Dictamen 26/2025 sobre el proyecto de Decisión de Ejecución de la Comisión Europea con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido

Adoptado el 16 de octubre de 2025

Resumen

El 22 de julio de 2025, la Comisión Europea inició el proceso para la adopción de su proyecto de decisión de ejecución sobre la protección adecuada de los datos personales por parte del Reino Unido de conformidad con el artículo 45, apartado 2, del RGPD. El presente proyecto de decisión prorroga la validez de determinadas partes de la decisión de adecuación anterior, de 28 de junio de 2021, mediante referencia, hasta diciembre de 2031.

Ese mismo día, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos («el CEPD»). La evaluación por parte del CEPD de la adecuación del nivel de protección ofrecido por el Reino Unido se realizó sobre la base del examen del propio proyecto de decisión y tras analizar la documentación facilitada por la Comisión Europea.

El CEPD centró su evaluación tanto en los aspectos generales relacionados con el RGPD del proyecto de decisión como en el acceso de las autoridades públicas a los datos personales transferidos desde el EEE al Reino Unido con fines policiales y de seguridad nacional, incluidas las vías de recurso disponibles para los ciudadanos del EEE.

El CEPD también evaluó si se aplican y resultan eficaces las salvaguardias previstas en el marco jurídico británico.

Como referencia principal para este trabajo, el CEPD utilizó sus criterios de referencia sobre la adecuación en virtud del RGPD (en lo sucesivo, «las Referencias sobre adecuación con arreglo al RGPD») adoptados el 28 de noviembre de 2017, revisados por última vez y adoptados el 6 de febrero de 2018, y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.

El CEPD acoge con satisfacción la continua armonización entre el marco de protección de datos del Reino Unido y de la UE, a pesar de la reciente evolución del marco jurídico pertinente del Reino Unido. En este contexto, el presente dictamen pone de relieve varios puntos que requieren un análisis más profundo, así como algunas cuestiones que la Comisión debería supervisar atentamente en los próximos años como parte de su obligación de supervisión en virtud del artículo 45, apartado 4, del RGPD.

El CEPD observa que el Reino Unido introdujo cambios en relación con el marco jurídico general «heredado» de la UE en virtud de la Ley británica sobre el Derecho de la Unión conservado (revocación y reforma) de 2023 [*Retained EU Law (Revocation and Reform Act 2023*] («la Ley REUL»), que, entre otras cosas, elimina el principio de primacía del Derecho de la UE (con garantías para algunas disposiciones del RGPD) y la aplicación directa de los principios del Derecho de la UE, como el derecho a la privacidad y a la protección de datos, tal como se deriva de la Carta de los Derechos Fundamentales. El CEPD invita a la Comisión a explicar y realizar una evaluación más detallada de los cambios introducidos por la Ley REUL y a evaluar su impacto en el marco jurídico del Reino Unido en general y en su marco de protección de datos en particular. El CEPD también considera que se trata de un ámbito que la Comisión deberá supervisar atentamente en el futuro.

El CEPD señala que se han otorgado nuevas facultades al Secretario de Estado para la introducción de cambios en el nuevo marco de protección de datos a través de normativa secundaria, que requiere un menor control parlamentario en determinados casos, por ejemplo, las transferencias internacionales, la toma de decisiones automatizada y la gobernanza de la Comisión de Información (CI). El CEPD invita a la Comisión a destacar en la Decisión de Adecuación final los ámbitos que pretende supervisar

atentamente, ya que existe el riesgo de que se produzcan nuevas divergencias con la legislación de la UE en materia de protección de datos a través de la legislación secundaria del Reino Unido.

El CEPD observa cambios en las normas que rigen la transferencia de datos personales, en particular la nueva lista indicativa de elementos que deben tenerse en cuenta en la prueba de adecuación, que no incluye elementos importantes que figuraban en la anterior prueba de adecuación del Reino Unido[1]. Esto se aplica tanto a las transferencias a terceros países realizadas en virtud del RGPD del Reino Unido (*UK GDPR*) como a las transferencias de datos tratados con fines policiales. El CEPD anima a la Comisión a que profundice específicamente en su evaluación de estos aspectos y supervise la evolución y la aplicación práctica de esta nueva prueba de adecuación.

El CEPD invita a la Comisión a realizar una evaluación más detallada de la reestructuración de la autoridad británica de protección de datos [Information Commissioner's Office (ICO), Oficina del Comisario de Información] como consejo de administración y de las normas para el nombramiento y la destitución de los miembros ejecutivos y no ejecutivos del consejo de administración. El CEPD también invita a la Comisión a proporcionar más detalles sobre la reciente consulta de la ICO, publicada después de este proyecto de decisión, para introducir un nuevo sistema de clasificación para la tramitación de reclamaciones. El CEPD invita a la Comisión a supervisar todos estos cambios una vez que entren en vigor. Si bien valora positivamente la política de transparencia de la ICO y la disponibilidad de los datos estadísticos y analíticos de sus actividades de control del cumplimiento normativo, el CEPD también invita a la Comisión a realizar una evaluación más detallada y supervisar la aplicación de las facultades correctivas, la eficacia de las sanciones y los recursos para las partes afectadas en el marco de protección de datos del Reino Unido.

El CEPD considera esencial evaluar las exenciones ampliadas por motivos de seguridad nacional en el marco de la aplicación de la ley y se mantiene especialmente atento a cualquier exención del principio de proporcionalidad, así como del requisito de tratar los datos personales con fines legítimos. Del mismo modo, cualquier exención de las competencias de la autoridad de control debe abordarse con cautela. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá respetar la esencia de estos y, con arreglo al principio de proporcionalidad, solo podrán introducirse cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. El CEPD pide a la Comisión que complemente su evaluación en la decisión final de adecuación y que supervise específicamente la aplicación en la práctica de las exenciones por motivos de seguridad nacional para las autoridades policiales.

El CEPD señala que las actividades de tratamiento llevadas a cabo por las autoridades policiales pueden, en circunstancias específicas, entrar en el ámbito de aplicación de las normas habitualmente aplicables al tratamiento de datos personales por parte de las autoridades de seguridad nacionales. En este contexto, debe prestarse especial atención a garantizar que el régimen de protección de datos para el tratamiento de la seguridad nacional no se amplíe a contextos no relacionados con el ámbito nacional. El CEPD invita a la Comisión a supervisar si las autoridades competentes cualificadas son capaces de mantener una distinción clara entre los diferentes fines de tratamiento a fin de aplicar el marco jurídico correspondiente en consecuencia.

[1] i) las normas del tercer país en materia de «seguridad pública, defensa, seguridad nacional y Derecho penal, así como el acceso a los datos personales por parte de las autoridades públicas», ii) la jurisprudencia, iii) la existencia de derechos efectivos y exigibles de los interesados y los recursos administrativos y judiciales que pueden interponer efectivamente los interesados cuyos datos personales se transfieren, y iv) una o varias autoridades de control independientes.

El CEPD acoge con satisfacción las aclaraciones alcanzadas entre el Reino Unido y los Estados Unidos en el contexto del Acuerdo sobre la Ley CLOUD entre el Reino Unido y los Estados Unidos (*UK-US Cloud Act Agreement*), que proporcionan una mayor claridad jurídica. Al mismo tiempo, el CEPD desea recordar la necesidad de mejorar el nivel de las salvaguardias previstas en el Acuerdo entre la Unión Europea y los Estados Unidos sobre la protección de los datos personales («el Acuerdo marco UE-EE. UU.»), cuyas salvaguardias en materia de privacidad y protección de datos se incorporaron al Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD. En general, el CEPD considera necesario aclarar la evaluación realizada por la Comisión del Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD y cualquier posible impacto en el nivel de protección. El CEPD invita a la Comisión a seguir incluyendo el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD en sus futuras evaluaciones y revisiones.

Como se señaló recientemente en la Declaración 5/2024, el CEPD considera que el cifrado es esencial para garantizar la seguridad y la confidencialidad de los datos personales y las comunicaciones electrónicas. Los requerimientos de capacidad técnica (*technical capacity notices*) en el marco de la Ley británica de Poderes de Investigación de 2016 (*Investigatory Powers Act 2016*, «la IPA 2016»), que obligan a las empresas a ofrecer la capacidad de eliminar el cifrado a petición del Gobierno, crean vulnerabilidades sistémicas y suponen una amenaza directa para la integridad y la confidencialidad de las comunicaciones electrónicas. Estos avances merecen ser tenidos en cuenta en la decisión de adecuación, en particular a la luz del artículo 45, apartado 2, letra a), del RGPD, que exige una evaluación no solo del marco jurídico sobre el papel, sino también de su aplicación en la práctica, y deben ser objeto de seguimiento.

El CEPD observa que la Ley británica de Enmienda de los Poderes de Investigación de 2024 (*Investigatory Powers Amendment Act 2024*) introdujo un régimen específico para la conservación y el examen de conjuntos de datos personales en bloque para los que las personas a las que se refieren dichos datos «no podrían tener ninguna expectativa de privacidad, o solo una expectativa baja y razonable». El CEPD considera que se necesitan más aclaraciones con respecto a los cambios pertinentes, en particular en lo que respecta a los conceptos de «autorizaciones individuales» y «autorizaciones por categoría». Además, el CEPD invita a la Comisión a que supervise atentamente la aplicación del término «una expectativa baja o ninguna expectativa razonable de privacidad» en la práctica.

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, «el RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo (EEE) y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[2],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. INTRODUCCIÓN

1.1. ÁMBITO DE APLICACIÓN DEL PROYECTO DE DECISIÓN DE LA COMISIÓN

1. El 22 de julio de 2025, la Comisión Europea («la Comisión») solicitó el dictamen del Comité Europeo de Protección de Datos («el CEPD») sobre el proyecto de Decisión de Ejecución por la que se modifica la Decisión de Ejecución (UE) 2021/1772 de la Comisión, de 28 de junio de 2021, con arreglo al RGPD, relativa a la protección adecuada de los datos personales por parte del Reino Unido («el proyecto de Decisión»). En su proyecto de Decisión, la Comisión concluyó que el Reino Unido sigue garantizando un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea al Reino Unido en el ámbito de aplicación del RGPD.

2. El CEPD señala que este proyecto de Decisión prorroga por seis años la validez de la Decisión de Ejecución (UE) 2021/1772 de la Comisión, de 28 de junio de 2021, con arreglo al RGPD, relativa a la protección de los datos personales por parte del Reino Unido («la anterior Decisión de Adecuación relativa al Reino Unido»), que debía expirar el 27 de junio de 2025 (cláusula de extinción). La anterior Decisión de Adecuación relativa al Reino Unido se había prorrogado por un período de seis meses, hasta el 27 de diciembre de 2025 en virtud de la Decisión (UE) 2025/1225, de 24 de junio de 2025, para que el Reino Unido pudiera finalizar sus reformas en materia de protección de datos[3].

3. En su proyecto de Decisión, la Comisión evaluó «si la conclusión de que el Reino Unido garantiza un nivel adecuado de protección sigue estando justificada desde el punto de vista fáctico y jurídico a la luz de los acontecimientos que se han producido desde la adopción de la anterior Decisión de Adecuación relativa al Reino Unido».

4. La Comisión centró su evaluación en las novedades introducidas en la legislación británica en materia de protección de datos, en particular las introducidas por la Ley de Datos (uso y acceso) de 2025 [*Data (Use and Access) Act 2025*] («la DUAA»). La Comisión consideró específicamente los elementos

[2] Las referencias a los «Estados miembros» realizadas en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».
[3] El CEPD, previa solicitud, emitió el Dictamen 6/2025, relativo a la prórroga de las Decisiones de Ejecución de la Comisión Europea en el marco del RGPD y de la Directiva sobre protección de datos en el ámbito penal sobre la protección adecuada de los datos personales en el Reino Unido.

enumerados en el considerando 281 de la anterior Decisión de Adecuación relativa al Reino Unido, que figuran todos en el proyecto de Decisión.

5. El CEPD está de acuerdo en que la evaluación debe centrarse principalmente en todos los nuevos avances pertinentes en la legislación del Reino Unido y en los elementos destacados en la anterior Decisión de Adecuación relativa al Reino Unido, en la medida en que se evalúen todos los elementos establecidos en el artículo 45, apartado 2, del RGPD. Por lo tanto, el CEPD apreciaría que, en su Decisión de Adecuación final, la Comisión aclarara explícitamente que se han evaluado todos los elementos enumerados en el artículo 45, apartado 2, del RGPD para concluir que el marco jurídico general del Reino Unido sigue garantizando un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea al Reino Unido. El CEPD también acogería con satisfacción que la Comisión aclarase que evaluará estos elementos de forma continua como parte de su función de seguimiento.

1.2. ALCANCE DEL PRESENTE DICTAMEN DEL CEPD

6. Se espera que el CEPD proporcione a la Comisión un dictamen independiente para la evaluación de la adecuación del nivel de protección en un tercer país[4], y que determine las insuficiencias en el marco de adecuación, en su caso, y se esfuerce por realizar propuestas para abordarlas[5]. Debido a la situación específica del Reino Unido, la nueva decisión de adecuación complementa la decisión de adecuación de 2021, que sigue siendo válida para las partes que no se abordan específicamente en este proyecto de decisión. Del mismo modo, con este Dictamen, el CEPD se basa en su dictamen 14/2021 y lo desarrolla aún más[6]. En consecuencia, el análisis y las observaciones formuladas por el CEPD en su dictamen previo sobre la anterior Decisión de Adecuación relativa al Reino Unido siguen siendo, en general, pertinentes.

7. Teniendo en cuenta lo anterior, el CEPD ha centrado sus comentarios en determinados puntos presentados en el proyecto de Decisión, en particular cuando se requieran más aclaraciones, información adicional o un futuro seguimiento por parte de la Comisión Europea.

8. El CEPD también señala que, de conformidad con los artículos 47 y 94 del Reglamento (UE) 2018/1725[7], las instituciones, órganos y organismos de la Unión Europea podrán transferir datos personales a un tercer país, territorio, sector u organización internacional reconocidos por la Comisión Europea, en virtud del artículo 45, apartado 3, del RGPD, que garanticen un nivel adecuado de protección, siempre que la transferencia se lleve a cabo exclusivamente a efectos del cumplimiento de las funciones que competen al responsable del tratamiento, sin necesidad de autorización adicional. El CEPD invita a la Comisión a recordar esta posibilidad jurídica en los considerandos de la Decisión de Adecuación final.

[4] Véase el artículo 70, apartado 1, letra s), del RGPD.
[5] Véase el Grupo de Trabajo del Artículo 29, Referencias sobre adecuación en virtud del RGPD, capítulo 2 «Aspectos procesales para las conclusiones sobre la adecuación en virtud del RGPD», adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018, WP254 rev.01 (refrendado por el CEPD, véase https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines), (en lo sucesivo, «las Referencias sobre adecuación en virtud del RGPD»).
[6] 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, https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.
[7] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE («EUDPR») (DO L 295 de 21.11.2018, p. 39).

1.3. EVOLUCIÓN DEL MARCO JURÍDICO DEL REINO UNIDO

9. Como se explica en el proyecto de Decisión[8], una vez finalizado el período de ejecución acordado en el Acuerdo de Retirada entre la Unión Europea y el Reino Unido[9] el 31 de diciembre de 2020, el Reino Unido tenía la intención de adoptar un nuevo régimen de protección de datos que se apartaría del marco jurídico de la UE. Finalmente, el Reino Unido introdujo cambios limitados en su actual marco de protección de datos, en particular en virtud de la Ley británica de Datos (uso y acceso) de 2025 (DUAA).

10. Más allá de la protección de datos, uno de los cambios más importantes en el marco jurídico del Reino Unido, desde que se adoptó la anterior Decisión de Adecuación relativa al Reino Unido, se refiere al marco jurídico general «heredado» de la UE (denominado «el Derecho de la Unión conservado»), es decir, las disposiciones legales integradas en el Derecho del Reino Unido a través de la Ley británica sobre la Retirada del Reino Unido de la Unión Europea de 2018 [*European Union (Withdrawal) Act 2018*]. El Derecho de la Unión conservado abarcaba los principios generales del Derecho de la Unión Europea, entre ellos los derechos fundamentales derivados de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»[10]) y los principios de proporcionalidad y necesidad, que han influido en el desarrollo y la interpretación de la legislación sobre protección de datos en el Reino Unido. En virtud de la Ley británica sobre la Retirada del Reino Unido de la Unión Europea de 2018, el Derecho de la Unión conservado había mantenido su supremacía sobre la legislación secundaria del Reino Unido y debía interpretarse de conformidad con los principios generales del Derecho de la Unión Europea. Sin embargo, desde la introducción de la Ley británica sobre el Derecho de la Unión conservado (revocación y reforma) de 2023 [*Retained EU Law (Revocation and Reform) Act 2023*, «la Ley REUL»)[11], el Reino Unido ha eliminado de su legislación nacional la aplicación directa de los principios del Derecho de la Unión, entre ellos los derechos fundamentales derivados de la Carta. La Ley REUL también eliminó el principio de primacía del Derecho de la Unión, ya que el Derecho de la Unión conservado (actualmente denominado «el Derecho asimilado») debe interpretarse ahora de manera compatible con el Derecho nacional del Reino Unido y no en consonancia con los principios del Derecho de la Unión. Esto constituye un cambio significativo en el ordenamiento jurídico del Reino Unido.

11. Además, aunque actualmente está en suspenso, podría introducirse, en virtud de la Ley REUL, un nuevo criterio jurídico más flexible para que los jueces del Tribunal de Apelación (Court of Appeal) y del Tribunal Supremo (Supreme Court) del Reino Unido se desvíen de la jurisprudencia conservada de la Unión[12]. De aprobarse, este cambio podría suponer un cambio significativo en el Reino Unido.

12. A pesar de estos cambios, el CEPD acoge con satisfacción la inclusión de garantías en la Ley REUL para garantizar que no se invalide la legislación en materia de protección de datos en determinadas circunstancias. Entre estas garantías está el requisito de que cualquier acto legislativo «que imponga una obligación o confiera una facultad para tratar datos personales no anule un requisito de la legislación principal en materia de protección de datos relativo al tratamiento de datos personales» y que el marco de protección de datos siga prevaleciendo sobre otra legislación del Reino Unido[13]. No

[8] Véase el considerando 2 del proyecto de Decisión.
[9] El período de ejecución es un período de tiempo acordado en el Acuerdo de Retirada entre la Unión Europea y el Reino Unido, durante el cual el Reino Unido dejará de ser miembro de la UE, pero seguirá estando sujeto a las normas de la UE y seguirá siendo miembro del mercado único y de la unión aduanera. Véase la Ley británica sobre la Retirada del Reino Unido de la Unión Europea de 2020 [*European Union (Withdrawal Agreement) Act 2020*].
[10] Carta de los Derechos Fundamentales de la Unión Europea (DO C 326 de 26.10.2012, p. 391).
[11] Véase el considerando 11 del proyecto de Decisión.
[12] Véase el artículo 6 de la Ley británica sobre el Derecho de la Unión conservado (revocación y reforma) de 2023, modificado por el Reglamento (entrada en vigor n.º 2 y disposiciones transitorias) de 2024 [*Retained EU Law (Revocation and Reform) Act 2023, (Commencement No. 2 and Saving Provisions) (Revocation) Regulations 2024*].
[13] Véase el artículo 183A de la DPA 2018 introducido por el artículo 106, apartado 2, de la DUAA.

obstante, el CEPD señala que estas garantías también contemplan dos excepciones: i) cuando el Parlamento del Reino Unido puede optar por anular deliberadamente los requisitos de protección de datos[14]; y ii) cuando determinadas disposiciones de la Ley británica de Protección de Datos [*Data Protection Act 2018* (DPA 2018)] estén exentas y, como tales, prevalezcan sobre el RGPD del Reino Unido[15]. Las implicaciones de la segunda exención aún son inciertas y objeto de debate en el Reino Unido.

13. En lo que respecta a la protección de los derechos fundamentales consagrados en la Carta, el considerando 12 del proyecto de Decisión explica que todas las referencias a los derechos y libertades fundamentales en el RGPD del Reino Unido y la DPA 2018 se sustituyeron por referencias los derechos recogidos en el Convenio Europeo de Derechos Humanos, incorporado a la legislación nacional con arreglo a la Ley británica de Derechos Humanos de 1998 (*Human Rights Act 1998*)[16].

14. El CEPD invita a la Comisión a realizar una evaluación más detallada de estos cambios en el ordenamiento jurídico del Reino Unido descritos en los apartados 10, 11 y 12 anteriores, con el fin de explicar los cambios introducidos por la Ley REUL y evaluar sus repercusiones en el marco de protección de datos del Reino Unido. El CEPD también considera que se trata de un ámbito que la Comisión deberá supervisar atentamente en el futuro, y le invita a hacerlo.

15. Por último, el CEPD señala varios cambios introducidos por la DUAA en el marco jurídico aplicable a las comunicaciones electrónicas, incluidas las *cookies*, y recuerda que el tratamiento de datos personales podría entrar en el ámbito de aplicación material del RGPD del Reino Unido[17]. Por tanto, invita a la Comisión a que las incluya en su evaluación con vistas a la decisión final en la medida en que puedan afectar a la protección de datos. El CEPD insta además a la Comisión a que supervise atentamente el efecto práctico de los cambios relacionados con las *cookies* exentas de consentimiento.

1.4. OBSERVACIONES GENERALES Y MOTIVOS DE PREOCUPACIÓN

1.4.1. COMPROMISOS INTERNACIONALES CONTRAÍDOS POR EL REINO UNIDO

16. En relación con los compromisos internacionales contraídos por el Reino Unido[18], el CEPD celebra que el Reino Unido siga adhiriéndose al CEDH y sometiéndose a la jurisdicción del Tribunal Europeo de Derechos Humanos (TEDH). Asimismo, el Reino Unido también se ha adherido al Convenio 108[19] y a su Protocolo Adicional[20], además de haber firmado el Convenio 108+[21] en 2018. Estos compromisos

[14] Véase el artículo 183, sección A, apartado 3, de la DPA 2018 introducido por el artículo 106, apartado 2, de la DUAA.
[15] Estas disposiciones se enumeran en el artículo 186, apartado 3, de la DPA 2018. Esto significa que, cuando exista un conflicto entre el artículo 23 del RGPD del Reino Unido y una de las disposiciones enumeradas —por ejemplo, el anexo 2 de la DPA 2018 que contiene las exenciones a los derechos de los interesados—, prevalecerá la interpretación de la DPA 2018.
[16] Véase el artículo 8 del Convenio Europeo de Derechos Humanos.
[17] Comité Europeo de Protección de Datos, Dictamen 5/2019 sobre la interacción entre la Directiva sobre la privacidad y las comunicaciones electrónicas y el Reglamento general de protección de datos, en particular en lo que respecta a la competencia, funciones y poderes de las autoridades de protección de datos, adoptado el 12 de marzo de 2019, disponible en https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.
[18] Véase el capítulo 1: información general relacionada con el concepto de adecuación de las Referencias sobre Adecuación.
[19] Véase el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 («el Convenio 108+»).
[20] Véase el Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de control y a los flujos transfronterizos de datos, abierto a la firma el 8 de noviembre de 2001.
[21] Véase el Protocolo que modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 18 de mayo de 2018 («el Convenio 108+»).

internacionales representan consideraciones importantes[22] y deben tenerse en cuenta como parte de la evaluación para la renovación tanto de las decisiones de adecuación relativas al Reino Unido en virtud del RGPD como de la Directiva sobre protección de datos en el ámbito penal.

17. En general, el CEPD apoya los esfuerzos encaminados a una rápida ratificación del Convenio 108+ por parte de terceros países, como un paso significativo hacia la armonización con los principios de protección de datos reconocidos internacionalmente y como una señal de su compromiso con derechos fundamentales y normas más amplios.

1.4.2. PODERES DEL SECRETARIO DE ESTADO DEL REINO UNIDO PARA INTRODUCIR CAMBIOS EN LA DUAA MEDIANTE NORMATIVA SECUNDARIA

18. Aunque la mayoría de los cambios introducidos en el marco de protección de datos del Reino Unido tienen por objeto aclarar y facilitar el cumplimiento de la ley, algunos pueden repercutir, dependiendo de su aplicación, en el nivel de protección de los datos personales en el Reino Unido.

19. A este respecto, el CEPD señala que se han concedido a la Secretaría de Estado del Reino Unido nuevas facultades para introducir cambios en la DUAA a través de normativa secundaria, que requiere un menor control parlamentario. En determinados casos —por ejemplo, las transferencias internacionales (véase la sección 2.3), la toma de decisiones automatizada (sección 2.4) y la gobernanza de la CI (sección 3)—, estas nuevas facultades son amplias y en el proyecto de Decisión no se proporciona más información sobre qué salvaguardias se aplicarán y cómo se pretende emplear estas facultades en la práctica.

20. El CEPD invita a la Comisión a destacar en la Decisión de Adecuación final los ámbitos que pretende supervisar atentamente, ya que existe el riesgo de que se produzcan nuevas divergencias con la legislación de la UE en materia de protección de datos a través de la legislación secundaria del Reino Unido.

2. ASPECTOS GENERALES RELATIVOS A LA PROTECCIÓN DE DATOS

2.1. INTERESES LEGÍTIMOS RECONOCIDOS

2.1.1. OBSERVACIONES GENERALES

21. En los considerandos 22, 23 y 24, la Comisión centra su evaluación en la introducción de una nueva base jurídica, a saber, el tratamiento necesario para la satisfacción de un interés legítimo reconocido. En el anexo 1 del RGPD actualizado del Reino Unido se enumeran dichos intereses legítimos reconocidos.

22. Según las directrices de la ICO sobre este tema[23], los responsables del tratamiento de datos que se basan en un interés legítimo reconocido como fundamento jurídico siguen estando obligados a cumplir todos los demás requisitos del RGPD del Reino Unido, entre ellos el de garantizar que el tratamiento sea necesario y proporcionado para alcanzar el fin previamente aprobado. Dado que esto no se

[22] Véase el considerando 105 del RGPD.
[23] Véase la guía de la autoridad británica de protección de datos (Information Commissioner's Office, ICO) sobre intereses legítimos, disponible en https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/.

recuerda en el proyecto de Decisión y constituye un elemento esencial para alcanzar la conclusión de que esta nueva base jurídica no socava el nivel de protección de los derechos de los interesados, el CEPD invita a la Comisión a aclarar este punto.

23. Enumerar los intereses legítimos reconocidos en la ley no parece problemático en sí mismo, ni tampoco lo parece la decisión de introducir esa nueva base jurídica, que aporta mayor claridad a los responsables del tratamiento y debe acogerse con satisfacción.

24. Sin embargo, el CEPD observa que determinados intereses legítimos reconocidos consisten en: i) la necesidad de tratar datos personales para salvaguardar la seguridad nacional o proteger la seguridad pública o por motivos de defensa («condición de seguridad nacional, seguridad pública y defensa»); ii) la necesidad de tratar datos personales para detectar, investigar o prevenir un delito («condición de delito»); y ii) la «divulgación para los fines de tratamiento descritos en el artículo 6, apartado 1, letra e)».

25. En lo que respecta a la condición de «seguridad nacional, seguridad pública y defensa» y a la condición de «delito», el CEPD señala que en el proyecto de Decisión no se ha incluido más información sobre el uso práctico de estas bases jurídicas por parte de los responsables y encargados del tratamiento. El CEPD agradecería que la Comisión proporcionara más detalles sobre la información adicional y las garantías recibidas de las autoridades competentes del Reino Unido en relación con la aplicación práctica de esta base jurídica, e invita a la Comisión a supervisar la aplicación de dicha base jurídica.

26. El CEPD también señala que la ICO está trabajando en orientaciones específicas sobre este asunto, que, en el momento de la emisión del presente Dictamen, incluyen una definición de dichos conceptos. Dada la importancia de las aclaraciones en relación con estos conceptos, el CEPD insta a la Comisión a que siga de cerca la elaboración de las orientaciones de la ICO.

2.1.2. DIVULGACIÓN PARA LOS FINES DE TRATAMIENTO DESCRITOS EN EL ARTÍCULO 6, APARTADO 1, LETRA E)

27. El CEPD observa que el interés legítimo reconocido recientemente establecido que permite la «divulgación para los fines de tratamiento descritos en el artículo 6, apartado 1, letra e)», introduce la posibilidad de divulgar datos personales a las autoridades públicas de forma voluntaria. Como aclara la ICO en su reciente orientación[24], este interés legítimo reconocido no confiere por sí mismo a las autoridades solicitantes el derecho de acceso a los datos personales, pero un responsable del tratamiento puede invocar este interés previamente aprobado cuando las autoridades indiquen que necesitan los datos para el desempeño de sus tareas o funciones públicas. El CEPD también señala que estas solicitudes de divulgación para el cumplimiento de funciones públicas no solo pueden emitirse para datos personales destinados a ser utilizados para los fines contemplados por el RGPD del Reino Unido, sino que también pueden referirse a los fines de tratamiento en virtud de la parte 3 y la parte 4 de la Ley británica de Protección de Datos de 2018 (DPA 2018). Por consiguiente, esta enmienda también es pertinente en lo que respecta al acceso por parte del Gobierno con fines de aplicación de la ley y de seguridad nacional.[25]

[24] Véase la nota a pie de página n.º 23.

[25] Véanse las orientación de la ICO sobre la condicionalidad de las solicitudes de divulgación por parte de organismos públicos de datos personales necesarios para el desempeño de funciones públicas («*Public task disclosure request condition*»), disponible en https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/.

28. En este contexto, se plantea la cuestión de qué criterios debe evaluar el responsable del tratamiento para decidir si facilita datos voluntariamente en respuesta a una solicitud de información. En particular, como señala la ICO en sus orientaciones[26], el CEPD entiende que la prueba de necesidad para esta condición de interés legítimo reconocido es diferente de las demás condiciones especificadas en el anexo 1. En el caso de las solicitudes de divulgación de datos personales por parte de organismos públicos con el fin de poder llevar a cabo sus funciones, la necesidad implica que el responsable del tratamiento debe examinar qué tratamiento es necesario para divulgar la información personal solicitada. El responsable del tratamiento debe considerar si la información que desea divulgar es proporcionada y necesaria para atender la solicitud. Por el contrario, la prueba de necesidad no se extiende a si los datos personales son realmente necesarios para desempeñar la tarea o función pública en cuestión, ya que el responsable del tratamiento puede basarse en la declaración del solicitante de que necesita los datos personales para una tarea pública específica[27]. De hecho, en muchos casos, especialmente cuando las solicitudes se realicen con fines policiales o de seguridad nacional, el responsable del tratamiento no estará en condiciones de llevar a cabo dicha evaluación.

29. En este contexto, el CEPD insta a la Comisión a supervisar atentamente la aplicación práctica de esta disposición.

30. En opinión del CEPD, las autoridades policiales y de seguridad nacional no deberían utilizar este mecanismo para eludir las restricciones legales existentes sobre sus facultades vinculantes en materia de recopilación de datos ni para obtener más datos de los estrictamente necesarios para el cumplimiento de sus funciones. Además, el CEPD considera importante que los responsables del tratamiento tengan en cuenta la orientación de la ICO sobre cómo validar una solicitud de divulgación de datos personales para el desempeño de funciones públicas e invita a la Comisión a incluir este aspecto en la revisión periódica de la decisión.[28]

2.2. DERECHOS INDIVIDUALES

31. El CEPD coincide con el análisis de la Comisión de que los cambios en el ámbito de los derechos individuales han sido limitados. Esto incluye, entre otros, cambios en el artículo 12 y un nuevo artículo 12A del RGPD del Reino Unido, que detallan con mayor precisión los plazos para responder a las solicitudes de los interesados.[29] Además, el artículo 13, apartado 5, del RGPD del Reino Unido incluye una exención del derecho a la información en el caso de que los datos personales se traten con fines de investigación científica o histórica en virtud de otras salvaguardias del artículo 84B del RGPD del Reino Unido. El CEPD considera que ninguno de los dos cambios socava el nivel de protección esencialmente equivalente que ofrece el RGPD del Reino Unido.

2.2.1. DERECHOS DE ACCESO

32. El artículo 15, apartado 1A, del RGPD del Reino Unido introduce una evaluación de la proporcionalidad, tal como se ha desarrollado en la jurisprudencia nacional del Reino Unido. En particular, los

[26] Véase la nota a pie de página n.º 23.
[27] Véase la nota a pie de página n.º 23.
[28] La ICO, en su orientación sobre la condicionalidad de las solicitudes de divulgación por parte de organismos públicos de datos personales necesarios para el desempeño de funciones públicas (véase la nota a pie de página 25), aclara que los responsables del tratamiento deben, por ejemplo, solicitar que la solicitud se presente por escrito y realizar comprobaciones para garantizar la autenticidad de la solicitud o la autoridad del empleado del organismo en cuestión para actuar en su nombre.
[29] Principalmente debido a la necesidad de confirmar la identidad del interesado o de realizar el pago de una tasa.

responsables del tratamiento solo tienen que realizar «búsquedas razonables y proporcionadas» para satisfacer las solicitudes de acceso.

33. El CEPD observa que dicha evaluación de la proporcionalidad no está presente en el marco de protección de datos de la UE, que no prevé ninguna reserva general a la proporcionalidad en relación con las medidas que debe tomar el responsable del tratamiento para satisfacer la solicitud del interesado con arreglo al artículo 12 del RGPD, sino que solo establece motivos de denegación en su apartado 5[30].

34. Por lo tanto, en opinión del CEPD, es importante definir adecuadamente el concepto de «búsquedas razonables y proporcionadas», que debe interpretarse de manera restrictiva y suficientemente uniforme. Los responsables del tratamiento deben tener una comprensión uniforme de lo que es «razonable y proporcionado», ya se base en la jurisprudencia o en las orientaciones de una autoridad de control, ya que la aplicación de este concepto podría dar lugar a normas diferentes en el cumplimiento del derecho de acceso, en particular en función del nivel de las medidas técnicas y organizativas que el responsable del tratamiento establezca para tramitar las solicitudes de acceso. El CEPD apreciaría que la Comisión facilitara información más detallada sobre la interpretación de la expresión «búsquedas razonables y proporcionadas», sobre la base de las orientaciones nacionales y la jurisprudencia disponible. En este contexto, el CEPD invita a la Comisión a supervisar que el derecho de acceso no se limite indebidamente.

2.2.2. SALVAGUARDIAS RELATIVAS A LA «EXENCIÓN PARA EL CONTROL DE LA INMIGRACIÓN»

35. La anteriormente denominada «exención para el control de la inmigración»[31] permitía a los responsables del tratamiento que participan en el «control de la inmigración» no aplicar algunos derechos de los interesados, previstos en la DPA 2018, si esto pudiera perjudicar determinadas actividades de control de la inmigración[32]. Debido a las impugnaciones en cuanto a la legalidad de esta exención en el momento de la adopción de la anterior Decisión de Adecuación relativa al Reino Unido, el tratamiento de datos personales en virtud de la exención quedó excluido del ámbito de aplicación de dicha decisión.

36. Desde la anterior Decisión de Adecuación relativa al Reino Unido, la exención para el control de la inmigración se ha complementado con salvaguardias en dos ocasiones[33]. Actualmente contempla las siguientes salvaguardias: i) solo debe invocarse caso por caso; ii) se tendrán en cuenta los derechos y libertades del interesado y sus posibles vulnerabilidades; iii) el Secretario de Estado llevará un registro sobre el uso de la exención para el control de la inmigración con el fin de ofrecer información general al interesado sobre el uso de dicho registro; y iv) se aclara que el uso de la exención para el control de la inmigración se limitará al tratamiento por parte del Secretario de Estado (incluido el Ministerio del

[30] Artículo 12, apartado 5, del RGPD: «*La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud».*

[31] Véase el anexo 2 de la DPA 2018, parte 1 de la versión anterior de la DPA.

[32] Véanse los apartados 61 («pudiera perjudicar el mantenimiento de un control efectivo de la inmigración») y 62 («la investigación o detección de actividades que socavarían el mantenimiento de un control efectivo de la inmigración») del Dictamen 14/2021 del CEPD.

[33] Mediante la aprobación de sendos reglamentos en 2022 y 2024.

Interior del Reino Unido y sus organismos). Además, se detallaba el necesario ejercicio de ponderación para determinar si es probable que el ejercicio de los derechos del interesado perjudique el control efectivo de la inmigración. La ICO también publicó orientaciones detalladas sobre el uso de la exención. En sus orientaciones, confirmó la interpretación restrictiva de la exención y que las restricciones mediante la exención para el control de la inmigración solo deben aplicarse de forma selectiva a derechos específicos del interesado. También señaló que, al llevar a cabo la prueba de la ponderación, los responsables del tratamiento deben garantizar que el riesgo para el control de la inmigración sea sustancial y supere el riesgo para los intereses del interesado.

37. El CEPD coincide con el análisis detallado realizado por la Comisión. En vista de los retos jurídicos que precedieron a esos cambios, el CEPD anima a la Comisión a supervisar su aplicación futura.

2.3. RESTRICCIONES SOBRE TRANSFERENCIAS ULTERIORES

38. El CEPD acoge con satisfacción la atención permanente que presta la Comisión a la aplicación práctica de las normas del Reino Unido sobre las transferencias de datos personales a terceros países, y anima a la Comisión a mantener y profundizar este compromiso. Esto resulta especialmente importante en lo que respecta a la facultad del Secretario de Estado del Reino Unido para promulgar nuevos reglamentos específicos con el fin de aprobar transferencias i) a un sector o zona geográfica concretos dentro de un tercer país, ii) a un responsable o encargado del tratamiento concreto, iii) a un destinatario concreto de los datos personales, iv) de determinados tipos específicos de datos personales, v) realizadas por determinados medios específicos, o vi) sobre la base de las leyes, regímenes, listas u otro tipo de disposiciones o documentos pertinentes, conforme vayan entrando en vigor, y para conferir una facultad discrecional a una persona (artículo 45A(4) del RGPD del Reino Unido).

39. El CEPD entiende que el artículo 45A, apartado 4, del RGPD del Reino Unido tiene por objeto permitir flexibilidad para la aprobación de determinadas transferencias. Por ejemplo, en lo que respecta a los incisos ii) y iii), el CEPD entiende que podrían abarcar las transferencias a entidades privadas en un tercer país. Esto significaría que dichas entidades privadas se han comprometido a cumplir con la prueba de protección de datos. No queda claro cómo evaluaría en la práctica el Secretario de Estado del Reino Unido el hecho de que los responsables del tratamiento específicos con sede en un tercer país —no considerado adecuado— puedan cumplir los requisitos de la prueba de protección de datos (por ejemplo, en lo que respecta a la reparación). Del mismo modo, sigue sin estar claro cómo se llevaría a cabo la prueba de protección de datos para el artículo 45A, apartado 4, incisos iv) y v), del RGPD del Reino Unido.

40. El CEPD apreciaría que la Comisión proporcionara más detalles sobre la información adicional y las garantías recibidas en relación con la aplicación práctica de la prueba de protección de datos, y que explicara su evaluación en cuanto a cómo se mantiene el nivel de protección en tales situaciones[34]. El CEPD también invita a la Comisión a seguir atentamente la evolución de la aplicación de esta disposición.

41. Además, el CEPD entiende, a partir de la información adicional facilitada por la Comisión, que el criterio de la «conveniencia de facilitar las transferencias de datos personales hacia y desde el Reino Unido» no constituye un elemento de la prueba de protección de datos, sino simplemente un factor adicional que el Secretario de Estado puede tener en consideración cuando se cumplan plenamente los criterios

[34] Véase el artículo 45A, apartado 4, del RGPD del Reino Unido.

de la prueba. El CEPD invita a la Comisión a que lo aclare en su Decisión de Adecuación final, ya que no queda totalmente claro en el texto legal, así como a que supervise sus implicaciones prácticas y la aplicación de dicho criterio.

42. En cuanto a la nueva prueba de protección de datos introducida por la DUAA[35], el CEPD señala que la nueva lista orientativa de elementos que deben tenerse en cuenta en la prueba de adecuación no es exhaustiva, y que la nueva prueba de adecuación establece que el nivel de protección de los interesados en terceros países u organizaciones internacionales destinatarios «no es sustancialmente inferior» al de la norma prevista para los interesados en la legislación pertinente del Reino Unido en materia de protección de datos. Esta lista elimina elementos importantes que figuraban en la anterior prueba de adecuación del Reino Unido y que desempeñan un papel importante a la hora de evaluar si un tercer país ofrece un nivel esencialmente equivalente de protección de los datos personales. La nueva prueba ya no hace referencia a: i) las normas del tercer país en materia de «seguridad pública, defensa, seguridad nacional y Derecho penal, así como el acceso a los datos personales por parte de las autoridades públicas»; ii) la jurisprudencia (en su lugar, la nueva prueba hace referencia a «la constitución, las tradiciones y la cultura del país»); iii) la existencia de derechos efectivos y exigibles de los que disfrutan los interesados y los recursos administrativos y judiciales que pueden interponer efectivamente los interesados cuyos datos personales se transfieren (en su lugar, la nueva prueba se refiere a b) la existencia, y las facultades, de una autoridad responsable de hacer cumplir la protección de los interesados en lo que respecta al tratamiento de datos personales en el país o por la organización, y a c) las disposiciones relativas a la reparación judicial o extrajudicial de los interesados en relación con dicho tratamiento); y iv) una o varias autoridades de control independientes (en cambio, la nueva prueba se refiere a una «autoridad responsable de hacer cumplir la protección de los interesados en relación con el tratamiento de datos personales en el país o por parte de la organización»).

43. Si bien se reconoce que las Referencias sobre adecuación en virtud del RGPD solo proporcionan detalles limitados sobre este aspecto, el CEPD recuerda su referencia a que «el nivel de protección de las personas físicas cuyos datos se transfieren no debe verse menoscabado por la transferencia ulterior»[36], lo que no puede interpretarse en el sentido de que no incluye la necesidad de una autoridad de control independiente y de derechos efectivos y exigibles para los interesados.

44. El CEPD anima a la Comisión específicamente a que profundice en su evaluación de estos aspectos. Esta aclaración proporcionaría una gran seguridad jurídica y contribuiría a reforzar la confianza en el instrumento de adecuación. El CEPD también invita a la Comisión a seguir atentamente la evolución y la aplicación práctica de la nueva prueba de adecuación.

45. En lo que respecta a la adhesión (como miembro asociado) del Reino Unido a las Normas de Privacidad Transfronteriza (NPT) [*Cross-Border Privacy Rules*, (CBPR)], el CEPD señala que la adhesión actual no implica ninguna facilitación de las transferencias de datos desde el Reino Unido a otros miembros del Foro de las NPT. El CEPD acoge con satisfacción la postura adoptada por la Comisión al respecto, incluido el compromiso de seguir supervisando atentamente los nuevos acontecimientos en este ámbito, especialmente si el Reino Unido tiene la intención de convertirse en miembro de pleno derecho, y recuerda que las NPT no se consideran suficientes para garantizar un nivel adecuado de protección de los datos personales procedentes de la UE.

[35] Véase el considerando 42 del proyecto de decisión.

[36] Véase el capítulo 3: Principios generales de protección de datos para garantizar que el nivel de protección en un tercer país, territorio o uno o varios sectores específicos en ese tercer país u organización internacional sea esencialmente equivalente al garantizado por la legislación de la UE, de la Referencia sobre adecuación del RGPD.

2.4. TOMA DE DECISIONES AUTOMATIZADA

46. El CEPD toma nota del artículo 80 de la DUAA (por el que se introducen los artículos 22A a 22D del RGPD del Reino Unido), que introduce cambios significativos en el marco que rige la toma de decisiones automatizada, en particular cuando se basa en el tratamiento de categorías no especiales de datos. Hasta la adopción de la DUAA, el artículo 22 del RGPD del Reino Unido se hacía eco del marco de protección de datos de la UE estableciendo una prohibición general de toma de decisiones automatizada con excepciones limitadas.

47. El artículo 22B, apartado 1, del RGPD del Reino Unido prohíbe el tratamiento de categorías especiales de datos personales para las decisiones basadas únicamente en el tratamiento automatizado que tengan efectos jurídicos o igualmente significativos para el interesado, con determinadas excepciones (artículo 22B, apartado 2, punto 3, del RGPD del Reino Unido, inclusive cuando el tratamiento se base en el consentimiento o en un contrato o cuando lo exija la ley).

48. El CEPD observa que esta prohibición no se aplica cuando los responsables del tratamiento toman decisiones significativas utilizando procesos automatizados basados en categorías no especiales de datos, a menos que la base jurídica del tratamiento sea un interés legítimo reconocido con arreglo al artículo 6, apartado 1, letra ea), del RGPD del Reino Unido.

49. El objetivo principal de la ley pasa de restringir el uso de la toma de decisiones automatizada a garantizar que se establezcan salvaguardias para las decisiones significativas. Entre estas salvaguardias está: i) proporcionar información al interesado sobre el proceso de toma de decisiones; ii) permitirle presentar alegaciones sobre la decisión[37]; iii) impugnar dicha decisión; y iv) permitir al interesado solicitar la intervención humana del responsable del tratamiento. El CEPD señala que, aunque este nuevo enfoque representa una desviación del marco jurídico anterior, el artículo 22C del RGPD del Reino Unido exige que los responsables del tratamiento apliquen unas salvaguardias adecuadas que garanticen un nivel adecuado de protección de los interesados.

50. A la luz de la rápida evolución del entorno regulador y de los avances en las tecnologías automatizadas, como la inteligencia artificial (IA), el CEPD anima a la Comisión a ampliar su evaluación en su Decisión de Adecuación final de las repercusiones prácticas previstas de este nuevo enfoque, que aún no se ha probado en la práctica, así como a supervisar su aplicación.

2.4.1. TOMA DE DECISIONES AUTOMATIZADA E INTERVENCIÓN HUMANA

51. El CEPD acoge con satisfacción la aclaración acerca del significado de la toma de decisiones automatizada y la intervención humana. El artículo 22A del RGPD del Reino Unido aclara que una decisión basada únicamente en el tratamiento automatizado supone la ausencia de una intervención humana significativa en el proceso de toma de decisiones. Asimismo, los responsables del tratamiento deben evaluar en qué medida la elaboración de perfiles contribuye a la toma de una decisión con el fin de determinar si la intervención humana ha sido significativa.

52. Asimismo, el artículo 22D del RGPD del Reino Unido otorga al Secretario de Estado la facultad de especificar mediante reglamentos en qué medida se da una intervención humana significativa en la toma de decisiones descrita en el reglamento. Del mismo modo, el Secretario de Estado también tiene

[37] Es decir, proporcionar información adicional y una justificación, lo que aún no constituye un recurso legal formal.

la facultad de determinar si se considera o no que la decisión descrita en el reglamento tiene un efecto igualmente significativo en los interesados.

53. El alcance y la discrecionalidad de estas facultades no están claros. Por lo tanto, el CEPD invita a la Comisión a analizar estas nuevas facultades conferidas al Secretario de Estado y a supervisar cualquier novedad a este respecto. Por otra parte, las facultades adicionales del Secretario de Estado en relación con las salvaguardias exigidas por el artículo 22C del RGPD del Reino Unido constituyen un cambio positivo, ya que ampliarán o complementarán las salvaguardias ya exigidas, así como determinarán lo que es insuficiente en términos de salvaguardias.

3. MECANISMO PROCESAL Y DE APLICACIÓN

3.1. SUPERVISIÓN Y APLICACIÓN

3.1.1. SUPERVISIÓN INDEPENDIENTE

54. El CEPD señala que, con la entrada en vigor de la DUA[38], la autoridad británica de protección de datos (ICO), estructurada anteriormente como persona jurídica unipersonal (*corporation sole*), se transformará en una nueva estructura mediante la creación de una persona jurídica colectiva (*body corporate*) (un comité), a saber, la Comisión de Información (CI) de conformidad con el artículo 148 y el anexo 12A de la DPA 2018.

55. El CEPD observa que la reestructuración de una autoridad para transformarla de una persona jurídica unipersonal a una persona jurídica colectiva no afecta en sí misma a la independencia de la autoridad ni a su aplicación efectiva. Se debe prestar atención a otros elementos, como las normas relativas al nombramiento y la destitución, y, en relación con este punto, el CEPD acoge con satisfacción que solo Su Majestad el Rey pueda destituir al presidente de la CI de su cargo, siguiendo la recomendación de ambas cámaras del Parlamento del Reino Unido, en caso de falta grave.

56. Las normas detalladas sobre el trabajo y el funcionamiento de la nueva CI figuran en el anexo 12A de la DPA 2018. Este regula, entre otras cosas, el marco estructural y organizativo de la CI, los requisitos para el nombramiento de sus miembros ejecutivos y no ejecutivos, así como de otros miembros del personal (empleados y un comité externo) e incluye disposiciones sobre el mandato, la remuneración, la gestión de cuentas y la destitución. Los números 5 y 6 del Anexo 12A[39] contienen normas y salvaguardias que deben observarse a efectos del nombramiento de miembros no ejecutivos, y que podrían ser pertinentes para la constitución del organismo colectivo y para la independencia de este (por ejemplo, selección basada en méritos y conflicto de intereses).

57. El CEPD observa que el proyecto de Decisión no proporciona ninguna información detallada sobre los cambios en el trabajo y el funcionamiento de la nueva autoridad de protección de datos. Además, no se ofrecen detalles sobre el procedimiento para el nombramiento y la destitución de los miembros ejecutivos y no ejecutivos. Dado que estos elementos son pertinentes para la evaluación del mecanismo de supervisión, el CEPD invita a la Comisión a describir en mayor detalle los cambios y la evaluación pertinente, en particular en lo que respecta a la estructura y organización de la CI, así como al nombramiento y la destitución de sus miembros, incluidos los miembros no ejecutivos.

[38] Véase la parte 6, artículo 117 «La Comisión de Información», de la DUAA, pp. 133 y siguientes.
[39] Véase el anexo 12A de la DPA 2018.

58. Por lo que se refiere a la independencia de la CI, el CEPD señala que, en virtud del artículo 6 del anexo 12A de la DPA 2018, los conflictos de intereses pueden impedir el nombramiento por parte del Secretario de Estado como presidente o como miembro no ejecutivo de la CI. Al especificar el término «conflicto de intereses», el artículo 6, apartado 5, se refiere a «un interés financiero o de otro tipo que pueda afectar de manera perjudicial al desempeño por parte de la persona de sus funciones como miembro de la Comisión». En cuanto a la independencia de los miembros de la CI, esos «otros intereses», por ejemplo, la proximidad económica especial o las relaciones comerciales, también pueden ser indicio de conflictos de intereses y deben tenerse en cuenta en el proceso de nombramiento de los miembros de la CI. Por lo tanto, el CEPD invita a la Comisión a supervisar que las restricciones se apliquen en la práctica.

59. En relación con los objetivos actualizados que la CI debe tener en cuenta en el desempeño de sus tareas y en la preparación de su estrategia —como, entre otros, el fomento de la innovación y la competencia (artículo 120B de la DPA 2018)—, la Comisión recuerda que «Del mismo modo, la legislación de la UE en materia de protección de datos también equilibra la protección de los datos personales con otros derechos y objetivos fundamentales», y cita los considerandos 2 y 4 y el artículo 23 del RGPD. El CEPD reconoce que la protección de datos no es un derecho absoluto y debe equilibrarse con otros derechos y objetivos fundamentales, de conformidad con el principio de proporcionalidad. Sin embargo, el CEPD observa que los considerandos 2 y 4 del RGPD, así como el artículo 23 del RGPD, difieren de una disposición legal que exija expresamente a las autoridades de protección de datos que tengan en cuenta una serie de objetivos en el ejercicio de sus funciones. En aras de la claridad, el CEPD invita a la Comisión a que reformule este considerando para evitar dar la impresión de que los considerandos 2 y 4, así como el artículo 23 del RGPD, tienen el mismo significado que el artículo 120B de la DPA 2018, y a que supervise que la aplicación de estos objetivos actualizados en la práctica no dé lugar a un desequilibrio excesivo en detrimento del derecho a los datos personales que socavaría el nivel de protección de los datos personales.

3.1.2. APLICACIÓN, INCLUIDAS LAS SANCIONES

60. El CEPD acoge con satisfacción el hecho de que la disposición incluida en el anterior proyecto de ley para reformar el marco de protección de datos del Reino Unido [el Proyecto de Ley de Protección de Datos e Información Digital (*Data Protection and Digital Information Bill*, «*DPDI Bill*»)[40]], y que estipulaba que la ICO debía tener en cuenta la opinión del Secretario de Estado en el ejercicio de sus competencias, ya no figure en el nuevo marco de protección de datos.

61. El CEPD también considera positivo que, desde la adopción de la anterior Decisión de Adecuación relativa al Reino Unido, la ICO haya publicado numerosos códigos de prácticas, directrices, dictámenes y otros documentos de orientación útiles para las partes pertinentes.

62. Al igual que en su Dictamen 14/2021[41], el CEPD destaca que un mecanismo de supervisión eficaz que permita la investigación independiente de las reclamaciones, así como procedimientos de recurso administrativos y judiciales eficaces, es crucial para evaluar si un sistema de protección de datos proporciona un nivel adecuado de protección. Además, la existencia de sanciones eficaces desempeña un papel importante a la hora de garantizar el cumplimiento de las normas.

[40] Véase el nuevo artículo 120 E, F, G y H de la sección 32 del Proyecto de Ley de Protección de Datos e Información Digital (*Data Protection and Digital Information Bill*).
[41] Véase el Dictamen 14/2021, apartados 112 a 114, del CEPD.

63. En este contexto, el CEPD llama la atención de la Comisión sobre la consulta pública publicada por la ICO el 22 de agosto en relación con sus propuestas para la tramitación de reclamaciones[42], que no se inició hasta después de la publicación del proyecto de decisión de la Comisión. En su introducción[43] a las propuestas de la consulta pública, la ICO afirma que espera que, una vez que entre en vigor la DUAA, las propias organizaciones resuelvan más reclamaciones sin la intervención de la ICO. Esta evaluación por parte de la ICO se basa en el hecho de que la DUAA establece nuevos requisitos para que las organizaciones introduzcan un procedimiento de reclamación específico para cuestiones relacionadas con la protección de datos. El artículo 164A de la DPA 2018[44] establece que los responsables del tratamiento deben adoptar medidas para ayudar a las personas que deseen presentar reclamaciones sobre el uso de sus datos personales. Por ejemplo, deben proporcionar un formulario de reclamación que pueda cumplimentarse electrónicamente y por otros medios, deben acusar recibo de las reclamaciones en un plazo de 30 días y, «sin demora indebida», tomar las medidas adecuadas para responder a la reclamación e informar al reclamante del resultado de la misma. En el caso de que las reclamaciones deben ser tramitadas por la ICO, las propuestas presentadas a consulta pública deberán constituir la base para la tramitación de las reclamaciones por parte de la ICO. A este respecto, la ICO propone una especie de sistema de clasificación, según el cual las reclamaciones deben tramitarse con diferentes prioridades y tipos de conclusión. Esto debería permitir a la ICO, en su calidad de regulador estratégico, centrar sus recursos en los riesgos más importantes y determinar los problemas sistémicos en una fase más temprana. La propuesta de la ICO establece criterios en una lista no exhaustiva que pueden incrementar o reducir la probabilidad de que una reclamación sea tramitada de forma más exhaustiva[45].

64. Los cambios descritos en el apartado 57 pueden dar lugar a un cambio en el enfoque de la CI respecto a la gestión de las reclamaciones. Debido al inicio de la consulta pública tras la publicación del proyecto de decisión de la Comisión, estos cambios aún no se han reflejado en el proyecto de Decisión.

65. El CEPD pide a la Comisión que incluya este elemento en su evaluación y que haga un seguimiento, en particular, de los resultados de la consulta pública de la ICO. Además, el CEPD invita a la Comisión a que supervise atentamente la futura tramitación de reclamaciones por parte de la CI con objeto de garantizar que siga estando asegurado un nivel equivalente de protección.

66. El CEPD señala, además, que las amplias competencias reguladoras concedidas al Secretario de Estado por la DUA, como la facultad de adoptar disposiciones legales, pueden tener implicaciones para el funcionamiento de la labor de la CI y de sus miembros. El CEPD hace referencia, por ejemplo, a la necesidad de que la CI consulte al Secretario de Estado en relación con algunas de sus tareas. En particular, el artículo 124A de la DPA 2018[46] exige a la CI que establezca códigos de prácticas adecuados que contengan directrices para el tratamiento adecuado de los datos personales cuando así lo requiera un reglamento adoptado por el Secretario de Estado. La CI debe consultar al Secretario de Estado antes de modificar o desarrollar dichos códigos.

[42] Véase la consulta de la ICO sobre los cambios propuestos en la forma en que gestionamos las reclamaciones relacionadas con la protección de datos: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/; https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf

[43] Véase la nota a pie de página 41.

[44] Véase el artículo 164A de la DPA 2018.

[45] Véase la nota a pie de página 41.

[46] Código de prácticas para el tratamiento de datos personales.

67. Dada la importancia de la independencia de la CI, el CEPD insta a la Comisión a que supervise atentamente estos nuevos poderes del Secretario de Estado, en particular su efecto práctico en el trabajo de la CI.

68. Como ya subrayó el CEPD en su Dictamen 14/2021, la ICO está correctamente dotada de las competencias necesarias, que se corresponden estrechamente con las competencias de las autoridades de control de los Estados miembros de la UE, tal como se establece en el artículo 58 del RGPD. Al mismo tiempo, como ya ha destacado el CEPD, la existencia de sanciones eficaces desempeña un papel importante a la hora de garantizar el cumplimiento de las normas. El CEPD invita a la Comisión a realizar una evaluación más detallada y a supervisar la aplicación de las facultades correctivas, así como la eficacia de las sanciones y de las medidas correctivas para las partes afectadas en el marco de protección de datos del Reino Unido[47].

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

69. El proyecto de Decisión se centra en los avances pertinentes para la evaluación del nivel de protección en el Reino Unido desde la adopción de la anterior Decisión de Adecuación relativa al Reino Unido, que sigue siendo válida para aquellos aspectos del marco de protección de datos del Reino Unido que no se hayan visto modificados ni afectados. Este planteamiento general también abarca el análisis de la Comisión sobre el acceso y el uso de datos personales por parte de las autoridades públicas del Reino Unido. Este aspecto específico se suele denominar «acceso gubernamental» y es uno de los elementos enumerados en el artículo 45, apartado 2, letra a), del RGPD que debe tener en cuenta la Comisión a la hora de determinar si el nivel de protección es esencialmente equivalente.

70. En este contexto, en las siguientes secciones se abordan una serie de cuestiones específicas planteadas en el proyecto de Decisión que se está examinando actualmente y que son pertinentes en relación con los datos personales transferidos desde el EEE con arreglo a la Decisión de Adecuación en virtud del RGPD relativa al Reino Unido, y consultados y tratados por las autoridades públicas del Reino Unido, incluidas las transferencias ulteriores. Por lo general, el análisis y las observaciones del CEPD presentados en el Dictamen 14/2021[48] siguen siendo válidos.

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

71. El marco de protección de datos que regula la consulta y el uso de los datos por parte de las autoridades públicas del Reino Unido con fines de aplicación de la legislación penal ha sido objeto de cambios legislativos desde la anterior evaluación de la Comisión recogida en la anterior Decisión de Adecuación relativa al Reino Unido. Entre ellos figuran la Ley de Seguridad Nacional de 2023 (*National Security Act 2023*), la Ley de Enmienda de los Poderes de Investigación de 2024 (*Investigation Powers Amendment Act 2024*) y la introducción de la DUAA. Esta última también se aborda en el proyecto de Decisión de Ejecución de la Comisión por la que se modifica la Decisión de Ejecución (UE) 2021/1773, así como en

[47] Véase el Dictamen 14/2021 del CEPD, apartado 113.
[48] Véase el dictamen 14/2021 del CEPD.

el correspondiente dictamen del CEPD emitido sobre la base del artículo 51, apartado 1, letra g), de la Directiva sobre protección de datos en el ámbito penal.

4.1.1. BASES JURÍDICAS Y SALVAGUARDIAS APLICABLES

4.1.1.1. PODERES DE INVESTIGACIÓN A EFECTOS DE APLICACIÓN DE LA LEY

72. En los considerandos 81 a 85 del proyecto de Decisión, la Comisión describe las enmiendas a la Ley británica de Poderes de Investigación de 2016 (IPA 2016) introducidas por la Ley de Enmienda de los Poderes de Investigación de 2024, en la medida en que se refieren al tratamiento policial[49]. En general, la Comisión proporciona información detallada. Sin embargo, en lo que respecta a una enmienda concreta, el CEPD considera que el proyecto de decisión se beneficiaría de una aclaración ulterior.

73. La Ley británica de Enmienda de los Poderes de Investigación de 2024 revisó la definición de «operador de telecomunicaciones», es decir, los posibles destinatarios de un requerimiento de conservación de datos en virtud de la IPA 2016[50]. La definición modificada incluye ahora a cualquier persona que «controle o proporcione un sistema de telecomunicaciones que: i) no se encuentre (total o parcialmente) en el Reino Unido o no esté controlado desde él; y ii) sea utilizado por otra persona para ofrecer o prestar un servicio de telecomunicaciones a personas en el Reino Unido». Si bien la Comisión se remite a las notas explicativas de la Ley británica de Enmienda de los Poderes de Investigación de 2024, en las que se afirma que el artículo 261, apartado 10, letra c), «proporciona una aclaración adicional que garantiza que las grandes empresas con estructuras empresariales complejas estén cubiertas en su totalidad por la IPA 2016», así como que «la enmienda [...] no pretende incluir a otras empresas en el ámbito de aplicación», las implicaciones de este cambio siguen sin estar claras, por ejemplo, no está claro si ampliaría el volumen de datos personales potencialmente sujetos a un requerimiento de conservación. Por consiguiente, el CEPD invita a la Comisión a abordar los efectos de esta enmienda en mayor detalle y a supervisar específicamente este aspecto, en particular a la luz de los principios de necesidad y proporcionalidad.

4.1.1.2. EXENCIONES POR MOTIVOS DE SEGURIDAD NACIONAL PARA LAS AUTORIDADES ENCARGADAS DE GARANTIZAR LA APLICACIÓN DE LA LEY

74. El artículo 88 de la DUAA actualiza las exenciones por motivos de seguridad nacional existentes en el marco de la aplicación de la ley para reflejar las disponibles en virtud del RGPD del Reino Unido y los regímenes de los servicios de inteligencia[51]. Si bien las autoridades policiales ya pueden limitar el cumplimiento de determinadas obligaciones por motivos de protección de la seguridad nacional, como las relativas a los derechos de los interesados, el artículo 78A de la Ley británica de Protección de Datos

[49] La Comisión señala que, tal y como se describe en los considerandos 139 a 141 de la Decisión de Ejecución (UE) 2021/1772, las autoridades encargadas de garantizar el cumplimiento de la ley específicas también pueden hacer uso de poderes de investigación específicos en virtud de la IPA 2016 con el fin de prevenir o detectar delitos graves. Por lo tanto, las enmiendas a dichas disposiciones no solo se refieren al acceso a los datos para fines de seguridad nacional, sino también a efectos de aplicación de la ley.

[50] Artículo 261, apartado 10, letra c), de la IPA 2016, insertado por el artículo 19 de la Ley británica de Enmienda de los Poderes de Investigación de 2024.

[51] Véase también Department for Science, Innovation & Technology, *Data (Use and Access) Act factsheet: UK GDPR and DPA* [Departamento de Ciencia, Innovación y Tecnología del Reino Unido, Hoja informativa sobre la Ley de Datos (uso y acceso): el RGPD del Reino Unido y la Ley de Protección de Datos], publicada el 27 de junio de 2025, p. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa.

de 2018[52] también incluirá la mayoría de los principios de protección de datos[53] y determinados requisitos en materia de transferencia internacional de datos[54] como disposiciones que pueden dejar de aplicarse si fuese necesario con el fin de salvaguardar la seguridad nacional. Además, algunos de los poderes del Comisario de Información del Reino Unido para realizar inspecciones y tomar medidas coercitivas[55] pueden no aplicarse en tales circunstancias.

75. Estas enmiendas no se mencionan ni en el proyecto de decisión de adecuación en virtud del artículo 45 del RGPD ni en el proyecto de decisión de adecuación en virtud del artículo 36 de la Directiva sobre protección de datos en el ámbito penal. Sin embargo, el CEPD considera esencial evaluar estas exenciones ampliadas a la luz de los principios de necesidad y proporcionalidad. En este contexto, el CEPD recuerda la segunda de las cuatro denominadas «garantías esenciales europeas»: «[c]ualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por ley y respetar el contenido esencial de dichos derechos y libertades. Solo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».[56] El CEPD está preocupado por las excepciones a los principios fundamentales de protección de datos, los requisitos para la transferencia internacional de datos y los poderes del Comisario de Información del Reino Unido.

76. Con arreglo a la norma revisada, cinco de los seis principios de protección de datos pueden dejar de aplicarse cuando sea necesario para salvaguardar la seguridad nacional[57]. Estos principios estipulan, entre otras cosas, que el propósito de aplicación de la ley para el que se recopilen los datos personales debe ser específico, explícito y legítimo, y que los datos personales deben ser adecuados, pertinentes y no excesivos en relación con ese propósito. También especifican que los datos personales deben ser exactos y conservarse únicamente durante el tiempo que sea necesario. Como se ha mencionado anteriormente, las futuras exenciones abarcan además algunos de los requisitos para la transferencia internacional, como la denominada segunda condición para las transferencias internacionales establecida en el artículo 73, apartado 3, de la Ley británica de Protección de Datos de 2018. Esta condición exige que las transferencias se basen en reglamentos de adecuación, salvaguardias adecuadas o, en el caso de que no se aplique ninguna de ellas, en circunstancias especiales. Las exenciones también afectan a las competencias del Comisario de Información del Reino Unido, por ejemplo, la autoridad para emitir requerimientos de información y de cumplimiento[58].

[52] La Ley británica de Datos (uso y acceso) (DUAA, por sus siglas en inglés) se introducirá gradualmente en varias fases. Los principales cambios en la legislación en materia de protección de datos de la parte 5 de la DUAA entrarán en vigor dentro de la fase 3, aproximadamente seis meses después de la Aprobación Real: https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement.

[53] Véase el artículo 78A, apartados 1, 2, letra a), y 3, de la Ley británica de Protección de Datos de 2018 (DPA 2018), introducida por el artículo 88 de la DUAA.

[54] Véase el artículo 78A, apartados 1, 2, letra d), y 4, de la Ley británica de Protección de Datos de 2018 (DPA 2018), introducida por el artículo 88 de la DUAA.

[55] Véase el artículo 78A, apartados 1, 2, letras e), f) y g), de la Ley británica de Protección de Datos de 2018 (DPA 2018), introducida por el artículo 88 de la DUAA.

[56] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020: p. 10.

[57] De conformidad con el artículo 78A, apartados 2 y 3, de la Ley británica de Protección de Datos de 2018 (DPA 2018), el capítulo 2 de la parte 3 de dicha ley no se aplica si es necesario para garantizar la seguridad nacional, excepto: a) el artículo 35, apartado 1 (el primer principio de protección de datos), en la medida en que exija que el tratamiento de datos personales sea lícito; b) el artículo 35, apartados 2 a 5 (licitud del tratamiento y restricciones del tratamiento sensible); c) el artículo 42 (salvaguardas: tratamiento sensible); y d) el anexo 8 (condiciones para el tratamiento sensible).

[58] Los requerimientos de información exigen que el responsable o el encargado del tratamiento faciliten al Comisario la información razonablemente necesaria para el desempeño de sus funciones. Los requerimientos de cumplimiento facultan

77. El CEPD señala que, si bien las exenciones se apartan claramente de la Directiva sobre protección de datos en el ámbito penal, son muy similares a las excepciones y restricciones para la seguridad nacional previstas en el artículo 11 del Convenio 108 modernizado del Consejo de Europa («el Convenio 108+»)[59], que el Reino Unido firmó el 10 de octubre de 2018, pero que, en la fecha de emisión del presente dictamen, no ha sido ratificado por el Reino Unido ni ha entrado en vigor aún.[60] A este respecto, el CEPD recuerda que el Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (T-PD) ha publicado recientemente unas Directrices sobre los principios generales del artículo 11 del Convenio 108 modernizado (*Guidelines on the general principles of Article 11 of the Modernised Convention 108*, disponible en inglés)[61].

78. En su documento de orientación, el Consejo de Europa destaca explícitamente que no es aplicable ninguna excepción, entre otros motivos, por la proporcionalidad y la legitimidad de la finalidad de los principios de tratamiento. Esto implica que debe garantizarse la proporcionalidad del tratamiento de los datos, así como que se den los requisitos para tratar los datos personales con un fin legítimo. De conformidad con las orientaciones del T-PD, el CEPD se mantiene especialmente vigilante con respecto a cualquier excepción al principio de proporcionalidad, así como al requisito de tratar los datos personales con fines legítimos. Del mismo modo, en opinión del CEPD, cualquier excepción a los poderes de la autoridad de control debe abordarse con cautela. Si bien los requisitos específicos para las actividades de supervisión —como las autorizaciones de seguridad— pueden ser adecuados en el contexto del tratamiento relacionado con la seguridad nacional, es crucial garantizar una supervisión eficaz a fin de evitar la creación de un vacío de supervisión. En este mismo sentido, el artículo 11, apartado 3, del Convenio 108+ estipula que las excepciones a su artículo 15[62] «se entienden sin perjuicio del requisito de que las actividades de tratamiento con fines de seguridad y defensa nacionales estén sujetas a un control y una supervisión independientes y eficaces con arreglo a la legislación nacional» de las partes en el Convenio. Además, cualquier exención debe interpretarse de la manera más restrictiva posible. El hecho de que los datos personales se traten con fines de seguridad nacional no debe ser suficiente por sí solo para invocar una exención. Debe quedar claro que la exención del régimen de protección de datos debe aplicarse caso por caso y solo si dicha medida es necesaria y proporcionada[63].

79. Dado que los proyectos de decisiones de adecuación no abordan este punto, el CEPD pide a la Comisión que complemente su evaluación en el proyecto de decisión, así como que supervise específicamente la aplicación en la práctica de las exenciones por motivos de seguridad nacional para las autoridades policiales.

---

al Comisario para exigir a una persona que adopte (o se abstenga de adoptar) medidas específicas cuando el Comisario esté convencido de que la persona incumple determinadas obligaciones en materia de protección de datos.

[59] Véase el Protocolo que modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 223).

[60] https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

[61] https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146

[62] Véase el artículo 15 del Convenio 108+, que especifica cómo las partes en el Convenio, al establecer una o varias autoridades de control, garantizarán el cumplimiento de las disposiciones del Convenio.

[63] Véase también el artículo 11 del Convenio 108+, que especifica que las excepciones deben estar previstas por la ley, respetar la esencia de los derechos y libertades fundamentales y constituir una medida necesaria y proporcionada en una sociedad democrática. De acuerdo con las directrices del TP-D sobre los principios generales del artículo 11, esto implica que deben sopesarse los intereses en juego entre la necesidad de prever excepciones a determinadas disposiciones del Convenio y el respeto de los derechos humanos y las libertades fundamentales de las personas, y que debe justificarse tal sopesamiento.

4.1.2. EJERCICIO CONJUNTO DE LA RESPONSABILIDAD DEL TRATAMIENTO ENTRE LOS ORGANISMOS DE INTELIGENCIA Y LAS AUTORIDADES POLICIALES DEL REINO UNIDO

80. Sobre la base de las modificaciones introducidas por la DUAA, las actividades de tratamiento llevadas a cabo por las autoridades policiales pueden, en circunstancias específicas, entrar en el ámbito de aplicación de las normas habitualmente aplicables al tratamiento de datos personales por parte de las autoridades de seguridad nacionales[64]. En otras palabras, con arreglo a las condiciones establecidas en el artículo 89 de la DUAA, el régimen de protección de datos para el tratamiento de datos con fines de seguridad nacional establecido en la parte 4 de la Ley británica de Protección de Datos de 2018 se amplía al tratamiento de datos por parte de las autoridades policiales.

81. La Comisión hace hincapié en que las condiciones del artículo 89 de la DUAA ofrecen salvaguardias estrictas: se debe especificar una autoridad competente como «autoridad competente cualificada» en los reglamentos adoptados por el Secretario de Estado, quien, además, debe designar una determinada actividad de tratamiento realizada por la autoridad competente cualificada como responsable conjunta del tratamiento con al menos un servicio de inteligencia con el fin de salvaguardar la seguridad nacional[65].

82. Si bien reconoce que estas salvaguardias implican restricciones significativas, el CEPD invita a la Comisión a supervisar la aplicación práctica de estas normas. Debe prestarse especial atención a garantizar que la parte 4 de la Ley británica de Protección de Datos de 2018 se aplique estrictamente a las operaciones de tratamiento por motivos de seguridad nacional, sin que se amplíe a otros contextos. Aunque se concede a los Estados un amplio margen de discrecionalidad en materia de seguridad nacional, como también reconoce el TEDH[66], el CEPD considera que las amenazas a la seguridad nacional deben distinguirse por su naturaleza, gravedad y circunstancias específicas de los riesgos generales para la seguridad pública, o de las infracciones penales graves. Solo en tales casos la actuación de las autoridades policiales en el marco del régimen de protección de datos de los servicios de inteligencia es compatible con los principios de necesidad y proporcionalidad[67]. Además, el CEPD considera necesario supervisar si las autoridades competentes cualificadas son capaces en la práctica de mantener una distinción clara entre los distintos fines de tratamiento a fin de aplicar el marco jurídico correspondiente en consecuencia.

4.1.3. EL DERECHO DE ACCESO

83. La DUAA especifica que los interesados en el tratamiento de los datos solo tienen derecho a acceder a la información pertinente en la medida en que el responsable del tratamiento pueda proporcionarla mediante una búsqueda razonable y proporcionada. Esta enmienda se introduce tanto en el régimen de aplicación de la ley como en el de seguridad nacional[68].

---

[64] Véase el considerando 72 del proyecto de Decisión.
[65] Véase el considerando 73 del proyecto de Decisión.
[66] Véase, por ejemplo, TEDH, asunto Big Brother Watch y otros contra el Reino Unido, 25 de mayo de 2021, apartado 350.
[67] De la jurisprudencia del TJUE, al aplicar la prueba de necesidad y proporcionalidad a la legislación de los Estados miembros que permite la conservación y el acceso a los datos personales por parte de las autoridades públicas, se desprende que los objetivos legítimos, como la seguridad nacional o la lucha contra los delitos graves, son diferentes y, por tanto, podrían justificar diferentes tipos de injerencia. 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.
[68] Véase el artículo 78, apartados 3 y 4, de la Ley británica de Datos (uso y acceso) [*Data (Use and Access) Act*, DUAA], por la que se modifican los artículos 45 y 94 de la Ley británica de Protección de Datos de 2018 (*Data Protection Act 2018*).

84. La Comisión explica que se trata de una aclaración en consonancia con las normas establecidas desarrolladas con arreglo a la jurisprudencia nacional, que también tienen en cuenta los intereses del interesado en el tratamiento de los datos. Sin embargo, el CEPD habría acogido con satisfacción información más detallada sobre cómo se interpreta el concepto de «búsqueda razonable y proporcionada», también porque el artículo 14 de la Directiva sobre protección de datos en el ámbito penal no contiene este elemento. El CEPD reconoce que, efectivamente, pueden darse situaciones en las que los esfuerzos de un responsable del tratamiento por identificar y localizar información sobre el interesado puedan considerarse poco razonables y desproporcionados sin que ello comprometa la equivalencia esencial[69]. El CEPD recuerda el análisis y la conclusión del apartado 34 del presente Dictamen, que son igualmente pertinentes para el régimen de aplicación de la ley y de seguridad nacional.

4.1.4. TRANSFERENCIAS ULTERIORES

4.1.4.1. UNA NUEVA PRUEBA DE PROTECCIÓN DE DATOS

85. Cuando una autoridad competente tenga la intención de divulgar datos personales tratados con arreglo a la parte 3 de la DPA 2018 con las autoridades policiales de un tercer país, se aplicarán requisitos específicos. En particular, dichas transferencias podrán tener lugar cuando sean aprobadas por reglamentos elaborados por el Secretario de Estado del Reino Unido o, en ausencia de tales reglamentos, sobre la base de las salvaguardias adecuadas. Si una transferencia no puede basarse ni en un reglamento ni en salvaguardias adecuadas, solo podrá tener lugar en determinadas circunstancias específicas, denominadas «circunstancias especiales» correspondientes a las situaciones y condiciones que se consideren «excepciones» con arreglo al artículo 38 de la Directiva sobre protección de datos en el ámbito penal.

86. Si bien la Comisión observa que «el régimen de transferencias internacionales de datos personales desde el Reino Unido se mantiene muy próximo a las normas establecidas en el capítulo V de la Directiva (UE) 2016/680», el proyecto de Decisión también indica que se han reformulado la norma jurídica relativa a los reglamentos para la aprobación de transferencias, a los que se hacía referencia como «reglamentos de adecuación» en el antiguo artículo 74A de la DPA 2018, y las salvaguardias adecuadas. En lugar de hacer referencia a un nivel de protección adecuado, la nueva «prueba de protección de datos» establecida en el artículo 74AB de la Ley británica de Protección de Datos de 2028 exige que el nivel de protección de los interesados en los terceros países u organizaciones internacionales destinatarios no sea «sustancialmente inferior» al nivel previsto para los interesados en la legislación pertinente del Reino Unido en materia de protección de datos.

87. En este contexto, el CEPD observa que los elementos que debe tener en cuenta el Secretario de Estado en la evaluación con arreglo al artículo 74 AB, apartado 2, de la DPA 2018 parecen haberse reducido en comparación con la evaluación anterior de los reglamentos de adecuación[70]. El CEPD señala la eliminación de determinados factores que, en su opinión, desempeñan un papel importante a la hora de evaluar si un tercer país ofrece un nivel de protección de los datos personales esencialmente equivalente, y recuerda el análisis y las conclusiones formuladas en los apartados 42 y 43 del presente Dictamen. En particular, el CEPD i) anima a la Comisión a abordar específicamente los cambios y a

[69] Por ejemplo, se podría decir que esta situación se da en el caso de la búsqueda de dispositivos incautados que aún no se hayan analizado o descifrado.
[70] La disposición del artículo 74A, apartado 4, de la DPA 2018, que se omitió en la DUAA, preveía una lista de criterios idéntica a la del artículo 36, apartado 3, de la Directiva sobre protección de datos en el ámbito penal.

profundizar en su evaluación de la nueva prueba de protección de datos. El CEPD entiende que las nuevas normas sobre las transferencias de datos personales a terceros países tienen por objeto ofrecer una flexibilidad adicional. Al mismo tiempo, el CEPD invita a la Comisión a supervisar la aplicación práctica de estas normas en el ámbito de la cooperación policial y judicial en materia penal. Esto es especialmente pertinente en lo que respecta a la nueva autoridad del Secretario de Estado para elaborar reglamentos que especifiquen y aprueben una transferencia, sobre la base de la nueva prueba de protección de datos, por cualquier medio, inclusive por referencia a sectores geográficos dentro de un país; los responsables o encargados del tratamiento; los destinatarios de los datos; los tipos de datos; los medios de transferencia; y los instrumentos jurídicos. Por ejemplo, sigue sin estar claro cómo un responsable o encargado del tratamiento específico con sede en un tercer país que no se considere adecuado cumpliría los requisitos de protección de datos en lo que respecta a la reparación efectiva o a los derechos de los interesados que aún no están establecidos en el marco jurídico de ese tercer país.

88. Asimismo, el CEPD recuerda las conclusiones expuestas en el apartado 41 en relación con el uso del criterio de la «conveniencia de facilitar las transferencias de datos personales hacia y desde el Reino Unido» (artículo 74AA, apartado 3, de la Ley británica de Protección de Datos de 2018) e invita a la Comisión a que aclare en su decisión que este criterio no es un elemento de la prueba de protección de datos, sino simplemente un factor adicional que el Secretario de Estado puede tener en consideración cuando se cumplen plenamente los criterios de la prueba, ya que esto no queda totalmente claro en el texto legislativo. En este sentido, el CEPD invita a la Comisión a que supervise las implicaciones prácticas del artículo 74AA, apartado 3, de la Ley británica de Protección de Datos de 2018, ya que queda por ver qué papel desempeñará en este contexto la «conveniencia de facilitar las transferencias de datos personales hacia y desde el Reino Unido».

4.1.4.2. EL ACUERDO ENTRE EL REINO UNIDO Y LOS ESTADOS UNIDOS SOBRE LA LEY CLOUD

89. Otro avance importante en el ámbito de las transferencias ulteriores es la entrada en vigor, en octubre de 2022, del «Acuerdo entre el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte y el Gobierno de los Estados Unidos de América sobre el acceso a datos electrónicos con el fin de combatir delitos graves» (*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*, «el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD»). Como señala acertadamente la Comisión, los datos personales transferidos desde la UE a proveedores de servicios del Reino Unido podrían estar sujetos a órdenes de presentación de pruebas emitidas por las autoridades encargadas de garantizar la aplicación de la ley en los Estados Unidos en virtud de este acuerdo[71].

90. Dado que, en el momento de la adopción de la anterior Decisión de Adecuación relativa al Reino Unido, el acuerdo se había celebrado pero aún no había entrado en vigor, la Comisión hizo hincapié en que cualquier información y aclaración futura sobre la forma en que los Estados Unidos cumplirán sus obligaciones en virtud del acuerdo deben ser comunicadas por el Reino Unido a la Comisión con el fin de garantizar un seguimiento adecuado de la anterior Decisión de Adecuación relativa al Reino Unido, de conformidad con el artículo 45, apartado 4, del RGPD. La Comisión señaló que debía prestarse especial atención a la aplicación y adaptación de las salvaguardias establecidas en el Acuerdo marco

[71] Véase el considerando 87 del proyecto de Decisión.

UE-EE. UU.[72] al tipo específico de transferencias cubiertas por el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD[73]. Como seguimiento de esta declaración, la Comisión se refiere en su proyecto de Decisión a varias aclaraciones alcanzadas entre el Reino Unido y los Estados Unidos en el contexto de la aplicación del Acuerdo marco UE-EE.UU. al Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD. El CEPD acoge con satisfacción estas aclaraciones, que aportan mayor claridad jurídica. Al mismo tiempo, cabe señalar que el Acuerdo marco UE-EE. UU. aún no se ha revisado, lo que limita en cierta medida las conclusiones que pueden extraerse sobre el impacto y la eficacia de su aplicación al Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD[74]. Además, habida cuenta del Acuerdo marco UE-EE. UU., el CEPD desea recordar la necesidad de mejorar el nivel de las salvaguardias previstas en dicho Acuerdo. Esto se refiere, en particular, a la disponibilidad de recursos judiciales. En virtud de la Ley estadounidense de Recurso Judicial (*Judicial Redress Act*), los interesados de la UE distintos de ciudadanos de la UE carecen de fundamento jurídico para interponer recursos. Además, la Ley estadounidense de Privacidad (*Privacy Act*) contiene excepciones, que no han sido modificadas por la Ley de Recurso Judicial, que reducen la capacidad de las personas para solicitar una reparación en determinadas situaciones relacionadas con la aplicación de la ley y la seguridad nacional. Si bien la Comisión señala que la Ley estadounidense de Recurso Judicial no es el único mecanismo para solicitar una reparación, el proyecto de Decisión simplemente establece que «dependiendo de las circunstancias y el contexto del caso específico, otras leyes estadounidenses aplicables ofrecen vías alternativas para solicitar un recurso judicial»[75]. Esto no deja claro si concederá el derecho a un recurso judicial en los Estados Unidos a todos los ciudadanos de la UE cuyos datos puedan estar sujetos al Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD.

91. El CEPD también señala que una salvaguardia recíproca específica establecida en el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD, en virtud de la cual ambas partes limitan las repercusiones que el acuerdo puede tener para las personas del Reino Unido y de los Estados Unidos, respectivamente, no es, por su naturaleza, aplicable a los ciudadanos de la UE[76]. El CEPD observa que, por esta razón, es fundamental contar con salvaguardias sólidas en materia de protección de datos con objeto de garantizar que los derechos de los interesados de la UE estén adecuadamente protegidos si se tratan en virtud de dicho acuerdo. Por lo tanto, el CEPD invita a la Comisión a seguir incluyendo el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD en sus futuras evaluaciones y revisiones de la decisión de adecuación.

92. En general, el CEPD considera necesario aclarar la evaluación de la Comisión sobre el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD y cualquier posible repercusión del acuerdo en

[72] Véase el Acuerdo entre la Unión Europea y los Estados Unidos sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, DO L 336 de 10.12.2016, pp. 3-13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01).

[73] Véase el considerando 155 de la Decisión de Ejecución (UE) 2021/1772. De conformidad con el artículo 9, apartado 1, del Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD, el Acuerdo marco UE-EE. UU. se aplica *mutatis mutandis* al Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD. Solo puede aplicarse *mutatis mutandis*, ya que el Acuerdo marco regula las transferencias transfronterizas entre autoridades policiales y judiciales y no la cooperación directa entre un proveedor de servicios y una autoridad policial y judicial.

[74] Véase el artículo 23 del Acuerdo marco entre la UE y los Estados Unidos, que establece que las partes llevarán a cabo revisiones conjuntas periódicas de las políticas y los procedimientos por los que se aplican el Acuerdo, realizándose la primera revisión conjunta a más tardar tres años a partir de la fecha de entrada en vigor del acuerdo. El Acuerdo marco UE-EE. UU. entró en vigor en febrero de 2017.

[75] Véase el considerando 93 del proyecto de Decisión.

[76] Véanse el artículo 4, apartado 3, y el artículo 7, apartado 1, del acuerdo, que prevén restricciones específicas en las que se establece que las órdenes sujetas al acuerdo no pueden aplicarse intencionadamente a una «persona destinataria». Por lo tanto, los Estados Unidos no pueden aplicar el acuerdo intencionadamente a una persona situada en el territorio del Reino Unido, y el Reino Unido debe cumplir una restricción similar.

el nivel de protección evaluado en la anterior Decisión de Adecuación relativa al Reino Unido. Las conclusiones de la primera revisión del Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD —que, en virtud del artículo 12, apartado 1, del acuerdo, se llevará a cabo en el plazo de un año a partir de la entrada en vigor del acuerdo— podrían ser especialmente esclarecedoras de cara a este análisis ulterior.

4.1.5. SUPERVISIÓN Y REPARACIÓN

93. El CEPD señala que el sistema de supervisión de los organismos encargados de hacer cumplir el Derecho penal en virtud de la Ley británica de Protección de Datos de 2018 (DPA 2018) y la Ley británica de Poderes de Investigación de 2016 (IPA 2016), así como los mecanismos de recurso disponibles en virtud de la parte 3 de la DPA 2018, la IPA 2016 y la Ley británica de Derechos Humanos de 1998, se mantienen en gran medida inalterados. En particular, la supervisión en el Reino Unido sigue estando garantizada, además de por la Oficina del Comisario de Información (ICO), por una combinación de diferentes comisarios, a saber, el Comisario de Poderes de Investigación (Investigatory Powers Commissioner, IPC), asistido por otros Comisarios Judiciales, así como el Comisario de Biometría y Cámaras de Vigilancia (Biometrics and Surveillance Camera Commissioner).

94. Tal y como explica la Comisión en el considerando 97 del proyecto de Decisión, la Ley británica de Enmienda de los Poderes de Investigación de 2024 solo ha introducido modificaciones limitadas, en particular mediante la introducción de IPC adjuntos en los que el IPC principal puede delegar poderes específicos cuando no pueda desempeñar sus funciones o no esté disponible para hacerlo. Estos IPC adjuntos deben ser Comisarios Judiciales y son nombrados por el IPC.

95. El CEPD valora positivamente que se hayan descartado las ideas anteriores recogidas en el Proyecto de Ley de Protección de Datos e Información Digital (DPDI Bill), que precedió a la DUUA, de suprimir el cargo de Comisario de Biometría y Cámaras de Vigilancia y transferir sus funciones al Comisario de Poderes de Investigación (IPC)[77]. A este respecto, el CEPD invita a la Comisión a prestar más atención y a proporcionar una evaluación más detallada del papel del Comisario de Biometría y Cámaras de Vigilancia en el sistema de supervisión durante su seguimiento y futuras revisiones del proyecto de Decisión.

96. Como ya ha destacado el CEPD en su Dictamen 14/2021, aunque la ICO está debidamente dotada de los poderes necesarios, que se corresponden en gran medida con los poderes de las autoridades de control de los Estados miembros de la UE establecidas en el artículo 58 del RGPD, la existencia de sanciones efectivas desempeña un papel importante a la hora de garantizar el cumplimiento de las normas[78].

97. El CEPD valora positivamente la política de transparencia de la ICO y la disponibilidad de datos estadísticos y analíticos, incluidos ejemplos, sobre las actividades de control del cumplimiento de la ICO frente a los organismos encargados de garantizar el cumplimiento de la ley[79]. A este respecto, el CEPD observa la preferencia de la autoridad de control del Reino Unido por las amonestaciones en caso de infracciones de la legislación en materia de protección de datos por parte de las fuerzas policiales. Una excepción notable es el requerimiento de cumplimiento (*enforcement notice*) emitido

[77] Véase https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner
[78] Véase el Dictamen 14/2021, apartado 112, del CEPD.
[79] Véanse, por ejemplo, los conjuntos de datos detallados sobre reclamaciones en materia de protección de datos, disponibles en https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/.

al Ministerio Fiscal del Reino Unido (Crown Prosecution Service) en enero de 2024[80]. El CEPD también considera positivo que la ICO haya publicado numerosos códigos de prácticas, directrices, dictámenes y otros documentos de orientación para las partes interesadas.

98. A la luz de lo anterior, y en particular en vista de los inminentes cambios sustanciales en la estructura y la organización de la autoridad de control del Reino Unido, como ya se ha analizado en el apartado 68 del presente Dictamen, el CEPD invita a la Comisión Europea a seguir supervisando la eficacia de las sanciones y las vías de recurso pertinentes en el marco de protección de datos del Reino Unido.

4.2. ACCESO A LOS DATOS Y USO DE LOS MISMOS POR PARTE DE LAS AUTORIDADES PÚBLICAS DEL REINO UNIDO A EFECTOS DE LA SEGURIDAD NACIONAL

99. El proyecto de Decisión solo ofrece detalles limitados sobre el acceso a los datos personales y su utilización por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional. La Comisión explica que la DUAA solo introdujo modificaciones menores en el marco que regula el tratamiento de datos por parte de los servicios de inteligencia del Reino Unido[81], algunas de las cuales también se han incorporado al régimen de aplicación de la Ley británica de Protección de Datos de 2018. Estas enmiendas se mencionan brevemente en el considerando 75 del proyecto de Decisión. Además, los cambios realizados en la IPA 2016 desde la adopción de la anterior Decisión de Adecuación relativa al Reino Unido ya se abordan en la sección 3.2 del proyecto de Decisión, cuando se refieren tanto al tratamiento de datos con fines de aplicación de la ley como de seguridad nacional[82]. En consecuencia, las solicitudes de aclaración y supervisión descritas en las secciones 4.1.1.1 y 4.1.3 anteriores se aplican igualmente al acceso a los datos personales y el uso de estos por motivos de seguridad nacional.

4.2.1. EL USO DE REQUERIMIENTOS DE CAPACIDAD TÉCNICA

100. A principios de este año, los medios de comunicación revelaron que el Gobierno del Reino Unido había emitido supuestamente un requerimiento de capacidad técnica (*technical capacity notice*, TCN) en virtud del artículo 253 de la IPA 2016 a una importante empresa tecnológica, exigiendo al proveedor que mantuviera el acceso a los datos cifrados de sus usuarios en forma descifrada[83]. En la práctica, supuestamente, esto supondría eludir el cifrado de extremo a extremo que el proveedor ofrece para su solución de almacenamiento en la nube. Por lo tanto, esta medida fue calificada de «demanda clandestina».

101. Aunque la base jurídica para los requerimientos de capacidad técnica ya existía en el momento de la adopción de la anterior Decisión de Adecuación relativa al Reino Unido, este caso notificado parece marcar el primer caso conocido de una solicitud de este tipo. Como tal, constituye un avance significativo digno de atención, en particular a la luz del artículo 45, apartado 2, letra a), del RGPD, que exige una evaluación no solo del marco jurídico sobre el papel, sino también de su aplicación[84]. Por lo

[80] Véase https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/
[81] Véase el considerando 75 del proyecto de Decisión.
[82] Véase el considerando 98 del proyecto de Decisión. Los poderes de investigación en cuestión pueden ser ejercidos no solo por los organismos nacionales de inteligencia, sino también por determinadas autoridades policiales.
[83] Véase «*U.K. orders Apple to let it spy on users' encrypted accounts» [«El Reino Unido ordena a Apple que le permita espiar las cuentas cifradas de los usuarios*», disponible en inglés] (*Washington Post*, 7 de febrero de 2025). https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.
[84] Además, el artículo 45, apartado 3, del RGPD especifica que la Comisión tendrá en cuenta todos los acontecimientos pertinentes en el tercer país cuando revise periódicamente sus conclusiones sobre la adecuación.

tanto, el CEPD habría esperado que el proyecto de Decisión abordara esta cuestión de manera explícita y anima a la Comisión a complementar la decisión en consecuencia.

102. A pesar de que los detalles de este caso no son plenamente conocidos por el público debido al carácter confidencial de los requerimientos de capacidad técnica, de la publicación de la solicitud de audiencia reservada en el sitio web del Tribunal de Poderes de Investigación (Investigatory Powers Tribunal), así como del extracto públicamente accesible de la sentencia reservada relativa a dicha audiencia, se desprende que no se trata de una cuestión de especulación de los medios[85]. La cuestión merece ser mencionada, mientras que debería señalarse para su futuro seguimiento la supuesta aplicación del artículo 253 de la IPA 2016 con el fin de emitir una «demanda clandestina».

103. Como se señaló recientemente en la Declaración 5/2024, el CEPD considera que el cifrado es esencial para garantizar la seguridad y la confidencialidad de los datos personales y las comunicaciones electrónicas. En particular, el cifrado auténtico de extremo a extremo que abarca los dispositivos terminales y los datos que estos contienen, con las claves de descifrado en poder exclusivo del usuario, es una herramienta fundamental para garantizar la confidencialidad de las comunicaciones electrónicas[86]. Los requerimientos de capacidad técnica (*technical capacity notices*) que obligan a las empresas a ofrecer la capacidad de eliminar el cifrado a petición del Gobierno crean vulnerabilidades sistémicas y suponen una amenaza directa para la integridad y la confidencialidad de las comunicaciones electrónicas. A este respecto, el CEPD llama la atención sobre el caso PODCHASOV contra RUSIA, en el que el TEDH consideró que «la obligación de descifrar las comunicaciones cifradas de extremo a extremo corre el riesgo de equivaler a exigir a los proveedores de dichos servicios que debiliten el mecanismo de cifrado para todos los usuarios, por lo que, no es proporcionada a los objetivos legítimos perseguidos»[87].

104. Si bien se da por hecho que el Gobierno del Reino Unido trataría principalmente de acceder a datos de usuarios no cifrados si existiera un riesgo para la seguridad nacional, el CEPD considera que la solicitud de evaluación del uso de los requerimientos de capacidad técnica, tal y como se ha expuesto anteriormente, es igualmente pertinente en el contexto del acceso a los datos por parte del Gobierno con fines policiales.

4.2.2. BASES JURÍDICAS Y SALVAGUARDIAS APLICABLES

105. La Ley británica de Enmienda de los Poderes de Investigación de 2024 (*Investigatory Powers Amendment Act 2024*) introdujo un régimen específico para la conservación y el examen de conjuntos de datos personales en bloque para los que las personas a las que se refieren dichos datos «no podrían tener ninguna expectativa de privacidad, o solo una expectativa baja y razonable», tal como se expresa en la citada ley[88]. Para la conservación y el examen de este subconjunto específico de conjuntos de datos personales en bloque, la IPA 2016 prevé ahora la posibilidad de «autorizaciones individuales» y «autorizaciones por categoría». [89]

[85] Véase https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/
[86] Véase la Declaración 5/2024 sobre las Recomendaciones del Grupo de Alto Nivel sobre el Acceso a los Datos para una Aplicación Eficaz de la Ley, adoptada el 4 de noviembre de 2024, pp. 4 y 5.
[87] Véase la sentencia del TEDH de 13 de febrero de 2024, 33696/19, apartado 79.
[88] Véase el artículo 226A, apartado 1, de la Ley británica de Poderes de Investigación de 2016 (*Investigatory Powers Act 2016*, IPA 2016).
[89] Véanse los artículos 226A y 226BA de la IPA 2016, introducidos por el artículo 2 de la Ley británica de Enmienda de los Poderes de Investigación
de 2024 (*Investigatory Powers Amendment Act 2024*).

106. El concepto de conjuntos de datos personales en bloque es amplio y puede abarcar una gran variedad de conjuntos de datos[90]. Puede aplicarse a información sensible, pero también puede abarcar datos disponibles públicamente y con fines comerciales. En este contexto, el Gobierno del Reino Unido consideró necesario revisar el régimen anterior, que aplicaba el mismo nivel de salvaguardias a todos los conjuntos de datos personales recogidos en bloque, y prever, en su lugar, diferentes salvaguardias para la conservación y el examen de los conjuntos de datos personales en bloque, en función de la sensibilidad o la disponibilidad pública de su contenido, o del nivel de intrusión asociado a los servicios de inteligencia que los conserven y examinen[91]. El CEPD entiende que estas consideraciones han dado lugar, en última instancia, a la creación de un régimen distinto para los conjuntos de datos personales en bloque cuando solo existe una expectativa baja o ninguna expectativa razonable de privacidad.

107. Si bien la Comisión analiza brevemente el nuevo concepto de «autorización por categoría», el proyecto de Decisión afirma que «es importante que, a efectos de la conservación y el examen de conjuntos de datos personales en bloque, se mantenga el régimen evaluado en los considerandos 239 y 240 de la Decisión de Ejecución (UE) 2021/1772, en particular la necesidad de una orden que sea aprobada en primer lugar por el Secretario de Estado y, posteriormente, por el Comisario Judicial, con arreglo a los requisitos de necesidad y proporcionalidad de la medida, tal como se establece en la parte 7 de la IPA 2016»[92]. Sin embargo, este análisis parece incompleto. El CEPD señala que no solo la introducción de «autorizaciones por categoría», sino también de «autorizaciones individuales», constituye un cambio importante introducido por la Ley de Enmienda de los Poderes de Investigación de 2024 en relación con el conjunto de datos específico mencionado anteriormente: una «autorización individual», que puede ser concedida por el jefe de un servicio de inteligencia, o una persona que actúe en su nombre, sustituye la necesidad de obtener una orden para conservar, o conservar y examinar, conjuntos de datos personales en bloque para los que solo exista una expectativa baja o ninguna expectativa razonable de privacidad[93]. Por lo tanto, los términos «orden» y «autorización individual» no deben confundirse y no pueden utilizarse indistintamente[94]. Esto se debe, en particular, a que la aprobación judicial necesaria para las autorizaciones individuales se limita a la cuestión de si el conjunto de datos específico cumple los criterios para considerarse que solo justifica una expectativa baja o ninguna expectativa razonable de privacidad con arreglo al artículo 226A de la IPA 2016[95]. Una «autorización por categoría» es diferente de una «autorización individual» y, en la práctica, no aplica —según el artículo 226B, apartado 6, letra a), de la IPA 2016— el requisito de la citada aprobación judicial de una autorización individual cuando dicha autorización se refiere a un conjunto de datos que entra dentro de una autorización por categoría. Esto se debe a que ya se habrá tomado la decisión, aprobada por

[90] Véase el artículo 199 de la IPA 2016, que especifica que «un servicio de inteligencia conservará un conjunto de datos personales en bloque si: a) el servicio de inteligencia obtiene un conjunto de información que incluya datos personales relativos a una serie de personas; b) la naturaleza del conjunto es tal que la mayoría de las personas no son ni es probable que lleguen a ser de interés para el servicio de inteligencia en el ejercicio de sus funciones; c) tras cualquier examen inicial de los contenidos, el servicio de inteligencia conserva el conjunto para el ejercicio de sus funciones, y d) el conjunto se conserva, o debe conservarse, en formato electrónico para su análisis en el ejercicio de dichas funciones».

[91] Véase Home Office, *Policy paper Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets* [Ministerio del Interior del Reino Unido, Documento de orientación relativo al Proyecto de Ley de los Poderes de Investigación (enmienda): conjuntos de datos personales en bloque y conjuntos de datos personales en bloque de terceros], disponible en inglés en https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets.

[92] Véase el considerando 99 del proyecto de Decisión.

[93] Artículo 200, apartados 1 y 2, de la IPA 2016.

[94] Sin embargo, este parece ser el caso en los considerandos 99 y 100 del proyecto de Decisión.

[95] El artículo 226BB, apartado 1, de la IPA 2016 estipula que, al decidir si aprueba una decisión de concesión de una autorización individual o de una autorización por categoría, un Comisario Judicial debe revisar las conclusiones de la persona que concedió la autorización para verificar si el artículo 226A es aplicable al conjunto de datos personales en bloque descrito en la autorización o, respectivamente, si el artículo 226A es aplicable a cualquier conjunto de datos que pertenezca a la categoría de conjuntos de datos descritos en la autorización.

un Comisario Judicial, de que todo conjunto de datos que se ajuste a la descripción de la autorización por categoría es, efectivamente, un conjunto de datos al que se aplicaría el artículo 226A.

108. Aunque estas modificaciones se refieren a la conservación y el examen de conjuntos de datos personales en bloque y no a su interceptación o recogida inicial, el CEPD desea hacer hincapié en la importancia que el TEDH concede a la autorización previa independiente en el contexto del tratamiento de datos personales en bloque. El Tribunal dictaminó que «para minimizar el riesgo de que se abuse de la facultad de interceptación en bloque, [...] el proceso debe estar sujeto a "garantías de extremo a extremo", lo que significa que, a nivel nacional, se debe evaluar en cada etapa del proceso la necesidad y la proporcionalidad de las medidas que se adoptan, que la interceptación en bloque debe estar sujeta a una autorización independiente desde el principio, cuando se definen el objeto y el alcance de la operación, y que la operación debe estar sujeta a supervisión y a una revisión independiente *a posteriori*»[96]. Teniendo esto en cuenta y basándose en un enfoque holístico, que tiene en cuenta todas las circunstancias del caso a la hora de evaluar la adecuación, el CEPD considera que la conservación y el examen de conjuntos de datos personales masivos deben estar sujetos, como mínimo, a una autorización previa por parte de una autoridad independiente o a una revisión independiente sistemática *a posteriori* por parte de un tribunal o un organismo equivalente, es decir, un organismo independiente que pueda dictar resoluciones vinculantes.

109. En vista de las aclaraciones que siguen siendo necesarias, el CEPD insta a la Comisión a que examine más a fondo los conceptos de «autorizaciones individuales» y «autorizaciones por categoría» en el marco de la Ley británica de Enmienda de los Poderes de Investigación de 2024. Además, el CEPD invita a la Comisión a que supervise atentamente la aplicación del término «una expectativa baja o ninguna expectativa razonable de privacidad» en la práctica. Aunque el artículo 226A de la IPA 2016 establece una serie de criterios para llegar a tal conclusión, el CEPD considera importante observar su aplicación, ya que pueden dar lugar a interpretaciones amplias[97].

4.2.3. SUPERVISIÓN Y REPARACIÓN

110. Como se indica en el proyecto de Decisión y se analizó previamente en el Dictamen 14/2021, el Comisario de Poderes de Investigación (Investigatory Powers Commissioner, IPC) y su Oficina (IPCO) desempeñan un papel central en la supervisión del uso de los poderes de investigación por parte de las agencias de inteligencia del Reino Unido. Además, el Tribunal de Poderes de Investigación (IPT) es el órgano judicial competente para proporcionar reparación en este sentido. Como ya se ha indicado en la sección 3.1.5 sobre la supervisión en el ámbito de la aplicación de la ley, la Ley británica de Enmienda de los Poderes de Investigación de 2024 solo ha introducido modificaciones limitadas, en particular mediante la introducción de los IPC adjuntos. Por lo tanto, los comentarios del CEPD en su Dictamen 14/2021 siguen siendo plenamente válidos[98].

111. El CEPD valora positivamente la transparencia de los informes anuales de la IPCO, incluida la disponibilidad de estadísticas detalladas para el período 2019-2023, entre otras cosas sobre el uso de facultades en bloque por parte de la comunidad de inteligencia del Reino Unido y sobre las decisiones de selección de objetivos y las autorizaciones específicas con el fin de adquirir datos de conformidad con el Acuerdo entre el Reino Unido y los Estados Unidos sobre la Ley CLOUD (Acuerdo entre el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte y el Gobierno de los Estados Unidos de

[96] TEDH, Big Brother Watch y otros contra el Reino Unido, 25 de mayo de 2021, apartado 350.
[97] El artículo 226A de la IPA 2016 hace referencia, por ejemplo, a la naturaleza de los datos, al grado en que los datos se han hecho públicos o al grado en que los datos son ampliamente conocidos.
[98] Véase el Dictamen 14/2021, apartados 200 a 215.

América sobre el acceso a datos electrónicos con el fin de combatir delitos graves). El CEPD también toma nota específicamente de las actividades de supervisión realizadas por la IPCO sobre la interceptación en bloque de datos por parte de la Oficina Central de Comunicaciones del Gobierno británico (Government Communications Headquarters, GCHQ), puestas de relieve por la Comisión en el considerando 102 del proyecto de Decisión. En este contexto, el CEPD invita a la Comisión a que siga llevando un riguroso control de la eficacia del sistema de supervisión en este ámbito, en particular en lo que respecta a la proporcionalidad de las solicitudes de interceptación en bloque[99].

112. Además, el CEPD observa que el Tribunal de Poderes de Investigación (IPT) también ha publicado un informe sobre sus actividades y jurisprudencia correspondientes al período 2021-2023[100]. El informe destaca, entre otros, avances importantes y pertinentes, como la sentencia del Tribunal Europeo de Derechos Humanos en el asunto Wieder y Guarnieri contra el Reino Unido, , que dictaminó que cualquier persona en cualquier parte del mundo puede presentar una reclamación ante el IPT, si la conducta denunciada fue llevada a cabo por un organismo público del Reino Unido y tuvo lugar en el Reino Unido. Por consiguiente, el CEPD invita a la Comisión a incluir también las actividades del IPT en su evaluación y en las futuras revisiones del proyecto de Decisión.

5. REVISIÓN, DURACIÓN Y RENOVACIÓN DEL PROYECTO DE DECISIÓN

113. El CEPD señala que la Decisión de Adecuación final sería aplicable durante seis años, es decir, hasta el 27 de diciembre de 2031. Por lo tanto, seguiría siendo el único tercer país cuya decisión de adecuación cuenta con una cláusula de expiración que se combina con la revisión periódica obligatoria establecida en el artículo 45, apartado 3, del RGPD. El CEPD entiende que el nuevo marco jurídico del Reino Unido merecerá una atención específica y pide a la Comisión que supervise atentamente la aplicación de la DUAA, incluidos los ámbitos de interés destacados en el presente Dictamen, así como todos los demás acontecimientos pertinentes en el Reino Unido a este respecto.

114. El CEPD acoge con satisfacción que el considerando 68 del proyecto de Decisión haga referencia al papel del CEPD (y de los grupos de la sociedad civil) en el mecanismo de revisión periódica, de conformidad con la Recomendación 01/2021 del CEPD[101]. En cuanto a la participación práctica del CEPD y sus representantes en la preparación y el procedimiento de la futura revisión, el CEPD reitera que toda la documentación pertinente debe compartirse por escrito con el CEPD con suficiente antelación.

115. A partir de las explicaciones adicionales facilitadas por la Comisión en relación con el considerando 113, el CEPD entiende que la intención es llevar a cabo una revisión al final de los cuatro años sobre cuya base la Comisión preparará un informe público[102]. Esta revisión ayudará a la Comisión a determinar si, a más tardar seis meses antes de la finalización del proyecto de Decisión, se debe iniciar el procedimiento para prorrogar la duración del proyecto de Decisión[103].

116. El CEPD acoge con satisfacción esta intención y señala que, dado que la revisión tiene una finalidad diferente a la cláusula de expiración, desempeña un papel importante en la supervisión del marco

[99] Para obtener más información, véase el Informe anual de 2023 del Comisario de Poderes de Investigación (Investigatory Powers Commissioner), disponible en inglés en el siguiente enlace: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, página 31, apartado 6.41.
[100] https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf
[101] Véase el considerando 19 de la Recomendación 01/2021 del CEPD.
[102] Véase el considerando 110 del proyecto de Decisión.
[103] Véase el considerando 113 del proyecto de Decisión.

jurídico. Por lo tanto, el CEPD espera que la revisión se lleve a cabo en cuatro años y anima a la Comisión a realizarla a su debido tiempo.

117. El CEPD entiende que esta futura revisión tendrá en cuenta los elementos descritos en la Decisión de Ejecución (UE) 2021/1772 de la Comisión y que los considerandos relativos a la suspensión y derogación de la decisión siguen siendo válidos[104]. En aras de la seguridad jurídica, el CEPD considera que dicha aclaración podría figurar en la Decisión de Adecuación final.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Anu Talus)

[104] Véanse los considerandos 168 a 171 de la Decisión de Ejecución (UE) 2021/1173 de la Comisión.