En vista de la importancia de este aspecto, al CEPD le preocupa que el IPC todavía no haya llevado a cabo un examen detallado de los selectores y criterios de búsqueda, y pide a la Comisión Europea que siga atentamente los acontecimientos a este respecto, especialmente teniendo en cuenta que aún está por aclarar la forma concreta de la supervisión.

33. El CEDP subraya que, en lo que respecta a las comunicaciones en el extranjero, la aplicación de la exención de seguridad nacional prevista en la legislación del Reino Unido puede dar lugar a la ausencia de garantías que aseguren el respeto de los principios de limitación de la finalidad, necesidad y proporcionalidad o que dispongan que los derechos de las personas, la supervisión y la tutela judicial también deben estar previstos o ser respetados en el tercer país destinatario. Por consiguiente, el CEPD recomienda a la Comisión Europea que examine más a fondo las garantías generales previstas en la legislación del Reino Unido en lo que respecta a la comunicación en el extranjero, en particular teniendo en cuenta la aplicación de las exenciones de seguridad nacional.

34. Por último, al CEPD le preocupan otras formas de intercambio y comunicación de información basadas en otros instrumentos, particularmente en los diversos acuerdos internacionales celebrados entre el Reino Unido y otros países terceros, sobre todo en los casos en los que estos instrumentos siguen siendo inaccesibles para el público, como es el caso del *UK-US Communication Intelligence Agreement* (Acuerdo de inteligencia en materia de comunicaciones entre el Reino Unido y los Estados Unidos). El efecto de dicho acuerdo podría dar lugar a la elusión de las garantías identificadas en relación con el acceso y uso de datos personales con fines de seguridad nacional. El CEPD considera que la celebración de futuros acuerdos bilaterales o multilaterales con terceros países con fines de

[13] Véase el Informe sobre la revisión de los poderes de interceptación en bloque elaborado por el Independent Reviewer of Terrorism Legislation (supervisor independiente del Reino Unido de la legislación en materia de terrorismo), de agosto de 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

cooperación de los servicios de inteligencia que proporcionen una base jurídica para la interceptación y obtención directa de datos personales o para la transferencia de datos personales a estos países también puede tener un impacto significativo en las condiciones para el uso 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.

1.3. Conclusión

35. El CEPD considera que la evaluación de la adecuación del Reino Unido es única debido a su anterior estatus como Estado miembro de la Unión. Además, también se trataría de la primera decisión de adecuación que incluye una cláusula de extinción.

36. Por consiguiente, el CEPD reconoce múltiples ámbitos de convergencia entre los marcos de protección de datos del Reino Unido y de la UE. Sin embargo, al mismo tiempo, tras un estudio detenido del proyecto de Decisión de la Comisión Europea y de la legislación sobre protección de datos del Reino Unido, el CEPD ha detectado una serie de desafíos que se analizan en profundidad en el presente dictamen. En este contexto, el CEPD desea hacer hincapié en el papel clave de la Comisión Europea en el seguimiento de todos los acontecimientos pertinentes que se produzcan en el Reino Unido.

37. En vista del anterior, el CEPD recomienda a la Comisión Europea que aborde los desafíos planteados en el presente dictamen. Asimismo, invita a la Comisión a seguir atentamente todos los acontecimientos pertinentes del Reino Unido que puedan afectar a la equivalencia sustancial del nivel de protección de los datos personales, y que adopte rápidamente medidas adecuadas cuando sea necesario.

2. INTRODUCCIÓN

2.1. Marco de protección de datos del Reino Unido

38. El marco de protección de datos del Reino Unido se basa en gran medida en el marco de protección de datos de la UE (concretamente, el RGPD y la Directiva sobre protección de datos en el ámbito penal) debido a que el Reino Unido fue un Estado miembro de la UE hasta el 31 de enero de 2020. Asimismo, la *UK Data Protection Act 2018*, que entró en vigor el 23 de mayo de 2018 y derogó la *UK Data Protection Act 1998*, especifica en mayor medida la aplicación del RGPD al Derecho del Reino Unido, transpone la Directiva sobre protección de datos en el ámbito penal y otorga poderes e impone obligaciones a la autoridad nacional de control en materia de protección de datos, que en el caso del Reino Unido es la ICO.

39. Como se menciona en el considerando 12 del proyecto de Decisión de la Comisión Europea, 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 legales, para realizar las modificaciones necesarias en el Derecho de la Unión conservado tras la retirada del Reino Unido de la UE a fin de adaptarlo al contexto nacional.

40. Por consiguiente, el marco jurídico pertinente aplicable en el Reino Unido una vez finalizado el período de transición[14] 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 2018*, modificado por la normativa *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* [Reglamentos en materia de Protección de Datos, Privacidad y Comunicaciones Electrónicas (modificaciones, etc.) (salida de la UE) de 2019, o «*DPPEC Regulations 2019*»];
- la *UK Data Protection Act 2018* (en lo sucesivo, la «*DPA 2018*»), modificada por la normativa *DPPEC Regulations 2019* y la normativa *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020* [Reglamentos en materia de Protección de Datos, Privacidad y Comunicaciones Electrónicas (modificaciones, etc.) (salida de la UE) de 2020, o *DPPEC Regulations 2020*], y
- la *IPA 2016*

(conjuntamente, el «marco de protección de datos del Reino Unido»).

2.2. Alcance de la evaluación del CEPD

41. 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 70, apartado 1, letra s), del RGPD, 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.

42. Tal y como se menciona en el documento de trabajo relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos: «la información ofrecida por la Comisión Europea debe ser exhaustiva y colocar al CEPD en una posición que le permita realizar su propia evaluación sobre el nivel de protección de datos en el tercer país»[15].

43. 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[16].

[14] El período 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 «período puente» está fijado para el 30 de junio de 2021, a más tardar, y se refiere al período adicional durante el cual la transmisión de datos personales desde el EEE al Reino Unido no se considera una transferencia.

[15] Véase el documento WP254 rev.01, p. 3.

[16] En lo que respecta a las siguientes cuestiones: el artículo 48 del RGPD (nota a pie de página 78 del proyecto de Decisión); las garantías y medidas de seguridad mejoradas que aplican los responsables del tratamiento a aquel que se produce en el contexto de la seguridad nacional (nota al pie de página 64 del proyecto de Decisión); el requisito de que el responsable del tratamiento valore si existe la necesidad de acogerse a la exención caso por caso incluso cuando se ha emitido un certificado de seguridad nacional (considerando 126 y nota al pie de página 172 del proyecto de Decisión); el hecho de que las protecciones del Acuerdo marco UE-

44. 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.

45. 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 sustancialmente equivalentes. En vista de su papel en el proceso 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. Asimismo, en consonancia con la jurisprudencia del TJUE, una parte muy importante del análisis trata sobre el régimen jurídico del acceso por parte de la seguridad nacional a los datos personales transferidos al Reino Unido y sobre la práctica del aparato de seguridad nacional en el Reino Unido. Sin embargo, debe tenerse en cuenta que la seguridad nacional es, sin duda, un ámbito del Derecho y de la práctica en el cual la legislación de los Estados miembros no está armonizada a escala de la UE y en el que, por tanto, pueden existir divergencias.

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

47. El objetivo de este análisis es proporcionar a la Comisión Europea un dictamen sobre la evaluación de 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 Unión»[17]. 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

EE. UU. se aplicarán a toda la información personal producida o conservada en virtud del *UK-US CLOUD Act Agreement*, independientemente de la naturaleza o el tipo de organismo que realiza la solicitud, en relación con los detalles concretos de la aplicación de las garantías de protección de datos que todavía están siendo objeto de conversaciones entre el Reino Unido y Estados Unidos, y la confirmación de que las autoridades del Reino Unido solo permitirán que este Acuerdo entre en vigor cuando consideren que su aplicación cumple las obligaciones jurídicas previstas en el mismo, especialmente la claridad con respecto al cumplimiento de las normas de protección de datos en relación con cualquier dato solicitado en virtud de este Acuerdo (considerando 153 del proyecto de Decisión); las situaciones en las que se transfieran datos de la UE al Reino Unido dentro del alcance de este proyecto de Decisión, y el hecho de que siempre habría una «conexión con las Islas Británicas» y, por lo tanto, cualquier interferencia de equipos que cubriera dichos datos estaría sujeta al requisito de autorización obligatoria de la sección 13, apartado 1, de la *IPA 2016* (considerando 206 del proyecto de Decisión), y los ejemplos de fines operativos facilitados (considerando 216 y nota al pie de página 369 del proyecto de Decisión).

[17] Véase Sentencia del TJUE de 6 de octubre de 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, (en lo sucesivo, «Schrems I»), apartados 73-74.

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[18].

2.3. Observaciones generales y preocupaciones

2.3.1. Compromisos internacionales contraídos por el Reino Unido

48. Con arreglo a lo dispuesto en el artículo 45, apartado 2, letra c), del RGPD y el documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos[19], al evaluar la adecuación del nivel de protección de un tercer país, la Comisión Europea tendrá en cuenta, entre otras cosas, los compromisos internacionales asumidos por el tercer país, u otras obligaciones 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 respecto al tratamiento automatizado de datos de carácter personal (en lo sucesivo, «el Convenio 108»)[20], y su Protocolo adicional[21].

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

2.3.2. Posible divergencia del marco de protección de datos del Reino Unido en el futuro

50. Como se menciona en el considerando 281 del proyecto de Decisión, la Comisión Europea debe tener en cuenta que, al finalizar el período de transición previsto en el Acuerdo de Retirada[23], el Reino Unido administra, aplica y hace cumplir su propio régimen de protección de datos y, en cuanto deje de aplicarse la disposición puente en virtud del artículo FINPROV.10A del Acuerdo de Comercio y Cooperación[24], 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.

51. Por ello, la Comisión Europea ha decidido incluir una cláusula de extinción en su proyecto de Decisión[25] y ha fijado un plazo de vigencia de cuatro años desde su entrada en vigor.

---

[18] Véanse WP254 rev.01, p. 2.
[19] Véanse WP254 rev.01, p. 2.
[20] 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.
[21] 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.
[22] Véase el Protocolo que modifica el 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.
[23] 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).
[24] 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).
[25] Véase el artículo 4 del proyecto de Decisión. Véase igualmente el considerando 282 del proyecto de Decisión.

52. Cabe tener en cuenta que la posibilidad de que los ministros y el Secretario de Estado del Reino Unido introduzcan Derecho derivado una vez que finalice el período 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.

53. De hecho, el Gobierno del Reino Unido ha manifestado su intención de desarrollar políticas separadas e independientes sobre protección de datos, lo que podría conllevar una divergencia respecto de la legislación en materia de protección de datos de la UE[26]. Esta intención engloba la inclusión de cuestiones en materia de datos personales en los acuerdos comerciales[27], una práctica que conlleva el riesgo de reducir el nivel de protección de los datos personales que proporciona el Reino Unido[28].

54. 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 puente y su Tribunal Supremo no está vinculado por ninguna jurisprudencia de la UE conservada[29].

---

[26] La *National Data Strategy* (Estrategia Nacional sobre Datos Personales) del Reino Unido (actualizada por última vez el 9 de diciembre de 2020) https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) incluye lo siguiente entre sus objetivos: «Abanderar la circulación internacional de datos. *La circulación transfronteriza de datos estimula las operaciones comerciales, las cadenas de suministro y el comercio globales, potenciando así el crecimiento en todo el mundo. Asimismo, desempeña un papel más extenso en la sociedad. La transferencia de datos personales garantiza el pago de los salarios de las personas y las ayuda a mantenerse en contacto con sus seres queridos en la distancia. Y, tal y como ha demostrado la pandemia de COVID-19, compartir datos sanitarios puede contribuir a investigaciones científicas indispensables sobre enfermedades, así como a unir a países en sus respuestas a las emergencias sanitarias globales.* ***Tras su salida de la Unión Europea, el Reino Unido abogará por los beneficios que brindan los datos.*** Promoveremos unas buenas prácticas a escala nacional y colaboraremos con socios internacionales **para garantizar que los datos no se ven limitados inadecuadamente por las fronteras nacionales ni son fragmentados por los regímenes normativos** de modo que sea posible aprovechar todo su potencial» (negrita añadida).

[27] *Ibid*: «Facilitar la circulación transfronteriza de los datos: ***trabajaremos globalmente para eliminar las barreras innecesarias a la circulación internacional de datos.*** **Estableceremos disposiciones ambiciosas en materia de datos en nuestras negociaciones comerciales** y aprovecharemos nuestra nueva posición como miembro independiente de la Organización Mundial del Comercio para influir positivamente en las reglas comerciales en lo que respecta a los datos. ***Eliminaremos los obstáculos a las transferencias internacionales de datos*** *que promueven el crecimiento y la innovación, especialmente mediante el desarrollo de una nueva capacidad del Reino Unido para facilitar mecanismos nuevos e innovadores de transferencia internacional de datos.* También colaboraremos con los nuestros socios en el G20 para generar interoperabilidad entre los regímenes de datos nacionales a fin de minimizar las fricciones al transferir datos entre países» (negrita añadida).

[28] Véase la Resolución del Parlamento Europeo, de 12 de diciembre de 2017, relativa a «Hacia una estrategia de comercio digital» [(2017/2065(INI)], punto V, donde se hace hincapié en que «la protección de los datos de carácter personal no es una cuestión negociable en los acuerdos comerciales [de la UE]», disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_ES.pdf. Véase también la Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación, apartado 28, donde se enuncia lo siguiente: «apoya la práctica de la Comisión de abordar la protección de datos y la circulación de datos personales al margen de los acuerdos comerciales», disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_ES.html.

[29] Véase la sección 6, apartados 3 a 6, de la *EU (Withdrawal) Act* de 2018.

55. **Teniendo en cuenta los riesgos relacionados con la posible divergencia entre el marco de protección de datos del Reino Unido y el acervo de la Unión una vez finalizado el «período puente», el CEPD acoge 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[30]. 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.**

56. 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») tanto en el sector comercial como en el público, y en particular sobre las reclamaciones presentadas por los interesados en el EEE en relación con la transferencia de datos personales del EEE al Reino Unido.

3. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

3.1. Principios relativos al contenido

57. El capítulo 3 del documento relativo al documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos trata sobre los principios relativos al contenido. El sistema de un tercer país debe incluirlos para que su nivel de protección de datos se considere sustancialmente equivalente al que se garantiza en la UE. El CEPD reconoce el hecho de que el Reino Unido no dispone de una constitución codificada en la medida en que no existe un único documento que establezca sus normas de gobierno fundamentales. Sin embargo, el derecho al respeto de la vida privada y familiar (y el derecho a la protección de los datos que se incluye en dicho derecho), así como el derecho a un juez imparcial[31] están incluidos en la *Human Rights Act 1998* (Ley de derechos humanos de 1998), y los tribunales del Reino Unido han reconocido el valor constitucional de dicha ley. De hecho, la *Human Rights Act 1998* incorpora los derechos previstos en el CEDH[32]. Asimismo, la *Human Rights Act 1998* establece que cualquier acto de las autoridades públicas debe ser compatible con el CEDH[33], algo que resulta de vital importancia.

58. Además de las diferencias estructurales y formales entre la legislación del Reino Unido y de la Unión Europea, el CEPD señala, como cabe esperar, que el planteamiento de la protección de datos en el Reino Unido es similar al de la UE debido a que fue Estado miembro de esta hasta el 31 de enero de 2020. Por tanto, muchos de los principios relativos al contenido coinciden con los del RGPD, de modo que proporcionan un nivel de protección sustancialmente equivalente al que garantiza la UE. El CEPD ha decidido no desarrollar en mayor profundidad el análisis de dichos principios relativos al contenido puesto que se encuentran en consonancia con la legislación de la UE, y encuentra satisfactorio el análisis facilitado por la Comisión Europea en su proyecto de Decisión. Dichos

[30] Véase el artículo 45, apartado 4, del RGPD.
[31] Véanse los artículos 6 y 8 del CEDH (anexo 1 a la *Human Rights Act 1998*).
[32] Para más información, véanse los considerandos 8-10 del proyecto de Decisión.
[33] Véase el artículo 6 de la *Human Rights Act 1998*.

principios relativos al contenido son, por ejemplo, los siguientes: conceptos (por ejemplo, «datos personales», «tratamiento de datos personales», «responsable del tratamiento»); motivos para el tratamiento lícito y equitativo para fines legítimos; limitación de la finalidad; calidad de los datos y proporcionalidad; retención de datos, seguridad y confidencialidad; transparencia; categorías especiales de datos; mercadotecnia directa; decisiones automatizadas y elaboración de perfiles. Asimismo, el CEPD señala que el RGPD del Reino Unido y la *DPA 2018* incluyen principios relativos al contenido que superan lo exigido por el documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos y equivalen a los principios incluidos en el RGPD, elevando así el nivel de protección que se garantiza en el Reino Unido. Dichos principios relativos al contenido son, por ejemplo, los relativos a las notificaciones de violaciones de la seguridad de los datos, al delegado de protección de datos, a las evaluaciones de impacto relativas a la protección de datos y a la protección de datos desde el diseño y por defecto.

59. Sin embargo, como se menciona en la introducción, el CEPD desea abordar específicamente en este Dictamen algunas cuestiones que le suscitan preocupación y sobre las cuales desea solicitar aclaración a la Comisión Europea.

3.1.1. Derechos de acceso, rectificación, supresión y oposición

60. La denominada «exención para el control de la inmigración», establecida en el **anexo 2 a la *DPA 2018,* parte 1**, apartado 4, permite a los responsables del tratamiento que participan en el «control de inmigración» no aplicar algunos derechos de los interesados, previstos en la *DPA 2018*, si esto «pudiera perjudicar el mantenimiento de un control efectivo de la inmigración» o «la investigación o detección de actividades que socavarían el mantenimiento de un control efectivo de la inmigración».

61. Tal y como reconoce la Comisión Europea en su proyecto de Decisión[34], y como se menciona en la Opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo sobre la celebración, en nombre de la Unión, del Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido[35], esta exención **se formula de manera «amplia»**. La exención se aplica a los siguientes derechos: derecho de información; derecho de acceso; derecho de supresión; derecho a la limitación del tratamiento y derecho de oposición.

62. Asimismo, resulta importante señalar que esta exención también se aplica en el caso de que los datos personales no se recojan con el fin de llevar a cabo un control de la inmigración por parte de un responsable de un tratamiento («responsable del tratamiento 1»), pero que, sin embargo, este

[34] Véanse los considerandos 62 a 65 del proyecto de Decisión.

[35] En este sentido, en la **formulación amplia** de la exención para el control de la inmigración, véase la Opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior sobre la celebración, en nombre de la Unión, del 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, y del Acuerdo entre la Unión Europea y el Reino Unido de Gran Bretaña e Irlanda del Norte sobre procedimientos de seguridad para el intercambio y la protección de información clasificada [2020/0382(NLE)], de 5 de febrero de 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_ES.pdf, apartado 10: «recuerda, a este respecto, las Resoluciones del Parlamento de febrero y junio de 2020, en las que se destaca la **amplia exención general** para el tratamiento de los datos personales para fines de inmigración de la *UK Data Protection Act* y del marco jurídico del Reino Unido sobre la conservación de datos de telecomunicaciones electrónicas». Véase asimismo el apartado 11: «considera que la **amplia exención general** para el tratamiento de los datos personales para fines de inmigración de la *UK Data Protection Act* [...] debe modificarse antes de que pueda concederse una decisión de adecuación favorable» (negrita añadida).

último los ponga a disposición de otro responsable del tratamiento («responsable del tratamiento 2»), quien lleva a cabo su tratamiento con fines de control de la inmigración (por ejemplo, el Ministerio del Interior del Reino Unido)[36].

63. En *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 October 2019)*, las partes demandantes cuestionaron la legalidad de la exención para el control de la inmigración arguyendo que contravenía el artículo 23 del RGPD y era incompatible con los derechos otorgados por los artículos 7 y 8 de la Carta de la UE relativos a la vida privada y la protección de los datos de carácter personal. El Tribunal Superior de Inglaterra y Gales (en lo sucesivo, el «Tribunal Superior») estudió si la exención para el control de la inmigración que consta en el anexo 2, parte 1, apartado 4, de la *DPA 2018* es legal, y dictaminó que sí lo era.

64. El Tribunal Superior consideró en particular que:

- «[...] la exención para el control de la inmigración es sencillamente una cuestión "de interés público importante" y persigue un fin legítimo [...]», en el apartado 30;
- *«la exención para el control de la inmigración satisface los requisitos para que una medida sea "de conformidad con el Derecho"* [...]», en el párrafo 38;
- *«solo es posible acogerse a la exención para el control de la inmigración si, y en la medida en que, el cumplimiento de las "disposiciones mencionadas del RGPD"* ***pudiera perjudicar*** *el mantenimiento de un control efectivo de la inmigración o la investigación o detección de actividades que socavarían el mantenimiento de un control efectivo de la inmigración. La expresión "pudiera perjudicar", en el contexto de la UK Data Protection Act 1998 (sucedida por la DPA 2018), se había interpretado en el sentido de "una posibilidad muy significativa e importante de perjuicio para el interés público que corresponda.* El grado de riesgo debe ser tal que "existan muchas probabilidades" de que pueda haber un perjuicio a dichos intereses, aun cuando el riesgo quede lejos de ser probable [...]», en el párrafo 39 (negrita añadida).

[36] Véase el ejemplo facilitado en la *Guide to the General Data Protection Regulation (GDPR)* [Guía del Reglamento General de Protección de Datos (RGPD)], versión de 1 enero de 2021, p. 307 (negrita añadida): *«Una organización privada (responsable del tratamiento 1) advierte al Ministerio del Interior (responsable del tratamiento 2) de que cree que un empleado ha presentado documentación falsa para demostrar su identidad y sus cualificaciones con el objetivo de conseguir un puesto. El empleador proporciona al Ministerio del Interior toda la información pertinente. El derecho de información del interesado acerca de la transmisión de sus datos personales al Ministerio del Interior queda limitado en la medida en que informarlo podría perjudicar la investigación.*
Por tanto, el ***empleador no tiene ninguna obligación de informar al interesado de que ha facilitado sus datos al Ministerio del Interior*** *y, del mismo modo, el* ***Ministerio del Interior*** *no tiene ninguna obligación de informar al interesado de que es el Ministerio quien está tratando sus datos personales. La exención se aplica a ambos responsables del tratamiento en la misma medida.*
Sin embargo, el empleado solicita una copia de sus datos personales al Ministerio del Interior, que está ahora investigándolos. El ***Ministerio del Interior puede acogerse a la exención*** *para retener una parte de los datos si considera que facilitarlos podría perjudicar a la investigación. En el caso de que el empleado realice una solicitud similar a* ***su empleador, este también podría aplicar la exención*** *en la misma medida».*
En otras palabras, como se aclara en la página 300: *«En la mayoría de los casos, el Ministerio del Interior, o una de sus agencias y contratistas, será el responsable del tratamiento que aplique esta exención. No obstante, es importante señalar que la aplicación de esta exención no se limita únicamente al Ministerio del Interior, sino que también podría resultar pertinente para otros responsables del tratamiento, como empresas, universidades y la policía, que colaboren con el Ministerio del Interior en cuestiones de inmigración».*

65. Cabe señalar que, al leal saber y entender del CEPD, esta sentencia no es firme y se ha interpuesto recurso contra ella.

66. Tal y como detallan las *EDPB Guidelines on restrictions under Article 23 GDPR* (Directrices del CEPD sobre las restricciones en virtud del artículo 23 del RGPD, en lo sucesivo, «Directrices sobre las restricciones del artículo 23 del RGPD»)[37], «[...] en el contexto del RGPD, las restricciones deben **establecerse en una medida legislativa**, afectar a un **número limitado de derechos de los interesados o de obligaciones de los responsables del tratamiento** que figuran en el artículo 23 del RGPD, **respetar en lo esencial** los derechos y libertades fundamentales en cuestión, ser una **medida necesaria y proporcionada** en una sociedad democrática y salvaguardar uno de los aspectos recogidos en el artículo 23, apartado 1, del RGPD [...]»[38].

67. El CEPD recuerda también que el considerando 41 del RGPD establece que «[c]uando el presente Reglamento hace referencia a **una base jurídica o a una medida legislativa**, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser **clara y precisa y su aplicación previsible para sus destinatarios**, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea [...] y del Tribunal Europeo de Derechos Humanos» (negrita añadida).

68. Aunque el TEDH especificó que «[a]simismo, en lo que respecta a las expresiones "prevista por la ley" y "previstas por la ley", que aparecen en los artículos 8 y 11 del Convenio, el [CEDH] observa que siempre ha entendido el término "ley" en sentido "material" y no "formal"; *ha incluido al mismo tiempo el "derecho escrito", que abarca tanto los textos de rango inferior al rango legislativo, como actos reglamentarios adoptados por un colegio profesional, por delegación del Parlamento, en el marco de sus facultades normativas autónomas, y el derecho no escrito.* Ha de entenderse que la "ley" engloba tanto los textos escritos como el **"derecho elaborado" por los jueces**»[39]. Las Directrices sobre las restricciones del artículo 23 del RGPD recuerdan que «[s]egún la jurisprudencia del TJUE, cualquier **medida legislativa** adoptada sobre la base del artículo 23, apartado 1, [del] RGPD debe, en particular, **cumplir los requisitos específicos previstos en el artículo 23, apartado 2, del RGPD**. El artículo 23, apartado 2, [del] RGPD establece que las medidas legislativas que limiten los derechos de los interesados y las obligaciones de los responsables del tratamiento contendrán, en su caso, **disposiciones específicas relativas a diversos criterios que se detallan a continuación**. Por norma, todos los requisitos detallados a continuación **deben estar incluidos en la medida legislativa** que imponga limitaciones de conformidad con el artículo 23 [del] RGPD»[40].

---

[37] Véanse las *EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR*, versión 1.0, adoptadas el 15 de diciembre de 2020, que actualmente se encuentran en proceso de finalización tras someterse a consulta pública, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Véase el artículo 23 de las *EDPB Guidelines on restrictions under Article 23 GDPR*, apartado 9, página 5.

[39] Véase la sentencia del TEDH de 14 de septiembre de 2010, Sanoma Uitgevers B.V./Países Bajos, EC:ECHR:2010:0914JUD003822403, apartado 83 (negrita añadida).

[40] Véase el artículo 23 de las Directrices sobre las restricciones del artículo 23 del RGPD, apartados 45 y 46, p. 11. De conformidad con el artículo 52, apartado 3, de la Carta de la UE, «[e]n la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa». En cuanto al concepto de «**establecida por la ley**» que figura en el artículo 52,

69. En este sentido, puede observarse que **la exención para el control de la inmigración** de por sí **no especifica los siguientes elementos a los que se hace referencia en el artículo 23, apartado 2, del RGPD**:

- «d) las garantías para evitar accesos o transferencias ilícitos o abusivos»;
- «e) la determinación del responsable del tratamiento o de categorías de responsables del tratamiento»[41].
- «g) los riesgos para los derechos y las libertades de los interesados»;
- «h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta».

70. La *Guide to the General Data Protection Regulation (GDPR)* [Guía del Reglamento General de Protección de Datos (RGPD)] de la ICO[42], especialmente un capítulo sobre la «exención para el control de la inmigración», sí proporciona aclaraciones sobre esta, pero **no puede** establecer *per se* normas vinculantes que la complementen. Asimismo, la cuestión de la «calidad de la ley» resulta particularmente relevante, a la vista de la importancia de los derechos que limita y la amplitud de la exención[43].

---

apartado 1, de la Carta de la UE, los criterios desarrollados por el TEDH deben utilizarse tal y como sugieren diversas conclusiones del Abogado General del TJUE; véanse, por ejemplo, las conclusiones sobre los asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, apartados 137-154, y el asunto C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, apartados 88-114. Por tanto, puede hacerse referencia, entre otros, a la sentencia del TEDH en el asunto Weber y Saravia/Alemania, apartado 84: *«El Tribunal reitera que la expresión "**establecida por la ley**" en el sentido que se le otorga en el artículo 8, apartado 2, [del CEDH] exige, en primer lugar, que la medida impugnada tenga alguna base en el **Derecho nacional**;* también hace referencia a la **calidad de la ley** en cuestión, que exige que sea accesible al interesado, quien también debe poder prever sus consecuencias, y que sea compatible con el Estado de Derecho» (negrita añadida).
Véase también el considerando 41 del RGPD: «Sin embargo, dicha base jurídica o medida legislativa debe ser clara y **precisa** y su aplicación **previsible para sus destinatarios**, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea [...] y del Tribunal Europeo de Derechos Humanos» (negrita añadida).

[41] Véase el asunto del Tribunal Superior antedicho, apartado 54: *«Considero que no hay nada ilícito en el hecho de que la exención para el control de la inmigración esté al alcance de **todos los responsables del tratamiento** que traten datos con los fines especificados. Como señalan las partes demandadas, sin el apartado 4, puntos 3) a 4), la exención para el control de la inmigración quedaría sin efecto en aquellos casos en que los datos se obtengan de terceros (como una autoridad local o HM Revenue and Customs [la Agencia Tributaria británica]) para los fines de mantener un control eficaz de la inmigración»* (negrita añadida), lo cual confirma la aplicación **generalizada** de las restricciones.

[42] *Guide to the General Data Protection Regulation (GDPR)* [Guía del Reglamento General de Protección de Datos (RGPD)] de la ICO, versión de 1 enero de 2021, pp. 299-307.

[43] Véase el apartado 57 del asunto del Tribunal Superior antedicho: *«El señor Knight me informa de que el Comisario está finalizando las directrices sobre la Exención, pero que estas tendrán carácter "estatutario" solo en la medida en que se emiten en virtud de los poderes del Comisario de conformidad con el artículo 57, apartado 1, del RGPD.* No tendrán carácter reglamentario en el marco de la *DPA 2018*».
La justificación de la introducción de directrices jurídicamente vinculantes que respalda la ICO se menciona específicamente en los apartados 56-60 de la sentencia:
«56. Por último, me remito al argumento del Comisario según el cual, si no va acompañada de directrices estatutarias que proporcionen garantías sobre el significado y la aplicación de la exención para el control de la inmigración, la exención no constituiría una aplicación proporcionada del artículo 23, apartado 1, del RGPD. El señor Knight considera que, complementada por dichas directrices, la disposición resulta proporcionada.

71. *A fortiori*, la «**evaluación del perjuicio**» no establece las garantías para evitar accesos o transferencias ilícitos o abusivos, que debe establecer, por ejemplo, el Ministerio del Interior.

72. A la vista de todo lo expuesto, el CEPD señala que hacen falta más aclaraciones sobre la aplicación de la exención para el control de la inmigración.

73. Asimismo, el CEPD hace hincapié en la ausencia de un instrumento jurídicamente vinculante que aclare la exención para el control de la inmigración en lo que respecta a si se considera sustancialmente equivalente al artículo 23 del RGPD y los artículos 7 y 8 de la Carta de la UE. Al mismo tiempo, el CEPD considera que la Comisión Europea debe demostrar en mayor profundidad la

---

57. El señor Knight me informa de que el Comisario está finalizando las directrices sobre la Exención, pero que estas tendrán carácter "estatutario" solo en la medida en que se emiten en virtud de los poderes del Comisario de conformidad con el artículo 57, apartado 1, del RGPD. No tendrán carácter reglamentario en el marco de la *DPA 2018*. *Entiendo también que el Ministerio del Interior ha elaborado unas directrices internas para el personal sobre la exención para el control de la inmigración (véase el apartado 22 que antecede). En la práctica, las directrices emitidas por el Comisario son influyentes, independientemente de su base jurídica.* No obstante, el Comisario carece de poderes para emitir directrices "vinculantes" tales como las que el Tribunal Supremo tenía en mente en el asunto relativo al Christian Institute (véanse los apartados 101 a 107). Parece que harían falta normas de Derecho primario si se considerase necesario que existan directrices en lo que respecta a la exención para el control de la inmigración con el mismo carácter jurídico que los códigos prácticos establecidos en las secciones 121 a 124 de la *DPA 2018*.

58. En su alegato por unas directrices de naturaleza estatutaria, el señor Knight sostiene que el contexto en el que resultará necesario recurrir a la exención para el control de la inmigración hace alusión necesariamente a las cuestiones que suscitan preocupación en torno a la necesidad y proporcionalidad de su existencia y aplicación. En concreto, destaca dos cuestiones en el contexto jurídico. En primer lugar, los datos personales a los que se aplica la exención para el control de la inmigración, por su naturaleza, probablemente incluirán categorías especiales de datos personales, conforme a su definición en el artículo 9, apartado 1, del RGPD (es decir, «datos personales que revelen el origen étnico o racial»). Dichos datos aparecen identificados en el RGPD porque precisan de mayor protección (*Opinion 1/15 [2019] 3 C.M.L.R.25*, apartado 141). En segundo lugar, uno de los dictados fundamentales de la legislación en materia de protección de datos es que, concretamente, el derecho de acceso de los interesados es de gran importancia, pues abre la puerta al ejercicio de otros derechos que asisten a los interesados (véase el asunto YS/Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081;*[2015] 1 C.M.L.R.18*, apartado 44).

59. El señor Knight identifica cuatro aspectos de carácter práctico. En primer lugar, cuando los responsables del tratamiento no explican a los interesados que se han basado en una exención de carácter estatutario ni facilitan un resumen general de los motivos por los que lo han hecho, el interesado no estará al corriente de que se ha aplicado la exención y, en consecuencia, no podrá impugnarla de manera efectiva. En segundo lugar, los interesados dependerán especialmente de que los responsables del tratamiento apliquen la exención con rigurosidad y solo en la medida en que resulte necesario. Aunque todos los interesados tienen derecho a presentar reclamaciones ante el Comisario en relación con la aplicación de la exención o a incoar procedimientos judiciales ante los tribunales, es probable que el interesado desconozca sus derechos y carezca de los fondos para emprender medidas legales, en circunstancias en las que resulta necesario cumplir los derechos en materia de protección de datos de manera ágil y precisa. En tercer lugar, por su condición de inmigrantes, es probable que los interesados se encuentren en una posición de vulnerabilidad. En cuarto lugar, esta no es una cuestión abstracta, a la vista de las pruebas de las partes demandadas en lo que respecta al uso de la exención para el control de la inmigración (véase el apartado 4 más arriba).

60. El señor Knight sugiere que existe un estrecho paralelismo entre la presente impugnación de la exención para el control de la inmigración y el razonamiento del Tribunal en el asunto relativo al *Christian Institute [2016] UKSC 51*. Al igual que con el Christian Institute, sostiene que la exención para el control de la inmigración es amplia, utiliza términos indefinidos, aplica un umbral bajo, está sujeta a controles que no resultan evidentes en la disposición y se aplica a un amplio abanico de contextos y derechos. Al contrario que en el asunto del Christian Institute, no existen directrices de dominio público, y aún menos con carácter estatutario a las que sea necesario atenerse, sobre la exención para el control de la inmigración».

necesidad y la proporcionalidad del amplio ámbito de aplicación *ratione personae* de la exención para el control de la inmigración, apoyándose en pruebas a dicho efecto.

74. **En conclusión, el CEPD invita a la Comisión Europea a verificar el estado del proceso *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* al que se hace referencia más arriba y, puesto que esta sentencia no es firme (*res judicata*), a verificar si resulta confirmada o revisada por la sentencia resultante del recurso, a fin de tener en cuenta cualquier modificación en este sentido y hacerla constar en la decisión de adecuación. El CEPD también pide a la Comisión Europea que facilite más información sobre la necesidad y la proporcionalidad de la exención para el control de la inmigración, particularmente en lo que respecta al amplio ámbito de aplicación *ratione personae*.**

75. **Al mismo tiempo, el CEPD invita a la Comisión Europea a seguir investigando si existen garantías adicionales en el marco jurídico del Reino Unido, o si se prevé que estas existan, por ejemplo, por medio de instrumentos jurídicamente vinculantes que complementarían a la exención para el control de la inmigración mejorando su previsibilidad por parte de los interesados y las garantías que les asisten, y permitiendo también una evaluación y una supervisión mejores y más rápidas de los requisitos de necesidad y proporcionalidad.**

3.1.2. Limitaciones en materia de transferencias ulteriores

76. El artículo 44 del RGPD establece que solo se realizarán transferencias de datos personales, incluidas las transferencias ulteriores, cuando estas no menoscaben el nivel de protección de las personas físicas amparadas por el RGPD. Por tanto, los datos personales transferidos del EEE al Reino Unido sobre la base de la decisión de adecuación disfrutarán de un nivel de protección sustancialmente equivalente al que proporciona el marco de protección de datos de la UE. **Esto no solo significa que la legislación del Reino Unido será «sustancialmente equivalente» a la de la UE en lo que respecta al tratamiento de datos personales transferidos al Reino Unido en el marco del proyecto de Decisión, sino que las normas aplicables en el Reino Unido en lo que respecta a las transferencias ulteriores de dichos datos a terceros países garantizarán que seguirá proporcionándose un nivel de protección sustancialmente equivalente.**

77. Como resultado de ello, es importante que cualquier transferencia ulterior de datos personales del EEE que se realice desde el Reino Unido a otro tercer país cuente con las debidas garantías de protección o se lleve a cabo de conformidad con las normas sobre excepciones[44] para garantizar la continuidad de la protección que garantiza la legislación de la UE. **De hecho, en el caso de que no pueda brindarse dicha protección, no deben llevarse a cabo transferencias ulteriores de datos personales del EEE.**

78. El CEPD reconoce que el Reino Unido ha reflejado, en gran medida, el capítulo V del RGPD en el RGPD del Reino Unido (artículos 44-49) y en la *DPA 2018*[45]. **Sin embargo, el CEPD ha identificado algunos aspectos del marco legislativo del Reino Unido en lo que respecta a las transferencias ulteriores que podrían menoscabar el nivel de protección de los datos personales que se transfieran desde el EEE.**

79. **El primer obstáculo** que ha identificado el CEPD guarda relación con el reconocimiento por parte del Reino Unido, una vez completado el procedimiento previsto en la *DPA 2018*, de los terceros países,

[44] Véase el artículo 49 del RGPD del Reino Unido.
[45] Véanse las secciones 17A, 17B, 17C y 18 de la *DPA 2018*.

las organizaciones internacionales o los territorios[46] como destinatarios adecuados. De hecho, podrían producirse transferencias ulteriores de datos personales del EEE desde el Reino Unido a otros países terceros sobre la base de una posible norma de adecuación del Reino Unido en el futuro[47].

80. Más concretamente, como se explica en el considerando 77 del proyecto de Decisión, el Secretario de Estado del Reino Unido tiene el poder de reconocer a un tercer país (o 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 garante de un nivel adecuado de protección de los datos personales, previa consulta a la ICO[48]. Al evaluar la adecuación del nivel de protección, el Secretario de Estado del Reino Unido debe tener en cuenta los mismos elementos que la Comisión Europea está obligada a evaluar con arreglo al artículo 45, apartado 2, letras a) a c), del RGPD, interpretado junto con su considerando 104 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 «sustancialmente equivalente» al garantizado en el Reino Unido. Aunque el CEPD señala la capacidad del Reino Unido, en virtud del RGPD del Reino Unido, para reconocer a los territorios como garantes de 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 «sustancialmente equivalente» al garantizado en la UE. Esto podría conllevar posibles riesgos para la protección que se proporciona a los datos personales transferidos desde el EEE, especialmente si el marco de protección de datos del Reino Unido divergiera del acervo de la Unión en el futuro. Cabe señalar que, en julio de 2020, el asunto emblemático del TJUE Schrems II[49] se tradujo en la invalidación de la Decisión sobre el Escudo de la Privacidad UE-EE. UU. ya que, según el TJUE, no se podía considerar que el marco jurídico estadounidense proporcionara un nivel de protección sustancialmente equivalente al 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 puente y su Tribunal Supremo no está vinculado por ninguna jurisprudencia de la UE conservada[50].

81. **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 del RGPD. Cuando la Comisión Europea estime que un tercer país considerado adecuado por el Reino Unido no garantiza un nivel de protección sustancialmente equivalente al garantizado dentro de la UE, 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 garantías específicas para los datos personales procedentes del EEE, o considerar la suspensión de la decisión de adecuación del Reino Unido, cuando los datos personales transferidos desde el EEE al Reino**

[46] Véase el artículo 17A de la *DPA 2018*.
[47] El equivalente en el Reino Unido de una decisión de adecuación en el marco del RGPD.
[48] Véase la sección 182, apartado 2, de la *DPA 2018*. Véase también el *Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments* (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/.
[49] Véase Schrems II.
[50] Véase la sección 6, apartados 3 a 6, de la *EU (Withdrawal) Act 2018*.

Unido sean objeto de transferencias ulteriores al tercer país en cuestión sobre la base de una norma de adecuación del Reino Unido.

82. **El segundo obstáculo** guarda relación con la próxima revisión de las decisiones de adecuación ya existentes, otorgadas por la Comisión Europea en el marco de la Directiva 95/46/CE. Tras la revisión, la Comisión Europea podría decidir que determinados países que se han beneficiado hasta ahora de una decisión de adecuación ya no proporcionan un nivel de protección sustancialmente equivalente, teniendo en cuenta la legislación de la UE actual y la jurisprudencia reciente. No obstante, conforme a lo dispuesto en el anexo 21, apartado 4, de la *DPA 2018*, el Reino Unido ya ha reconocido que dichos países proporcionan un nivel adecuado de protección. Aunque el Secretario de Estado del Reino Unido debe llevar a cabo una revisión de dichas decisiones de adecuación en un plazo de cuatro años, la Comisión Europea señala en su proyecto de Decisión que estas decisiones de adecuación no dejarán de existir automáticamente en el caso de que el Secretario de Estado del Reino Unido no lleve a cabo la revisión necesaria en el plazo estipulado de cuatro años[51].

83. **El CEPD invita a la Comisión Europea a supervisar si, una vez que se complete la revisión de la UE de las decisiones de adecuación ya existentes, el Reino Unido sigue considerando que un país proporciona un nivel adecuado de protección aun cuando la UE ya no lo considere así. En ese caso, el CEPD invita a la Comisión Europea, atendiendo a los considerandos 277 a 280 del proyecto de Decisión, a tomar cualesquiera medidas adecuadas para poner remedio a la situación, por ejemplo, modificando la decisión de adecuación a fin de añadir requisitos específicos para los datos personales procedentes del EEE o suspendiendo la decisión de adecuación, en el caso de que los datos personales transferidos del EEE al Reino Unido sean transferidos ulteriormente al tercer país en cuestión. El CEPD invita a la Comisión Europea a que continúe este ejercicio de control durante el período de vigencia de la decisión de adecuación.**

84. **El tercer obstáculo** está relacionado con la transferencia ulterior de datos personales desde el EEE a países que no proporcionen un nivel adecuado de protección sobre la base de los instrumentos de transferencia previstos en los artículos 46 y 47 del RGPD del Reino Unido. Aunque el RGPD del Reino Unido establece los mismos instrumentos de transferencia que el RGPD, el CEPD subraya la necesidad de asegurar que las garantías que contienen exijan una protección efectiva en el tercer país, especialmente al hilo de la sentencia Schrems II.

85. Tras la sentencia Schrems II, en la que el TJUE recuerda que la protección otorgada a los datos personales en la UE debe acompañar a los datos allá donde vayan, el CEPD ya ha adoptado recomendaciones iniciales sobre medidas complementarias[52] para ayudar a los exportadores, cuando resulte necesario, a garantizar que los interesados cuentan con un nivel de protección sustancialmente equivalente al que se proporciona en la UE.

86. Según el TJUE, corresponde a los exportadores comprobar, caso por caso y, si es preciso, en colaboración con el importador de los datos en el tercer país, si el Derecho o la práctica del tercer país pone menoscaba la eficacia de las garantías adecuadas que prevén los instrumentos de

[51] Véase el considerando 82 del proyecto de Decisión.

[52] Véanse las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020 por el CEPD, que actualmente están en proceso de finalización tras someterse a consulta pública, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf.

transferencia del artículo 46 del RGPD[53]. Cuando sea el caso, los exportadores de datos deben aplicar medidas complementarias que pongan remedio a estas deficiencias en la protección y la adecúen al nivel exigido por el Derecho de la UE.

87. **El CEPD invita a la Comisión Europea, a fin de garantizar la continuidad de la protección, a que introduzca en el proyecto de Decisión confirmación de que, cuando los exportadores de datos en el Reino Unido utilicen los instrumentos de transferencia previstos en los artículos 46 y 47 del RGPD del Reino Unido para realizar transferencias ulteriores de datos procedentes del EEE a otros terceros países, dichos exportadores evalúan caso por caso el marco de protección de los datos de dicho tercer país, y, en caso necesario, a que tome las medidas adecuadas para garantizar que se respetan de manera efectiva las garantías correspondientes al instrumento de transferencia escogido a fin de garantizar un nivel de protección sustancialmente equivalente al que se proporciona en la UE. Sin estas confirmaciones, el CEPD subraya que existe el riesgo de que el nivel de protección sustancialmente equivalente al que se proporciona en la UE se diluya a través de transferencias ulteriores que se produzcan desde el Reino Unido.**

88. **El cuarto obstáculo** relacionado con las transferencias ulteriores atañe a los acuerdos internacionales que el Reino Unido ha celebrado o vaya a celebrar en el futuro, así como al posible acceso directo, por parte de las autoridades de terceros países signatarios de dichos acuerdos, a datos personales del EEE. En efecto, al CEPD le preocupa considerablemente el *UK-US CLOUD Act Agreement*, ya celebrado, y la Comisión Europea reconoce este problema, señalando que «la posible entrada en vigor del Acuerdo podría afectar al nivel de protección evaluado en esta Decisión»[54]. De hecho, sobre la base de este Acuerdo, una vez que entre en vigor, los datos personales transferidos desde el EEE al Reino Unido en el marco del proyecto de Decisión quedarían sujetos a las disposiciones de este Acuerdo, en el que se establecen condiciones para el acceso directo por parte de las autoridades estadounidenses, lo cual afecta al marco de protección de datos del Reino Unido, especialmente a las disposiciones sobre transferencias ulteriores. Como resultado, el nivel de protección proporcionado a los datos transferidos desde el EEE podría verse considerablemente afectado por las disposiciones del Acuerdo formalizado con Estados Unidos. El CEPD señala en este contexto que la Comisión Europea se remite, en el considerando 153 de su proyecto de Decisión, a las explicaciones facilitadas por las autoridades del Reino Unido, sin citar ni proporcionar ninguna confirmación o compromiso específicos por escrito ni señalar ninguna disposición legal concreta del Derecho del Reino Unido que pudiera dar efecto a dichas explicaciones.

89. El CEPD ya ha manifestado anteriormente estas inquietudes en una carta dirigida al Parlamento Europeo con fecha del 15 de junio de 2020[55]. El CEPD subrayó que, sobre la base del «acervo de la Unión en el ámbito de la protección de datos personales, y concretamente en lo que respecta al RGPD y a la Directiva sobre protección de datos en el ámbito penal», tiene reservas sobre si las garantías del Acuerdo sobre el acceso a los datos personales en el Reino Unido se aplicarían en determinadas circunstancias que obliguen a facilitar datos a Estados Unidos, y sobre si dichas garantías resultan suficientes, con respecto a las normas de la UE, para evitar el menoscabo del nivel de protección garantizado en la UE.

[53] Véase *Schrems II*, apartado 134.
[54] Véase el considerando 153 del proyecto de Decisión.
[55] Véase la respuesta del CEPD a los diputados al Parlamento Europeo Sophie in 't Veld y Moritz Körner sobre el Acuerdo sobre la Ley CLOUD entre el Reino Unido y los Estados Unidos, de 15 de junio de 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

90. Asimismo, las disposiciones del *UK-US CLOUD Act Agreement* podrían afectar considerablemente a las condiciones materiales y procesales en virtud de las cuales las autoridades estadounidenses puedan acceder directamente a los datos personales que obren en el poder de los responsables o encargados del tratamiento en el Reino Unido, lo que afectaría al nivel de protección garantizado por el Derecho del Reino Unido. Para proporcionar un nivel de protección sustancialmente equivalente al que se garantiza mediante el Derecho de la UE, por ejemplo, es «esencial que las garantías previstas en dicho acuerdo incluyan una autorización judicial previa obligatoria, que constituya una garantía fundamental para el acceso a metadatos y datos de contenido. Sobre la base de su evaluación preliminar, el CEPD, al tiempo que señala que el acuerdo hace referencia a la aplicación del Derecho nacional, no pudo identificar una disposición clara al respecto en el acuerdo concluido entre el Reino Unido y Estados Unidos»[56].

91. Mientras que la Comisión Europea subraya que los datos obtenidos en el marco de este Acuerdo se beneficiarían de protecciones equivalentes a las garantías específicas proporcionadas en el Acuerdo marco UE-EE. UU., al CEPD le preocupa si la incorporación de dichas garantías al Acuerdo sobre el *UK-US CLOUD Act Agreement* mediante una mera referencia *mutatis mutandis* satisfaría los criterios de unas normas claras, precisas y accesibles a la hora de acceder a los datos personales, o si consagraría de manera suficiente dichas garantías de modo que estas resultaran efectivas y aplicables en el marco del Derecho del Reino Unido.

92. **Por tanto, el CEPD recomienda que la Comisión Europea aclare cómo y en base a qué instrumento jurídico otorgaría eficacia y carácter vinculante en el Derecho del Reino Unido a las protecciones equivalentes a las garantías previstas en el Acuerdo marco UE-EE. UU.**

93. El CEPD también señala que las disposiciones del *UK-US CLOUD Act Agreement*, leídas conjuntamente con la sección 3 de la Ley CLOUD estadounidense[57], plantea preguntas sobre la verdadera aplicación de las garantías que ofrece el Acuerdo para el acceso, por parte de las fuerzas o cuerpos de seguridad estadounidenses, a los datos personales en el Reino Unido tratados por proveedores de servicios de comunicación electrónica o servicios informáticos a distancia (en lo sucesivo, «proveedores de servicios en nube») sujetos a la jurisdicción estadounidense. De hecho, en el caso de que uno de dichos proveedores estuviese ubicado en el Reino Unido y sujeto a la legislación estadounidense (por ejemplo, una filial de una empresa de Estados Unidos), queda pendiente confirmar si las autoridades estadounidenses estarían obligadas a atenerse al *UK-US CLOUD Act Agreement* para obtener dichos datos. Al igual que la Comisión Europea señala que «debe prestarse especial atención a la aplicación y adaptación de las protecciones del Acuerdo marco al tipo específico de transferencias cubiertas por el Acuerdo entre el Reino Unido y los Estados Unidos», el CEPD subraya que, sobre la base de su evaluación preliminar, no está claro si las garantías consagradas en el *UK-US CLOUD Act Agreement*, y por tanto la prevista en el Acuerdo marco UE-EE. UU, serían de aplicación a todas, o a alguna, de las solicitudes de acceso a los datos en el Reino Unido formuladas por las autoridades estadounidenses en el marco de la Ley CLOUD estadounidense.

94. El Reino Unido podría formalizar en el futuro otros acuerdos o arreglos internacionales con terceros países, que podrían aplicarse a los datos personales que se transmitan desde el EEE al Reino Unido en el marco del proyecto de Decisión[58]. En función de las disposiciones de dichos acuerdos y de la aplicación de cláusulas de salvaguardia específicas, estos acuerdos internacionales, puesto que afectan al marco de protección de datos del Reino Unido, también podrían afectar

[56] Véase la carta del CEPD antedicha.
[57] Véase la Ley CLOUD estadounidense, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] Véase el apartado 2.3.3 que antecede.

considerablemente a las condiciones materiales y procesales del acceso a los datos personales en el Reino Unido por parte de autoridades de terceros países. Este es el caso, en particular, del borrador del Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (en lo sucesivo, el «Convenio de Budapest), que está en proceso de negociación entre las partes signatarias, entre las que se incluyen varios países no pertenecientes a la Unión. De hecho, el borrador del Protocolo incluye cláusulas que pueden invocar las partes de manera discrecional, por ejemplo, en lo que respecta a la autorización para otorgar acceso o no a los datos de contenido. Mientras que todos los Estados miembros de la UE activarían las cláusulas de conformidad con las normas de la UE para la protección de datos, no se ha establecido ninguna garantía relativa al Reino Unido, cuyo nivel de protección de los datos podría divergir del que se garantizaría en ese caso en la UE. Otro ejemplo de los problemas previstos anteriormente es el Acuerdo de Asociación Económica Integral entre el Reino Unido y Japón («CEPA»)[59], el primer acuerdo comercial del Reino Unido tras el Brexit, que entró en vigor el 1 de enero de 2021[60], y que incluye disposiciones sobre datos personales[61]. Asimismo, el CEPD señala que el Reino Unido también ha anunciado formalmente, el 1 de febrero de 2021, su solicitud para unirse al Tratado Integral y Progresista de Asociación Transpacífico («CPTPP»), que incluye al Acuerdo de Asociación Transpacífico («TPP»)[62].

95. El CEPD señala que, aparte del *UK-US CLOUD Act Agreement*, en el proyecto de Decisión no se hace referencia a los acuerdos internacionales mencionados anteriormente.

96. **El CEPD invita a la Comisión Europea a:**

- **Examinar la interacción entre el marco de protección de datos del Reino Unido y sus acuerdos internacionales, más allá del *UK-US CLOUD Act Agreement*, particularmente para garantizar la continuidad del nivel de protección en el caso de las transferencias ulteriores a otros países terceros de datos personales transferidos desde el EEE al Reino Unido a tenor de una decisión de adecuación del Reino Unido, y a supervisar de manera continua y adoptar medidas, cuando sea necesario, con respecto a la celebración de otros acuerdos internacionales entre el Reino Unido y terceros países que amenacen con menoscabar el nivel de protección de los datos personales garantizado en la UE.**

- **Proporcionar al CEPD compromisos escritos de las autoridades del Reino Unido e identificar disposiciones específicas en el marco del Derecho del Reino Unido en relación con la**

[59] Véase *UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020]* (Reino Unido/Japón: Acuerdo de Asociación Económica Integral), https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Véase *UK Government's guidance on UK trade agreements with non-EU countries* (Directrices del Gobierno del Reino Unido sobre los acuerdos comerciales del Reino Unido con países no pertenecientes a la UE), https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] A tenor del artículo 8.80, apartado 5, del CEPA, las partes se comprometen a impulsar el desarrollo de mecanismos para promover la compatibilidad entre sus distintos planteamientos jurídicos relativos a la protección de datos (personales). De conformidad con el artículo 8.84, las partes se abstendrán de prohibir o limitar las transferencias transfronterizas de información por medios electrónicos, incluyendo la información personal, cuando esta actividad sea para la conducción de un negocio de una persona cubierta, conforme a la definición prevista en el CEPA.

[62] En virtud del artículo 14.11, apartado 2, del TPP, las partes permitirán las transferencias transfronterizas de información por medios electrónicos, incluyendo la información personal, cuando esta actividad sea para la conducción de un negocio de una persona cubierta.

explicación relativa a la posible aplicación del *UK-US CLOUD Act Agreement*, tal y como se menciona en el considerando 153 del proyecto de Decisión.

- **Supervisar, en este contexto, si además de las garantías que podrían proporcionarse mediante la adecuada aplicación de la adaptación del Acuerdo marco UE-EE. UU., el *UK-US CLOUD Act Agreement* ofrece garantías adicionales adecuadas para tener en cuenta el nivel de sensibilidad de las categorías de los datos en cuestión y los requisitos específicos de la transferencia de pruebas electrónicas directamente por parte de proveedores de servicios en nube, en lugar de entre autoridades.**
- **Evaluar el impacto y los posibles riesgos de las disposiciones en materia de datos personales recogidas en los acuerdos internacionales formalizados recientemente por el Reino Unido, como el CEPA.**

97. **El quinto obstáculo** identificado guarda relación con la aplicación de excepciones a las transferencias de datos personales a un tercer país. Aunque las excepciones disponibles en el marco del RGPD del Reino Unido son las mismas que las del RGPD, es importante que la ICO aplique, ahora y en el futuro, una interpretación sobre el uso de estas excepciones que sea congruente con la del CEPD. Si no es el caso, o si el Reino Unido adoptase una interpretación divergente en el futuro, existiría el riesgo de menoscabo del nivel de protección de los datos transferidos desde el EEE a terceros países a través del Reino Unido.

98. **El CEPD invita a la Comisión Europea, en el marco de esta tarea de supervisión, a que compruebe específicamente que la interpretación del Reino Unido sobre el uso de las excepciones continúa siendo congruente con la interpretación de la UE. Si, por el contrario, el Reino Unido se rigiese por una interpretación distinta del uso de las excepciones, menoscabando así el nivel de protección, es fundamental que la Comisión Europea adopte las medidas necesarias modificando la decisión de adecuación para garantizar que el nivel de protección proporcionado a los datos personales del EEE que se transfieren al Reino Unido no se verá perjudicado cuando dichos datos sean objeto de transferencias ulteriores desde el Reino Unido a terceros países atendiendo a una interpretación distinta de las excepciones.**

99. **El sexto obstáculo**, y el último de este apartado, hace referencia a la ausencia de las protecciones previstas en el artículo 48 del RGPD en el marco de protección de datos del Reino Unido.

100. En concreto, la Comisión Europea aclara en su proyecto de Decisión que, en ausencia de normas de adecuación o garantías adecuadas, una transferencia solo puede llevarse a cabo sobre la base de las excepciones previstas en el artículo 49 del RGPD del Reino Unido, «con la excepción del artículo 48 del Reglamento (UE) 2016/679, que el Reino Unido ha optado por no incluir en el RGPD del Reino Unido».[63] La ausencia de una disposición sustancialmente equivalente al artículo 48 del RGPD en el marco de protección de datos del Reino Unido, en relación con las transferencias o comunicaciones exigidas por una sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país, podría generar inseguridad jurídica ante la duda de si el nivel de protección de los datos personales transferidos desde el EEE al Reino Unido en el marco del proyecto de Decisión se vería considerablemente afectado.

101. En su documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos, el CEPD señala que, cuando se trata de transferencias ulteriores, «solo deben permitirse las transferencias ulteriores de datos personales por parte del destinatario inicial de la

[63] Véase la nota 78 del proyecto de Decisión.

transferencia de datos original cuando el destinatario ulterior también esté sujeto a unas normas que garanticen un nivel adecuado de protección y atienda a las instrucciones pertinentes cuando lleve a cabo el tratamiento de los datos en nombre del responsable del tratamiento»[64]. Asimismo, el CEPD subraya que «el destinatario inicial de los datos transferidos desde la UE tendrá la responsabilidad de garantizar que se proporcionan las garantías adecuadas para las transferencias ulteriores de datos cuando no exista una decisión de adecuación. Dichas transferencias ulteriores de datos solo deben producirse con unos fines limitados y específicos, y siempre y cuando exista una base jurídica para el tratamiento»[65]. El artículo 48, que forma parte del capítulo V del RGPD, debe tenerse plenamente en cuenta a la hora de evaluar si el marco jurídico del Reino Unido garantiza un nivel sustancialmente equivalente de protección en este sentido[66].

102. El CEPD hace hincapié en este contexto en la jurisprudencia del TJUE relacionada con el riesgo de accesos y usos abusivos o ilícitos de los datos, y señala particularmente que «en lo que respecta al nivel de protección de los derechos y libertades fundamentales que se garantizan en la Unión Europea, la legislación de la UE que conlleve alguna interferencia con los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de la UE debe, según la reiterada jurisprudencia del TJUE, establecer normas claras y precisas que rijan el alcance y la aplicación de una medida e impongan unas garantías mínimas, de modo que las personas cuyos datos personales se vean afectados dispongan de las garantías suficientes como para que sus datos estén protegidos de manera efectiva frente al riesgo de accesos y usos abusivos o ilícitos. La necesidad de dichas garantías es aún más acusada en aquellos casos en que los datos personales sean objeto de tratamiento automatizado y cuando exista un riesgo considerable de que se produzca un acceso ilícito a los mismos»[67].

103. En este sentido, el CEPD señala que, atendiendo a la información recogida en el proyecto de Decisión, el marco de protección de datos del Reino Unido no establece claramente que toda resolución de un órgano jurisdiccional y toda decisión de una autoridad administrativa de un tercer país que exija a un responsable o encargado del tratamiento transferir o comunicar datos personales solo deba ser reconocida o ejecutable de alguna forma si se basa en un acuerdo internacional vigente entre el tercer país solicitante y el Reino Unido. El artículo 48 del RGPD es una disposición fundamental de su capítulo V, puesto que establece que cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan la transferencia o comunicación de datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del capítulo V del RGPD. De hecho, el CEPD recuerda que «una solicitud de una autoridad extranjera, por sí misma, no constituye una base jurídica para la transferencia. La orden solo puede ser reconocida "si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado

[64] Véase el documento WP254 rev.01, p. 6.
[65] Véase el documento WP254 rev.01, p. 6.
[66] Véase la última frase del artículo 44 del RGPD, donde se dispone lo siguiente: «Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado».
[67] Véase Schrems I, apartado 91.

miembro"»[68]. Por tanto, es fundamental que en el Derecho del Reino Unido puedan encontrarse disposiciones sustancialmente equivalentes.

104. En el proyecto de Decisión, la Comisión Europea recoge explicaciones de las autoridades del Reino Unido, según las cuales, a tenor del *common law* o el Derecho escrito, no es posible ejecutar en el Reino Unido una sentencia extranjera por la que se soliciten datos si no existe un acuerdo internacional, y cualquier transferencia de datos solicitada por un órgano jurisdiccional o una autoridad administrativa de otro país precisa de un instrumento de transferencia, como una norma de adecuación o las garantías adecuadas, salvo que se aplique una de las excepciones previstas en el artículo 49 del RGPD del Reino Unido. No obstante, el CEPD no ha recibido los intercambios mantenidos entre la Comisión Europea y las autoridades del Reino Unido[69] a este respecto y, por tanto, no puede analizar ni evaluar de manera independiente si las garantías ofrecidas por las autoridades del Reino Unido son sustancialmente equivalentes para garantizar un nivel de protección esencialmente equivalente en relación con las garantías previstas en el artículo 48 del RGPD.

105. **El CEPD invita a la Comisión Europea a que facilite confirmaciones adicionales y referencias específicas a la legislación del Reino Unido que garanticen que el nivel de protección en el marco jurídico del Reino Unido es sustancialmente equivalente al que se garantiza en el EEE. Por tanto, el CEPD invita a la Comisión Europea a que facilite explicaciones y compromisos por escrito de las autoridades del Reino Unido en relación con la aplicación de protecciones sustancialmente equivalentes a las que se otorgan en el marco del artículo 48 del RGPD.**

106. **El CEPD considera que la identificación de disposiciones en el Derecho del Reino Unido que garanticen un nivel de protección sustancialmente equivalente en relación con las garantías previstas en el artículo 48 del RGPD es, si cabe, más importante a la vista de las inquietudes manifestadas en relación con las solicitudes de acceso a los datos en el Reino Unido que presenten las autoridades estadounidenses o de otros terceros países, y teniendo en cuenta que, de conformidad con la decisión de adecuación, podrían transferirse datos personales del EEE al Reino Unido sin más garantías o compromisos vinculantes del destinatario en relación con las solicitudes de acceso a los datos por parte de las autoridades de otros terceros países.**

3.2. Mecanismos relativos al procedimiento y la ejecución

107. Sobre la base de los criterios previstos en el documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos, el CEPD ha analizado los siguientes aspectos del marco de protección de datos del Reino Unido, conforme a lo previsto en el proyecto de Decisión: la existencia y el funcionamiento efectivo de una autoridad de control independiente; la existencia de un sistema que garantice un buen nivel de cumplimiento, y un sistema de acceso a los mecanismos de reparación adecuados por el cual las personas en la UE dispongan de los medios para ejercitar sus derechos y obtener reparación administrativa y judicial sin grandes obstáculos.

[68] Véase el anexo a la Respuesta conjunta del CEPD y el SEPD a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo sobre el impacto de la Ley CLOUD estadounidense sobre el marco jurídico europeo en materia de protección de datos personales, de 10 de julio de 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_es.

[69] Véase la nota a pie de página 78 del proyecto de Decisión.

3.2.1 Autoridad de control competente independiente

108. El CEPD acoge favorablemente los esfuerzos de la Comisión Europea por examinar exhaustivamente la creación, el funcionamiento y los poderes de la autoridad de control del Reino Unido en el capítulo 2.6 del proyecto de Decisión. En el Reino Unido, el Comisario de Información (en lo sucesivo, el «Comisario») se encarga de supervisar y garantizar el cumplimiento del RGPD del Reino Unido y la *DPA 2018*. Según el anexo 12 a esta última, el Comisario constituye una «corporation sole» (persona jurídica unipersonal), es decir, una entidad jurídica independiente constituida por una sola persona física.

109. En lo que respecta a la independencia del Comisario, el CEPD subraya que el artículo 51 del RGPD del Reino Unido no aclara expresamente que el Comisario sea una autoridad pública independiente, tal y como se establece en el artículo 51 del RGPD en lo que respecta a las autoridades de control. Sin embargo, el CEPD reconoce que el RGPD del Reino Unido refleja en su artículo 52 las normas correspondientes a la independencia que constan en el artículo 52, apartados 1 al 3, del RGPD.

110. Asimismo, el CEPD señala que el artículo 52 del RGPD del Reino Unido no impone obligaciones que se correspondan con las del artículo 52, apartados 4 a 6, del RGPD, que expresamente garantizan que las autoridades de control correspondientes dispongan de los recursos necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes. No obstante, el CEPD reconoce que la *DPA 2018* contiene disposiciones destinadas a garantizar la adecuada financiación de la ICO[70], y señala también que la ICO es actualmente una de las mayores autoridades de control con respecto a otras en la UE o el EEE. Puesto que es necesaria una asignación permanente de recursos suficientes, especialmente en términos de personal y presupuesto[71], para garantizar el buen funcionamiento de una autoridad de control a fin de satisfacer todas sus funciones, algo que recientemente el Parlamento Europeo también ha declarado como de vital importancia[72], el CEPD considera esencial que se preste especial atención a los futuros avances en este ámbito.

111. **Por tanto, el CEPD invita a la Comisión Europea a observar cualesquiera avances en lo que respecta a la asignación de recursos a la ICO que pudieran ir en detrimento de la adecuada satisfacción de las funciones de esta.**

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

112. El proyecto de Decisión lleva a cabo un análisis exhaustivo de los poderes de los que dispone la ICO en el marco del artículo 58 del RGPD del Reino Unido y la *DPA 2018* a fin de garantizar la supervisión y la aplicación de la legislación. El CEPD reconoce que el artículo 58 del RGPD del Reino Unido refleja de manera muy similar las normas correspondientes relativas a los poderes de las autoridades de control que se establecen en el artículo 58 del RGPD. En lo que respecta al poder de imponer multas administrativas según las circunstancias de cada caso particular, el artículo 83 del RGPD del Reino Unido contiene disposiciones similares y cantidades máximas, al igual que el artículo 83 del RGPD. Por tanto, el CEPD considera que el marco jurídico del Reino Unido a este respecto se encuentra en consonancia con las normas previstas en la legislación correspondiente de la UE. Sin embargo, en

[70] Véanse las secciones 137, 138, 182 y el anexo 12, apartado 9, de la *DPA 2018*.
[71] Véase el documento WP 254 rev.01, p. 7.
[72] Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación, apartado 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_ES.html.

este sentido, el CEPD subraya que la existencia de sanciones *efectivas* desempeña un papel importante a la hora de garantizar que se cumplen las normas[73].

113. **A la vista de lo anterior, el CEPD invita a la Comisión Europea a supervisar la efectividad de las sanciones y los remedios pertinentes en el marco de protección de datos del Reino Unido.**

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

114. Una instancia de supervisión eficaz, que permita la realización de investigaciones independientes de las reclamaciones a fin de identificar y sancionar la vulneración de los derechos de los interesados en la práctica, así como unos mecanismos de reparación administrativos y judiciales efectiva (incluida la indemnización por daños y perjuicios derivados del tratamiento ilícito de los datos personales del interesado), son elementos fundamentales para evaluar si un sistema de protección de los datos proporciona un nivel adecuado de protección.

115. El CEPD acoge favorablemente que la ICO proporcione información exhaustiva y directrices en su sitio web, cuyo objetivo es concienciar a los responsables y encargados del tratamiento sobre sus obligaciones y deberes, así como brindar apoyo a los interesados para que se informen sobre sus derechos en materia de datos personales y hagan valer sus derechos individuales en el marco del RGPD del Reino Unido y la *DPA 2018*.

116. **A pesar de la situación actual, el CEPD invita a la Comisión Europea a que observe de manera continuada el nivel de apoyo que la ICO proporciona específicamente a las personas cuyos datos personales se han transferido al Reino Unido en el marco de la decisión de adecuación, a la hora de ayudarlas a ejercitar sus derechos en el marco de protección de datos del Reino Unido.**

4. ACCESO Y USO POR PARTE DE LAS AUTORIDADES PÚBLICAS DEL REINO UNIDO DE DATOS PERSONALES TRANSFERIDOS DESDE LA UE

4.1. Acceso a los datos y uso de los mismos por parte de las autoridades públicas del Reino Unido a efectos de control de la aplicación del Derecho penal

4.1.1. Base jurídica y limitaciones/garantías aplicables

117. Con respecto a la evaluación realizada por la Comisión Europea y documentada en los considerandos 132 y siguientes del proyecto de decisión **sobre el acceso con fines de aplicación de la ley**, la Comisión Europea proporciona información matizada y detallada y, en general, llega a conclusiones comprensibles. Por consiguiente, el CEPD se abstiene de reproducir en el presente dictamen la mayor parte de las apreciaciones y evaluaciones de los hechos. No obstante, en algunos casos, la descripción de los hechos o la explicación de las conclusiones no son suficientes para que el CEPD los apoye.

4.1.1.1. El uso del consentimiento

118. El CEPD toma nota de que la Comisión Europea afirma en la nota a pie de página 184 del proyecto de decisión[74] que **el uso del 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. En consecuencia,

[73] Véase el documento WP 254 rev.01, p. 7.
[74] Véase la página 37 del proyecto de decisión.

la Comisión Europea no evalúa el uso del consentimiento como base jurídica en las funciones policiales.

119. A este respecto, el CEPD recuerda que el artículo 45, apartado 2, letra a), del Reglamento General de Protección de Datos 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».

120. El CEPD observa, basándose también en la información proporcionada por la Comisión Europea en el considerando 38 de su proyecto de decisión de ejecución de conformidad con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo sobre la protección adecuada de datos personales por parte del Reino Unido («proyecto de Decisión de adecuación relativa a la Directiva sobre protección de datos en el ámbito penal»), que el uso del consentimiento, tal como se enmarca en el régimen del Reino Unido en el contexto policial, requerirá siempre una base jurídica de la que depender. 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.

121. **El CEPD invita a la Comisión Europea a introducir en la decisión de adecuación el análisis sobre el posible uso del consentimiento en un contexto policial que se realiza en el proyecto de Decisión de adecuación relativa la Directiva sobre protección de datos en el ámbito penal**.

4.1.1.2. Órdenes de registro y órdenes de entrega

122. Si bien el CEPD no tiene ningún comentario respecto a la obtención de pruebas por parte de la policía a través de órdenes de registro y órdenes de entrega en general, del considerando 136 del proyecto de decisión se deduce que la Comisión Europea ha centrado sus consideraciones sobre el acceso por parte de las fuerzas de seguridad en la policía, y que el procesamiento de datos personales por parte de otras autoridades con funciones coercitivas se ha analizado en menor medida.

123. Por ejemplo, la sección F del *UK Explanatory Framework for Adequacy Discussions*: *Law Enforcement* (Marco explicativo sobre los debates acerca de la adecuación: Fuerzas del orden)[75], sugiere en la página 11 que **la *National Crime Agency*** (Agencia Nacional 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[76]. La NCA es también uno de los principales interlocutores

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

[76] 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.

para la colaboración policial internacional y desempeña un papel fundamental en el intercambio de información criminal[77].

124. 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, el *HM Revenue and Customs*, («HMRC»), y otros departamentos gubernamentales[78]. Sus actividades están relacionadas con la lucha contra el abuso sexual de menores; el fraude; otros tipos de delitos económicos, incluido el blanqueo de capitales; el uso de la tecnología con fines delictivos; la ciberdelincuencia; la inmigración ilegal organizada, incluida la trata de personas; el tráfico de drogas y armas de fuego, y otras actividades de tráfico ilícito.

125. **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 Europea 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.**

4.1.1.3. Poderes de investigación con fines de aplicación de la ley

126. En el capítulo 4 del documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos *Essential guarantees in third **countries for law enforcement** and national security access to limit interferences to fundamental rights* («Garantías esenciales de los terceros país para el acceso con fines de aplicación de la ley y seguridad nacional destinadas a limitar las injerencias en los derechos fundamentales»), el CEPD recuerda que en este contexto, el Tribunal también señaló de manera crítica que la anterior Decisión sobre los principios de puerto seguro «no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las **posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos**, como

[77] 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 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 *Crime and Courts Act* (Ley de Delitos y Tribunales), 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».

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

la seguridad nacional»[79]. En dicho documento, el CEPD señala que **para que se considere que ofrecen un nivel de protección adecuado, todos los terceros países deben respetar las garantías esenciales europeas[80] para acceder a datos, ya sea con** fines de seguridad nacional o **de aplicación de la ley,** en particular, **se debe demostrar la necesidad y proporcionalidad con respecto a los objetivos legítimos perseguidos.**

127. En esta sección del proyecto de decisión, la Comisión Europea concluye (considerando 139) que «dado que los poderes de investigación selectiva que proporciona la IPA 2016 son los mismos que los disponibles para las agencias de seguridad nacional, las condiciones, limitaciones y garantías aplicables a dichos poderes se tratan en detalle en la sección sobre acceso y el uso de datos personales por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional». Sin embargo, de la jurisprudencia del TJUE se desprende que al aplicar la prueba de necesidad y proporcionalidad a la legislación de los Estados miembros que permite que las autoridades públicas conserven y accedan a datos personales, los objetivos legítimos, como la seguridad nacional o la lucha contra los delitos graves son distintos y, por lo tanto, en algunos casos se podría justificar cierto tipo de injerencia[81].

128. **Por consiguiente, el CEPD desearía que se realizara una evaluación específica en el marco de la decisión sobre la necesidad y proporcionalidad de las condiciones, limitaciones y garantías descritas en los considerandos 174 y siguientes (la sección dedicada a las medidas que persiguen objetivos de seguridad nacional), sobre la aplicación de estas condiciones, limitaciones y garantías en el contexto de una medida que persigue un objetivo de aplicación de la ley. Por lo tanto, invita a la Comisión Europea a aclarar si la conservación de datos personales descrita y el acceso a los mismos a efectos de aplicación de la ley son lo suficientemente limitados como para garantizar un nivel de protección sustancialmente equivalente al que se garantiza en la UE.**

4.1.2. Uso ulterior de la información recogida con fines de aplicación de la ley (considerandos 140-154)

129. El CEPD observa que el marco de protección de datos del Reino Unido proporciona garantías y limitaciones similares a las previstas en la legislación de la UE en relación con el uso ulterior de la información recogida con fines de aplicación de la ley.

4.1.2.1. Uso ulterior con fines de aplicación de la ley

130. La DPA de 2018 prevé efectivamente que los datos personales recogidos por una autoridad competente con fines de aplicación de la ley puedan tratarse posteriormente (ya sea por parte del responsable original del tratamiento o por parte de otro responsable) para cualquier otro fin de aplicación de la ley, siempre que el responsable del tratamiento esté autorizado por ley para tratar datos para dicho fin y el tratamiento sea necesario y proporcionado para ese otro fin. La Comisión Europea señala que todas las garantías que establece la parte 3 de la DPA de 2018 se aplican al tratamiento que realiza la autoridad receptora. Sin embargo, el CEPD subraya que, en la parte 3 del DPA 2018, las secciones 44, apartado 4, 45, apartado 4, 48, apartado 3, y 68, apartado 7, prevén la posibilidad de restringir los derechos del interesado, y la sección 79 contempla la posibilidad de emitir certificados que acrediten que una restricción es una medida necesaria y proporcionada para

[79] Véase WP254 rev.01, p.9.
[80] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.
[81] Véase TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, 6 de octubre de 2020, ECLI:EU:C:2020:791.

proteger la seguridad nacional. **Por consiguiente, el CEPD recomienda que la Comisión Europea evalúe en mayor medida el posible impacto de dichas restricciones en el nivel de protección de los datos personales en relación con el uso ulterior de la información recogida. Asimismo, se debe aclarar también el marco jurídico del Reino Unido que permite ese intercambio ulterior, en particular, la *Digital Economy Act 2017* (Ley sobre la Economía Digital de 2017), así como la *Crime and Courts Act* 2013 que permite el intercambio de información con la NCA.**

4.1.2.2. Uso ulterior con fines de aplicación de la ley en el Reino Unido

131. La DPA de 2018 también establece que los datos personales recogidos para cualquier propósito de aplicación de la ley pueden tratarse para un fin distinto siempre que dicho tratamiento esté autorizado por la ley. En este caso, la base jurídica que autoriza el intercambio es la sección 19 de la *Counter-Terrorism Act 2008* (Ley antiterrorista de 2008). A este sentido, el CEPD observa que el ámbito de aplicación y las disposiciones de la sección 19 de la *Counter-Terrorism Act* no se abordan plenamente en la evaluación de la Comisión Europea y puede implicar un uso ulterior amplio, en particular por 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».

132. El CEPD señala también que la referencia de la Comisión Europea al hecho de que las autoridades competentes son autoridades públicas que deben actuar de conformidad con el CEDH, incluido su artículo 8, por lo que se garantiza que todo intercambio de datos entre las fuerzas de seguridad y los servicios de inteligencia cumple la legislación en materia de protección de datos y el CEDH, se podría justificar más identificando los actos y leyes pertinentes en el marco del ordenamiento jurídico del Reino Unido que establecen de forma clara y precisa dichos límites.

4.1.2.3. Uso ulterior en el contexto de transferencias ulteriores fuera del Reino Unido

133. Si bien la Comisión Europea se ha referido al hecho de que el *UK-US CLOUD Act Agreement* puede afectar a las transferencias ulteriores hacia los Estados Unidos desde proveedores de servicios en nube en el Reino Unido, el CEPD destaca además que la entrada en vigor de este Acuerdo también puede afectar a las transferencias ulteriores desde las fuerzas o cuerpos de seguridad en el Reino Unido, en particular en relación con la emisión y transmisión de órdenes según el artículo 5 del *UK-US CLOUD Act Agreement*.

134. En general, el CEPD considera que la celebración de futuros acuerdos bilaterales 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 uso 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. Por lo tanto, el CEPD recomienda que la Comisión Europea evalúe más detenidamente este punto, identificando la existencia de acuerdos internacionales, y aclare si las disposiciones de dichos acuerdos pueden afectar a la aplicación de la legislación británica en materia de protección de datos y prevén 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 de datos a otros terceros países y el uso ulterior de los mismos.

4.1.3. Supervisión

135. 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 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.

136. 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.

137. **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.**

4.2. Marco jurídico general sobre la protección de datos en el ámbito de la seguridad nacional

4.2.1. Certificados de seguridad nacional

138. Según la sección 111 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 exenciones a las obligaciones y los derechos consagrados en las partes 4 a 6 de la DPA de 2018 son una medida necesaria y proporcionada para la protección de la seguridad nacional. 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 exenciones de seguridad nacional, sino que constituyen una medida de transparencia[82].

139. 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 *UK Data Protection Act 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

[82] Véase Ministerio del Interior, *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, apartado 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

o revocado, los antiguos certificados se trataban como si se hubieran emitido conforme a la DPA de 2018.

140. Sin embargo, cuando en un certificado de seguridad nacional expedido en virtud de la *UK Data Protection Act 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[83]. Aunque la protección que ofrecen estos antiguos certificados se limita al tratamiento de datos personales en virtud de la *UK Data Protection Act 1998*, el CEPD toma nota 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[84].

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

4.2.2. Derecho a la rectificación y supresión

142. En lo que respecta al derecho de rectificación y supresión, el CEPD toma nota de que, con arreglo a las secciones 100 y 149 de la DPA de 2018, los interesados tienen la posibilidad de recurrir al Tribunal Superior (en Escocia, la *Court of Session*) para que ordene a los responsables del tratamiento rectificar o suprimir sus datos sin dilación indebida.

143. **El CEPD subraya que el ejercicio de los derechos de los interesadosdebe garantizarse de forma eficaz. Por consiguiente, invita a la Comisión Europea a describir en su proyecto de decisión cómo funciona en la práctica la sección 100 de la DPA de 2018, y a supervisar de cerca su aplicación.**

4.2.3. Exenciones por seguridad nacional

144. El CEPD desea llamar la atención sobre la sección 110 de la DPA de 2018, y en particular el anexo 11, que establece los fines específicos para los que los servicios de inteligencia pueden desviarse de determinados principios de protección de datos, también en relación con los derechos de los interesados, y no están obligados a comunicar violaciones de los datos personales a la ICO[85].

145. El **CEPD pide a la Comisión Europea que aclare el ámbito de aplicación de las exenciones, pues se pregunta si todas las exenciones previstas en el anexo 11 de la DPA de 2018 son pertinentes para el trabajo de los servicios de inteligencia y si garantizan la equivalencia con el principio de necesidad y proporcionalidad**. En particular, **el CEPD invita a la Comisión Europea a aclarar en qué**

[83] Véase Ministerio del Interior, *The Data Protection Act 2018, National Security Certificates Guidance*, de agosto de 2020, p. 5.
[84] Véase Ministerio del Interior, *The Data Protection Act 2018, National Security Certificates Guidance*, de agosto de 2020, apartado 8, p. 5.
[85] Estos fines incluyen la prevención y detección de «delitos», «la información que deba divulgarse por ley, etc. o en relación con procedimientos judiciales», la «inmunidad parlamentaria», los «procedimientos judiciales», «el honor y la dignidad de la Corona», las «fuerzas armadas», el «bienestar económico», la «protección de la confidencialidad de la comunicación entre abogados y clientes», las «negociaciones», «las referencias confidenciales dadas por el responsable del tratamiento», «los exámenes y las calificaciones de los mismos», «las investigación y estadísticas» y el «archivo de interés público».

circunstancias el servicio de inteligencia podría basarse en la sección 10 del anexo 11 de la DPA de 2018, que establece que «[l] as disposiciones enumeradas no se aplican a los datos personales que consisten en registros de las intenciones del responsable del tratamiento con respecto a las negociaciones con el interesado en la medida en que la aplicación de dichas disposiciones pueda perjudicar dichas negociaciones».

4.3. Acceso y uso por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional

146. Como observación general, el CEPD reconoce que a los Estados se les concede un amplio margen de apreciación en materia de seguridad nacional, que considera también es el TEDH. El CEPD recuerda además que, como se subraya en sus recomendaciones actualizadas sobre las garantías esenciales europeas para medidas de vigilancia[86], el artículo 6, apartado 3, del Tratado de la Unión Europea establece que los derechos fundamentales consagrados en el CEDH constituyen principios generales del Derecho de la Unión. Sin embargo, como recuerda el TJUE en su jurisprudencia, dicho Convenio no constituye, en la medida en que la Unión Europea no lo haya suscrito, un instrumento jurídico incorporado formalmente al Derecho de la Unión[87]. De tal manera, el nivel de protección de los derechos fundamentales exigido por el artículo 45 del RGPD debe determinarse en función de las disposiciones de dicho Reglamento, leído a la luz de los derechos fundamentales consagrados en la Carta de la UE. Dicho esto, de acuerdo con el artículo 52, apartado 3, de la Carta de la UE, los derechos que figuran en ella y se corresponden con derechos que garantiza el CEDH deben tener el mismo significado y alcance que los dispuestos en dicho Convenio. En consecuencia, como ha recordado el TJUE, la jurisprudencia del TEDH sobre derechos que están también previstos en la Carta de la Unión Europea se ha de tener en cuenta como umbral mínimo de protección para interpretar los derechos correspondientes en la Carta de la UE[88]. Sin embargo, con arreglo a la última frase del artículo 52, apartado 3, de la Carta de la UE «[e]sta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa».

147. Por lo tanto, en la siguiente evaluación, el CEPD ha tenido en cuenta la jurisprudencia del TEDH, en la medida en que la Carta de la UE, tal como la interpreta el TJUE, no prevé un nivel de protección superior que prescribe otros requisitos distintos de la jurisprudencia del TEDH.

4.3.1. Base jurídica, limitaciones y garantías - Poderes de investigación ejercidos en el contexto de la seguridad nacional

4.3.1.1. Observaciones generales

148. El CEPD recuerda que la IPA 2016 es una ley reciente que modifica varias disposiciones de la *Intelligence Services Act 1994*. La API establece en qué medida se pueden utilizar determinados poderes de investigación para interferir en la vida privada[89]. Aunque dos informes del IPC proporcionan información útil sobre la aplicación de este nuevo marco jurídico, todavía no se han revisado determinados aspectos, en particular los referentes a los selectores y criterios de búsqueda utilizados.

[86] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.
[87] Véase el asunto Schrems II, apartado 98.
[88] Véase TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, 6 de octubre de 2020, ECLI:EU:C:2020:791, apartado 124.
[89] Véase la sección 1 de la IPA 2016.

149. Además, como observación general sobre la IPA 2016 y su ámbito de aplicación, el CEPD señala los siguientes cuatro aspectos destacables:

150. En relación con el **primer aspecto destacable**, con respeto a las características de la ley, el CEPD desea subrayar dos aspectos:

151. En primer lugar, el CEPD observa que, para el recurso de los procedimientos previstos en la IPA 2016, la legislación hace referencia a fines generales y no a las categorías de personas a las que puede afectar la recopilación de datos en virtud de las partes 2 a 7 de la dicha Ley. En este sentido, el CEPD recuerda que debe existir un vínculo entre las categorías de personas que pueden ser objeto de medidas de vigilancia y los fines que persigue la legislación para definir el ámbito personal de la ley.

152. Además, el CEPD subraya que la definición de «operadores de telecomunicaciones», «servicio de telecomunicaciones» y «sistema de telecomunicaciones», que determinan el ámbito de aplicación de la ley, también es muy amplia y hasta cierto punto no queda clara. De hecho, el CEPD destaca que estos conceptos, en el ámbito de la IPA 2016, deben entenderse de una manera mucho más amplia que en las legislaciones sobre telecomunicaciones, por ejemplo, como se definen en el Código Europeo de las Comunicaciones Electrónicas[90]. El CEPD observa que se indica que las definiciones de «servicio de telecomunicaciones» y «sistema de telecomunicaciones» en la Ley son intencionalmente amplias para que sigan siendo pertinentes para las nuevas tecnologías. Igualmente, la definición de operador de telecomunicaciones también es muy amplia y podría incluir, por ejemplo, los videojuegos en línea con una función de chat incluida, u otros sitios web en línea que simplemente incluyan ventanas de chat[91].

153. Además, si bien, en general, se prevén los procedimientos y la supervisión relativos a la evaluación de la necesidad y proporcionalidad de la recogida de datos y el acceso a los mismos, en la Ley no se definen los criterios para proceder a dicha evaluación. Se pueden encontrar elementos adicionales en otros documentos, como los códigos prácticos.

154. Sin embargo, como se recuerda en las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, el TJUE ha señalado que «el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate»[92]. Concretamente, el TJUE aclara que «[p]ara cumplir el requisito de proporcionalidad, una normativa debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes

[90] Véase el artículo 2, apartado 5, del Código Europeo de las Comunicaciones Electrónicas que define, por ejemplo, «servicio de comunicaciones interpersonales» como «el prestado por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio».

[91] Véase Ministerio del Interior, *Code of practice on the interception of communications* (Código práctico sobre la interceptación de comunicaciones), marzo de 2018, apartados 2.5 y siguientes, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Véase el asunto Schrems II, apartado. 175, y la jurisprudencia citada, así como TJEU, asunto C-623/17, Privacy International c. Secretary of State for Foreign and Commonwealth Affairs y otros, 6 de octubre de 2020, ECLI:EU:C:2020:790 («Privacy International»), apartado. 65.

que permitan proteger de manera eficaz esos datos frente a los riesgos de abuso. Dicha normativa debe ser legalmente imperativa en Derecho interno y, en particular, indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario»[93].

155. El TEDH también hizo hincapié en la importancia de que la ley sea clara para dar a las personas «una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están facultadas para recurrir a tales medidas»[94].

156. **Por consiguiente, el CEPD pide a la Comisión Europea que evalúe más detenidamente estos aspectos relacionados con la precisión, claridad y exhaustividad de la ley pertinente, y que aporte otros elementos para demostrar que proporciona un nivel de protección sustancialmente equivalente al garantizado en la UE en lo que respecta a las características de la ley. El CEPD destaca, asimismo, que las definiciones amplias también deben evaluarse en relación con la proporcionalidad de las medidas de interceptación.**

157. Además, aunque varios códigos internos de las autoridades competentes de los servicios de inteligencia desarrollan en parte algunos de estos elementos, por ejemplo, en relación con la evaluación de la necesidad y proporcionalidad de la recogida de datos, el CEPD señala que los requisitos del TJUE en relación con la naturaleza de la ley implican que los elementos básicos deben estar previstos en la legislación que establece derechos exigibles, en particular, para que las personas puedan invocar dichos elementos en el marco de la reparación[95]. De hecho, el anexo 7, apartado 6, de la IPA 2016 menciona que los tribunales (y las autoridades de control) «al determinar una cuestión en tales procedimientos, tienen en cuenta el hecho de que una persona no haya aplicado un código» sin aclarar si las personas pueden alegar el incumplimiento de los códigos ante los tribunales (o las autoridades de control). Además, los elementos previstos hasta la fecha en el proyecto de decisión se refieren al reconocimiento por parte del TEDH de la previsibilidad de las normas contempladas[96] en dichos códigos, más que a su «exigibilidad» en los tribunales, como requiere el TJUE, o al hecho de que, en algunos casos, los órganos jurisdiccionales del Reino Unido han hecho referencia a los códigos, si bien ninguno de los casos mencionados ilustra la posibilidad de que las personas exijan los derechos derivados de los códigos. **Si se concluye que la legislación del Reino Unido no indica suficientemente las circunstancias y condiciones en las que se puede adoptar una medida y que estos elementos están efectivamente previstos en los códigos internos de las autoridades de los servicios de inteligencia**, **el CEPD pedirá a la Comisión Europea que evalúe más detenidamente si las personas pueden exigir y hacer valer ante los tribunales las limitaciones y garantías previstas en los diferentes códigos internos de dichas autoridades.**

158. **El segundo aspecto destacable** se refiere al hecho de que las disposiciones relativas a la adquisición y conservación selectivas de datos de comunicaciones, y a la recopilación en bloque, ya sea en la IPA

[93] Véase el asunto Privacy International, apartado 68.

[94] Véase TEDH, Zakharov c. Rusia, 4 de diciembre de 2015, CE:ECHR:2015:1204JUD004714306, apartado 229.

[95] A este respecto, el TJUE consideró que, por ejemplo, el PPD-28 de EE. UU. no cumplía los requisitos, aunque también preveía algunas limitaciones con respecto a la recopilación en bloque de datos, véase el asunto Schrems II, apartado 181.

[96] Véase TEDH, Big Brother Watch y otros c. Reino Unido, 13 de septiembre de 2018, ECLI:CE:ECHR:2018:0913JUD005817013 («Big Brother Watch»), apartado 325: «Dado que el código de la ICO es un documento público, sujeto a la aprobación de ambas cámaras del Parlamento, y debe ser tenido en cuenta tanto por quienes ejercen funciones de interceptación como por los juzgados y tribunales, la Corte ha aceptado expresamente que sus disposiciones podrían tenerse en cuenta al evaluar la previsibilidad del régimen de la RIPA».

2016 o en otras legislaciones como la *Intelligence Services Act 1994*, o la *Regulation of Investigatory Powers Act 2000* (Ley sobre la Regulación de las Facultades de Investigación, de 2000, en lo sucesivo «RIPA de 2000»), también se aplicarán a los datos transferidos de la UE al Reino Unido. Con respecto a la recopilación en bloque, el CEPD subraya que las disposiciones pertinentes de la legislación del Reino Unido permiten la recopilación de datos fuera de dicho país, que pueden incluir datos en tránsito transferidos del EEE al Reino Unido sobre la base de la decisión de adecuación[97]. Por otra parte, el CEPD observa que la Comisión Europea indica que «[c]abe señalar que la conservación y adquisición de datos de comunicaciones, por lo general, no se refieren a los datos personales de interesados de la UE transferidos al Reino Unido en virtud de la presente Decisión. La obligación de conservar o comunicar datos de comunicaciones, con arreglo a las partes 3 y 4 de la IPA 2016, cubre los datos recogidos por los operadores de telecomunicaciones en el Reino Unido directamente de los usuarios de un servicio de telecomunicaciones»[98]. No obstante, el CEPD destaca la falta de claridad con respecto a que solo los establecimientos de los operadores situados en el Reino Unido pueden recibir solicitudes de las autoridades competentes de dicho país, ya que la definición de operador de telecomunicaciones prevista en la sección 261, apartado 10, de la IPA 2016 señala que «un operador es una persona que ofrece o presta un servicio de telecomunicaciones a personas en el Reino Unido *o que controla o proporciona un sistema de telecomunicaciones que está (total o parcialmente) en el Reino Unido o se controla desde el Reino Unido*». En consecuencia, los datos personales de los interesados del EEE podrían realmente verse afectados, por ejemplo, en el caso de datos recogidos o generados por un establecimiento de un operador de telecomunicaciones del Reino Unido situado en el EEE, que se transfieran a un establecimiento de ese mismo operador situado en el Reino Unido sobre la base de la decisión de adecuación (con fines comerciales) y posteriormente recojan, en dicho país, las autoridades públicas competentes.

159. **Por consiguiente, el CEPD opina que es también pertinente analizar estas disposiciones a fin de evaluar el nivel de adecuación del marco legal del Reino Unido y pide a la Comisión Europea que aclare este aspecto y analice con más detenimiento hasta qué punto esto es cierto. En particular, el CEPD pide a la Comisión Europea que aclare su entendimiento sobre el ámbito de aplicación de esta legislación, con indicación de lo que cubre la noción de «usuarios de servicios de telecomunicaciones» y si dada la definición muy amplia de operadores de telecomunicaciones, podrían solicitarse datos de establecimientos de operadores de telecomunicaciones fuera del Reino Unido, en la medida que afecta a los datos de los interesados del EEE.**

160. **El tercer aspecto destacable** se refiere al procedimiento de «doble llave». El CEPD observa que en la IPA 2016 se ha introducido un nuevo procedimiento de «doble llave». No obstante, el CEPD también entiende que incluso si, en principio, la recogida de datos o el acceso a los mismos con fines de seguridad nacional o inteligencia solo puede llevarse a cabo con una orden aprobada por un comisario judicial, la IPA 2016 prevé que «en casos específicos limitados es posible la interceptación legal sin una orden judicial y solo se requiere la autorización previa de las propias autoridades competentes de los servicios de inteligencia [véase más abajo el punto sobre la supervisión], también en el caso de interceptaciones de conformidad con solicitudes en el extranjero (sección 52 de la IPA de 2016)». Como se señala a continuación, esto también coincide con las preocupaciones del CEPD con respecto, en particular, a las comunicaciones en el extranjero. Asimismo, el CEPD observa que, en el caso de la interferencia de equipos, ya sea selectiva o en bloque, también es posible una excepción al procedimiento de doble llave y que el comisario judicial solo está facultado a aprobar la

[97] Véanse los apartados 183 y siguientes del asunto Schrems II sobre la evaluación de una legislación que prevé el acceso a datos en tránsito entre la UE y un tercer país en el marco de una decisión de adecuación.
[98] Véase el considerando 196 del proyecto de decisión.

renovación de las órdenes en bloque (*bulk warrants*) después de un período inicial máximo de 6 meses. **El CEPD pide a la Comisión Europea que evalúe en mayor medida y demuestre que, incluso en los casos en que no se aplica el procedimiento de doble llave, el marco jurídico del Reino Unido ofrece salvaguardias adecuadas, en particular, mediante una supervisión *ex post* efectiva y las posibilidades de recurso que se ofrecen a las personas, para garantizar que el nivel de protección proporcionado es sustancialmente equivalente al que se prevé en la UE (véase también más abajo el punto 4.3.3 sobre la supervisión).**

161. Además, aunque la IPA 2016 ha introducido el procedimiento de «doble llave», el CEPD sigue estando preocupado por determinadas características de la nueva legislación. Tras la presentación de las secciones correspondientes del proyecto de decisión, el CEPD ha analizado los siguientes tipos de recogida de datos y acceso a los mismos en el mismo orden en que los presenta la Comisión Europea. Por lo tanto, el orden de los aspectos evaluados no refleja una jerarquía en cuanto al nivel de preocupación del CEPD.

4.3.1.2. Adquisición y conservación selectivas de los datos de comunicaciones

162. El CEPD observa que hay dos funcionarios que pueden conceder autorizaciones específicas para la obtención de datos de comunicaciones: el ordenador de la *Office for Communications Data Authorisations* («el IPC») y un funcionario experimentado designado (la persona que ocupa el cargo o rango prescrito en la autoridad pública pertinente). Además, en determinados casos, se requiere la autorización de un comisario judicial. No obstante, para el CEPD sigue sin estar claro exactamente qué funcionario, según la ley y al código pertinente, autoriza qué tipo de adquisición selectiva de datos de comunicaciones y hasta qué punto un funcionario designado sería suficientemente independiente[99].

163. **En consecuencia, el CEPD pide a la Comisión Europea que analice más a fondo este aspecto y aporte una explicación más clara sobre estos elementos.**

164. En cuanto a los avisos que exigen la conservación de datos de comunicaciones, el CEPD también observa que dichos avisos pueden dirigirse a una «descripción de operadores». Esta noción parece implicar que se puede solicitar al mismo tiempo a varios operadores que retengan datos. De hecho, la naturaleza selectiva de la adquisición no se refiere al número de operadores, sino al nombre o descripción de las personas, organizaciones, ubicación o grupo de personas que constituyen el «objetivo», una descripción de la naturaleza de la investigación y una descripción de las actividades para las que se emplean el/los equipo(s). Por lo tanto, el CEPD destaca que, dependiendo del número de operadores afectados por dicha «descripción de operadores», los avisos pueden ser más amplios de lo que parece implicar el procedimiento de retención selectiva. **El CEPD invita a la Comisión Europea a analizar con más detenimiento este aspecto y a ofrecer más garantías de que, incluso cuando los avisos se dirigen a varios operadores, se limitan a lo que es estrictamente necesario y proporcionado.**

4.3.1.3. Interferencia de equipos

165. El CEPD observa que, en caso de urgencia, la «interferencia de equipos» puede constituir una excepción al procedimiento de doble llave[100]. En este sentido, el CEPD manifiesta su preocupación por que los fines para los que se requiere la interferencia de equipos son amplios y los criterios de

[99] Véase también más abajo el análisis sobre el procedimiento de doble llave y la independencia del comisario judicial.
[100] Véase la sección 109 de la IPA 2016.

urgencia (en cuyo caso el comisario judicial no está obligado a proporcionar una autorización previa tras evaluar la necesidad y proporcionalidad de dicha interferencia) siguen sin estar claros. Dado que en esta última situación «la orden deja de tener efecto y no podrá renovarse», el CEPD entiende que en caso de que el comisario judicial no autorice *ex post* la interferencia de equipos, los datos recogidos entretanto seguirán considerándose legalmente recogidos. El comisario judicial podrá emitir una orden específica para eliminar estos datos[101].

166. **El CEPD pide a la Comisión Europea que evalúe más detenidamente las condiciones en las que se puede invocar la urgencia y que aclare las posibles vías para el ejercicio de los derechos de los interesados, así como las posibles vías de recurso que se les ofrecen en el marco de operaciones de interferencia de equipos, especialmente cuando tienen lugar en un contexto de urgencia que conlleva una excepción al procedimiento de doble llave.**

4.3.1.4. Interceptación en bloque de los datos de los portadores

167. Como se describe en el informe sobre la revisión de los poderes de interceptación en bloque[102], «[l]a interceptación en bloque normalmente implica la recopilación de comunicaciones mientras transitan entre portadores particulares (enlaces de comunicación)». La ficha informativa oficial de la IPA 2016 describe la «interceptación en bloque» como «el proceso de recopilación de un número de comunicaciones, seguido de la selección de las comunicaciones específicas que se leerán, examinarán y escucharán cuando sea necesario y proporcionado». El CEPD señala que la «interceptación en bloque» de datos en realidad implica la recogida de datos incluso antes de cualquier filtrado por parte de los selectores (ya sea simple, en el marco del seguimiento de personas que ya se sabe que representan una amenaza, o complejo, en el marco de la identificación de nuevas amenazas y de personas de interés previamente desconocidas).

168. La adquisición de los datos de comunicaciones en bloque fue también una de las cuestiones (además de si esta recogida de datos se realizó en el marco de la legislación de la UE, incluso con fines de seguridad nacional) que examinó el TJUE en el asunto Privacy International, que dio lugar a una sentencia de la Gran Sala emitida el 6 de octubre de 2020. La IPA 2016 sustituye la legislación que fue objeto de esta sentencia.

169. El CEPD observa que, con la introducción de la IPA 2016 en el Derecho del Reino Unido, ahora también se exige una orden para interceptar datos en bloque. El proceso para emitir dicha orden se basa en la determinación de «fines operativos». Los jefes de los servicios de inteligencia establecen la lista de estos fines operativos, que posteriormente aprueba el Secretario de Estado. Esta decisión es aprobada, a su vez, por un comisario judicial independiente que deberá examinar si la orden es necesaria y proporcionada a los fines operativos. El CEPD entiende que el comisario judicial no está facultado para evaluar los fines operativos en sí mismos, solo si la orden es necesaria y proporcionada a los fines operativos que figuran en ella. La Comisión Parlamentaria de Inteligencia y Seguridad recibe una copia de la lista cada tres meses, y el Primer Ministro la revisa por lo menos una vez al año.

170. No obstante, basándose en los elementos que proporciona la Comisión Europea en el proyecto de decisión, parece difícil evaluar el alcance de los fines operativos previstos en la lista y si la recogida

[101] Véase la sección 110, subsección 3, letra b), de la IPA 2016.

[102] Véase el Informe sobre la revisión de los poderes de interceptación en bloque elaborado por el Independent Reviewer of Terrorism Legislation (supervisor independiente del Reino Unido de la legislación en materia de terrorismo), de agosto de 2016.

de datos que permiten cumple el umbral que establece el TJUE (por ejemplo, la circunscripción de la recogida de datos a una zona geográfica podría reducirse a unas pocas calles o a todo el EEE).

171. Además, el CEPD subraya que los datos recogidos en bloque pueden conservarse durante largos períodos (y estar disponibles para el acceso ulterior con el fin de ser examinados). De hecho, el CEPD señala que la sección 150, apartados 5 y 6, de la IPA 2016 solo prevén la destrucción de las copias de los datos recogidos y únicamente si su conservación no es necesaria, o no es probable que sea necesaria, en interés de la seguridad nacional, por cualquier otro motivo que entre en el ámbito de aplicación de la sección 138, apartado 2, de la IPA 2016 o si la retención no es necesaria para una serie de otros fines[103]. El CEPD hace hincapié en que estos motivos parecen muy amplios y, en cualquier caso, solo se mencionan las copias de los datos obtenidos.

172. Además, el CEPD observa que, en casos urgentes, la IPA 2016 también permite la modificación de órdenes sin la autorización previa de un comisario judicial y que, en tal caso, si el comisario judicial consultado *ex post*, dentro de los tres días hábiles siguientes a la modificación, se niega a autorizarla, la orden tendrá efecto como si la modificación no se hubiera realizado, pero los datos recopilados entretanto se considerarán legalmente recogidos[104]. El comisario judicial podrá emitir una orden específica para eliminar estos datos[105].

173. **Por consiguiente, el CEPD pide a la Comisión Europea que clarifique y evalúe más detalladamente las interceptaciones en bloque, en particular en lo que respecta a la selección y aplicación de selectores en el marco de estos procedimientos de interceptación en bloque, a fin de aclarar hasta qué punto el acceso a los datos personales cumple con el umbral establecido por el TJUE (véase también más abajo la sección 4.3.1.7., en particular la relativa a la supervisión de los selectores), y qué salvaguardias existen para proteger los derechos fundamentales de las personas cuyos datos son interceptados en este contexto, también en lo que respecta a los períodos de conservación de dichos datos. Sería especialmente útil una evaluación independiente de las autoridades de control competentes del Reino Unido.**

174. **El CEPD señala, además, que es aún más crítico que en el caso de las «comunicaciones relacionadas con el extranjero» que están dentro del alcance de las prácticas de interceptación en bloque, el Reino Unido podría interceptar directamente y recoger en bloque datos en el EEE, incluidos los datos en tránsito entre el EEE y el Reino Unido que entraría en el ámbito de aplicación del proyecto de decisión (véase más adelante la sección 4.3.2. sobre el uso ulterior de la información recogida con fines de seguridad nacional y comunicación en el extranjero).**

4.3.1.5. Protección y garantías para datos secundarios

175. Además, al CEPD manifiesta su preocupación por el hecho de que la legislación pertinente del Reino Unido relacionada con la interceptación en bloque no prevea el mismo nivel de protección para todos los datos de las comunicaciones. Según la sección 137 de la IPA 2016, los «datos secundarios», que pueden obtenerse con una orden en bloque incluyen tanto los «datos de sistema», «que están comprendidos en la comunicación, incluidos como parte de ella, adjuntos o asociados lógicamente con la misma (ya sea por el remitente o de otra forma)», como los «datos de identificación», «que están comprendidos en la comunicación, incluidos como parte de ella, adjuntos o asociados lógicamente con la misma (ya sea por el remitente o de otra forma) que se pueden separar lógicamente del resto de la comunicación y si se separan, no revelan nada de lo que razonablemente

[103] Véanse las subsecciones 3 y 6 de la sección 150 de la IPA 2016.
[104] Véase la sección 147 de la IPA 2016 (parte 6, capítulo I).
[105] Véase la sección 181, subsección 3, letra b), de la IPA 2016.

podría considerarse el significado (si lo hubiera) de la comunicación, sin tener en cuenta cualquier significado resultante de la comunicación en sí o de los datos relativos a la transmisión de la comunicación»[106].

176. El CEPD observa que cuando estos «datos secundarios», también conocidos como «metadatos»[107], se recogen en bloque no parecen ser objeto de las mismas garantías que los datos recogidos con una orden específica o los datos de contenido recopilados en bloque. De hecho, el CEPD advierte que la selección de los contenidos interceptados está sujeta a más garantías[108] que la selección de datos secundarios[109].

177. Asimismo, el CEPD destaca que tanto el TEDH[110] como el TJUE[111] han cuestionado que estos datos sean menos sensibles que otros, en particular, que los datos de contenido. De hecho, el Código práctico relativo a las interceptaciones presenta como ejemplos de «datos secundarios» los «datos de sistemas», como las configuraciones de encaminadores, las direcciones de correo electrónico o los identificadores de los usuarios, pero también los identificadores de cuenta alternativos y los «datos de identificación», como la ubicación de una reunión en una cita del calendario y la información sobre fotografías, como la hora, la fecha y el lugar en que se tomó. **Por ello, el CEPD destaca la evaluación coherente del TEDH y el TJUE, y recuerda las preocupaciones expresadas con respecto a que los datos secundarios deberían estar sujetos a garantías específicas debido a su sensibilidad. Por consiguiente, el CEPD pide a la Comisión Europea que analice cuidadosamente si las salvaguardias previstas en la legislación del Reino Unido para dicha categoría de datos personales garantizan un nivel de protección sustancialmente equivalente al que se garantiza en la UE.**

[106] Los «datos de sistemas» y los «datos de identificación» se definen en la sección 263 de la IPA 2016.
[107] Véase el Informe sobre la revisión de los poderes de interceptación en bloque elaborado por el Independent Reviewer of Terrorism Legislation (supervisor independiente del Reino Unido de la legislación en materia de terrorismo), de agosto de 2016.
[108] Véanse la sección 152, subsección 1, letra c), y las subsecciones 3 y siguientes de la IPA 2016.
[108] Véanse la sección 152, subsección 1, letra c), y las subsecciones 3 y siguientes de la IPA 2016.
[109] Véase la sección 152, subsección 1, letras a) y b), de la IPA 2016.
[110] Véase TEDH, Big Brother Watch, apartado 357, remitido a la Gran Sala: «En consecuencia, si bien el Tribunal no duda que los datos de las comunicaciones conexas son una herramienta fundamental para los servicios de inteligencia en la lucha contra el terrorismo y los delitos graves, no considera que al eximirlos en su totalidad de las garantías aplicables a la búsqueda y examen de contenidos, las autoridades hayan logrado un justo equilibrio entre los intereses públicos y privados en conflicto. Si bien el Tribunal no sugiere que los datos de las comunicaciones conexas solo deban ser accesibles a efectos de determinar si una persona se encuentra o no en las Islas Británicas, ya que hacerlo requeriría la aplicación a dichos datos de normas más estrictas que las que se aplican al contenido, no obstante, debe haber suficientes salvaguardias para garantizar que la exención de los datos las de comunicaciones conexas de los requisitos de la sección 16 de la RIPA se limite a lo necesario para determinar si una persona se encuentra, por el momento, en las Islas Británicas».
[111] Véase TJEU, asunto Privacy International, apartado 71: «La injerencia que supone la transmisión de los datos de tráfico y de localización a las agencias de seguridad e inteligencia en el derecho consagrado en el artículo 7 de la Carta debe considerarse especialmente grave, habida cuenta, en particular, del carácter sensible de la información que pueden proporcionar esos datos y, en particular, de la posibilidad de determinar a partir de ellos el perfil de las personas afectadas, ya que tal información es tan sensible como el propio contenido de las comunicaciones. Además, puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante (véanse, por analogía, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 27 y 37, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 99 y 100)».

4.3.1.6. Tratamiento automatizado de los datos de las comunicaciones

178. El CEPD observa que las autoridades de los servicios de inteligencia no solo utilizan selectores simples o complejos para filtrar los datos adquiridos en bloque. Según el informe de 2015 de la Comisión Parlamentaria de Inteligencia y Seguridad, disponen, además, de otras herramientas de procesamiento automatizado para analizar «grandes volúmenes de información que permiten a las agencias encontrar también vínculos, patrones, asociaciones o comportamientos que pueden suponer una amenaza grave que debe ser investigada»[112]. **El CEPD es consciente de que este informe público se refiere a prácticas con arreglo al marco jurídico anterior, que posteriormente fue sustituido por la IPA 2016. No obstante, considera necesario que las autoridades de control competentes del Reino Unido lleven a cabo una evaluación y supervisión independientes sobre el uso de herramientas de procesamiento automatizado y pide a la Comisión Europea que evalúe más detenidamente este problema y las garantías que se reconocerían o que podrían reconocerse, en este contexto, a los interesados del EEE**.

4.3.1.7. Riesgos de cumplimiento y prácticas no conformes de las autoridades competentes de los servicios de Inteligencia

179. El CEPD toma nota de que hay informes de supervisión detallados disponibles que aportan elementos valiosos con respeto a lo que consideran prácticas de cumplimiento positivas, así como a los riesgos de cumplimiento y las prácticas no conformes identificadas.

180. En este sentido, según indica el IPC en su informe de 2019, varios elementos relativos a la aplicación del marco jurídico por parte de las distintas autoridades competentes han revelado (el riesgo de) una serie de incumplimientos por parte de dichas autoridades.

181. En primer lugar, el CEPD observa que para MI5 y el SIS, en particular para M15, los criterios para clasificar un conjunto de datos como conjunto de datos personales en bloque o como datos específicos no siempre parecen claros, lo que puede dar lugar a que no se apliquen a estos datos las garantías adecuadas[113]. En su informe de 2019, el IPC sugirió que «esta cuestión debía resolverse con carácter prioritario»[114]. Asimismo, en relación con los conjuntos de datos personales en bloque, el CEPD observa que en el caso del GCHQ, aunque la clasificación de dichos conjuntos de datos parece ser satisfactoria (pero todavía tiene que ser auditada por el IPC), en marzo de 2019, en el marco de la revisión interna del cumplimiento de las órdenes que llevó a cabo un equipo especializado, se manifestaron serias preocupaciones y el 50 % de las justificaciones relativas a las órdenes de

[112] Véase Comisión Parlamentaria de Inteligencia y Seguridad, *Privacy and Security: A modern and transparent legal framework* (Privacidad y Seguridad: Un marco jurídico moderno y transparente), 2015, apartado 18, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Véase el apartado 8.39 del informe anual de 2019 del Comisario de Facultades de Investigación, 15 de diciembre de 2020, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: «Se ha observado una evolución positiva del [Bulk Oversight Panel (BOP)] y su impacto en la gestión del cumplimiento interno. *Se sigue tratando de aclarar en mayor medida el proceso que MI5 utiliza para llevar a cabo el examen inicial de los nuevos conjuntos de datos, a fin de comprender mejor la decisión de clasificar un conjunto de datos como datos personales en bloque o, por ejemplo, como datos específicos. Suscitó preocupación una acción no resuelta en las actas del BOP en torno a la resolución de discrepancias entre MI5 y el SIS con respecto a la asignación de datos personales en bloque. Dado el diferente uso que se hace de los datos y los distintos cortes de datos que se mantienen, es posible que ambas agencias tengan el mismo conjunto de datos, o versiones del mismo, y que una pueda categorizarlo legalmente como en bloque y la otra como específico.* Existe el riesgo de que, si una de las agencias ha categorizado incorrectamente los datos almacenados como específicos, esos datos se mantengan sin la autorización adecuada y puedan no estar sujetos a las garantías adecuadas».

[114] Véase el apartado 8.39 del informe anual de 2019 del Comisario de Facultades de Investigación.

adquisición en bloque de datos que revisó el equipo de cumplimiento del GCHQ no cumplían los criterios requeridos. Según el IPC, el equipo de cumplimiento había comenzado a trabajar para investigar el problema y volver a formar al personal a fin de mejorar esta situación. La formación actualizada sobre las disposiciones de la IPA 2016 y la formación complementaria que impartieron las redes de políticas y cumplimiento («PCN») han mejorado el nivel cumplimiento del GCHQ en este ámbito. El IPC no espera que el nivel se reduzca en las inspecciones futuras, pero continuará revisando de cerca esta cuestión[115]. **Por consiguiente, el CEPD comparte la opinión de que se necesita un examen más profundo y una mayor seguimiento de dichos elementos por parte de la Comisión Europea en el marco de la evaluación del nivel de protección a fin de garantizar que se mejore el nivel de cumplimiento, como se subraya en el informe del IPC, y recuerda que, según lo dispuesto en el artículo 45 del RGPD, la ejecución y la aplicación concreta del marco jurídico también deberán tenerse en cuenta al evaluar la equivalencia esencial de un tercer país.**

182. En términos más generales, el CEPD hace hincapié los aspectos destacables que el IPC comparte con respecto a las «búsquedas basadas en actividades» lideradas por funcionarios de MI5, que permiten a un investigador llevar a cabo más de una búsqueda de los conjuntos de datos personales en bloque a su disposición, y los «riesgos graves de cumplimiento asociados con determinados entornos tecnológicos que utiliza MI5» relativos al lugar donde se almacenan los datos en el entorno, quién tiene acceso a ellos, hasta qué punto se copian o comparten, los procesos de eliminación que se aplican y los períodos de conservación. Aunque el IPC indica que se han adoptado medidas y se han introducido salvaguardias, algunas de las cuales siguen siendo manuales y lideradas por personas a título individual, destaca que es fundamental que «MI5 continúe manteniendo estos nuevos procesos y proporcionando recursos suficientes para que funcionen con eficacia». «Si el MI5 identifica un aumento en comportamientos no conformes»[116], el IPC espera que se le informe a la mayor brevedad. **Por consiguiente, el CEPD pide a la Comisión Europea que supervise estrechamente estos aspectos en el futuro**.

183. En lo que respecta al GCHQ, la CEPD entiende también por el informe del IPC que, en el caso de las operaciones realizadas con arreglo a órdenes en bloque, «la calidad de las solicitudes de autorización interna era variable y se considera que hay margen de mejora en la forma en que se realizan dichas solicitudes»[117], y en el caso de la interferencia selectiva de equipos, las explicaciones sobre el uso de descriptores generales a veces eran demasiado generales e imprecisas[118]. Además, el CEPD observa que en el marco de la interferencia en bloque de equipos, el IPC recomienda que «las solicitudes registren de manera consistente y explícita el vínculo entre el objetivo, el fin legal y los requisitos de inteligencia»[119], que «al evaluar la proporcionalidad, todas las solicitudes aborden claramente la cuestión del potencial de intromisión colateral y las medidas de mitigación pertinentes»[120], y destaca que, a pesar de los progresos, «todavía hay margen de mejora»[121] y se debe prestar más atención también en el futuro.

184. En relación con el régimen de interceptación en bloque en virtud de la RIPA de 2000, que desde entonces ha sido sustituida por las disposiciones de la IPA 2016, el CEPD recuerda que la supervisión insuficiente tanto de la selección de los portadores de internet para la interceptación como del

[115] Véase el apartado 10.48 del informe anual de 2019 del Comisario de Facultades de Investigación.
[116] Véase el apartado 8.52 del informe anual de 2019 del Comisario de Facultades de Investigación.
[117] Véase el apartado 10.2 del informe anual de 2019 del Comisario de Facultades de Investigación.
[118] Véanse los apartados 10.16 y 10.17 del informe anual de 2019 del Comisario de Facultades de Investigación.
[119] Véase el apartado 10.23 del informe anual de 2019 del Comisario de Facultades de Investigación.
[120] Véase el apartado 10.23 del informe anual de 2019 del Comisario de Facultades de Investigación.
[121] Véase el apartado 10.23 del informe anual de 2019 del Comisario de Facultades de Investigación.

filtrado, la búsqueda y la selección de las comunicaciones interceptadas para el examen, fue uno de los aspectos fundamentales que, en el asunto Big Brother Watch, ahora remitido a la Gran Sala, el TEDH consideró que incumplía el artículo 8 del CEDH con respecto a la legislación anterior sobre los facultades de investigación de las autoridades del Reino Unido en el contexto de la seguridad nacional. **El CEPD invita a la Comisión Europea a verificar el estado de los procedimientos, a tener en cuenta estos elementos y especificarlos en la decisión de adecuación en caso de que la Comisión Europea la adopte.**

185. En este asunto, el TEDH indicó: no estar «convencido de que las salvaguardias que rigen la selección de los portadores para la interceptación y del material interceptado para su examen sean lo suficientemente sólidas como para ofrecer garantías adecuadas contra el abuso. Sin embargo, la mayor preocupación es la ausencia de una supervisión independiente sólida de los selectores y los criterios de búsqueda utilizados para filtrar las comunicaciones interceptadas»[122]. Como ha destacado el IPC, «esta conclusión encuentra eco en una recomendación similar en el informe de la Comisión Parlamentaria de Inteligencia y Seguridad *Privacy and Security: A modern and transparent legal framework report (Privacidad y Seguridad: Un marco jurídico moderno y transparente), de marzo 2015»*[123]. **El CEPD acoge con satisfacción que, a consecuencia de ello, en 2019, el IPC llevó a cabo una revisión de su método de inspección de las interceptaciones en bloque «que incluyó una revisión cuidadosa de las formas técnicamente complejas en las que realmente se llevan a cabo»[124] y se comprometió a incluir en las inspecciones de estas interceptaciones «un examen detallado de los selectores y criterios de búsqueda aludidos previamente por el TEDH»[125] a partir de 2020. Dada la importancia de esta cuestión, al CEPD manifiesta su preocupación por el hecho de que el IPC todavía no haya llevado a cabo un examen detallado de los selectores y criterios de búsqueda, y pide a la Comisión Europea que siga de cerca los avances al respecto, especialmente porque todavía no se ha aclarado la estructura concreta de dicha supervisión[126].**

4.3.2. Uso ulterior de la información recogida con fines de aplicación de la ley y comunicación en el extranjero

186. En lo que respecta al uso ulterior de la información recogida con fines de seguridad nacional, en su evaluación, la Comisión Europea hace referencia a la sección 87, apartado 1, de la DPA de 2018, que en efecto establece que «los datos personales así recopilados no deben tratarse de una manera que sea incompatible con la finalidad para la que se recogen». No obstante, el CEPD señala que, según la sección 110 de la DPA de 2018, esta disposición puede estar sujeta a exenciones de seguridad nacional. Además, el CEPD observa que, ya sea para la interceptación y el examen selectivo, para la adquisición y retención selectiva de los datos de comunicaciones, para la interferencia selectiva de equipos o para la interceptación en bloque y la interferencia en bloque de equipos, la legislación prevé la posibilidad de «comunicación en el extranjero».

[122] Véase TEDH, Big Brother Watch, apartado 347.
[123] Véase el apartado 10.28 del informe anual de 2019 del Comisario de Facultades de Investigación.
[124] Véase el apartado 10.28 del informe anual de 2019 del Comisario de Facultades de Investigación.
[125] Véase el apartado 10.28 del informe anual de 2019 del Comisario de Facultades de Investigación.
[126] Véase el apartado 10.28 del informe anual de 2019 del Comisario de Facultades de Investigación: «Todavía no se ha acordado la estructura exacta de esta inspección».

4.3.2.1. Uso ulterior, comunicación en el extranjero y el marco jurídico aplicable en el Reino Unido

187. La Comisión Europea ha identificado la parte 4 de la DPA de 2018 y, en particular, su sección 109 como disposiciones pertinentes que establecen requisitos específicos para el uso ulterior de la información recogida y especialmente la transferencia internacional de datos personales por parte de los servicios de inteligencia a terceros países u organizaciones internacionales. Sin embargo, el CEPD observa que la sección 110 de la DPA de 2018 establece una exención de seguridad nacional que especifica que determinadas disposiciones de dicha Ley no se aplicarán, si se solicita una exención de las mismas con el fin de salvaguardar la seguridad nacional. Las disposiciones en cuestión incluyen el capítulo 2 de la parte 4 de la DPA de 2018 relacionado con los principios de protección de datos, incluida la limitación de los fines, así como el capítulo 3 de la parte 4 de dicha Ley relativa a los derechos de los interesados. La sección 109 de la DPA de 2018, leída en combinación con la sección 110 de dicha Ley y las condiciones en las que se aplica pueden dar lugar a casos en los que los servicios de inteligencia lleven a cabo transferencias internacionales de datos personales a terceros países sin aplicar las disposiciones relacionadas con los principios de protección de datos y los derechos de los interesados.

188. Como ha determinado la Comisión Europea, dicha exención debe examinarse caso por caso y solo puede invocarse en la medida en que la aplicación de una disposición en particular tenga consecuencias negativas para la seguridad nacional. De hecho, el objetivo de expedir un certificado nacional a los servicios de inteligencia del Reino Unido es certificar que se requiere una exención con respecto a los datos personales específicos que se someten a tratamiento con el fin de salvaguardar la seguridad nacional. No obstante, el CEPD observa que en su orientación relativa al certificado de seguridad nacional en virtud de la DPA de 2018, el Ministerio del Interior del Reino Unido aclara que «[e]s importante tener en cuenta desde el principio que no se exige un certificado para acogerse a la exención de seguridad nacional. De hecho, en la mayoría de los casos, los responsables del tratamiento determinarán por sí mismos la aplicabilidad de la exención de seguridad nacional». [127] Además, en dicha orientación se señala que «los certificados de seguridad nacional pueden aplicarse a datos personales que pueden identificarse específicamente o cubrir una categoría más amplia de datos personales. Pueden ser tanto preventivos como retroactivo». [128] Por consiguiente, la exención de seguridad nacional podrá aplicarse a una transferencia internacional de datos personales por parte de los servicios de inteligencia a terceros países en ausencia de un certificado de seguridad nacional.

189. Además, el CEPD señala que, por ejemplo, el certificado de seguridad nacional DPA/ S27/Security Service[129] establece que hasta el 24 de julio de 2024, los datos personales que se hayan tratado «para los servicios de seguridad, en su nombre, a petición o con la ayuda o asistencia de ellos» y «cuando dicho tratamiento sea necesario para facilitar el desempeño adecuado de las funciones de los servicios de seguridad que se describen en la sección 1 de la *Security Service Act 1989* [Ley de Servicios de Seguridad de 1989]» están exentos de las disposiciones de la legislación del Reino Unido correspondientes al capítulo V del RGPD relativas a las transferencias de datos personales a terceros países u organizaciones internacionales. Si bien los otros certificados de seguridad nacional que son públicos no prevén una exención de las disposiciones de la sección 109 de la DPA de 2018, cabe

[127] Véase Ministerio del Interior, *The Data Protection Act 2018, National Security Certificates Guidance*, de agosto de 2020, apartado 3, p. 3.
[128] Véase Ministerio del Interior, *The Data Protection Act 2018, National Security Certificates Guidance*, de agosto de 2020, apartado 5, p. 4.
[129] Véase el certificado de referencia: DPA/ S27/Security Service, sección 27 de la DPA de 2018, Certificado de la Secretaría de Estado, 24 de julio de 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

recordar que parte o la totalidad del texto de un certificado de seguridad nacional puede omitirse si su publicación es contraria a intereses de seguridad nacional, al interés público o puede poner en peligro la seguridad de alguna persona.

190. En general, al evaluar el proyecto de Decisión en relación con estas disposiciones, el CEPD observa que las garantías para estas comunicaciones únicamente hacen referencia a la exigencia de que el destinatario de los datos respete los requisitos relativos a la seguridad de los mismos, a la limitación del alcance de la comunicación a lo necesario, a la retención de datos y a la restricción de su acceso a un número limitado de personas. Por lo tanto, **el CEPD subraya que en lo que respecta a las comunicaciones en el extranjero, la aplicación de la exención de seguridad nacional prevista en la legislación del Reino Unido puede dar lugar a situaciones en las que en el tercer país de destino, no se prevean ni respeten plenamente ni las salvaguardias que garantizan los principios de limitación, necesidad y proporcionalidad de los fines, ni los derechos de las personas, la supervisión y los recursos. Por consiguiente, el CEPD recomienda a la Comisión Europea que examine más a fondo las garantías generales previstas en la legislación del Reino Unido en lo que respecta a las comunicaciones en el extranjero, en particular teniendo en cuenta la aplicación de las exenciones de seguridad nacional.**

4.3.2.2. Comunicación en el extranjero e intercambio de inteligencia en el marco de la cooperación internacional

191. El CEPD señala, además, que, en el marco de su evaluación sobre la adecuación, la Comisión Europea no ha considerado los acuerdos internacionales vigentes celebrados entre el Reino Unido y terceros países u organizaciones internacionales que pueden prever disposiciones específicas para la transferencia internacional de datos personales por parte de los servicios de inteligencia a terceros países.

192. Asimismo, el CEPD destaca que la evaluación de la Comisión Europea se basa principalmente en el análisis de la parte 4 de la DPA de 2018 y le preocupado, en particular, que la IPA 2016 se centra en las «solicitudes» de intercambio de inteligencia con socios extranjeros, pero no aborda otras formas de intercambio de inteligencia. A este respecto, el CEPD observa que el proyecto de decisión de la Comisión Europea no hace referencia ni evalúa la articulación entre el marco legislativo del Reino Unido y el Acuerdo de inteligencia en materia de comunicaciones entre el Reino Unido y los Estados Unidos («Acuerdo IC Reino Unido-EE. UU.»). En una declaración reciente con motivo del 75.º aniversario de este acuerdo, la NSA señaló que esta asociación permite «que las agencias compartan toda la información posible, con restricciones mínimas» y que «este documento innovador establece las políticas y procedimientos para que los profesionales de inteligencia del Reino Unido y EE. UU. compartan información sobre comunicaciones, traducción, análisis y descifrado de códigos»[130]. Además, este acuerdo se ha convertido en la base de otras asociaciones de inteligencia con Australia, Canadá y Nueva Zelanda.

193. La naturaleza secreta de este acuerdo y sus disposiciones específicas plantean un serio desafío en términos de claridad y previsibilidad de la ley en relación con el uso ulterior y la comunicación en el extranjero de la información recabada por las autoridades del Reino Unido con fines de seguridad nacional. En este contexto, el CEPD recuerda que en lo que respecta al nivel de protección garantizado en la UE, el TJUE ha subrayado que la legislación que implique una injerencia en el derecho fundamental a la protección de datos personales debe «contener reglas claras y precisas

[130] Véase el comunicado de prensa de la NSA, *GCHQ and NSA Celebrate 75 Years of Partnership* (El GCHQ y la NSA celebran 75 años de asociación), 5 de febrero de 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de estos. La necesidad de dichas salvaguardias es aún más acusada en aquellos casos en que los datos personales sean objeto de tratamiento automatizado y cuando exista un riesgo considerable de que se produzca un acceso ilícito a los mismos»[131]. Por consiguiente, el CEPD estima que en el marco de su evaluación de adecuación, la Comisión Europea debería considerar el impacto del Acuerdo IC Reino Unido-Estados Unidos.

194. En su sentencia de la primera sección, de 13 de septiembre de 2018, en el asunto Big Brother Watch, el TEDH analizó el régimen de intercambio de inteligencia del Reino Unido y, en particular, el Acuerdo IC Reino Unido-EE. UU. El TEDH señaló, de hecho, que «[e]l marco jurídico que permite a los servicios de inteligencia del Reino Unido solicitar material interceptado de agencias de inteligencia extranjeras no está contenido en la RIPA. El Acuerdo de inteligencia de comunicaciones entre el Reino Unido y los EE. UU, de 5 de marzo de 1946, permite específicamente el intercambio de material entre los Estados Unidos y el Reino Unido»[132] y consideró que existe «una base jurídica para solicitar inteligencia a agencias de inteligencia extranjeras, y que esa ley es suficientemente accesible»[133]. Si bien el TEDH ha concluido que no se ha violación el artículo 8[134] del CEDH en relación con el régimen de intercambio de inteligencia, el CEPD observa que esta sentencia se ha remitido a la Gran Sala, cuya decisión aún está pendiente. Además, el CEPD señala que en una opinión en parte concurrente y en parte disidente a esta sentencia, el juez Koskelo, junto con el juez Turković[135], ha concluido que existe una violación del artículo 8 del CEDH en relación con el régimen de intercambio de inteligencia, afirmando que «[e]s fácil estar de acuerdo con el principio de que no debe permitirse que cualquier acuerdo en virtud del cual la inteligencia de las comunicaciones interceptadas se obtenga a través de servicios de inteligencia extranjeros, ya sea sobre la base de solicitudes para llevar a cabo dicha interceptación o para transmitir sus resultados, implique la elusión de las garantías que deben existir para toda vigilancia por parte de las autoridades nacionales (véanse los apartados 216, 423 y 447). De hecho, cualquier otro planteamiento sería inverosímil».

195. Como se destacaba en varios informes de medios de comunicación y organizaciones no gubernamentales[136], [137], la versión más reciente del Acuerdo IC Reino Unido-EE. UU. que se ha hecho pública data de 1956 y, desde entonces, la tecnología de la comunicación y la naturaleza de la inteligencia de señales han cambiado significativamente. Por ejemplo, los informes de los medios de comunicación han revelado que el GCHQ intercepta los datos que se transiten a través de cables submarinos y llegan al Reino Unido, y los pone a disposición de la NSA[138].

---

[131] Véase el asunto Schrems I, apartado 91.
[132] Véase TEDH, Big Brother Watch, apartado 425.
[133] Véase TEDH, Big Brother Watch, apartado 427.
[134] Véase TEDH, Big Brother Watch, apartado 448.
[135] Véase TEDH, Big Brother Watch, opinión en parte concurrente y en parte disidente del juez Koskelo, junto con el juez Turković.
[136] Véase BBC, *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes*, 5 de marzo de 2021, https://www.bbc.com/news/uk-56284453.
[137] Véase Privacy International, *Policy Briefing - UK Intelligence Sharing Arrangements* (Nota Informativa: Los Acuerdos de Intercambio de Inteligencia del Reino Unido), abril de 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Véase The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications*, 21 de junio de 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

196. Para el CEPD, una cuestión fundamental en relación con el intercambio de inteligencia es si la sección 109 de la DPA de 2018 y las disposiciones de la IPA 2016 siguen siendo aplicables cuando los servicios de inteligencia del Reino Unido actúan de conformidad con el Acuerdo IC Reino Unido-EE. UU. Otro aspecto clave que debe evaluarse es si las disposiciones o la aplicación efectiva de dicho acuerdo tienen un impacto en el nivel de protección de los datos personales en tránsito desde el EEE al Reino Unido, o permiten un acceso directo y la adquisición de datos personales por parte de los servicios de inteligencia de otros terceros países.

197. En consecuencia, además de las reservas expresadas en cuanto a las «comunicaciones en el extranjero» con arreglo a la parte 4 de la DPA 2018 y la exención de seguridad nacional que le es aplicable, así como a las solicitudes en el marco de la IPA 2016, **el CEPD manifiesta su preocupación por otras formas de intercambio de información y comunicaciones en virtud de otros instrumentos, en particular, los diversos acuerdos internacionales celebrados por el Reino Unido con otros terceros países, especialmente cuando estos instrumentos siguen siendo inaccesibles para el público, como el Acuerdo IC Reino Unido-EE. UU. El efecto de dicho acuerdo podría dar lugar a la elusión de las garantías identificadas en relación con el acceso y uso de datos personales con fines de seguridad nacional.**

198. De hecho, el CEPD comparte la opinión expresada por el Relator Especial de las Naciones Unidas, Joe Cannatacci, de que «el intercambio de inteligencia no debe resultar en una puerta trasera para obtener o facilitar a otros la obtención de inteligencia sin respetar las garantías nacionales, ni una escapatoria para que los gobiernos extranjeros con normas menos rigurosas sobre la protección de la privacidad (u otros derechos humanos) obtengan información de inteligencia del Reino Unido que podría dar lugar a violaciones de derechos humanos»[139].

199. Asimismo, **el CEPD considera que la celebración de acuerdos bilaterales o multilaterales con terceros países con fines de cooperación en materia de inteligencia que proporcionen una base jurídica para la interceptación o adquisición directa de datos personales o la transferencia de dichos datos 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.**

4.3.3. Supervisión

200. El CEPD hace hincapié en la importancia de una supervisión exhaustiva por parte de autoridades de control independientes para garantizar un nivel adecuado de protección de datos. El objetivo de la garantía de independencia (en el sentido del artículo 8, apartado 3, de la Carta de la UE) de las autoridades de control es asegurar un control eficaz y confiable del cumplimiento de las normas sobre protección de las personas en lo que respecta al tratamiento de datos personales.

201. Cuando se accede a datos personales y se utilizan estos datos con fines de seguridad nacional, la función de supervisión la llevan a cabo principalmente el IPC y los comisarios judiciales (en lo sucesivo, «comisarios judiciales»).

[139] Véase *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland*. Londres («Declaración de fin de misión del Relator Especial sobre el derecho a la privacidad al concluir su misión en el Reino Unido de Gran Bretaña e Irlanda del Norte»), 29 de junio de 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

202. **EL CEPD generalmente reconoce como una mejora significativa la introducción de comisarios judiciales en la IPA 2016.** De acuerdo con una de las solicitudes anteriores, se invita a la Comisión Europea a evaluar con más detenimiento la independencia de los **comisarios judiciales y, en particular, hasta qué punto la independencia del IPC y la oficina del IPC («IPCO») está garantizada legalmente, ya que esto no se refleja en la IPA 2016.** Esto resulta especialmente importante dado que el IPC decide sobre los recursos presentados por el gobierno cuando una solicitud de una **medida** de vigilancia ha sido denegada **por** un comisario judicial.

203. El IPC tiene funciones de control *ex ante* y *ex post*. En lo que respecta al control *ex ante*, el CEPD entiende que la función de los comisarios judiciales es aprobar, en casos individuales, diferentes medidas de vigilancia, incluida la interceptación selectiva y la adquisición en bloque de datos de comunicaciones. El CEPD observa, además, que no puede deducirse de la jurisprudencia del TJUE que la autorización previa de medidas de vigilancia sea un requisito absoluto para garantizar la proporcionalidad de dichas medidas[140].

204. Sin embargo, a fin de evaluar la eficacia de este nivel de control, el CEPD considera necesario aclarar las situaciones en las que es posible una interceptación legal sin la autorización previa de los comisarios judiciales.

205. En su proyecto de decisión, la Comisión Europea menciona en las notas a pie de página 201 y 266 que las secciones 44 a 52 de la IPA 2016 prevén «casos específicos limitados» con respecto a las interceptaciones selectivas. El CEPD observa que las secciones 45 a 51 de la IPA 2016 son exenciones que, según se afirma, los servicios de inteligencia no utilizan regularmente. Además, el **CEPD entiende** que en los **casos en que se aplican las exenciones** (p. ej., proveedores de telecomunicaciones y servicios postales), si las fuerzas o cuerpos de seguridad o los servicios de inteligencia **solicitan** acceso a estos datos, se requerirá la autorización previa de los comisarios judiciales**, e invita a la Comisión Europea a confirmar en su decisión que esto es correcto**.

206. El CEPD reconoce que la sección 44, apartado 2, de la IPA 2016 permite la interceptación de comunicaciones si una de las partes (el remitente o el destinatario) ha dado su consentimiento y existe una autorización en virtud de la RIPA 2000 o la *Regulation of Investigatory Powers (Scotland) Act 2000* (Ley de Escocia sobre la Regulación de las Facultades de Investigación de 2000) (2000 asp 11), es decir, la situación jurídica previa al establecimiento de los comisarios judiciales. El CEPD **invita** a la Comisión Europea a aclarar si esto significa que en los casos en que existe un consentimiento unilateral, no se aplicaría en absoluto el procedimiento de autorización previa.

207. Por lo que se refiere al control *ex post*, también es importante verificar que se garantiza una supervisión independiente y eficaz sin lagunas, en particular cuando no está previsto que sea previa.

208. El CEPD señala que según las secciones 48 a 52 de la IPA 2016, los comisarios judiciales llevan a cabo una revisión *ex post* **e invita a la Comisión Europea a aclarar qué requisitos se aplican y a iniciativa de quién se lleva a cabo dicha revisión**.

209. De acuerdo con la sección 229, apartado 4, de la IPA 2016, el IPC no hará un seguimiento del ejercicio de determinadas funciones. En este sentido, el CEPD invita a la Comisión Europea a aclarar las disposiciones de la sección 229, apartado 4, letras d) y e), de la IPA 2016 en lo que respecta a sus

[140] No obstante, el CEPD señala también que al invalidar el Escudo de la privacidad en el asunto Schrems II, el TJUE tomó nota de que, según la legislación estadounidense, la denominada FISA, «no autoriza medidas de vigilancia individuales, sino programas de vigilancia (como PRISM o Upstream) sobre la base de certificaciones anuales elaboradas por el fiscal general y el director de Inteligencia Nacional». (apartado 179).

efectos prácticos en la competencia de revisión del IPC. **El CEPD entiende que la ICO es la autoridad de control competente cuando se aplican las exenciones previstas en la sección 229, apartado 4, de la IPA 2016, e invita a la Comisión Europea a confirmar en su decisión que esto es correcto.**

210. **Parece que cuando lleva a cabo** un control *ex post*, el cometido **del IPC** se **limita** a 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. **El CEPD invita a la Comisión Europea a aclarar cómo garantiza la IPCO de manera eficaz el cumplimiento de la ley.**

211. **Por último, el CEPD entiende que las personas afectadas no pueden dirigirse directamente a la IPCO, sino que deben presentar una reclamación ante la ICO, que, sin embargo, tiene competencias limitadas en el ámbito de la seguridad nacional. Por consiguiente, el CEPD invita a la Comisión Europea a aclarar de qué forma se garantiza jurídicamente que la IPCO atienda las reclamaciones en estos casos.**

4.3.4. Recursos

212. A la luz de las sentencias del TJUE en los asuntos Schrems I y Schrems II, está claro que la protección judicial efectiva en el sentido del artículo 47 de la Carta de la UE es fundamental para suponer la adecuación de la legislación de un tercer país. Asimismo, las sentencias han demostrado que se debe prestarse especial atención, en particular, a la protección judicial efectiva en el ámbito del acceso a datos personales con fines de seguridad nacional.

213. **El CEPD reconoce que el Reino Unido ha establecido el *Investigatory Powers Tribunal* (Tribunal de Facultades de Investigación, «IPT»). El IPT no solo es competente para ver causas sobre el uso de poderes de investigación por parte de las fuerzas o cuerpos de seguridad, sino también por los servicios de inteligencia. El CEPD entiende que el IPT funciona como un tribunal competente en el sentido del artículo 47 de la Carta de la UE. En cuanto a sus facultades, se invita a la Comisión Europea a confirmar que el IPT tiene todas las facultades que se señalan en el considerando 262 del proyecto de decisión, independientemente del fundamento jurídico de la reclamación.**

214. La vigilancia discreta por parte de las agencias de inteligencia implica generalmente que el objeto de la vigilancia, el interesado, no es ni será consciente de dicha vigilancia. En este contexto, cuando ha tenido que analizar la legislación de los EE. UU., el CEPD ha manifestado muchas veces su preocupación por el requisito de «legitimación», tal como se interpreta en la legislación de dicho país, en los casos de vigilancia. En este sentido, el CEPD observa que las denuncias ante el IPT solo requieren una prueba de creencia (*belief test*), conforme a la cual el denunciante tiene que demostrar que corre un riesgo potencial de ser sometido a una medida.

215. Al analizar la función del IPT, el CEPD también presta especial atención al hecho de que su funcionamiento se ha considerado repetidamente conforme con lo dispuesto en el CEDH, tal como ha interpretado el TEDH.