2025/2574

23.12.2025

DECISIÓN DE EJECUCIÓN (UE) 2025/2574 DE LA COMISIÓN

de 19 de diciembre de 2025

por la que se modifica la Decisión de Ejecución (UE) 2021/1772 de la Comisión 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

[notificada con el número C(2025) 8771]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el 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 (Reglamento general de protección de datos) ([1]), y en particular su artículo 45, apartado 3,

Considerando lo siguiente:

1. INTRODUCCIÓN

(1) Mediante la Decisión de Ejecución (UE) 2021/1772 ([2]) se concluye que, a efectos del artículo 45 del Reglamento (UE) 2016/679, el Reino Unido garantiza un nivel adecuado de protección para los datos personales transferidos, dentro del ámbito de aplicación de dicho Reglamento, desde la Unión Europea al Reino Unido ([3]).

(2) Al adoptar la Decisión de Ejecución (UE) 2021/1772, la Comisión tuvo en cuenta que, al final del período transitorio establecido en el Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica ([4]) y una vez que la disposición provisional del artículo 782 del Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra ([5]), hubiera dejado de aplicarse, el Reino Unido puede adoptar, aplicar y hacer cumplir un nuevo régimen de protección de datos distinto del vigente cuando estaba vinculado por el Derecho de la Unión.

(3) Dado que estas circunstancias pueden haber supuesto modificaciones del marco de protección de datos evaluado en la Decisión de Ejecución (UE) 2021/1772 u otros cambios pertinentes, se consideró apropiado establecer que dicha Decisión se aplicaría durante un período de cuatro años a partir de su entrada en vigor. La Decisión de Ejecución (UE) 2021/1772 dejaba de tener validez el 27 de junio de 2025, salvo que se prorrogase de conformidad con el procedimiento indicado en el artículo 93, apartado 2, del Reglamento (UE) 2016/679.

([1]) DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Decisión de Ejecución (UE) 2021/1772 de la Comisión, de 28 de junio de 2021, 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 (DO L 360 de 11.10.2021, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).
([3]) Véase el artículo 1, apartado 1, de la Decisión de Ejecución (UE) 2021/1772. De conformidad con el artículo 1, apartado 2, de dicha Decisión, esta no se aplica a los datos personales transferidos con fines de control de la inmigración en el Reino Unido ni a los que entran en el ámbito de aplicación de la exención de determinados derechos de los interesados con el fin de mantener un control eficaz de la inmigración, de conformidad con el apartado 4, párrafo 1, del anexo 2 de la Ley de protección de datos del Reino Unido de 2018.
([4]) DO C 384I de 12.11.2019, p. 1.
([5]) DO L 149 de 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Para decidir si procede la prórroga de la Decisión de Ejecución (UE) 2021/1772, la Comisión debe evaluar si la conclusión de que el Reino Unido garantiza un nivel adecuado de protección sigue estando justificada de hecho y de Derecho, habida cuenta de los cambios acaecidos desde la adopción de la Decisión de Ejecución (UE) 2021/1772 con respecto a los elementos enumerados en el artículo 45, apartado 2, del Reglamento (UE) 2016/679.

(5) En particular, el 23 de octubre de 2024, el Gobierno del Reino Unido presentó al Parlamento del Reino Unido el Data (Use and Access) Bill ([6]) [proyecto de Ley sobre datos (uso y acceso)], en el que se proponían modificaciones del Reglamento General de Protección de Datos del Reino Unido (RGPD del Reino Unido) y la Data Protection Act [Ley de protección de datos] de 2018 (DPA de 2018), evaluados en la Decisión de Ejecución (UE) 2021/1772. El 24 de junio de 2025, la Comisión adoptó la Decisión de Ejecución (UE) 2025/1226 ([7]), que prorrogaba la validez de la Decisión (UE) 2021/1772 por un período de seis meses, hasta el 27 de diciembre de 2025. Esta prórroga técnica de duración limitada permitió a la Comisión concluir su evaluación para determinar si el nivel de protección de los datos personales garantizado por el Reino Unido sobre la base de un marco jurídico estable es adecuado, esto es, tras la finalización del expediente legislativo en curso ([8]).

(6) Tras la adopción de la Decisión de Ejecución (UE) 2021/1772, la Comisión supervisó de forma permanente los acontecimientos pertinentes en el Reino Unido ([9]). De conformidad con el considerando 281 de la Decisión de Ejecución (UE) 2021/1772, se prestó especial atención a la aplicación práctica de las normas del Reino Unido relativas a la transferencias de datos personales a terceros países y al impacto que pueda tener en el nivel de protección que se garantiza a los datos transferidos en virtud de dicha Decisión; a la eficacia del ejercicio de los derechos individuales, en particular, cualquier avance pertinente en la legislación y en la práctica con respecto a las excepciones o limitaciones de dichos derechos (en particular, la relativa al mantenimiento de un control efectivo de la inmigración); así como al cumplimiento de las limitaciones y garantías con respecto al acceso del Gobierno. La supervisión de la Comisión se basó en, entre otros elementos, los avances de la jurisprudencia y la supervisión de la Information Commissioner's Office [Oficina del Comisionado de Información] (ICO) y otros organismos independientes.

(7) Basándose en la evaluación de estos cambios, también de las modificaciones del RGPD del Reino Unido y de la DPA de 2018 introducidas por la Data (Use and Access) Act [Ley sobre datos (uso y acceso)], la Comisión concluye que el Reino Unido sigue garantizando un nivel adecuado de protección para los datos personales transferidos, dentro del ámbito de aplicación del Reglamento (UE) 2016/679, desde la Unión Europea al Reino Unido.

(8) La Comisión también concluye que, habida cuenta de las modificaciones de las disposiciones pertinentes recogidas en el Derecho del Reino Unido ([10]), la exclusión de los datos personales transferidos con fines de control de la inmigración en el Reino Unido o que se comprenden dentro del ámbito de aplicación de la exención de ciertos derechos de los interesados a efectos del mantenimiento de un control de la inmigración efectivo («exención de inmigración»), de conformidad con el apartado 4, punto 1, del anexo 2 de la Data Protection Act del Reino Unido, del ámbito de aplicación de la Decisión de Ejecución (UE) 2021/1772 deja de estar justificada, como se explica en el considerando 37 de la presente Decisión.

([6]) Puede consultarse en el enlace siguiente (documento en inglés): https://bills.parliament.uk/bills/3825/news.

([7]) Decisión de Ejecución (UE) 2025/1226 de la Comisión, de 24 de junio de 2025, por la que se modifica la Decisión de Ejecución (UE) 2021/1772 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 (DO L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) La Data (Use and Access) Act recibió la sanción real el 19 de junio de 2025.

([9]) El artículo 45, apartado 4, del Reglamento (UE) 2016/679.

([10]) En mayo de 2021, el Tribunal de Apelación de Inglaterra y Gales había considerado la exención de inmigración tal como estaba formulada en aquel momento en el apartado 4, punto 1, del anexo 2 de la Data Protection Act del Reino Unido incompatible con la legislación del Reino Unido, dado que la medida legislativa carecía de disposiciones específicas que establecieran las garantías contempladas en el artículo 23, apartado 2, del RGPD del Reino Unido. Para dar cumplimiento a la sentencia, el Gobierno del Reino Unido revisó la exención de inmigración mediante la aprobación de la normativa Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 [Reglamentos de 2022 relativos a la Ley de protección de datos de 2018 (modificación de las exenciones del anexo 2)]. Sin embargo, la exención revisada volvió a ser impugnada sobre la base de que no cumplía todos los requisitos del artículo 23, apartado 2, del RGPD del Reino Unido. En una sentencia de 11 de diciembre de 2023, el Tribunal de Apelación declaró que la exención de inmigración revisada también era incompatible con el artículo 23, apartado 2, del Reglamento General de Protección de Datos del Reino Unido. Para darle cumplimiento, el Gobierno del Reino Unido aprobó la normativa Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 [Reglamentos de 2024 relativos a la Ley de protección de datos de 2018 (modificación de las exenciones del anexo 2)] que entró en vigor el 8 de marzo de 2024.

2. CAMBIOS IMPORTANTES EN LAS NORMAS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

2.1. El marco de protección de datos del Reino Unido

(9) Cuando se adoptó la Decisión de Ejecución (UE) 2021/1772, el marco jurídico sobre la protección de datos personales en el Reino Unido consistía en:

— el RGPD del Reino Unido ([11]), incorporado al Derecho del Reino Unido en virtud de la European Union (Withdrawal) Act [Ley de retirada de la Unión Europea] de 2018 ([12]) y modificado por la normativa Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 [Reglamentos en materia de protección de datos, privacidad y comunicaciones electrónicas (modificaciones, etc.) (salida de la UE) de 2019] (DPPEC Regulations) ([13]),

— la DPA de 2018 ([14]), en su versión modificada por la normativa DPPEC Regulations.

(10) Si bien estas dos leyes, que reflejaban fielmente las normas correspondientes aplicables en la Unión Europea, siguen conformando la legislación en materia de protección de datos del Reino Unido, han sido objeto de un número limitado de modificaciones posteriores, lo que constata que el Reino Unido ya no está sujeto al Derecho de la Unión Europea.

(11) En primer lugar, la Retained EU Law (Revocation and Reform) Act [Ley sobre el Derecho de la Unión conservado (revocación y reforma)] de 2023 (REUL Act) ([15]) aclaró que los principios generales del Derecho de la Unión ya no formaban parte del Derecho interno del Reino Unido después de finales de 2023 ([16]). Por otra parte, los tribunales del Reino Unido ya no están obligados a interpretar el «Derecho asimilado» no modificado, que anteriormente se denominaba «Derecho de la Unión conservado», de conformidad con los principios generales del Derecho de la Unión, sino que dicho Derecho debe interpretarse de manera compatible con el Derecho interno del Reino Unido ([17]). Sin embargo, los tribunales competentes del Reino Unido todavía deben interpretar el Derecho asimilado no modificado de conformidad con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea dictada antes del final del período transitorio ([18]), como también se menciona en el considerando 13 de la Decisión de Ejecución (UE) 2021/1772. La DPA de 2018 ha sido modificada por la Data (Use and Access) Act [Ley sobre datos (uso y acceso)] para aclarar el efecto de la REUL Act en la legislación del Reino Unido en materia de protección de datos. Por ejemplo, la sección 183A, apartado 1, de la DPA de 2018 establece como norma general que toda nueva legislación (aprobada a partir del 20 de agosto de 2025) que introduzca nuevas obligaciones o competencias para tratar datos personales se presume sujeta a la legislación del Reino Unido en materia de protección de datos. Esto significa que el marco de protección de datos del Reino Unido sigue prevaleciendo sobre

([11]) El General Data Protection Regulation del Reino Unido, que puede consultarse en el enlace siguiente: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) La European Union (Withdrawal) Act de 2018, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/16/contents, incorporaba legislación de la Unión al Derecho del Reino Unido directamente aplicable en el Reino Unido al final del período transitorio. Este denominado «Derecho de la Unión conservado» incluía el Reglamento (UE) 2016/679 en su totalidad, también sus considerandos [véanse las notas explicativas a la European Union (Withdrawal) Act de 2018, apartado 83, disponibles en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf]. De conformidad con dicha ley, los tribunales del Reino Unido debían interpretar el Derecho de la Unión conservado no modificado con arreglo a la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea y los principios generales del Derecho de la Unión, de modo que tuvieran efecto de manera inmediata antes del final del período transitorio (denominados «jurisprudencia de la Unión conservada» y «principios generales del Derecho de la Unión conservados», respectivamente).

([13]) La normativa Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations de 2019 puede consultarse en el siguiente enlace (documento en inglés): https://www.legislation.gov.uk/uksi/2019/419/contents/made, y en su versión modificada por la normativa DPPEC Regulations de 2020, disponible en el siguiente enlace (documento en inglés): https://www.legislation.gov.uk/ukdsi/2020/9780348213522. La normativa DDPEC Regulations modifica el Reglamento (UE) 2016/679 incorporado a la legislación del Reino Unido a través de la European Union (Withdrawal) Act de 2018, la DPA de 2018 y otra legislación en materia de protección de datos a fin de adaptarlo al contexto nacional.

([14]) La Data Protection Act de 2018 puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/ukpga/2018/12/contents. Antes de la retirada del Reino Unido de la Unión Europea y durante el período transitorio, la DPA de 2018 establecía normas nacionales, cuando lo permitía el Reglamento (UE) 2016/679, que especificaban y restringían la aplicación de las normas del Reglamento (UE) 2016/679 y transponían la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Sección 5 de la European Union (Withdrawal) Act de 2018, en su versión modificada por la REUL Act.

([17]) Sección 5(A2) de la European Union (Withdrawal) Act de 2018, en su versión modificada por la REUL Act.

([18]) Sección 6, apartados 3 y 7, de la European Union Withdrawal Act de 2018, en su versión modificada por la REUL Act.

otra legislación. De conformidad con la sección 183A, apartado 2, letra b), de la DPA de 2018, esta presunción puede dejar de aplicarse si el Parlamento del Reino Unido decide deliberadamente hacerlo expresamente en la legislación, preservando la soberanía parlamentaria. Además, la sección 186, apartado 2A, de la DPA de 2018 aclara que las limitaciones a los derechos de los interesados enumeradas en la sección 186, apartado 3, de la DPA de 2018 no quedan invalidadas por la sección 186, apartado 1, de la DPA de 2018, que establece que las disposiciones que prohíben o restringen la divulgación de información no prevalecen sobre determinados derechos de protección de datos. Esto garantiza que, por ejemplo, las restricciones a los derechos de los interesados establecidas en la DPA de 2018 no entren en el ámbito de aplicación de la «anulación de la protección de datos» general de la sección 186, apartado 1, de la DPA de 2018.

(12) En segundo lugar, desde la adopción de la Decisión de Ejecución (UE) 2021/1772, la legislación en materia de protección de datos del Reino Unido ha sido modificada por la normativa Data Protection (Fundamental Rights and Freedoms) Amendment Regulations [Reglamentos de modificación en materia de protección de datos (derechos y libertades fundamentales)] de 2023 ([19]). Dicha normativa define las referencias a los derechos fundamentales o las libertades fundamentales incluidas en el RGPD del Reino Unido y la DPA de 2018 (que se habían definido previamente para incluir los derechos fundamentales y las libertades fundamentales de la UE ([20])) como las referencias a los derechos consagrados en el Convenio Europeo de Derechos Humanos (CEDH), aplicados en el Derecho interno del Reino Unido a través de la Human Rights Act [Ley de derechos humanos] de 1998 ([21]). La Human Rights Act, de 1998, incorpora al Derecho del Reino Unido los derechos recogidos en el Convenio Europeo de Derechos Humanos. La Human Rights Act concede a toda persona los derechos y libertades fundamentales recogidos en los artículos 2 a 12 y 14 del Convenio Europeo de Derechos Humanos, los artículos 1 a 3 de su Protocolo n.º 1 y el artículo 1 de su Protocolo n.º 13, leídos en relación con los artículos 16, 17 y 18 de dicho Convenio. Esto incluye el derecho al respeto a la vida privada y familiar (y el derecho a la protección de los datos como parte del anterior derecho), así como el derecho a un proceso equitativo ([22]).

(13) Por último, el RGPD del Reino Unido y la DPA de 2018 han sido objeto de reformas específicas previstas en las partes 5 y 6 de la Data (Use and Access) Act. Si bien el ámbito de aplicación de esta va mucho más allá de la protección de los datos personales, prevé un número limitado de modificaciones de varios aspectos del régimen de protección de datos tales como, entre otros, las normas relativas al tratamiento de datos con fines de investigación científica, la base jurídica para el tratamiento de datos, las normas relativas al principio de limitación de la finalidad y las condiciones de las decisiones automatizadas. Además, la Data (Use and Access) Act [Ley sobre datos (uso y acceso)] introduce modificaciones en la estructura de gobernanza de la ICO. Una vez aplicadas, estas medidas sustituirán a la ICO por una nueva entidad, la Information Commission [Comisión de Información]. El papel y las funciones del regulador como autoridad independiente de control de la protección de datos en el Reino Unido se mantendrán sin cambios. La Ley también introduce nuevas competencias de ejecución para el regulador.

(14) La presente Decisión evalúa los avances legislativos, reglamentarios y de otra índole pertinentes para la conclusión sobre el nivel de protección garantizado por el Reino Unido expuesta en la Decisión de Ejecución (UE) 2021/1772. La evaluación llevada a cabo mediante la Decisión de Ejecución (UE) 2021/1772 sigue siendo válida en lo que respecta a aquellos aspectos del marco de protección de datos del Reino Unido que no han sido modificados ni se han visto afectados por otros acontecimientos desde la adopción de dicha Decisión de Ejecución.

(15) Los avances legislativos, reglamentarios y de otra índole se analizan en profundidad en las siguientes secciones sobre la base del principio de adecuación, según el cual la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «esencialmente equivalente» al que se garantiza en el contexto de la Unión ([23]). Tal como ha precisado el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico ([24]). En particular, los medios de que se sirve el tercer país en cuestión para la protección de los datos personales pueden ser diferentes de los aplicados en la Unión Europea, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ([25]). Por consiguiente, el principio de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión, sino que el criterio radica en si, a través de la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el ordenamiento jurídico en cuestión ofrece, en su conjunto, el nivel de protección exigido ([26]).

([19]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Los derechos fundamentales y las libertades fundamentales de la UE se habían mantenido en el Derecho del Reino Unido a través de la sección 4 de la European Union (Withdrawal) Act de 2018, que fue derogada a finales de 2023 por la REUL Act.

([21]) Sección 2, apartado 3, de la normativa Data Protection (Fundamental Rights and Freedoms) Amendment Regulations de 2023.

([22]) Artículos 6, 8, 10 y 13 del Convenio Europeo de Derechos Humanos (véase también el anexo 1 de la Human Rights Act, de 1998).

([23]) Considerando 104 del Reglamento (UE) 2016/679.

([24]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems I»), ECLI:EU:C:2015:650, apartado 73.

([25]) Schrems I, apartado 74.

([26]) Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Intercambio y protección de los datos personales en un mundo globalizado», de 10 de enero de 2017, sección 3.1, pp. 6-7 [COM(2017) 7], que puede consultarse en el enlace siguiente: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=ES.

2.1.1. *Definiciones*

(16) El régimen de protección de datos del Reino Unido sigue aplicando conceptos básicos de la protección de datos que reflejan la terminología del Reglamento (UE) 2016/679. Estos conceptos se han evaluado en el considerando 23 de la Decisión de Ejecución (UE) 2021/1772.

(17) Si bien la gran mayoría de las definiciones se mantienen sin cambios en la Data (Use and Access) Act, esta ha incorporado una serie de definiciones específicas relativas al tratamiento de datos personales con fines científicos, históricos y estadísticos en el artículo 4, apartados 2, 3, 4 y 5, del RGPD del Reino Unido. El apartado 2 define el «tratamiento con fines científicos» como el tratamiento de datos personales realizado a efectos de cualquier investigación que pueda describirse razonablemente como científica. Esta investigación puede estar financiada con fondos públicos o privados y emprenderse como una actividad comercial o no comercial. El apartado 3, que refleja el contenido del considerando 159 del Reglamento (UE) 2016/679, recoge una lista no exhaustiva de ejemplos de actividades de investigación que se considera que tienen fines científicos, como el desarrollo técnico, la demostración, la investigación fundamental y la investigación aplicada. El apartado 4 aclara que la «investigación histórica» incluye la investigación genealógica, que también se reconoce como un fin histórico en el considerando 160 del Reglamento (UE) 2016/679. Por último, el apartado 5 define el tratamiento con fines estadísticos como el tratamiento de datos para encuestas estadísticas o para la producción de resultados estadísticos, cuando los datos se hayan agregado hasta tal punto que ya no constituyan datos personales. Además, los datos tratados o la información resultante no deben utilizarse para tomar decisiones ni emprender acciones dirigidas a ninguna persona. Esta definición se ajusta a la interpretación de los fines estadísticos recogida en el considerando 162 del Reglamento (UE) 2016/679.

(18) En conclusión, si bien las modificaciones del artículo 4 del RGPD del Reino Unido incorporan definiciones específicas del tratamiento de datos con fines científicos, históricos y estadísticos, dichas definiciones son coherentes con la letra y el espíritu del Reglamento (UE) 2016/679, según lo previsto en los considerandos 159, 160 y 162 mencionados más arriba.

(19) Mediante la incorporación del apartado 6 al artículo 4 del RGPD del Reino Unido, la Data (Use and Access) Act también ha establecido un marco específico para la obtención del consentimiento del interesado para el tratamiento de datos personales con fines científicos. De manera muy similar al considerando 33 del Reglamento (UE) 2016/679, que reconoce que en el ámbito de la investigación científica no siempre es posible obtener el consentimiento del interesado para una finalidad específica del tratamiento, la nueva disposición contempla formas más amplias de consentimiento del interesado al permitir que los interesados den un consentimiento válido incluso cuando no sea posible determinar totalmente la finalidad exacta de la investigación en el momento de la recogida de los datos, siempre que la obtención del consentimiento sea coherente con las normas éticas generalmente aceptadas pertinentes para el ámbito de investigación específico. En cualquier caso, los interesados deben tener la oportunidad de dar su consentimiento para el tratamiento de sus datos personales únicamente para determinadas partes de la investigación, en la medida de lo posible.

(20) Por último, la Data (Use and Access) Act describe más detalladamente las garantías previamente incluidas en el artículo 89 del RGPD del Reino Unido y en la sección 19 de la DPA de 2018 para el tratamiento de datos con fines de archivo en interés público, científicos, históricos y de investigación estadística en un nuevo capítulo 8A del RGPD del Reino Unido ([27]). Estas garantías son similares a las exigidas en el artículo 89 del Reglamento (UE) 2016/679 e incluyen el requisito de prever medidas técnicas y organizativas adecuadas para garantizar el respeto del principio de minimización de los datos.

2.2. **Garantías, derechos y obligaciones**

2.2.1. *Licitud y lealtad del tratamiento*

(21) El marco de protección de datos del Reino Unido sigue exigiendo que los datos sean tratados de manera lícita, leal y legítima, tal como se evalúa en los considerandos 24, 25 y 26 de la Decisión de Ejecución (UE) 2021/1772.

([27]) Artículos 84A a 84D del RGPD del Reino Unido, introducidos por la sección 86 de la Data (Use and Access) Act.

(22) En el Derecho del Reino Unido, los principios de licitud y lealtad y los fundamentos de la licitud del tratamiento se siguen garantizando a través del artículo 5, apartado 1, letra a), y el artículo 6, apartado 1, del RGPD del Reino Unido, tal como se evalúa en la Decisión de Ejecución (UE) 2021/1772. Si bien dichas disposiciones se mantienen prácticamente idénticas ([28]) a las disposiciones correspondientes del Reglamento (UE) 2016/679, la Data (Use and Access) Act modifica en primer lugar el artículo 6, apartado 1, del RGPD del Reino Unido mediante la introducción de un fundamento lícito adicional para el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra e *bis*) ([29]). Según dicha disposición, el tratamiento será lícito si «es necesario para la satisfacción de un interés legítimo reconocido». A diferencia del fundamento jurídico del interés legítimo en virtud del artículo 6, apartado 1, letra f), del RGPD del Reino Unido, el nuevo fundamento jurídico del interés legítimo reconocido no exige sopesar caso por caso los intereses legítimos del responsable del tratamiento frente a los intereses o los derechos fundamentales y las libertades fundamentales del interesado, lo que tiene por objeto proporcionar una mayor seguridad jurídica a los responsables del tratamiento que no sean organismos públicos. El nuevo artículo 6, apartado 5, introducido en el RGPD del Reino Unido especifica que el tratamiento es necesario para la satisfacción de un interés legítimo reconocido únicamente si cumple una condición establecida en el anexo 1 ([30]), que pasa a enumerar una serie de situaciones en las que el tratamiento se considera necesario para la satisfacción de un interés legítimo reconocido, por ejemplo, cuando se realiza en respuesta a una solicitud de datos por parte de una autoridad pública que los necesita para el cumplimiento de una misión realizada en interés público que tiene un fundamento jurídico que cumple lo establecido en el artículo 6, apartado 3, del RGPD del Reino Unido, o cuando el tratamiento sea necesario para salvaguardar la seguridad nacional, proteger la seguridad pública o con fines de defensa, para responder a una emergencia, para la detección, investigación o prevención de la delincuencia o para proteger a personas vulnerables ([31]).

(23) Si bien la Data (Use and Access) Act amplía así la lista de fundamentos jurídicos del tratamiento de datos personales que están a disposición del responsable del tratamiento, el nuevo fundamento jurídico introducido relativo al interés legítimo reconocido está sujeto a varias limitaciones importantes. En primer lugar, los intereses legítimos reconocidos se limitan a situaciones concretas que están recogidas exhaustivamente en la ley. En segundo lugar, las autoridades públicas no pueden recurrir a este fundamento jurídico en el ejercicio de sus funciones ([32]). En tercer lugar, dicho fundamento concierne únicamente a aquellos ámbitos en los que exista un claro interés público en la actividad de tratamiento (de acuerdo con las condiciones establecidas en el anexo 1), es decir, en los que el tratamiento sirva a los objetivos enumerados en el artículo 23 del RGPD del Reino Unido [que corresponde al artículo 23 del Reglamento (UE) 2016/679] y no pueda invocarse con fines comerciales. En cuarto lugar, si bien la Data (Use and Access) Act otorga al secretario de Estado el derecho a modificar la lista del anexo 1 por conducto de

([28]) En aras de la claridad, la Data (Use and Access) Act también introduce en el artículo 6 del RGPD del Reino Unido un nuevo apartado que incluye ejemplos de tipos de tratamiento que pueden considerarse necesarios para la satisfacción de un interés legítimo en el sentido del artículo 6, apartado 1, letra f), del RGPD del Reino Unido. Dichos ejemplos (mercadotecnia directa, transmisión de datos dentro de un grupo con fines administrativos, y la seguridad de las redes y los sistemas de información) también se mencionan en los considerandos 47 y 48 del Reglamento (UE) 2016/679 como situaciones en las que se consideraría que el tratamiento es en interés legítimo del responsable.

([29]) Sección 70, apartado 2, letra b), de la Data (Use and Access) Act. La sección 70, apartado 5, de la Data (Use and Access) Act amplía el derecho de oposición recogido en el artículo 21 del RGPD del Reino Unido al nuevo artículo 6, apartado 1, letra e *bis*), del RGPD del Reino Unido.

([30]) Sección 70, apartado 4, de la Data (Use and Access) Act.

([31]) Véase el anexo 4 de la Data (Use and Access) Act. Según las autoridades del Reino Unido, algunos ejemplos de situaciones en las que organismos no públicos pueden tener que tratar datos personales para prevenir o detectar delitos son una empresa que tiene conocimiento de intentos de piratear ilegalmente sus sistemas informáticos, o un banco o institución financiera que tiene conocimiento de intentos fraudulentos de abrir una cuenta. El tratamiento de datos personales por parte de un organismo no público puede ser necesario, por ejemplo, para salvaguardar la seguridad nacional o la defensa cuando una organización comercial sospeche que la actividad en línea de un cliente indica una participación en actividades terroristas. La ICO está trabajando en orientaciones específicas sobre esta cuestión, incluida una definición de los conceptos pertinentes. Por ejemplo, se refiere a la probabilidad de que la «seguridad nacional» cubra la seguridad y el bienestar del Reino Unido en su conjunto, su población, sus instituciones y su sistema de gobierno. Véase el proyecto de orientaciones de la ICO sobre el interés legítimo reconocido, publicado para consulta pública, disponible en el siguiente enlace: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Artículo 6, apartado 1, último párrafo, en su versión modificada por la sección 70, apartado 2, letra c), de la Data (Use and Access) Act.

un reglamento ([33]), el secretario de Estado solamente puede elaborar dicho Reglamento tras haber consultado a la ICO ([34]) y añadir un interés legítimo reconocido a dicha lista si dicho tratamiento también es necesario para salvaguardar un objetivo de interés público enumerado en el artículo 23, apartado 1, letras c) a j), del RGPD del Reino Unido ([35]). Por último, como también confirman las orientaciones de la ICO ([36]), los responsables del tratamiento que se basen en un interés legítimo reconocido como base jurídica están obligados a cumplir todos los demás requisitos en virtud del RGPD del Reino Unido, incluida la garantía de que el tratamiento sea necesario y proporcionado para alcanzar el interés legítimo.

(24) En segundo lugar, la Data (Use and Access) Act aclara en el artículo 6, apartado 3, el artículo 9, apartado 2, letra g), y el artículo 10, apartado 1, del RGPD del Reino Unido, que corresponden a las disposiciones respectivas del Reglamento (UE) 2016/679, que la base para el tratamiento de datos personales, categorías especiales de datos personales y datos personales relativos a condenas e infracciones penales en cumplimiento de una obligación legal o para el cumplimiento de una misión en interés público pueden tener una base no solo en el Derecho interno, sino también en el Derecho internacional pertinente ([37]). El Derecho internacional pertinente queda limitado por el nuevo artículo 9A introducido en el RGPD del Reino Unido, conjuntamente con el anexo A1, a un único acuerdo, concretamente el 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, firmado el 3 de octubre de 2019 (el Acuerdo entre el Reino Unido y los Estados Unidos) ([38]). Las garantías dispuestas en dicho Acuerdo han sido evaluadas en los considerandos 153 a 155 de la Decisión de Ejecución (UE) 2021/1772 y su ejecución se analiza en los considerandos 87 a 93 de la presente Decisión.

2.2.2. *Tratamiento de categorías especiales de datos personales*

(25) El marco de protección de datos del Reino Unido sigue ofreciendo garantías específicas cuando intervienen categorías especiales de datos, tal como se evalúa en los considerandos 27 a 42 de la Decisión de Ejecución (UE) 2021/1772.

(26) Siguen vigentes tanto la definición de categorías especiales de datos personales como las normas específicas aplicables al tratamiento de dichas categorías de datos en el RGPD del Reino Unido y en la DPA de 2018. Al mismo tiempo, la Data (Use and Access) Act confiere nuevos poderes normativos al secretario de Estado para incorporar nuevas categorías especiales de datos, adaptar las condiciones aplicables a su utilización e incorporar nuevas definiciones, si fuera necesario ([39]). Es importante señalar que no permite al secretario de Estado suprimir ni modificar las categorías especiales de datos existentes, ni tampoco alterar las condiciones aplicables al tratamiento de dichas categorías ([40]). Así, el nuevo poder normativo introducido solamente permite al Gobierno añadir nuevas categorías de datos sensibles y determinar las condiciones para el tratamiento de dichas categorías, con lo que se pretende que el Gobierno pueda responder a los futuros avances tecnológicos y sociales cuando sea necesario.

(27) Por consiguiente, estas modificaciones no afectan al nivel de protección de las categorías especiales de datos personales considerado esencialmente equivalente al nivel que otorga en la UE la Decisión de Ejecución (UE) 2021/1772.

([33]) Antes de establecer reglamentos, el Secretario de Estado debe tener en cuenta los efectos de cualquier cambio en los intereses y los derechos y libertades fundamentales de los interesados, así como el hecho de que los menores (cuando proceda) merecen una protección específica de sus datos personales. Los reglamentos deben formularse mediante un instrumento jurídico y están sujetos al procedimiento de resolución afirmativa, es decir, deben ser aprobados activamente por el Parlamento del Reino Unido. Sección 70, apartado 4, párrafo octavo, de la Data (Use and Access) Act.

([34]) Artículo 182, apartado 2, de la DPA de 2018.

([35]) Sección 70, apartado 4, párrafo noveno, de la Data (Use and Access) Act.

([36]) Consulte las orientaciones de la ICO sobre intereses legítimos, disponibles en el siguiente enlace: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Sección 72 de la Data (Use and Access) Act.

([38]) 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, disponible en el enlace siguiente: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([39]) Sección 74 de la Data (Use and Access) Act. Dichos reglamentos están sujetos al procedimiento de resolución afirmativa, es decir, requieren la aprobación activa del Parlamento del Reino Unido.

([40]) Véase el nuevo artículo 11A, apartado 1, letra b), y apartado 2, del RGPD del Reino Unido, así como las notas explicativas del Data (Use and Access) Bill [proyecto de Ley sobre datos (uso y acceso)], apartado 571, disponible en el siguiente enlace: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Limitación de la finalidad*

(28) El régimen del Reino Unido para la protección de datos personales sigue exigiendo que los datos se traten con una finalidad específica y, posteriormente, se utilicen tan solo en la medida en que ello no sea incompatible con la finalidad original del tratamiento, tal como se evalúa en los considerandos 43 a 48 de la Decisión de Ejecución (UE) 2021/1772.

(29) En primer lugar, la Data (Use and Access) Act introduce unas cuantas modificaciones específicas en el principio de limitación de la finalidad establecido en el artículo 5, apartado 1, letra b), del RGPD del Reino Unido. Estas modificaciones aportan claridad con respecto a la aplicación de dicho principio sin cambiar la esencia. La sección 71, apartados 1, 2 y 3, de la Data (Use and Access) Act establece que el principio de limitación de la finalidad es aplicable cuando los datos se obtienen del interesado o de otro modo, que solamente es aplicable cuando los datos personales son tratados posteriormente por el mismo responsable del tratamiento o en su nombre (es decir, no es aplicable cuando hay un cambio de responsable), y que el tratamiento no es lícito por el mero hecho de ser compatible con los fines para los cuales se recogieron los datos personales.

(30) En segundo lugar, la Data (Use and Access) Act aclara las normas relativas al tratamiento ulterior de los datos personales mediante su reagrupación en el nuevo artículo 8A introducido en el RGPD del Reino Unido, que establece el régimen completo para el tratamiento ulterior de datos personales. El artículo 8A, apartado 2, del RGPD del Reino Unido enumera los elementos que deben tenerse en cuenta a la hora de determinar si una nueva finalidad de tratamiento es compatible con la finalidad original. Estos elementos se enumeraban anteriormente en el artículo 6, apartado 4, del RGPD del Reino Unido, que se corresponde con el artículo 6, apartado 4, del Reglamento (UE) 2016/679 ([41]). El artículo 8A, apartado 3, del RGPD del Reino Unido reagrupa en una disposición las situaciones en las que el tratamiento de datos personales para una nueva finalidad debe considerarse compatible con la finalidad original. Abarca situaciones en las que el interesado da su consentimiento al tratamiento de datos personales para una nueva finalidad o cuando el tratamiento es necesario para salvaguardar un objetivo enumerado en el artículo 23, apartado 1 ([42]), cuando el tratamiento se lleva a cabo con fines de investigación científica o histórica, fines de archivo en interés público o fines estadísticos ([43]). Por último, la Data (Use and Access) Act aclara que todo tratamiento efectuado para garantizar que el tratamiento cumpla los principios de protección de datos establecidos en el artículo 5, apartado 1, del RGPD del Reino Unido o para demostrarlo se considera compatible con la finalidad original. Las situaciones mencionadas se siguen correspondiendo con lo que también se considera tratamiento ulterior compatible en el Reglamento (UE) 2016/679.

(31) En tercer lugar, la Data (Use and Access) Act también introduce en el artículo 8A, apartado 3, letra d), del RGPD del Reino Unido situaciones adicionales nuevas en las que el tratamiento ulterior de datos personales para una finalidad nueva se considera compatible con la finalidad original. Estas situaciones se enumeran en el anexo 2 del RGPD del Reino Unido ([44]) e incluyen, por ejemplo, las siguientes: cuando el tratamiento se efectúa en respuesta a una solicitud por parte de una autoridad pública que necesita los datos para el cumplimiento de una misión realizada en interés público cuya base jurídica cumpla el artículo 6, apartado 3, del RGPD del Reino Unido; cuando el tratamiento es necesario para la protección de la seguridad pública, para responder a una emergencia, para la detección, investigación o prevención de la delincuencia, para la protección de los intereses vitales del interesado o de otra persona, para la protección de personas vulnerables, con fines fiscales o si es necesario para el cumplimiento de una obligación legal ([45]).

(32) Si bien la Data (Use and Access) Act amplía de este modo la lista de situaciones en las que el tratamiento ulterior para una finalidad diferente se considera compatible con la finalidad original del tratamiento, esta ampliación está sujeta a importantes limitaciones. En primer lugar, se limita a situaciones concretas que están recogidas exhaustivamente en la ley. En segundo lugar, concierne únicamente a aquellos ámbitos en los que exista un claro interés público en la actividad de tratamiento, es decir, en los que el tratamiento ulterior sirva a los objetivos

([41]) Al igual que en el Reglamento (UE) 2016/679, estos elementos incluyen cualquier relación entre la finalidad original y la nueva, el contexto en el que se recogieron los datos personales, en particular la relación entre el interesado y el responsable del tratamiento, la naturaleza del tratamiento y si incluye categorías especiales de datos, las posibles consecuencias del tratamiento previsto para el interesado, así como la existencia de unas garantías adecuadas.

([42]) Véase también el artículo 6, apartado 4, del Reglamento (UE) 2016/679.

([43]) Considerando 50 del Reglamento (UE) 2016/679.

([44]) El anexo 2 se introdujo en el RGPD del Reino Unido por medio del anexo 5 de la Data (Use and Access) Act; véase la sección 71, apartado 6, de dicha ley.

([45]) Véase el anexo 5 de la Data (Use and Access) Act.

enumerados en el artículo 23 del RGPD del Reino Unido [que corresponde al artículo 23 del Reglamento (UE) 2016/679]. Por tanto, no puede invocarse con fines comerciales. En tercer lugar, si bien la Data (Use and Access) Act otorga al secretario de Estado el derecho a modificar la lista del anexo 2 por conducto de un reglamento ([46]), el secretario de Estado solamente puede añadir tipos de tratamiento a dicha lista si dicho tratamiento también es necesario para salvaguardar un objetivo de interés público enumerado en el artículo 23, apartado 1, letras c) a j), del RGPD del Reino Unido ([47]). En cuarto lugar, cuando la recogida de datos personales por parte del responsable del tratamiento se base en el consentimiento del interesado, el tratamiento para una nueva finalidad en las situaciones enumeradas en el anexo 2 solamente se considera compatible con la finalidad original si no cabe esperar razonablemente que el responsable del tratamiento obtenga un nuevo consentimiento del interesado ([48]).

2.2.4. *Derechos individuales*

(33) En virtud del marco para la protección de datos personales del Reino Unido, los interesados siguen gozando de los mismos derechos individuales que los previstos en el Reglamento (UE) 2016/679 sin ninguna modificación significativa ([49]), y pueden hacer valer dichos derechos ante el responsable o el encargado del tratamiento, en concreto el derecho de acceso a los datos, el derecho a oponerse al tratamiento y el derecho de rectificación o supresión de datos, tal como se evalúa en los considerandos 51 a 54 de la Decisión de Ejecución (UE) 2021/1772.

(34) En primer lugar, la Data (Use and Access) Act aclara una serie de modalidades concretas en virtud de las cuales pueden ejercerse dichos derechos. Por una parte, a través de una modificación del artículo 12 y de la introducción de un nuevo artículo 12A en el RGPD del Reino Unido ([50]), especifica los plazos dentro de los cuales los responsables del tratamiento deben responder a las solicitudes de los interesados. Más concretamente, el artículo 12 del RGPD del Reino Unido se modifica de tal modo que ya no se exige al responsable del tratamiento que facilite información sobre la medida adoptada (o sobre los motivos por los que no se ha adoptado ninguna medida) en respuesta a la solicitud de un interesado de conformidad con los artículos 15 a 22 del RGPD del Reino Unido «en el plazo de un mes a partir de la recepción de la solicitud», sino «antes de que finalice el período de tiempo aplicable». El período de tiempo aplicable se define con más detalle en el nuevo artículo 12A introducido en el RGPD del Reino Unido como un período de un mes a partir de la fecha pertinente, que es la fecha en la que el responsable del tratamiento recibe la solicitud, en la que el responsable del tratamiento recibe cualquier información solicitada en relación con una solicitud en virtud del artículo 12, apartado 6, del RGPD del Reino Unido, o en la que se haya pagado una tarifa que se haya cobrado en relación con la solicitud en virtud del artículo 12, apartado 5, del RGPD del Reino Unido, cualquier fecha que sea posterior ([51]). El artículo 12A, apartado 3, permite además al responsable del tratamiento ampliar dos meses el período de tiempo aplicable cuando sea necesario debido a la complejidad de las solicitudes realizadas por el interesado o al número de dichas solicitudes. Por otro lado, en lo que respecta únicamente al derecho de acceso a la información y los datos personales, la Data (Use and Access) Act modifica el artículo 15 del RGPD del Reino Unido para incorporar la aclaración desarrollada en la jurisprudencia nacional vigente —basándose en el principio de proporcionalidad del Derecho de la Unión—, al aclarar que los responsables del tratamiento únicamente deben llevar a cabo búsquedas razonables y proporcionadas de la información y los datos personales solicitados ([52]). Se espera que la nueva disposición se interprete en consonancia con la jurisprudencia existente, que establece que «[…] lo que se pondera en el ejercicio de proporcionalidad es el objeto final de la búsqueda, a saber, el beneficio potencial que el suministro de la información podría aportar al interesado, en comparación con los medios por los que se obtiene dicha información. Se planteará la cuestión de evaluar en cada caso concreto si se realizará un esfuerzo desproporcionado para encontrar y facilitar la información en relación con los beneficios que podría aportar al interesado» ([53]).

([46]) Artículo 8A, apartado 5, del RGPD del Reino Unido, introducido por la sección 71, apartado 1, de la Data (Use and Access) Act.
([47]) Artículo 8A, apartado 6, del RGPD del Reino Unido, introducido por la sección 71, apartado 1, de la Data (Use and Access) Act.
([48]) Artículo 8A, apartado 4, letra b), del RGPD del Reino Unido, introducido por la sección 71, apartado 1, de la Data (Use and Access) Act.
([49]) La sección 31 de la Victims and Prisoners Act [Ley sobre víctimas y prisioneros] (VAP Act) de 2024 introdujo un fundamento adicional en el derecho de supresión previsto en el artículo 17 del RGPD del Reino Unido, con el que se otorgaba a los interesados el derecho a solicitar que los responsables del tratamiento supriman sus datos personales cuando hayan sido tratados como resultado de una alegación infundada relacionada con el interesado formulada por una persona malintencionada. Se considera que una persona es «malintencionada» si ha sido condenada por un delito especificado en la sección 31, apartado 3, de la VAP Act (por ejemplo, acoso) o tiene que cumplir una orden de protección por acecho. La VAP Act puede consultarse en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2024/21/contents. Además, la sección 77 de la Data (Use and Access) Act modifica el derecho a la información establecido en el artículo 13 del RGPD del Reino Unido de tal modo que ya no se exige al responsable del tratamiento que informe al interesado del tratamiento ulterior de sus datos personales con nuevos fines si estos son fines de investigación científica o histórica, de archivo en interés público o fines estadísticos; el tratamiento se efectúa de conformidad con las garantías establecidas en el nuevo artículo 84B del RGPD del Reino Unido, y la comunicación de la información resultaría imposible o supondría un esfuerzo desproporcionado.
([50]) Sección 76 de la Data (Use and Access) Act.
([51]) Artículo 12A, apartados 1 y 2, del RGPD del Reino Unido, introducidos por la sección 76 de la Data (Use and Access) Act.
([52]) Artículo 15, apartado 1A, del RGPD del Reino Unido, introducido por la sección 78 de la Data (Use and Access) Act.
([53]) *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Por consiguiente, si bien los plazos para responder a las solicitudes de los interesados y las obligaciones específicas de los responsables del tratamiento con respecto al derecho de acceso están sujetos a unas normas más exhaustivas, el sistema del Reino Unido sigue garantizando que las solicitudes de los interesados se tramiten en unos períodos de tiempo razonables determinados sobre la base de unos factores objetivos. Además, las obligaciones sustantivas del responsable del tratamiento al responder a las solicitudes de acceso se enmarcan en la base de las normas jurídicas establecidas que también toman en consideración los intereses del interesado. Por último, ya se establece en las actuales orientaciones de la ICO que un responsable del tratamiento no está obligado a realizar búsquedas que sean irrazonables o desproporcionadas con respecto a la importancia de proporcionar acceso a la información ([54]).

(36) Las limitaciones de estos derechos individuales establecidas en la DPA de 2018 y dentro del marco del artículo 23 del RGPD del Reino Unido, así como las limitaciones y garantías que enmarcan la aplicación de estas limitaciones, siguen vigentes en el marco del Reino Unido ([55]), tal como se describe de manera detallada en los considerandos 55 a 67 de la Decisión de Ejecución (UE) 2021/1772.

(37) En lo que respecta concretamente a la limitación aplicable a los datos personales tratados con fines de mantenimiento de un control efectivo de la inmigración o de investigación o detección de actividades que socavarían el mantenimiento de un control efectivo de la inmigración, en la medida en que la aplicación de dichas disposiciones podría perjudicar alguna de dichas cuestiones (la exención de inmigración) ([56]), el Gobierno del Reino Unido ha modificado el apartado cuarto del anexo 2 de la DPA de 2018 a través de la normativa Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations [Reglamentos sobre la Ley de protección de datos de 2018 (modificación de las exenciones del anexo 2)] de 2022 ([57]), y la normativa Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations [Reglamentos sobre la Ley de protección de datos de 2018 (modificación de las exenciones del anexo 2)] de 2024 ([58]), que complementa los Reglamentos de 2022 ([59]). Las modificaciones incorporan a los apartados 4A y 4B del anexo 2 de la DPA de 2018 las garantías para el ejercicio de la exención de inmigración exigidas en virtud del artículo 23, apartado 2, del RGPD del Reino Unido. En particular, exigen i) que la exención de inmigración solo se invoque caso por caso, separadamente respecto de cada una de las disposiciones pertinentes del RGPD del Reino Unido y nuevamente cada vez que el secretario de Estado considere la inaplicación o la limitación de alguna disposición pertinente del RGPD del Reino Unido ([60]), ii) que los derechos y libertades del interesado, así como sus posibles vulnerabilidades, se tengan en cuenta a la hora de aplicar la exención de inmigración ([61]), iii) que el secretario de Estado lleve un registro del uso de la exención de inmigración e informe de dicho uso al interesado (salvo en circunstancias concretas en que la información perjudicaría el objetivo de la exención) ([62]) y iv) que se aclare que el uso de la exención de inmigración está limitado al tratamiento de datos personales por parte del secretario de Estado ([63]), es decir, en la práctica, por parte del Ministerio del Interior para sus funciones relacionadas con el anexo 2, apartado 4, punto 1, de la DPA de 2018. Además, explican el ejercicio de ponderación que debe efectuarse a la hora de determinar si el ejercicio de los derechos del interesado podría perjudicar el control efectivo de la inmigración, y si es necesario y proporcionado limitar dichos derechos como resultado de ello.

([54]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) La sección 88, apartado 2, de la Data (Use and Access) Act introduce una pequeña modificación en la sección 26, apartado 2, letra f), de la DPA de 2018 (exención de seguridad nacional y defensa), aclarando que el derecho a presentar una reclamación ante el comisionado en virtud del artículo 77 del RGPD del Reino Unido no forma parte de las disposiciones cuya aplicación puede limitarse con fines de seguridad nacional o defensa.

([56]) Cuando se adoptó la Decisión de Ejecución (UE) 2021/1772, no se había resuelto la validez e interpretación de la exención de inmigración con arreglo al Derecho del Reino Unido tras la decisión del Tribunal de Apelación de Inglaterra y Gales, de 26 de mayo de 2021, que había concluido que la exención de inmigración, tal como estaba formulada en la DPA de 2018 en aquel momento, era incompatible con el Derecho del Reino Unido, dado que carecía de disposiciones específicas que establecieran las garantías contempladas en el artículo 23, apartado 2, del RGPD del Reino Unido, que refleja el artículo 23, apartado 2, del Reglamento (UE) 2016/679. Por ese motivo, los datos personales transferidos con fines de control de la inmigración en el Reino Unido o que quedan de otro modo comprendidos dentro del ámbito de aplicación de la exención de inmigración habían quedado excluidos del ámbito de aplicación de la Decisión de Ejecución (UE) 2021/1772.

([57]) Los Reglamentos entraron en vigor el 31 de enero de 2022 y pueden consultarse en el siguiente enlace: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Los Reglamentos entraron en vigor el 8 de marzo de 2024 y pueden consultarse en el siguiente enlace: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) La exención de inmigración revisada mediante los Reglamentos de 2022 volvió a ser impugnada mediante un control jurisdiccional, sobre la base de que todavía no cumplía todos los requisitos del artículo 23, apartado 2, del RGPD del Reino Unido. En diciembre de 2023, el Tribunal de Apelación concluyó que era incompatible con los requisitos del artículo 23, aparatado 2, del RGPD del Reino Unido. Como resultado de dicha sentencia, los Reglamentos de 2024 complementan los Reglamentos de 2022 e introducen nuevas modificaciones en la exención de inmigración.

([60]) Anexo 2, apartado 4A, punto 2, de la DPA de 2018.

([61]) Anexo 2, apartado 4AB, puntos 3 y 4, de la DPA de 2018. La ICO fue consultada sobre el proyecto de Reglamentos de 2024 y declaró públicamente que estaba satisfecha con la normativa. La carta publicada en respuesta a la consulta y en la que se confirma su opinión está disponible en el siguiente enlace: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Anexo 2, apartado 4B, puntos 1 y 2, de la DPA de 2018.

([63]) Anexo 2, apartado 4, punto 1, de la DPA de 2018.

(38) Por otro lado, la ICO del Reino Unido ha emitido orientaciones detalladas sobre el uso de esta limitación concreta ([64]). En particular, puntualizan lo siguiente: «No deben aplicar la exención de inmigración como una exención general para limitar […] los derechos con respecto a todos los datos que obren en su poder. El ámbito de aplicación de la exención se limita a aquellos derechos que, si se ejercen con respecto a todos los datos que se posean, perjudicarían los fines de inmigración definidos. […]. Por tanto, la posición por defecto del responsable del tratamiento debe ser la de cumplir los requisitos del Reglamento (UE) 2016/679 y la DPA en la medida de lo posible. […] El criterio del perjuicio presenta un margen muy amplio y no deben aplicar la exención de un modo indiscriminado. […] Deben considerar si la aplicación de la exención constituye una respuesta proporcionada a la solicitud de protección de datos de una persona. Pueden considerar que existe una necesidad social acuciante de aplicar la exención de inmigración, pero también deben tener en cuenta si esta pesa más que su obligación hacia las personas en virtud del Reglamento (UE) 2016/679. Las personas tienen derechos sobre sus datos personales que ustedes deben tener en cuenta en todos los casos, en particular, el derecho de acceso. Por tanto, es importante que consideren, en cada caso, si los derechos de protección de datos de la persona prevalecen sobre el riesgo de perjuicio detectado. Su aplicación de la exención debe ser proporcionada a las circunstancias y deben considerar y documentar cuidadosamente cada caso».

(39) En términos generales, la limitación de la inmigración contemplada en el apartado 4 del anexo 2 de la DPA de 2018, en su forma revisada por el Gobierno del Reino Unido en 2022 y 2024 y según la interpretación de la jurisprudencia ([65]) y las orientaciones de la ICO, está sujeta a una serie de estrictas condiciones que definen su aplicación y son muy similares a las condiciones establecidas en el Derecho de la Unión, más concretamente el artículo 23 del Reglamento (UE) 2016/679, en relación con la limitación de los derechos y las obligaciones en materia de protección de datos para objetivos importantes de interés público, como el control de la inmigración.

2.2.5. *Limitaciones a las transferencias ulteriores*

(40) El nivel de protección de los datos personales que se transfieren desde la Unión Europea a responsables o encargados del tratamiento en el Reino Unido sigue sin verse comprometido por la transferencia ulterior de dichos datos a destinatarios de un tercer país. El régimen sobre transferencias internacionales de datos personales desde el Reino Unido sigue siendo muy similar a las normas establecidas en el capítulo V del Reglamento (UE) 2016/679, tal como se evalúa en los considerandos 74 a 82 de la Decisión de Ejecución (UE) 2021/1772.

(41) Si bien la Data (Use and Access) Act modificó el capítulo 5 del RGPD del Reino Unido relativo a las transferencias de datos personales a terceros países u organizaciones internacionales, conserva el requisito esencial de que los datos personales solamente puedan ser transferidos a terceros países u organizaciones internacionales cuando la transferencia se base en i) unas normas de aprobación de la transferencia (nueva terminología para lo que antes se denominaban «normas en materia de adecuación»), ii) unas garantías adecuadas o iii) una excepción para situaciones específicas. Estos principios generales relacionados con las transferencias de datos se reflejan en el nuevo artículo 44A, que sustituye al artículo 44 del RGPD del Reino Unido ([66]), que también establece que las transferencias de datos personales a un tercer país o una organización internacional únicamente están permitidas si la transferencia se lleva a cabo en cumplimiento de las demás disposiciones previstas en el RGPD del Reino Unido.

(42) Por lo que se refiere específicamente a las normas por las que se aprueba una transferencia, el artículo 45A, apartado 2, del RGPD del Reino Unido especifica que el secretario de Estado solo puede adoptar dichas normas si considera que se cumple el criterio de protección de datos. Esto significa que la posibilidad, introducida en el artículo 45A, apartado 3, del RGPD del Reino Unido, de que el secretario de Estado tenga en cuenta la conveniencia de facilitar los flujos de datos al adoptar dichas normas está siempre sujeta a la condición de que se cumpla el criterio de protección de datos. La norma jurídica para el criterio de protección de datos que debe cumplirse se establece en el nuevo artículo 45B, apartado 1, del RGPD del Reino Unido, que exige que el nivel de protección de los interesados en los países receptores o en las organizaciones internacionales no sea sustancialmente inferior al nivel previsto para los interesados en virtud de la legislación pertinente del Reino Unido en materia de protección de datos. Así, el artículo 45B, apartado 2, del RGPD del Reino Unido ofrece una lista no exhaustiva de elementos que se han de tener en cuenta a la hora de evaluar si se cumple ese criterio, como el respeto del Estado de Derecho y de los derechos humanos, la existencia de una autoridad de protección de datos y los poderes de esta, las vías de recurso judicial y extrajudicial, las normas relativas a la transferencia de datos personales desde el país o por la organización

([64]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), apartados 40 y 41.

([66]) Sección 85 y anexo 7 de la Data (Use and Access) Act.

internacional a otros países u organizaciones internacionales, las obligaciones internacionales pertinentes del país o la organización, así como la constitución, las tradiciones y la cultura del país o la organización. Si bien reformula la lista de elementos pertinentes recogida en el antiguo artículo 45 del RGPD del Reino Unido, el nuevo artículo 45B, apartado 2, conserva los elementos fundamentales de dicha lista y, por tanto, se asemeja a lo establecido en el capítulo V del Reglamento (UE) 2016/679. Además, las autoridades del Reino Unido han confirmado que el secretario de Estado tendrá en cuenta elementos no enumerados en el artículo 45B, apartado 2, como las leyes y prácticas de un tercer país relativas a la forma en que las autoridades públicas acceden a los datos personales con fines como la seguridad nacional o la aplicación de la ley, en la medida en que afecten al nivel general de protección. Asimismo, las autoridades del Reino Unido consideran que la jurisprudencia pertinente en el tercer país será un componente esencial a la hora de considerar las cuestiones enumeradas de manera no exhaustiva en el artículo 45B, apartado 2, del RGPD del Reino Unido.

(43) Los reglamentos por los que se aprueba una transferencia siguen estando sujetos a los requisitos de procedimiento «generales» previstos en la sección 182 de la DPA de 2018, tal como se establece en el considerando 77 de la Decisión de Ejecución (UE) 2021/1772. En virtud de este procedimiento, el secretario de Estado debe consultar a la ICO al proponer la adopción de normas en materia de adecuación en el Reino Unido ([67]). Una vez que el secretario de Estado ha adoptado las normas, estas se presentan ante el Parlamento y están sujetas al procedimiento de «resolución negativa», en virtud del cual ambas cámaras del Parlamento pueden examinarlas y tienen la capacidad de aprobar una moción que anule las normas en un plazo de cuarenta días ([68]).

(44) Por lo que respecta a las garantías adecuadas, el nuevo apartado 1A del artículo 46 del RGPD del Reino Unido establece que únicamente podrá darse curso a dichas transferencias si se prevén las garantías pertinentes en los instrumentos disponibles con arreglo al artículo 46, apartados 2 y 3 ([69]), del RGPD del Reino Unido y el responsable del tratamiento, el encargado del tratamiento o los organismos públicos competentes, actuando de manera razonable y proporcionada, consideran que se cumple el criterio de protección de datos. Los nuevos apartados 6 y 7 introducidos aclaran que el criterio de protección de datos se cumple si, debido a las garantías requeridas, el nivel de protección proporcionado a los interesados no es significativamente inferior después de la transferencia al nivel establecido en la legislación pertinente del Reino Unido en materia de protección de datos, es decir, si, como establece el Reglamento (UE) 2016/679, se aplican las mismas normas jurídicas a ambas normas, tanto a las de aprobación de las transferencias como a las de las garantías adecuadas. De acuerdo con esos mismos apartados, lo que es razonable y proporcionado debe determinarse por referencia a todas las circunstancias, o a las circunstancias probables, de la transferencia o el tipo de transferencia, también la naturaleza y el volumen de los datos personales transferidos.

(45) En relación con las excepciones para situaciones específicas, en el artículo 49 del RGPD del Reino Unido, relativo a las condiciones bajo las cuales pueden aplicarse excepciones especiales, se han introducido una serie de modificaciones técnicas para que la disposición concuerde con los cambios introducidos en otras disposiciones, pero no afectan al nivel de protección de los datos personales en el Reino Unido. Además, se introduce un nuevo apartado 4A para reproducir el efecto de la sección 18, apartado 1, de la DPA de 2018, que otorga al secretario de Estado la facultad de establecer, mediante un reglamento, las circunstancias relacionadas con las transferencias de datos que se consideran necesarias por razones de interés público. Por último, un nuevo artículo 49A reproduce el efecto de la sección 18, apartado 2, de la DPA de 2018, que permite la posibilidad de que el secretario de Estado, mediante un reglamento, imponga limitaciones a las transferencias de datos cuando estas no sean aprobadas en virtud del artículo 45A (transferencias aprobadas mediante disposiciones reglamentarias) y cuando ello se considere necesario por motivos importantes de interés público.

(46) En términos de aplicación de las normas sobre transferencias internacionales del Reino Unido, ha habido algunos cambios desde la adopción de la Decisión de Ejecución (UE) 2021/1772.

([67]) Véase el memorando de entendimiento entre el secretario de Estado del Departamento de Cultura, Medios de Comunicación y Deporte y la Oficina del Comisionado de Información sobre la función de la ICO en relación con la nueva evaluación de adecuación del Reino Unido, disponible en el siguiente enlace: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Si se aprueba dicha votación, la norma dejará en última instancia de tener efecto jurídico.

([69]) El instrumento de transferencia disponible en virtud del artículo 46, apartados 2 y 3, del RGPD del Reino Unido consiste en instrumentos jurídicamente vinculantes y ejecutables entre autoridades u organismos públicos, normas corporativas vinculantes de conformidad con el artículo 47 del RGPD del Reino Unido, cláusulas tipo de protección de datos establecidas en la normativa formulada por el secretario de Estado o en un documento emitido por la Information Commission, un código de conducta aprobado y un mecanismo de certificación aprobado.

(47) Con respecto a las normas de aprobación de las transferencias, se han adoptado dos reglamentos nuevos hasta la fecha, que reflejan las decisiones de adecuación vigentes también en la Unión, esto es, en relación con las transferencias a la República de Corea y en relación con las transferencias a entidades comerciales que se hayan adherido a la Extensión del Marco de Privacidad de Datos UE-EE. UU. para el Reino Unido. Las normas en materia de adecuación aplicables a la República de Corea ([70]) entraron en vigor el 19 de diciembre de 2022 y permiten la transferencia de datos personales del Reino Unido a la República de Corea. La Extensión del Marco de Privacidad de Datos UE-EE. UU. para el Reino Unido, cuyas normas pertinentes ([71]) entraron en vigor el 12 de octubre de 2023, permite la libre circulación de datos personales a organizaciones estadounidenses certificadas.

(48) En lo que respecta a las garantías adecuadas, el Reino Unido ha publicado sus propias cláusulas contractuales tipo en materia de protección de datos, el Acuerdo de Transferencia Internacional de Datos ([72]) y una adenda de las cláusulas contractuales tipo de la UE, ambos en vigor desde marzo de 2022. El Acuerdo de Transferencia Internacional de Datos prevé un mecanismo específico para el Reino Unido destinado a ofrecer las garantías adecuadas para la transferencia de datos personales y presenta varias similitudes con las cláusulas contractuales tipo de la UE. La adenda, emitida por la ICO, permite a los responsables y encargados del tratamiento del Reino Unido acogerse a las cláusulas contractuales tipo de la UE en virtud del RGPD del Reino Unido para las transferencias internacionales. La ICO también ha publicado una herramienta de evaluación de riesgos de las transferencias para ayudar a las organizaciones del Reino Unido a evaluar los riesgos asociados a las transferencias internacionales.

(49) El Reino Unido también ha agilizado el proceso de aprobación de las normas corporativas vinculantes mediante nuevas directrices y alternativas para la aprobación de dichas normas. En julio de 2022, la ICO publicó orientaciones y tablas de referencia para explicar el enfoque aplicado por el Reino Unido con respecto a las normas corporativas vinculantes después del *Brexit*, y, en diciembre de 2023, se publicó una adenda de las normas corporativas vinculantes de la UE con el fin de garantizar que las normas corporativas vinculantes aprobadas con arreglo al marco de la Unión sean ejecutables en el Reino Unido ([73]).

(50) Por último, en julio de 2023, el Reino Unido se convirtió en miembro asociado del Foro Global de Normas de Privacidad Transfronteriza ([74]). Es importante señalar que dicha condición de miembro no conlleva la facilitación de transferencias de datos del Reino Unido a otros miembros del Foro. El Reino Unido ha aclarado que toda transferencia de datos personales del Reino Unido a terceros países u organizaciones internacionales debe cumplir las condiciones establecidas en la legislación del Reino Unido, como se ha descrito anteriormente, en particular el criterio de protección de datos, que exige que el nivel de protección proporcionado «no sea significativamente inferior» al establecido en el RGPD del Reino Unido.

(51) Como ya ha explicado la Comisión, las normas de privacidad transfronteriza no garantizan un nivel suficiente de protección de los datos personales originarios de la UE. En particular, no establecen derechos individuales exigibles ([75]). Es por tanto particularmente importante que, incluso si el Reino Unido es miembro asociado del Foro Global de Normas de Privacidad Transfronteriza, dichas normas no puedan constituir un mecanismo de transferencia válido con arreglo al Derecho en materia de protección de datos del Reino Unido. Si cambiase esta circunstancia, disminuiría el nivel de protección que se garantiza actualmente a los datos personales transferidos de la UE al Reino Unido. Por tanto, la Comisión seguirá vigilando de cerca cualquier cambio a este respecto.

([70]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) La ICO recibió un gran número de solicitudes de normas corporativas vinculantes del Reino Unido después del *Brexit*. Ya no era posible utilizar muchas normas corporativas vinculantes aprobadas, dado que, después del *Brexit* solamente se podían seguir utilizando aquellas en cuyo proceso de aprobación hubiera intervenido la ICO, pero sus titulares estaban obligados a presentar a la ICO documentación actualizada relativa a la conformidad de dichas normas con el RGPD del Reino Unido.

([74]) El Foro Global de Normas de Privacidad Transfronteriza está formado por los Estados Unidos de América, Canadá, Japón, la República de Corea, Filipinas, Singapur, Taiwán y Australia, y Mauricio, el Centro Financiero Internacional de Dubái y Bermudas son miembros asociados al igual que el Reino Unido.

([75]) Véase, por ejemplo, el análisis comparativo realizado por las autoridades de protección de datos del G7 sobre los elementos esenciales del régimen de certificaciones del RGPD y el sistema de las Normas de Privacidad Transfronteriza, que puso de manifiesto «diferencias notables» entre los sistemas, en particular en lo que respecta a la «aplicabilidad y el recurso legal, las normas relativas a la supervisión independiente y el acceso gubernamental». Puede consultarse en el enlace siguiente (documento en inglés): https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Véase el considerando 79 de la Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal (DO L 76, 19.3.2019, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Véase asimismo el dictamen 02/2014 del Grupo de Trabajo del Artículo 29, de 6 de marzo de 2014, sobre un documento de referencia para los requisitos en materia de normas corporativas vinculantes presentadas a las autoridades nacionales de protección de datos en la UE y normas de privacidad transfronterizas remitidas a los agentes de rendición de cuentas de dichas normas de la APEC.

2.2.6. *Mecanismo de decisión automatizado*

(52) Si bien conserva varios elementos de las normas relativas a las decisiones automatizadas evaluadas en el considerando 54 de la Decisión de Ejecución (UE) 2021/1772, la Data (Use and Access) Act ha modificado algunos aspectos de dichas normas.

(53) En primer lugar, el nuevo artículo 22B introducido en el RGPD del Reino Unido establece una prohibición general del tratamiento de categorías especiales de datos personales (definidas en el artículo 9, apartado 1, del RGPD del Reino Unido) en el caso de decisiones basadas únicamente en el tratamiento automatizado que tengan efectos jurídicos o similares para el interesado. No obstante, contempla tres excepciones a esta prohibición: que el interesado haya dado su consentimiento expreso para dicho tratamiento; o que la decisión sea necesaria para la celebración o la ejecución de un contrato entre el responsable del tratamiento y el interesado; o que el tratamiento sea obligatorio o esté autorizado por la ley. En las dos últimas excepciones, el tratamiento automatizado debe ser necesario por razones de interés público importante ([76]). La prohibición general no se aplica a las decisiones significativas basadas en el tratamiento automatizado de categorías no especiales de datos.

(54) Además, el nuevo artículo 22A del RGPD del Reino Unido aclara la definición de una decisión «basada únicamente en el tratamiento automatizado» al disponer que dicha decisión se caracteriza por la ausencia de una intervención humana significativa en el proceso decisorio. Es importante señalar que los responsables del tratamiento tienen la obligación de evaluar en qué medida la elaboración de perfiles contribuye a una decisión para determinar si la intervención humana ha sido significativa. El artículo 22A del RGPD del Reino Unido también aclara que una «decisión significativa» es aquella que produce efectos jurídicos en el interesado o le afecta significativamente de un modo similar ([77]).

(55) En segundo lugar, el nuevo artículo 22C del RGPD del Reino Unido exige que los responsables del tratamiento apliquen medidas para proporcionar las garantías pertinentes para cualquier decisión significativa basada total o parcialmente en datos personales y basada únicamente en el tratamiento automatizado (incluidas las categorías no especiales de datos personales). Dichas garantías deben incluir la facilitación de información relativa al proceso de toma de decisiones al interesado, permitiendo que este último impugne la decisión y presente observaciones, y asegurar que el interesado pueda contar con intervención humana en el proceso de toma de decisiones ([78]).

(56) Por último, el nuevo artículo 22D del RGPD del Reino Unido otorga al secretario de Estado la facultad de adoptar legislación derivada para describir qué constituye y qué no constituye una participación humana significativa, y qué decisión debe considerarse, y qué no debe considerarse, que tiene efectos significativos similares en los interesados. También permite al secretario de Estado elaborar legislación derivada para i) añadir nuevas salvaguardias; ii) imponer requisitos que complementen las garantías existentes; y iii) definir medidas que no cumplan las salvaguardias ([79]). Es importante señalar que, antes de adoptar reglamentos de conformidad con el artículo 22D del RGPD del Reino Unido, el secretario de Estado debe consultar a la ICO ([80]), los reglamentos no pueden modificar el artículo 22C del RGPD del Reino Unido ([81]) y los reglamentos están sujetos al procedimiento de resolución afirmativa ([82]), lo que significa que deben ser aprobados por ambas cámaras del Parlamento del Reino Unido antes de que puedan promulgarse.

(57) Si bien la Data (Use and Access) Act ha modificado así el marco aplicable a las decisiones automatizadas, conviene señalar que en el marco jurídico del Reino Unido las decisiones automatizadas siguen estando sujetas a una serie de garantías clave que exigen el derecho a obtener intervención humana en todos los casos de decisiones importantes basadas únicamente en el tratamiento automatizado, es decir, sobre la base del tratamiento de datos personales sensibles y no sensibles ([83]). Además, como ha observado la Comisión en decisiones de adecuación anteriores ([84]),

([76]) Artículo 22B del RGPD del Reino Unido, introducido por la sección 80, apartado 1, de la Data (Use and Access) Act.
([77]) Artículo 22A del RGPD del Reino Unido, introducido por la sección 80, apartado 1, de la Data (Use and Access) Act.
([78]) Artículo 22C del RGPD del Reino Unido, introducido por la sección 80, apartado 1, de la Data (Use and Access) Act.
([79]) Artículo 22D del RGPD del Reino Unido, introducido por la sección 80, apartado 1, de la Data (Use and Access) Act. Toda normativa elaborada en virtud de estas facultades está sujeta al procedimiento de resolución afirmativa, lo que garantiza la supervisión del Parlamento. Esta normativa no puede modificar los requisitos establecidos en el artículo 22C.
([80]) Artículo 182, apartado 2, de la DPA de 2018.
([81]) Artículo 22D, apartado 4, del RGPD del Reino Unido.
([82]) Artículo 22D, apartado 5, del RGPD del Reino Unido.
([83]) Artículo 22C, apartado 2, del RGPD del Reino Unido, introducido por la sección 80, apartado 1, de la Data (Use and Access) Act.
([84]) Véase, por ejemplo, el considerando 94 de la Decisión de Ejecución (UE) 2019/419 y el considerando 81 de la Decisión de Ejecución (UE) 2022/254 de la Comisión, de 17 de diciembre de 2021, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de la República de Corea en virtud de la Ley sobre la protección de la información personal (DO L 44 de 24.2.2022, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).

no es probable que las normas específicas sobre las decisiones automatizadas del RGPD del Reino Unido afecten al nivel de protección de los datos personales transferidos de la Unión al Reino Unido. En lo que respecta a los datos personales que hayan sido recogidos en la Unión, toda decisión basada en un tratamiento automatizado será adoptada normalmente por el responsable del tratamiento de los datos en la Unión (que tiene una relación directa con el interesado de que se trate) y está, por tanto, sujeta a las normas del Reglamento (UE) 2016/679.

2.3. **Supervisión y cumplimiento de las normas**

2.3.1. *Supervisión independiente*

(58) En el Reino Unido, de la supervisión y el cumplimiento de las normas del marco de protección de datos se sigue encargando una autoridad de control en materia de protección de datos independiente, como se analiza en los considerandos 85 a 91 de la Decisión de Ejecución (UE) 2021/1772. La Data (Use and Access) Act modifica la estructura de gobernanza de esta autoridad al constituir una persona jurídica, la Information Commission [Comisión de Información], que reemplazará a la ICO, que se había estructurado como una persona jurídica unipersonal.

(59) Más concretamente, las medidas de gobernanza establecidas en la Data (Use and Access) Act, una vez aplicadas, suprimirán la oficina de la ICO y transferirán las funciones, el personal y los bienes de la ICO al nuevo organismo, la Information Commission. La Information Commission está compuesta por miembros ejecutivos y no ejecutivos ([85]). La Ley también establece disposiciones para que el Information Commissioner pase a desempeñar la función de presidente de la Information Commission, que es uno de los miembros no ejecutivos ([86]). La Data (Use and Access) Act dispone además que en la medida en que resulte apropiado como consecuencia de la transferencia de funciones, las referencias al Information Commissioner en todos los actos legislativos u otros documentos (tanto durante su aprobación como durante su elaboración) deben tratarse como referencias a la Information Commission. Para desempeñar sus funciones, esta podrá crear comités y delegar funciones en un miembro, un empleado o un comité ([87]), y podrá adoptar disposiciones para regular su procedimiento y el procedimiento de los comités, también en lo que se refiere al *quorum* y a la adopción de decisiones por mayoría. Estos procedimientos deben hacerse públicos ([88]).

(60) Es importante señalar que la independencia de la Information Commission está sujeta a las mismas garantías, también respecto de las normas sobre el nombramiento y la destitución de su presidente, que las evaluadas en los considerandos 87 a 90 de la Decisión de Ejecución (UE) 2021/1772 ([89]). Se aplican protecciones similares a los demás miembros no ejecutivos de la Information Commission. En particular, su presidente es nombrado por Su Majestad sobre la base de una recomendación del secretario de Estado. Se selecciona en atención a sus méritos y sobre la base de un concurso justo y abierto ([90]). Los demás miembros no ejecutivos son nombrados por el secretario de Estado, previa consulta al presidente. Los candidatos solo pueden ser recomendados para su nombramiento o nombrados si son seleccionados sobre la base de sus méritos con arreglo a un concurso justo y abierto, y si el secretario de Estado está convencido de que no tienen un conflicto de intereses ([91]). Los miembros ejecutivos son empleados de la Information Commission contratados según los términos y condiciones determinados por los miembros no ejecutivos ([92]). El director ejecutivo es nombrado por el presidente y otros miembros no ejecutivos, tras consultar con el secretario de Estado. Los nombramientos de los miembros ejecutivos también están sujetos a una selección por méritos sobre la base de un concurso justo y abierto ([93]).

(61) El presidente solamente puede ser destituido de su cargo por Su Majestad en respuesta a un discurso de ambas cámaras del Parlamento y únicamente si el secretario de Estado ha presentado un informe ante dichas cámaras en el que manifieste su convencimiento de que el presidente es culpable de una falta grave, tiene un conflicto de intereses,

([85]) Anexo 12A, apartado 3, párrafo primero, de la DPA de 2018.
([86]) Secciones 117, 118, 119 y 120 junto con el anexo 14 de la Data (Use and Access) Act.
([87]) Anexo 12A, apartados 13 y 14, de la DPA de 2018.
([88]) Anexo 12A, apartado 16, de la DPA de 2018.
([89]) Artículo 52 del RGPD del Reino Unido y anexo 12A de la DPA de 2018, introducido por la sección 114A del Data (Use and Access) Bill.
([90]) Anexo 12A, apartado 5, párrafo primero, y apartado 3, párrafo segundo, de la DPA de 2018.
([91]) Anexo 12A, apartado 3, párrafo segundo, y apartados 5 y 6, de la DPA de 2018.
([92]) Anexo 12A, apartado 11, de la DPA de 2018.
([93]) Anexo 12A, apartado 5, párrafo segundo, de la DPA de 2018.

no cumple los requisitos de información específicos respecto de los posibles conflictos de intereses o bien está incapacitado o no es apto para desempeñar las funciones del presidente, o no desea hacerlo ([94]). El secretario de Estado solo podrá destituir a los miembros no ejecutivos si considera que se cumplen las condiciones específicas establecidas en la legislación. Entre ellas se incluyen los conflictos de intereses, las faltas graves o la incapacidad, falta de voluntad o incapacidad para desempeñar sus funciones. En cuanto a las garantías adicionales, el secretario de Estado está obligado a hacer pública la decisión de hacerlo y a proporcionar al miembro una exposición de los motivos de la expulsión ([95]).

(62) La función principal de la Information Commission seguirá siendo la del control y la aplicación del marco de protección de datos del Reino Unido «con el fin de proteger los derechos y las libertades fundamentales» de las personas ([96]). Con respecto a la función de la Information Commission de garantizar un nivel adecuado de protección de los datos personales, la Data (Use and Access) Act exige específicamente que la Information Commission tenga en cuenta los intereses de los interesados, los responsables del tratamiento y otras partes, así como las cuestiones de interés público general, y promueva la confianza del público en el tratamiento de los datos personales ([97]). Estos objetivos también se mencionan en el considerando 7 del Reglamento (UE) 2016/679.

(63) Además, la Data (Use and Access) Act especifica que la Information Commission deberá tener en cuenta la promoción de la innovación y la competencia, la importancia de la prevención, investigación, detección y enjuiciamiento de delitos penales, la necesidad de salvaguardar la seguridad pública y la seguridad nacional, y las necesidades específicas relacionadas con la protección de los menores al desempeñar sus funciones en virtud de la legislación sobre protección de datos ([98]). La legislación de la UE en materia de protección de datos también reconoce la necesidad de equilibrar la protección de los datos personales con otros derechos y objetivos fundamentales, como el progreso económico y social, la seguridad y la justicia, y la libertad de empresa ([99]).

2.3.2. *Ejecución, en particular las sanciones*

(64) Las competencias y funciones de la Information Commission siguen siendo equivalentes a las de las autoridades de control en materia de protección de datos de los Estados miembros en virtud de los artículos pertinentes del Reglamento (UE) 2016/679 ([100]), tal como se analiza en los considerandos 91 a 95 de la Decisión de Ejecución (UE) 2021/1772.

(65) La Data (Use and Access) Act ha introducido una serie de aclaraciones específicas relacionadas con el ejercicio de algunas de dichas competencias.

(66) Por un lado, la Data (Use and Access) Act aclara que la Comisión puede solicitar determinados «documentos» e «información» cuando haga uso de su competencia de emisión de avisos de información ([101]). Por otra parte, la Data (Use and Access) Act introduce dos nuevas facultades de investigación para la Information Commission: una nueva facultad para exigir un informe ([102]) y una nueva facultad para emitir «avisos de entrevista» a los responsables del tratamiento en caso de sospecha de infracción del RGPD del Reino Unido o de la DPA de 2018 ([103]).

([94]) Anexo 12A, apartado 7, párrafos sexto y séptimo, de la DPA de 2018.
([95]) Anexo 12A, apartado 9, párrafos sexto, séptimo, octavo y noveno, de la DPA de 2018.
([96]) Artículo 51 del RGPD del Reino Unido.
([97]) Sección 91 de la Data (Use and Access) Act, introducida por la sección 120A de la DPA de 2018.
([98]) Sección 91 de la Data (Use and Access) Act, introducida por la sección 120B de la DPA de 2018. La Data (Use and Access) Act introduce además una nueva sección 120C en la DPA de 2018 que exige a la Information Commission la elaboración y publicación de una estrategia que, entre otras cosas, refleje cómo tendrá en cuenta las cuestiones mencionadas y la promoción del crecimiento económico en el ejercicio de sus funciones reguladoras.
([99]) Véanse, en particular, los considerandos 2 y 4 y el artículo 23 del Reglamento (UE) 2016/679.
([100]) Artículos 57 y 58 del RGPD del Reino Unido.
([101]) Sección 97 de la Data (Use and Access) Act, que modifica la sección 142 de la DPA de 2018. Las consideraciones relativas al impacto de la tecnología y el papel de la protección de datos para generar confianza en la economía digital forman parte de las actividades de los reguladores del ámbito de la protección de datos tanto en el Reino Unido como en la UE. Véase, por ejemplo, la página 12 del informe anual de 2024 del Comité Europeo de Protección de Datos (CEPD): «El CEPD es un organismo dinámico y colaborativo que desempeña un papel fundamental a la hora de garantizar una aplicación coherente de la legislación en materia de protección de datos en toda Europa. Desde mi punto de vista como vicepresidente, considero que es un guardián de los derechos de privacidad de las personas, y equilibra hábilmente las necesidades de innovación y crecimiento económico».
([102]) Sección 98 de la Data (Use and Access) Act, que modifica la sección 146 de la DPA de 2018.
([103]) Sección 100 de la Data (Use and Access) Act por la que se introduce la sección 148A de la DPA de 2018.

(67) En lo que respecta al ejercicio de estas competencias por parte de la Information Commission, desde la entrada en vigor de la Decisión de Ejecución (UE) 2021/1772, el Information Commissioner ha tramitado alrededor de 40 000 reclamaciones de interesados al año, un volumen similar al de las reclamaciones tramitadas cuando el Reino Unido todavía formaba parte de la Unión y aplicaba el Reglamento (UE) 2016/679 ([104]). La ICO también ha llevado a cabo investigaciones *ex officio* relacionadas con gran variedad de cuestiones sectoriales y de cumplimiento, también con los derechos de los interesados ([105]).

(68) En cuanto a las medidas de ejecución, desde la entrada en vigor de la Decisión de Ejecución (UE) 2021/1772, el Commissioner ha emitido ciento veinte amonestaciones, treinta y dos avisos de información, tres avisos de evaluación, doce avisos de ejecución, dos advertencias y doce multas ([106]). Esto incluye varias sanciones monetarias importantes impuestas en virtud del RGPD del Reino Unido y la DPA de 2018. Por ejemplo, el Information Commissioner impuso en abril de 2023 una multa de 12,7 millones de libras esterlinas a una plataforma de redes sociales por el uso indebido de datos de menores ([107]). En marzo de 2025, una empresa de *software* fue multada con 3,07 millones de libras esterlinas por fallos de seguridad que pusieron en riesgo información personal de más de 70 000 personas ([108]). Muy recientemente, en junio de 2025, el Information Commissioner multó a una empresa de pruebas genéticas con 2,31 millones de libras esterlinas por no adoptar medidas de seguridad apropiadas para proteger la información personal de los usuarios del Reino Unido, tras haber sufrido un ciberataque de gran escala en 2023 ([109]).

(69) Desde la adopción de la Decisión de Ejecución (UE) 2021/1772, la ICO también ha formulado y publicado un número significativo de directrices, dictámenes y otros documentos de orientación, que aclaran la aplicación de las normas de protección de datos en importantes ámbitos tales como el reconocimiento facial, la equidad en la inteligencia artificial, los datos de los menores, la comercialización directa, la videovigilancia, el derecho de acceso, la transparencia en la atención sanitaria y la asistencia social, etc., para diferentes destinatarios, por ejemplo, pequeñas y medianas empresas, entidades específicas como escuelas, guarderías o autoridades públicas de pequeño tamaño, así como para las empresas en general, el gran público o los interesados ([110]).

3. CAMBIOS IMPORTANTES EN EL ACCESO Y USO POR LAS AUTORIDADES PÚBLICAS DEL REINO UNIDO DE DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA

3.1. Marco jurídico general

(70) El Reino Unido sigue siendo miembro del Consejo de Europa, mantiene su adhesión al Convenio Europeo de Derechos Humanos y sigue acatando la jurisdicción del Tribunal Europeo de Derechos Humanos. Por tanto, como se describe en los considerandos 116 a 119 de la Decisión de Ejecución (UE) 2021/1772, sigue estando sujeto a las obligaciones consagradas en el Derecho internacional, que enmarcan su sistema de acceso gubernamental a los datos personales sobre la base de principios, garantías y derechos individuales idénticos a los aplicables a los veintisiete Estados miembros como parte del Convenio Europeo de Derechos Humanos y que, en gran medida, se reflejan en la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea.

(71) La DPA de 2018 sigue garantizando derechos y garantías específicos en materia de protección de datos, cuando los datos los tratan las autoridades públicas del Reino Unido, por ejemplo, las autoridades encargadas de garantizar el cumplimiento de la ley y los cuerpos nacionales de seguridad, tal como se analiza en los considerandos 121 a 132 de la Decisión de Ejecución (UE) 2021/1772. La Data (Use and Access) Act solamente ha introducido modificaciones limitadas y específicas en las partes de la DPA de 2018 que establecen las normas para el tratamiento de datos personales en el ámbito penal (parte 3 de la DPA de 2018) y de la seguridad nacional (parte 4 de la DPA de 2018).

([104]) Informes anuales del Information Commissioner de 2021-2022, 2022-2023 y 2023-2024. Véase también la Decisión de Ejecución (UE) 2021/1772, considerando 96.

([105]) Informe anual del Information Commissioner de 2023-2024, página 41.

([106]) Informes anuales del Information Commissioner de 2021-2022, 2022-2023 y 2023-2024.

([107]) Puede consultarse más información sobre estas y otras medidas de ejecución en el sitio web de la ICO, disponible en el enlace siguiente: https://ico.org.uk/action-weve-taken/enforcement/.

([108]) Puede encontrarse información complementaria en el enlace siguiente (documento en inglés): https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) Puede encontrarse información complementaria en el enlace siguiente (documento en inglés): https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) En lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, la parte 3 de la DPA de 2018 sigue estableciendo principios, derechos y obligaciones similares a los establecidos en la Directiva (UE) 2016/680 ([111]).

(73) En particular, en la misma fecha que la presente Decisión, la Comisión ha adoptado una decisión sobre la base del artículo 36, apartado 3, de la Directiva (UE) 2016/680, en la que concluye que el régimen de protección de datos aplicable al tratamiento por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal del Reino Unido a efectos de control de su aplicación sigue garantizando un nivel de protección esencialmente equivalente al que garantiza la Directiva (UE) 2016/680.

(74) La Data (Use and Access) Act ha modificado y consolidado las exenciones existentes en la parte 3 de la DPA de 2018 a disposición de las autoridades competentes con fines de seguridad nacional. La exención relativa a la seguridad nacional permite a las autoridades competentes no aplicar determinadas disposiciones de dicha parte si es necesaria una exención de dicha disposición a efectos de salvaguardar la seguridad nacional ([112]). Refleja las exenciones de seguridad nacional previstas para el tratamiento de datos personales en virtud del RGPD del Reino Unido (previstas en la sección 26 de la DPA de 2018) y en la parte 4 de la DPA de 2018 (prevista en la sección 110 de la DPA de 2018).

(75) La exención de seguridad nacional está sujeta a las mismas limitaciones y garantías que las exenciones en virtud del RGPD del Reino Unido y de la parte 4 de la DPA de 2018, tal como se analiza en los considerandos 64 a 67 y 126 de la Decisión de Ejecución (UE) 2021/1772. En particular, la exención solo podrá aplicarse si es necesario para salvaguardar la seguridad nacional y en la medida en que sea necesario para ello. No se trata de una exención general y el responsable del tratamiento debe considerarla e invocarla caso por caso ([113]). Además, cualquier aplicación de la exención debe cumplir con las normas sobre derechos humanos (amparadas por la Human Rights Act de 1998 y el Convenio Europeo de Derechos Humanos), según las cuales cualquier injerencia en los derechos a la privacidad debe ser necesaria y proporcionada en una sociedad democrática ([114]). Esto también se confirma en las orientaciones de la ICO sobre la aplicación de las exenciones de seguridad nacional ([115]).

(76) Por otra parte, sobre la base de las modificaciones introducidas por la Data (Use and Access) Act ([116]), una actividad de tratamiento específica por parte de las autoridades competentes a efectos de control de la aplicación del Derecho penal también puede regirse por las disposiciones de la parte 4 de la DPA de 2018, que normalmente se aplica únicamente al tratamiento de datos por parte de las autoridades nacionales de seguridad.

([111]) La sección 69 de la Data (Use and Access) Act introduce la definición de consentimiento del interesado y las condiciones para basarse en el consentimiento del interesado como se dispone en el artículo 4, apartado 11, y el artículo 7, del RGPD del Reino Unido [que reflejan las disposiciones correspondientes del Reglamento (UE) 2016/679] a través de las nuevas secciones 33, apartado 1A, y 40A de la DPA de 2018, aclarando de este modo el concepto de consentimiento del interesado y las condiciones para ampararse en el consentimiento del interesado cuando se utiliza como una base jurídica para el tratamiento de datos personales por parte de las autoridades competentes a efectos de control de la aplicación del Derecho penal. Además, la sección 71, apartados 7 y 8, de la Data (Use and Access) Act aclara ligeramente la redacción de la sección 36, apartado 1, de la DPA de 2018. Por último, las modificaciones del RGPD del Reino Unido introducidas por la Data (Use and Access) Act descritas en la sección 2 también se reflejaron, en su caso, en la parte 3 de la DPA de 2018; véanse, por ejemplo, la sección 74, apartados 2 a 5, sobre el tratamiento sensible, la sección 76, apartados 4, 5 y 6, relativa a los plazos para responder a las solicitudes de los interesados, la sección 78, apartados 2 y 3, relativa a las búsquedas realizadas en respuesta a las solicitudes de los interesados, y la sección 80, apartados 3, 4 y 5, sobre decisiones automatizadas.

([112]) Sección 78A, apartado 1, de la DPA de 2018, introducida por la sección 88 de la Data (Use and Access) Act. De conformidad con la sección 78A, apartados 2 a 4, de la DPA de 2018, la exención permite dejar de aplicar los principios de protección de datos (excepto el principio de legalidad y las condiciones y salvaguardias para el tratamiento de datos sensibles), los derechos individuales, las obligaciones de los responsables y encargados del tratamiento de datos con respecto a las violaciones de la seguridad de los datos, determinadas partes de las normas sobre transferencias internacionales de datos y algunas de las competencias de entrada de la ICO para llevar a cabo inspecciones y adoptar medidas coercitivas.

([113]) Véase *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 («Baker v Secretary of State»).

([114]) Véase también *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), apartado 45; *Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), apartado 80.

([115]) Véanse las orientaciones de la ICO sobre la excepción de seguridad y defensa nacional, disponible en el siguiente enlace: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Secciones 89 y 90 de la Data (Use and Access) Act.

(77) Si bien el régimen de protección de datos para el tratamiento con fines de seguridad nacional se extiende por tanto, en determinadas situaciones, también al tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal, esto solamente sucede en determinadas circunstancias y con sujeción a determinadas condiciones y garantías estrictas, esto es, si i) una autoridad competente se define como «autoridad competente apta» en los reglamentos formulados por el secretario de Estado que requieran la aprobación parlamentaria ([117]), y ii) el secretario de Estado designa mediante un aviso una actividad de tratamiento específica llevada a cabo por la autoridad competente apta. Es importante señalar que dicha designación solamente puede producirse si el secretario de Estado considera que la designación de la actividad de tratamiento es necesaria con fines de salvaguardia de la seguridad nacional, esto es, cuando una autoridad encargada de garantizar el cumplimiento del Derecho penal actúa con fines de seguridad nacional, y la actividad de tratamiento es llevada a cabo por la autoridad competente apta en calidad de corresponsable del tratamiento con al menos un servicio de inteligencia ([118]). Como garantías adicionales, el secretario de Estado debe consultar al comisionado antes de notificar la designación ([119]), el texto de la notificación debe, en principio, publicarse ([120]), y una persona directamente afectada por una notificación de designación puede solicitar la revisión judicial ([121]). Por tanto, el objetivo de esta modificación consiste básicamente en aclarar que cuando las autoridades del Reino Unido tienen competencias en el ámbito tanto de la garantía del cumplimiento de la ley como de la seguridad nacional y tratan datos en el contexto de sus responsabilidades en virtud de dichas competencias, se puede aplicar el régimen de protección de datos para los servicios de seguridad nacional.

(78) La parte 4 de la DPA de 2018 regula el tratamiento de datos por parte de los servicios de inteligencia del Reino Unido. Sigue estableciendo los principios fundamentales de protección de datos, imponiendo condiciones sobre el tratamiento de categorías especiales de datos, estableciendo los derechos de los interesados, requiriendo la protección de datos desde el diseño, y regulando las transferencias de datos personales, tal como se describe en los considerandos 125 a 132 de la Decisión de Ejecución (UE) 2021/1772.

(79) Las modificaciones de este régimen introducidas por la Data (Use and Access) Act son limitadas. Con respecto al derecho de acceso de los interesados establecido en la sección 94 de la DPA de 2018, la Data (Use and Access) Act introduce una nueva subsección (la 2A) en la que se aclara que el interesado solamente tiene derecho a la información pertinente en la medida en que el responsable del tratamiento pueda proporcionarla sobre la base de una búsqueda razonable y proporcionada ([122]). Como se explica en el considerando 35, esta modificación enmarca el derecho de acceso sobre la base de las normas jurídicas establecidas, que también tienen en cuenta los intereses del interesado. Si bien en el ámbito de las decisiones automatizadas, se sigue prohibiendo que los responsables del tratamiento tomen una decisión que afecte significativamente a un interesado basada íntegramente en el tratamiento automatizado de datos personales relacionados con el interesado, a menos que dicha decisión sea requerida o esté autorizada por la ley, el interesado haya dado su consentimiento a que dicha decisión se tome sobre esa base, o la decisión se tome en el contexto de un contrato ([123]); la Data (Use and Access) Act introduce en la parte 4 de la DPA de 2018 ([124]) la misma definición del concepto de «decisión basada íntegramente en el tratamiento automatizado» que se recoge en el artículo 22A del RGPD del Reino Unido y se analiza en el considerando 53 de la presente Decisión.

3.2. **Cambios importantes en el acceso a los datos y uso de los mismos por parte de las autoridades públicas del Reino Unido con fines penales**

(80) El Derecho del Reino Unido sigue imponiendo una serie de limitaciones importantes al acceso y uso de datos personales con fines penales, y proporciona mecanismos de supervisión y reparación en este ámbito, tal como se analiza en los considerandos 134 a 174 de la Decisión de Ejecución (UE) 2021/1772.

([117]) Sección 82, apartados A1, 2A y 4, de la DPA de 2018, introducidos por la sección 89, apartado 2, de la Data (Use and Access) Act.

([118]) Sección 82A, apartados 1 y 2, introducidos por la sección 89, apartado 3, de la Data (Use and Access) Act. A modo de garantías adicionales, el secretario de Estado debe consultar con el Commissioner antes de entregar un aviso de designación, véase la nueva sección 82A, apartado 8, de la DPA de 2018, el texto del aviso debe, en principio, ser publicado, véase la nueva sección 82D, apartado 1, con sujeción a las excepciones establecidas en la nueva sección 82D, apartado 3, de la DPA de 2018, y una persona directamente afectada por un aviso de designación puede solicitar control jurisdiccional, véase la nueva sección 82E de la DPA de 2018.

([119]) Sección 82A, apartado 8, de la DPA de 2018.

([120]) Sección 82D, apartado 1, con sujeción a las exenciones establecidas en la nueva sección 82D, apartado 3, de la DPA de 2018.

([121]) Sección 82E de la DPA de 2018.

([122]) Sección 78, apartado 4, de la Data (Use and Access) Act.

([123]) Artículo 96 de la DPA de 2018.

([124]) A efectos de la nueva sección 96, apartado 4, de la DPA de 2018, una decisión se basa íntegramente en el tratamiento automatizado si el proceso decisorio no incluye la oportunidad de que un ser humano acepte o rechace dicha decisión, o influya en ella. Véase la sección 80, apartado 4, letra c), de la Data (Use and Access) Act.

3.2.1. *Base jurídica y limitaciones/garantías aplicables*

(81) La recogida de datos personales de operadores económicos en el Reino Unido a efectos de control de la aplicación del Derecho penal sigue estando permitida en el ordenamiento jurídico del Reino Unido sobre la base de órdenes de registro y órdenes de entrega, con sujeción a las condiciones y salvaguardas descritas en los considerandos 135 a 138 de la Decisión de Ejecución (UE) 2021/1772.

(82) Además, la National Security Act [Ley de seguridad nacional] de 2023 ([125]), que tiene por objeto abordar las amenazas para la seguridad nacional mediante espionaje, sabotaje o acciones de personas que actúen para potencias extranjeras, ha introducido nuevos poderes de entrada, registro e incautación para la policía del Reino Unido, como la posibilidad de obtener datos personales, cuando existan motivos razonables para sospechar que se va a obtener material que es probable que demuestre que se ha cometido o se va a cometer uno de los delitos más graves o actividades que supongan una amenaza para la seguridad nacional en virtud de la National Security Act de 2023 ([126]). Estos poderes están sujetos a unas condiciones y garantías similares a las analizadas en la Decisión de Ejecución (UE) 2021/1772 aplicables a los poderes vigentes en ese momento. En particular, su utilización debe autorizarse mediante una orden judicial o de entrega o una orden de explicación emitidas por una autoridad judicial independiente, en principio, previa solicitud del agente de policía/agente investigador ([127]). Existen protecciones específicas para el material confidencial, como el material periodístico y los artículos sujetos a la prerrogativa de confidencialidad ([128]). Del mismo modo, la emisión de órdenes de divulgación ([129]), órdenes de información del cliente ([130]) y órdenes de supervisión de cuentas ([131]), también creadas por la National Security Act de 2023, deben ser autorizadas por un juez previa solicitud de un funcionario adecuado, y está sujeta a determinadas condiciones y garantías, en particular, que la orden se dicte con respecto a una persona concreta, con fines de investigación de una actividad que suponga una amenaza de una potencia extranjera, que la orden aumente la eficacia de la investigación, y que no se utilice para obtener información que esté sujeta a la prerrogativa de confidencialidad o esté excluida por otro motivo, como material periodístico y determinados historiales médicos ([132]).

(83) Como se describe en los considerandos 139 a 141 de la Decisión de Ejecución (UE) 2021/1772, en el marco jurídico del Reino Unido, determinadas autoridades encargadas de garantizar el cumplimiento de la ley, por ejemplo, la National Crime Agency [Agencia contra el Crimen] o la Metropolitan Police Service [Policía Metropolitana de Londres] también pueden utilizar poderes de investigación selectiva con arreglo a la Investigatory Powers Act [Ley de poderes de investigación] (IPA de 2016) ([133]) con fines de prevención o detección de delitos graves. Los poderes de investigación específicos en que pueden apoyarse esas autoridades encargadas de garantizar el cumplimiento de la ley son: interceptaciones selectivas (parte 2 de la IPA de 2016), adquisición de datos de comunicaciones (parte 3 de la IPA de 2016) e interferencia de equipos específicos (parte 5 de la IPA de 2016). Cuando el secretario de Estado emite avisos de conservación con arreglo a la parte 4 de la IPA de 2016, las autoridades policiales también pueden beneficiarse del acceso a los datos de comunicaciones conservados a través de los poderes de adquisición de datos de comunicaciones con arreglo a la parte 3 de la IPA de 2016.

([125]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Anexo 2 de la National Security Act de 2023. Se consideran delitos pertinentes en virtud de la National Security Act de 2023, por ejemplo, la obtención o divulgación de información protegida (sección 1), la obtención o divulgación de secretos comerciales (sección 3), la prestación de asistencia a un servicio de inteligencia extranjero (sección 4), la comisión de sabotaje (sección 12) o la manifestación de una conducta prohibida concreta para una potencia extranjera con la intención de crear una interferencia (sección 13).

([127]) Véase el apartado 2, punto 1, el apartado 3, punto 1, el apartado 4, punto 1, y el apartado 10, punto 1, del anexo 2 de la National Security Act de 2023.

([128]) Véase el apartado 2, punto 4, letra b), el apartado 3, punto 4, letra b) y c), el apartado 4, punto 4, letra b) y c), y el apartado 10, punto 1, del anexo 2 de la National Security Act de 2023.

([129]) En virtud de las órdenes de divulgación establecidas en el anexo 3 de la National Security Act de 2023, un funcionario puede dirigir un aviso a una persona en el que obligue a esta a aportar información, presentar documentos y/o responder a preguntas pertinentes para una investigación con el fin de detectar bienes relacionados con una actividad que suponga una amenaza de una potencia extranjera, como la circulación o la utilización de dichos bienes.

([130]) Mediante las órdenes de información del cliente establecidas en el anexo 4 de la National Security Act de 2023, un funcionario puede dirigir un aviso a una institución financiera para exigirle que aporte cualquier información de los clientes relacionada con una persona concreta.

([131]) Mediante las órdenes de supervisión de cuentas establecidas en el anexo 5 puede solicitarse a una institución financiera que proporcione a un funcionario la información especificada de acuerdo con la modalidad y el plazo establecidos en dicha orden, no pudiendo ser dicho plazo superior a noventa días.

([132]) Anexo 3, apartado 2, punto 1; anexo 4, apartado 1; y anexo 5, apartado 1, de la National Security Act de 2023.

([133]) La Investigatory Powers Act de 2016 (véase: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) reemplazó diversas leyes sobre interceptación de comunicaciones, interferencia de equipos y adquisición de datos de comunicación; en particular, la parte I de la RIPA de 2000, que proporcionaba el marco legislativo general anterior para el uso de los poderes de investigación por parte de las autoridades encargadas de garantizar el cumplimiento de la ley y las autoridades nacionales de seguridad.

(84) Desde la adopción de la Decisión de Ejecución (UE) 2021/1772, la IPA de 2016, junto con la Regulation of Investigatory Powers Act [Ley sobre la regulación de los poderes de investigación] de 2000 (RIPA) para Inglaterra, Gales e Irlanda del Norte y la Regulation of Investigatory Powers (Scotland) Act [Ley sobre la regulación de los poderes de investigación] de 2000 (RIPSA) para Escocia, sigue estableciendo la base jurídica y las limitaciones y garantías aplicables para el uso de tales poderes, como se describe en la Decisión de Ejecución (UE) 2021/1772. Es importante señalar que el marco jurídico sigue exigiendo que, para ejercer estos poderes, las autoridades deben obtener una orden ([134]) emitida por una autoridad competente ([135]) y aprobada por un comisionado judicial independiente ([136]) (el llamado procedimiento de «doble bloqueo»). Para obtener dicha orden debe seguir realizándose un examen de necesidad y proporcionalidad ([137]).

(85) Al mismo tiempo, desde la adopción de la Decisión de Ejecución (UE) 2021/1772, la Investigatory Powers (Amendment) Act [Ley (de modificación) sobre los poderes de investigación] de 2024, que recibió la sanción real en abril de 2024, modificó una serie de elementos concretos de la IPA de 2016 ([138]). En los siguientes apartados se analizan dichas modificaciones y otros cambios pertinentes en la medida en que guarden relación con las condiciones, limitaciones y garantías relativas al uso de los poderes de investigación específicos mencionados anteriormente por parte de las autoridades públicas del Reino Unido a efectos de control de la aplicación del Derecho penal, tal como se evalúa en los considerandos 177 a 215 de la Decisión de Ejecución (UE) 2021/1772. En lo que respecta a los elementos del marco del Reino Unido que no han sido modificados por la citada ley ni se han visto afectados por otros cambios pertinentes, sigue siendo válido el análisis realizado en la Decisión de Ejecución (UE) 2021/1772.

(86) En cuanto a la adquisición y conservación selectivas de los datos de comunicaciones ([139]), siguen vigentes las condiciones y garantías que rigen estos poderes, tal como se evalúa en la Decisión de Ejecución (UE) 2021/1772. La Investigatory Powers (Amendment) Act de 2024 aclaró las garantías existentes al introducir en la sección 11 de la IPA de 2016 (que penaliza la obtención indebida de datos de comunicaciones de un operador de telecomunicaciones) una lista de ejemplos de lo que debe entenderse que abarca el concepto de «autoridad legal» en dicha disposición ([140]). Además, la Investigatory Powers (Amendment) Act de 2024 aclaró en mayor medida la definición del concepto de «datos de comunicaciones» que figura en la sección 261 de la IPA de 2016 al especificar explícitamente que los datos de los abonados se consideran datos de comunicaciones ([141]).

([134]) En la parte 2, capítulo 2, de la IPA de 2016 se establece un número limitado de supuestos en los que puede realizarse una interceptación sin una orden judicial. En particular: la interceptación con el consentimiento del remitente o el destinatario, la interceptación con fines administrativos o de garantía del cumplimiento, la interceptación que se realice en determinadas instituciones (centros penitenciarios, hospitales psiquiátricos y centros de internamiento de inmigrantes), así como la interceptación realizada con arreglo a un convenio internacional.

([135]) En la mayoría de los casos, el secretario de Estado es la autoridad con potestad para emitir las órdenes en virtud de la IPA de 2016, mientras que los ministros escoceses están facultados para emitir órdenes de interceptación selectiva, órdenes de asistencia mutua y órdenes de interferencia de equipos específicos cuando las personas o instalaciones que van a interceptarse y los equipos que se interferirán se encuentran en Escocia (véanse las secciones 22 y 103 de la IPA de 2016). En caso de interferencia de equipos específicos, un responsable encargado del cumplimiento de la ley (descrito en las partes 1 y 2, anexo 6, de la IPA de 2016) puede emitir la orden judicial con arreglo a las condiciones de la sección 106 de la IPA de 2016.

([136]) Los comisionados judiciales asisten al Investigatory Powers Commissioner, un organismo independiente que ejerce funciones de supervisión sobre el uso de los poderes de investigación por parte de los servicios de inteligencia.

([137]) Véanse, en particular, las secciones 19 y 23 de la IPA de 2016.

([138]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) El término «datos de comunicaciones» cubre el «quién», «cuándo», «dónde» y «cómo» de la comunicación, pero no el contenido, es decir, no cubre lo que se dice o lo que está escrito. Los datos de comunicaciones pueden incluir el tiempo y la duración de la comunicación, el número o la dirección de correo electrónico del originador/remitente y el destinatario y, a veces, la ubicación de los dispositivos desde los que se realizó la telecomunicación, véase la sección 261, apartado 5, de la IPA de 2016. La IPA de 2016 permite que el secretario de Estado exija a los operadores de telecomunicaciones que retengan los datos de las comunicaciones con el fin de obtener acceso selectivo por parte de una serie de autoridades públicas, incluidos los organismos encargados de garantizar el cumplimiento de la ley y los servicios de inteligencia. En la parte 4 de la IPA de 2016 se dispone la conservación de los datos de comunicaciones, mientras que la parte 3 regula la adquisición selectiva de datos de comunicaciones. En las partes 3 y 4 de la IPA de 2016 también se establecen limitaciones específicas en cuanto al ejercicio de estas competencias y se disponen garantías específicas.

([140]) Por ejemplo, cuando la persona de que se trate obtenga los datos de comunicaciones en el ejercicio de un poder estatutario de la autoridad pública pertinente o cuando los datos de comunicaciones se obtengan de conformidad con una orden judicial u otra autorización judicial. Sección 11, apartado 3A, de la IPA de 2016, introducida por la sección 12, apartado 3, de la Investigatory Powers (Amendment) Act de 2024.

([141]) Sección 261, apartados 5A y 5B, introducida por la sección 13, apartado 3, de la Investigatory Powers (Amendment) Act de 2024.

(87) La emisión de avisos que exigen la conservación de datos de comunicaciones ([142]) sigue estando sujeta a limitaciones y garantías, como se describe en los considerandos 208 y 209 de la Decisión de Ejecución (UE) 2021/1772, en particular, a requisitos de necesidad y proporcionalidad y a la aprobación de un comisionado judicial independiente. Si bien la Investigatory Powers (Amendment) Act de 2024 introdujo la posibilidad de renovar dichos avisos, toda renovación está sujeta a las mismas condiciones de necesidad y proporcionalidad y a la aprobación del comisionado judicial ([143]).

(88) Con respecto a los datos de comunicaciones, la Investigatory Powers (Amendment) Act de 2024 también modificó la definición de operador de telecomunicaciones, es decir, los posibles destinatarios de un aviso de conservación. Esta definición incluye ahora a toda persona que «controle o suministre un sistema de telecomunicaciones que i) no esté (total o parcialmente) en el Reino Unido o esté controlado desde el Reino Unido, y ii) sea utilizado por otra persona para ofrecer o prestar un servicio de telecomunicaciones a personas en el Reino Unido» ([144]). Es importante señalar que la definición modificada siempre requiere un estrecho vínculo con el mercado del Reino Unido. La enmienda aclara, por tanto, que las grandes empresas con estructuras empresariales complejas están cubiertas en su totalidad por la IPA de 2016 sin ampliar el ámbito de aplicación de la definición a los proveedores de servicios de telecomunicaciones no dirigidos a personas en el Reino Unido. Esto también queda explicado en las notas explicativas de la Investigatory Powers (Amendment) Act de 2024, que establecen que el objetivo de esta modificación no consiste en incluir a empresas adicionales en el ámbito de aplicación de los poderes pertinentes con arreglo a la IPA de 2016 ([145]) sino que, básicamente, tiene una función aclaratoria.

(89) Por último, la Investigatory Powers (Amendment) Act de 2024 introdujo algunas modificaciones específicas al procedimiento de emisión de órdenes, también con respecto a la interceptación selectiva y la interferencia de equipos específicos, esto es, poderes que también pueden ser utilizados por autoridades encargadas de garantizar el cumplimiento de la ley específicas en el Reino Unido con fines de prevención o detección de delitos graves. Dichas modificaciones afectan únicamente al caso concreto en que dichos poderes sean utilizados para obtener comunicaciones o información acerca de una persona que sea miembro de un cuerpo legislativo pertinente ([146]). Si bien las órdenes relativas a la interceptación selectiva y la interferencia de equipos pueden ser emitidas, en circunstancias normales, por el secretario de Estado y son aprobadas por un comisionado judicial [véanse los considerandos 186 a 196 y 210 a 215 de la Decisión de Ejecución (UE) 2021/1772], las secciones 26 y 111 de la IPA exigen una aprobación adicional del primer ministro cuando la orden concierna a un miembro del Parlamento u otro cuerpo legislativo pertinente (el llamado procedimiento de «triple bloqueo»). La Investigatory Powers (Amendment) Act de 2024 permite ahora al primer ministro nombrar a cinco secretarios de Estado que estarán facultados para ejercer el poder del primer ministro para autorizar dichas órdenes, siempre que la necesidad de autorización sea urgente y el primer ministro no pueda autorizarla a causa de una incapacidad médica o por falta de acceso a comunicaciones seguras. Es importante señalar que siguen vigentes las limitaciones y garantías con respecto a la emisión de estas órdenes, descritas en los considerandos de la Decisión de Ejecución (UE) 2021/1772 mencionados más arriba.

3.2.2. *Uso ulterior de la información recogida*

(90) El intercambio de datos por parte de una autoridad encargada de garantizar el cumplimiento de la ley con una autoridad diferente para fines distintos de aquellos para los que se recogieron originalmente (el llamado «intercambio posterior») sigue estando sujeto a las condiciones analizadas en los considerandos 142 a 156 de la Decisión de Ejecución (UE) 2021/1772.

([142]) La emisión de dichos avisos de conservación en virtud de las secciones 87, 88 y 89 de la IPA de 2016 tiene como objetivo garantizar que los operadores de telecomunicaciones conserven, durante un período máximo de doce meses, los datos de comunicaciones pertinentes que, de otro modo, se eliminarían una vez que dejan de ser necesarios para fines comerciales. Los datos conservados deben estar disponibles durante el período requerido en caso de que, posteriormente, sea necesario que una autoridad pública los adquiera en virtud de una autorización para una adquisición selectiva de datos de comunicaciones contemplada por la parte 3 de la IPA de 2016.

([143]) Sección 94A de la IPA de 2016, introducida por la sección 20, apartado 4, de la Investigatory Powers (Amendment) Act de 2024.

([144]) Sección 261, apartado 10, letra c), de la IPA de 2016, introducida por la sección 19 de la Investigatory Powers (Amendment) Act de 2024.

([145]) Notas explicativas de la Investigatory Powers (Amendment) Act de 2024, apartado 359, disponibles en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Véanse los artículos 26 y 111 de la IPA de 2016.

(91) Por lo que respecta a la situación concreta de las transferencias ulteriores del Reino Unido a Estados Unidos, el 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 (el «Acuerdo entre el Reino Unido y EE. UU.») ([147]), celebrado en octubre de 2019, entró en vigor en octubre de 2022 y se aplica desde entonces. En virtud de dicho Acuerdo, las transferencias de datos desde la UE a proveedores de servicios del Reino Unido podrían estar sujetas a órdenes para la producción de pruebas emitidas por las autoridades competentes de Estados Unidos encargadas del cumplimiento de la ley, y que podrían aplicarse en el Reino Unido.

(92) Es importante señalar que siguen en vigor las condiciones y garantías en virtud de las cuales pueden emitirse y ejecutarse dichas órdenes, tal como se evalúa en el considerando 154 de la Decisión de Ejecución (UE) 2021/1772. En particular, los datos obtenidos en virtud del Acuerdo se benefician de protecciones equivalentes a las garantías específicas que brinda el denominado «Acuerdo marco UE-EE. UU.» ([148]), que se incorporan todas en este Acuerdo por referencia *mutatis mutandis* ([149]).

(93) Desde la adopción de la Decisión de Ejecución (UE) 2021/1772, el Reino Unido ha explicado que ha aclarado, incluso mediante la colaboración con las partes pertinentes en el contexto de la aplicación del Acuerdo entre el Reino Unido y los Estados Unidos, cómo las garantías específicas del Acuerdo marco UE-EE. UU. diseñadas para el ámbito de la cooperación policial. En particular, el Reino Unido ha explicado que las disposiciones del Acuerdo marco UE-EE. UU. que prevén una función para la autoridad competente pertinente (que no existe en una situación de cooperación directa entre un proveedor de servicios del Reino Unido y una autoridad encargada de garantizar el cumplimiento de la ley de Estados Unidos) se interpretan *mutatis mutandis* para referirse a la autoridad designada (definida en el Acuerdo entre el Reino Unido y EE. UU.) ([150]) de la Parte pertinente.

(94) Por ejemplo, en la notificación de un incidente de seguridad de la información en virtud del artículo 10 del Acuerdo marco UE-EE. UU., que requiere la notificación a la autoridad competente de transferencia, el Reino Unido ha explicado que esta disposición se aplica *mutatis mutandis* de modo que se entienda que la notificación debe realizarse a la autoridad competente de la Parte de la que se transfirieron los datos.

(95) Sobre la autorización de la autoridad competente de transferencia antes de la transferencia ulterior de información personal conforme a lo establecido en el artículo 7 del Acuerdo marco UE-EE. UU., el Reino Unido ha aclarado que aplicará dicha disposición *mutatis mutandis* de modo que se entienda que la autoridad designada de la Parte de la que se transfirieron los datos tendrá que autorizar toda transferencia ulterior.

(96) En lo que respecta a las obligaciones recogidas en el artículo 8 del Acuerdo marco UE-EE. UU. sobre el mantenimiento de la calidad y la integridad de la información, una interpretación *mutatis mutandis* de dicha disposición impondría a la autoridad designada de la Parte que reciba los datos la responsabilidad de comunicarse con el proveedor que haya transferido los datos en caso de problemas con respecto a la calidad y la integridad de los mismos.

([147]) 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, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([148]) Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales (DO L 336 de 10.12.2016, p. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Artículo 9, apartado 1, del Acuerdo.

([150]) En virtud del artículo 1, apartado 8, del Acuerdo entre el Reino Unido y EE. UU., por «autoridad designada» se entiende la entidad pública designada, en el caso del Reino Unido, por el secretario de Estado de Interior y, en el caso de Estados Unidos, por el fiscal general.

(97) Sobre los recursos judiciales, el Reino Unido ha subrayado que las transferencias en virtud del Acuerdo entre el Reino Unido y EE. UU. siempre incumbirán a la autoridad designada de cada Parte. Cuando Estados Unidos sea la Parte que recibe los datos de proveedores de servicios del Reino Unido, el Departamento de Justicia de Estados Unidos actuará como autoridad designada. Por lo tanto, según la interpretación del Reino Unido, cada solicitud emitida sobre la base del Acuerdo entre el Reino Unido y EE. UU. incumbirá al Departamento de Justicia en calidad de autoridad federal designada en virtud de la Judicial Redress Act [Ley de recurso judicial] de EE. UU., y se puede, por tanto, interponer un recurso judicial contra el Departamento de Justicia de conformidad con el artículo 19 del Acuerdo marco UE-EE. UU. Además, el Reino Unido ha confirmado a los servicios de la Comisión que la Judicial Redress Act no es el único mecanismo para interponer un recurso. Dependiendo de las circunstancias y del contexto de cada caso concreto, otra legislación aplicable de Estados Unidos prevé vías alternativas a través de las que puede interponerse un recurso judicial.

3.2.3. *Supervisión y reparación*

(98) Dependiendo de los poderes utilizados por las autoridades competentes en el tratamiento de los datos personales con fines de aplicación de la ley (tanto en virtud de la DPA de 2018 como de la IPA de 2016), diferentes organismos siguen garantizando la supervisión del uso de estos poderes, tal como se evalúa en los considerandos 158 a 174 de la Decisión de Ejecución (UE) 2021/1772, y siguen existiendo mecanismos de reparación disponibles en la parte 3 de la DPA de 2018, en la IPA de 2016 y en la Human Rights Act de 1998, tal como se analiza en los considerandos 250 a 269 de la Decisión de Ejecución (UE) 2021/1772.

(99) Con respecto a la supervisión contemplada en la parte 3 de la DPA de 2018, las funciones y las competencias de la Information Commission se analizan en los considerandos 158, 159, 160 y 162 de la Decisión de Ejecución (UE) 2021/1772, con sujeción a las modificaciones introducidas por la Data (Use and Access) Act descritas en las secciones 2.3.1 y 2.3.2 de la presente Decisión.

(100) En términos de ejecución de estas competencias, desde la adopción de la Decisión de Ejecución (UE) 2021/1772, el Information Commissioner ha tramitado numerosas reclamaciones ([151]) y ha llevado a cabo varias investigaciones y adoptado medidas de ejecución con respecto al tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento de la ley. Entre 2021 y 2025, el Information Commissioner llevó a cabo investigaciones y emitió amonestaciones contra varios órganos policiales por distintos incumplimientos de sus obligaciones en materia de protección de datos, por ejemplo, en la respuesta a solicitudes de acceso a los datos, en el establecimiento de medidas de seguridad relacionadas con datos de videovigilancia, en el tratamiento de antecedentes penales sensibles, al fusionar los datos de distintas personas, o al comunicar datos personales a terceros ([152]). El Information Commissioner también emitió directrices, dictámenes y documentos de orientación, por ejemplo, sobre el derecho de acceso o sobre cómo tramitar solicitudes manifiestamente infundadas o excesivas con arreglo a la parte 3 de la DPA de 2018 ([153]).

(101) En lo que respecta al uso de los poderes de investigación en virtud de la IPA de 2016, la supervisión judicial e independiente sigue correspondiendo al Investigatory Powers Commissioner, asistido por otros comisionados judiciales, a los que se hace referencia de forma conjunta como «comisionados judiciales» ([154]). En este ámbito, la Investigatory Powers (Amendments) Act de 2024 tan solo ha introducido modificaciones limitadas y específicas, que no afectan a la independencia, las funciones ni los poderes de los comisionados judiciales, sino que tienen por objeto reforzar en la práctica el funcionamiento del régimen de supervisión existente, en particular mediante la introducción de adjuntos al Investigatory Powers Commissioner en los que este pueda delegar determinados poderes cuando no pueda desempeñar sus funciones o no esté disponible para hacerlo. Dichos adjuntos al Investigatory Powers Commissioner deben ser comisionados judiciales y son nombrados por el Investigatory Powers Commissioner ([155]).

([151]) Por ejemplo, la Information Commission recibió en 2023-2024 1 890 reclamaciones sobre la base del RGPD o la DPA de 2018 relacionadas con organizaciones pertenecientes a los subsectores «autoridad policial», «fuerzas policiales» y «comisarios de policía». Véase también el *Annual Report and Financial Statements 2023-24* [«Informe anual y estados financieros 2023-2024», documento en inglés] del Information Commissioner, disponible en el siguiente enlace: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Puede encontrarse información complementaria en el enlace siguiente (documento en inglés): https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ y https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Véase el considerando 250 de la Decisión de Ejecución (UE) 2021/1772.

([155]) Sección 227 de la IPA de 2016, introducida por la sección 7 de la Investigatory Powers (Amendment) Act.

3.3. **Cambios importantes en el acceso a los datos y uso de los mismos por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional**

(102) Con respecto a los poderes de investigación ejercidos en el contexto de la seguridad nacional, la IPA de 2016 sigue proporcionando el marco jurídico para el uso de dichos poderes. Además de las modificaciones relacionadas con los poderes de investigación selectiva a los que también pueden recurrir, bajo condiciones específicas, determinadas autoridades encargadas de garantizar el cumplimiento de la ley, como se describe en los considerandos 77 a 85 de la presente Decisión, la Investigatory Powers (Amendment) Act de 2024 también ha introducido modificaciones en uno de los poderes otorgados por la IPA de 2016 que puede ejercerse de forma masiva.

(103) Más concretamente, la Investigatory Powers (Amendment) Act de 2024 ha introducido en la nueva parte 7A de la IPA de 2016 un régimen específico para la conservación y el examen de un determinado subconjunto de los conjuntos de datos personales masivos ([156]), esto es, referente a aquellos conjuntos de datos con respecto a los cuales las personas con las que están relacionados los datos personales no podrían tener expectativas razonables de privacidad, o solo podrían tener expectativas muy bajas ([157]). El jefe de un servicio de inteligencia determina si un conjunto de datos personales masivos forma parte de este subconjunto específico de conjuntos de datos basándose en las circunstancias, en particular, i) la naturaleza de los datos, ii) la medida en que las personas han hechos públicos los datos o han dado su consentimiento para que los datos se hagan públicos, iii) si los datos se han publicado, en qué medida se han publicado con sujeción a un control editorial o por una persona que actúe de conformidad con las normas profesionales, iv) si los datos se han publicado o son de dominio público, en qué medida son datos ampliamente conocidos, y v) en qué medida los datos han sido utilizados ya en el dominio público ([158]).

(104) Es importante señalar que, para la conservación y el examen de conjuntos de datos personales masivos, que no entran en esta categoría, es decir, aquellos que son más sensibles y, por lo tanto, implican una expectativa razonable de privacidad, sigue en vigor 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, a continuación, por el comisionado judicial, con sujeción a los principios de proporcionalidad y necesidad de la medida, tal como se establece en la parte 7 de la IPA de 2016 ([159]).

(105) La parte 7A de la IPA de 2016 prevé dos tipos de autorización: la autorización individual y la autorización de categoría. La conservación, o la conservación y el examen, de todos los conjuntos de datos personales masivos conservados en virtud de la parte 7A deberá autorizarse en virtud de una de estas autorizaciones. Ambas autorizaciones requieren, en principio ([160]), una autorización del jefe del servicio de inteligencia (o de una persona que actúe en su nombre) y la aprobación de un comisionado judicial independiente ([161]). El jefe de un servicio de inteligencia concede una autorización individual con arreglo a las condiciones establecidas en la sección 226B, apartado 4, de la IPA de 2016 y previa aprobación de los comisarios judiciales. El comisionado judicial debe revisar las conclusiones de la persona que concedió la autorización en relación con si el artículo 226A, es decir, la escasa o nula expectativa razonable del requisito de privacidad, se aplica al conjunto masivo de datos personales descrito en la autorización ([162]).

([156]) Las órdenes sobre conjuntos de datos personales masivos emitidas en virtud de la sección 200 de la IPA de 2016 autorizan a los servicios de inteligencia a conservar y examinar conjuntos de datos que contengan datos personales relacionados con una serie de personas que sean conjuntos de datos de una naturaleza tal que la mayoría de las personas carezcan de interés para el servicio de inteligencia en el ejercicio de sus funciones, y que sea improbable que lo adquieran, y que sean conservados por medios electrónicos por un servicio de inteligencia y mantenidos para fines de análisis en el ejercicio de sus funciones; véase también la sección 199 de la IPA de 2016.

([157]) Sección 226A, apartado 1, de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

([158]) Sección 226A, apartado 3, de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

([159]) La Investigatory Powers (Amendment) Act de 2024 ha modificado la sección 213 de la IPA de 2016 de modo que las órdenes sobre conjuntos de datos personales masivos dejen de ser válidas a los doce meses de su emisión. Anteriormente, dichas órdenes debían renovarse cada seis meses. Véase la sección 3 de la Investigatory Powers (Amendment) Act de 2024.

([160]) Solo podrá concederse una autorización individual sin aprobación judicial previa i) si la persona que concede la autorización individual considera que el conjunto de datos personales masivos en cuestión entra dentro de una autorización de categoría existente, o ii) en caso de urgencia, véase la sección 226B, apartado 6, de la IPA de 2016. En este último caso, la decisión de conceder una autorización individual urgente debe ser revisada por un comisionado judicial en un plazo de tres días hábiles a partir del día de su emisión (véase la sección 226BC de la IPA de 2016).

([161]) Sección 226B, apartado 1, de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act.

([162]) Sección 226BB, apartado 1, letra a), de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

(106) Una autorización de categoría autoriza la conservación, o la conservación y el examen, de una categoría de conjuntos de datos personales masivos descrita en la autorización.

(107) La decisión de conceder la autorización de categoría la adopta el jefe del servicio de inteligencia cuando considera que el artículo 226A se aplica a cualquier conjunto de datos dentro de la categoría y cuando la decisión de conceder la autorización es aprobada por un comisionado judicial independiente ([163]). Este último debe revisar si la sección 226A, es decir, la baja o nula expectativa razonable del requisito de privacidad, se aplica a cualquier conjunto de datos que pertenezca a la categoría de conjuntos de datos descrita en la autorización ([164]).

(108) Es importante destacar que, al aprobar una decisión para conceder una autorización individual o colectiva, el comisionado judicial debe «aplicar los mismos principios que aplicaría un tribunal en una solicitud de revisión judicial» ([165]) y considerar estas cuestiones con un grado de atención suficiente para garantizar que el comisionado judicial cumple los deberes impuestos en la sección 2 de la IPA de 2016 (deberes generales en relación con la privacidad) ([166]). Por otra parte, la emisión de autorizaciones está sujeta a una estricta supervisión *ex post*, en particular a través de la presentación de informes anuales al secretario de Estado y a la Intelligence and Security Committee of Parliament [Comisión de Información y Seguridad del Parlamento] ([167]) y de inspecciones periódicas de la Oficina del Investigatory Powers Commissioner ([168]).

(109) En cuanto a los cambios pertinentes en el ámbito de la supervisión, la Oficina del Investigatory Powers Commissioner ha publicado informes anuales correspondientes a los años 2021, 2022 y 2023, que proporcionan estadísticas e información detalladas sobre el uso de los poderes de investigación por parte de los servicios de inteligencia y las autoridades encargadas de garantizar el cumplimiento de la ley en el Reino Unido ([169]). Los informes describen también las auditorías e investigaciones de dicha Oficina, así como sus conclusiones, lo que confirma que el Investigatory Powers Commissioner sigue garantizando su función de supervisión, tan importante, conforme al régimen de poderes de investigación del Reino Unido. Por ejemplo, en 2023, revisó las justificaciones basadas en la necesidad y la proporcionalidad para el uso de los poderes de interceptación masiva [tal como se evalúa en los considerandos 218 a 225 de la Decisión de Ejecución (UE) 2021/1772] por parte del Cuartel General de Comunicaciones del Gobierno, y concluyó que la gran mayoría de las declaraciones se había articulado sobre una base sólida, aunque en algunos casos la proporcionalidad no se había expresado adecuadamente. Estas conclusiones se trataron con el equipo de cumplimiento de dicho cuartel general, que se comprometió a impartir formación interna adicional sobre concienciación a nivel de comisión para abordar esta cuestión ([170]).

(110) Además, el Investigatory Powers Tribunal emitió un informe público sobre sus actividades y jurisprudencia para el período 2021-2023 ([171]). El informe muestra que el número de asuntos recibidos por el Tribunal se ha duplicado con creces desde 2017, con más de 400 asuntos recibidos en 2023 ([172]). La mayoría de las denuncias se referían a

([163]) Sección 226BA de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act.

([164]) Sección 226BB, apartado 1, letra b), de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

([165]) Sección 226BB, apartado 2, letra a), de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

([166]) Sección 226BB, apartado 2, letra b), de la IPA de 2016, introducida por la sección 2 de la Investigatory Powers (Amendment) Act de 2024. De conformidad con los deberes generales en relación con la privacidad tal y como establecen ahora en la sección 2 de la IPA de 2016, una autoridad pública debe tener en cuenta a) si el objetivo que se pretende alcanzar gracias a la orden, autorización o aviso podría lograrse razonablemente por otros medios menos intrusivos, b) si el nivel de protección que debe aplicarse en relación con cualquier obtención de información con arreglo a la orden, autorización o aviso sea mayor debido a la sensibilidad particular de esa información, c) el interés público en la integridad y seguridad de los sistemas de telecomunicaciones y los servicios postales, y d) cualquier otro aspecto de interés público en la protección de la privacidad.

([167]) Secciones 226DA y 226DB de la IPA de 2016, introducidas por la sección 2 de la Investigatory Powers (Amendment) Act de 2024.

([168]) Véase el informe anual de 2023 del Investigatory Powers Commissioner, disponible 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, p. 3.

([169]) Todos los informes anuales pueden consultarse en el enlace siguiente: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Véanse los apartados 6.39 a 6.43 del informe anual de 2023 disponible 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.

([171]) Investigatory Powers Tribunal Report 2021-2023 [informe del Investigatory Powers Tribunal], disponible en el siguiente enlace: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Investigatory Powers Tribunal Report 2021-2023, p. 5.

los cuerpos y fuerzas de seguridad, seguidos de cerca por las autoridades de seguridad e inteligencia ([173]). Es importante señalar que, en 2022 y 2023, el Tribunal dictó sentencias en asuntos que había recibido antes de 2021 en las que declaró que las autoridades públicas del Reino Unido (Policía de Escocia ([174]), Policía del Gran Manchester ([175]), Policía de Surrey ([176]), MI5 y Ministro del Interior ([177]), respectivamente) habían actuado ilegalmente. En cuanto a las vías de recurso, el Investigatory Powers Tribunal ordenó, entre otras cosas, la destrucción de cualquier material obtenido ilegalmente y, en un caso, también el pago de 12 000 GBP como justa satisfacción por las infracciones detectadas. Así pues, el informe anual confirma que el Investigatory Powers Tribunal desempeña efectivamente su importante papel a la hora de garantizar la supervisión y las vías de recurso en el ámbito de la aplicación del Derecho penal y el acceso a los datos personales en materia de seguridad nacional.

(111) Además, el informe también destaca acontecimientos importantes, como una sentencia del Tribunal Europeo de Derechos Humanos en la que el Tribunal sostuvo que las personas de cualquier lugar del mundo pueden presentar una demanda ante el Investigatory Powers Tribunal en relación con el funcionamiento del régimen de interceptación masiva del Reino Unido si la conducta en cuestión fue llevada a cabo por un organismo público del Reino Unido y se produjo en el Reino Unido ([178]).

4. **CONCLUSIÓN**

(112) La Comisión considera que el RGPD del Reino Unido y la DPA de 2018, en su versión modificada por la Data (Use and Access) Act, siguen garantizando un nivel de protección de los datos personales transferidos desde la Unión Europea que es esencialmente equivalente al que garantiza el Reglamento (UE) 2016/679.

(113) Además, la Comisión considera que, en su conjunto, los mecanismos de supervisión y las vías de impugnación contemplados en el Derecho del Reino Unido siguen siendo suficientes para detectar y sancionar en la práctica las vulneraciones de la normativa de protección de datos y brindan al interesado medios jurídicos para solicitar el acceso a sus datos personales y, en su caso, su rectificación o supresión.

(114) Por último, sobre la base de la información disponible sobre el ordenamiento jurídico del Reino Unido, la Comisión considera que cualquier injerencia en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión Europea al Reino Unido por parte de las autoridades públicas del Reino Unido con fines de interés público, en particular con fines policiales y de seguridad nacional, sigue limitándose a lo estrictamente necesario para lograr el objetivo legítimo en cuestión, y que existe una tutela judicial efectiva contra tales injerencias.

(115) Por lo tanto, y habida cuenta de lo expuesto en la presente Decisión, debe concluirse que el Reino Unido sigue garantizando un nivel adecuado de protección a efectos del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

(116) Esta conclusión se basa tanto en el régimen nacional pertinente del Reino Unido, con los cambios que ha tenido desde la adopción de la Decisión de Ejecución (UE) 2021/1772, como en sus compromisos internacionales, en particular el hecho de que el Reino Unido sigue rigiéndose por el Convenio Europeo de Derechos Humanos y sigue acatando la jurisdicción del Tribunal Europeo de Derechos Humanos. Por tanto, que siga vinculándose por estas obligaciones internacionales es un elemento de especial importancia para la evaluación en la que se basa la presente Decisión.

([173]) Investigatory Powers Tribunal Report 2021-2023, p. 12.
([174]) Wilson v Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury v Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill v Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International v Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder and Guarnieri v UK*, [2023] ECHR 668, véase también el Investigatory Powers Tribunal Report 2021-2023, p. 6.

5. EFECTOS DE LA PRESENTE DECISIÓN Y ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

(117) Los Estados miembros y sus organismos están obligados a adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, ya que estos disfrutan de una presunción de legalidad y producen, por consiguiente, efectos jurídicos en tanto no hayan perdido vigencia o sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad.

(118) Por lo tanto, toda decisión de adecuación de la Comisión adoptada en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679 vincula a todos los organismos de los Estados miembros destinatarios, incluidas sus autoridades de control independientes. En particular, durante el período de aplicación de la Decisión de Ejecución (UE) 2021/1772, modificada por la presente Decisión, pueden producirse transferencias de un responsable o encargado del tratamiento en la Unión Europea a responsables o encargados del tratamiento en el Reino Unido sin necesidad de obtener ninguna autorización adicional.

(119) Cabe recordar que, de conformidad con el artículo 58, apartado 5, del Reglamento (UE) 2016/679 y como explicó el Tribunal de Justicia en la sentencia *Schrems I* ([179]), cuando una autoridad nacional de protección de datos cuestiona, en especial a raíz de una reclamación, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales del particular a la privacidad y la protección de los datos, el Derecho nacional debe prever las vías de acción para exponer las alegaciones correspondientes ante los tribunales nacionales, a los que podrá pedirse que planteen una cuestión prejudicial al TJUE ([180]).

6. SUPERVISIÓN

(120) De conformidad con el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión supervisará de manera continuada los acontecimientos pertinentes en el Reino Unido a fin de valorar si esta aún garantiza un nivel de protección esencialmente equivalente. Esta supervisión es especialmente importante porque el Reino Unido aplicará y hará cumplir un régimen modificado de protección de datos. Asimismo, el marco modificado de protección de datos del Reino Unido otorga al secretario de Estado la facultad de especificar en mayor medida este marco a través del Derecho derivado. A este respecto, debe prestarse especial atención a dichas especificaciones adicionales, así como a la aplicación en la práctica de las normas modificadas del Reino Unido sobre transferencias de datos personales a terceros países; a la eficacia del ejercicio de los derechos individuales, incluida cualquier evolución pertinente de la legislación y la práctica en relación con las excepciones o restricciones de dichos derechos recientemente introducidas, al funcionamiento de la ICO reestructurada, también con respecto a la tramitación de reclamaciones y la aplicación de poderes correctivos, así como al cumplimiento de las limitaciones y salvaguardias con respecto al acceso gubernamental, en particular con respecto a la parte 7A de la IPA de 2016 recientemente introducida. La supervisión de la Comisión se debe basar en, entre otros elementos, los avances de la jurisprudencia y la supervisión de la ICO y otros organismos independientes.

(121) Para facilitar esta supervisión, las autoridades del Reino Unido deben informar puntualmente a la Comisión de cualquier cambio sustancial en el ordenamiento jurídico del Reino Unido que tenga un impacto en el marco jurídico objeto de la Decisión de Ejecución (UE) 2021/1772, modificada por la presente Decisión, así como de cualquier evolución en las prácticas relacionadas con el tratamiento de los datos personales evaluados en la Decisión de Ejecución (UE) 2021/1772, modificada por la presente Decisión, tanto en lo que se refiere al tratamiento de datos personales por parte de los responsables y encargados del tratamiento con arreglo al RGPD del Reino Unido como a las limitaciones y garantías aplicables al acceso a los datos personales por parte de las autoridades. Esto debe incluir la evolución de los elementos mencionados en el considerando 120.

(122) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de supervisión, los Estados miembros deben informarle de cualquier medida pertinente adoptada por las autoridades nacionales de protección de datos, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la UE en relación con la transferencia de datos personales desde la UE a los responsables o encargados del tratamiento en el Reino Unido. También debe informarse a la Comisión de todo indicio de que las acciones de las autoridades públicas del Reino Unido responsables de la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de la seguridad nacional, incluidos los órganos de supervisión, no garantizan el nivel de protección necesario.

([179]) Schrems I, apartado 65.

([180]) *Schrems I*, apartado 65: «A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de esta».

(123) Cuando la información disponible, en particular la información resultante de la supervisión de la Decisión de Ejecución (UE) 2021/1772, modificada por la presente Decisión o proporcionada por las autoridades del Reino Unido o de los Estados miembros, revele que el nivel de protección ofrecido por el Reino Unido podría ya no ser adecuado, la Comisión debe informar sin demora a las autoridades competentes del Reino Unido y solicitar que se adopten medidas adecuadas dentro de un plazo determinado, el cual no podrá exceder de tres meses. En caso necesario, este plazo podrá ampliarse por un período determinado, teniendo en cuenta la naturaleza del asunto en cuestión o las medidas que deban tomarse. Por ejemplo, este procedimiento se activaría en los casos en que las transferencias ulteriores, incluso sobre la base de nuevas normas en materia de adecuación adoptadas por el secretario de Estado o de acuerdos internacionales celebrados por el Reino Unido, ya no se lleven a cabo con arreglo a salvaguardias que garanticen la continuidad de la protección en el sentido del artículo 44 del Reglamento (UE) 2016/679.

(124) Si, al vencer dicho plazo, las autoridades del Reino Unido competentes no han tomado dichas medidas o no han demostrado satisfactoriamente de otro modo que se sigue garantizando un nivel de protección adecuado a efectos de la presente Decisión, la Comisión debe iniciar el procedimiento a que se refiere el artículo 93, apartado 2, del Reglamento (UE) 2016/679 con el fin de suspender o derogar, total o parcialmente, la presente Decisión.

(125) La Comisión también puede iniciar ese procedimiento para modificar la presente Decisión, en particular con el fin de imponer condiciones adicionales a las transferencias de datos o con el fin de limitar la conclusión de adecuación solo a las transferencias de datos para las que se siga garantizando un nivel de protección adecuado.

(126) Por razones imperiosas de urgencia debidamente justificadas, la Comisión debe hacer uso de la competencia de adoptar, de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3, del Reglamento (UE) 2016/679, actos de ejecución inmediatamente aplicables que suspendan, deroguen o modifiquen la presente Decisión.

7. **REVISIÓN, DURACIÓN Y RENOVACIÓN DE LA PRESENTE DECISIÓN**

(127) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679 y teniendo en cuenta el hecho de que el nivel de protección que ofrece el régimen jurídico del Reino Unido puede ser objeto de modificación, la Comisión, tras la adopción de la presente Decisión, debe revisar periódicamente si las conclusiones relativas a la adecuación del nivel de protección garantizado por el Reino Unido siguen estando justificadas de hecho y de Derecho, teniendo en cuenta los elementos enumerados en el artículo 45, apartado 2, del Reglamento (UE) 2016/679. Estas evaluaciones deben tener lugar al menos cada cuatro años y deben abarcar todos los aspectos del funcionamiento de la presente Decisión, en particular el funcionamiento de los mecanismos de supervisión y ejecución pertinentes.

(128) Para llevar a cabo la revisión, la Comisión debe reunirse con los representantes pertinentes de las autoridades del Reino Unido, incluida la Information Commission. La participación en esta reunión debe estar abierta a los representantes de los miembros del Comité Europeo de Protección de Datos. En el marco de la revisión, la Comisión debe solicitar al Reino Unido que facilite información completa sobre todos los aspectos pertinentes a efectos de la conclusión de adecuación. La Comisión también debe pedir explicaciones sobre cualquier información pertinente para la presente Decisión que haya recibido, en particular del Comité Europeo de Protección de Datos, de las distintas autoridades de protección de datos y de los grupos de la sociedad civil y los informes públicos o las noticias los medios de comunicación o cualquier otra fuente de información disponible.

(129) Sobre la base de la revisión, la Comisión debe elaborar un informe público que presentará al Parlamento Europeo y al Consejo.

(130) La Comisión también debe tener en cuenta que el marco de protección de datos evaluado en la presente Decisión y en la Decisión de Ejecución (UE) 2021/1772 puede seguir evolucionando.

(131) Por tanto, conviene estipular que la presente Decisión se aplicará durante un período de seis años a partir de su entrada en vigor.

(132) Cuando, en particular, la información resultante de la supervisión de la presente Decisión revele que las conclusiones relativas a la adecuación del nivel de protección garantizado en el Reino Unido siguen estando justificadas de hecho y de derecho, la Comisión debe, a más tardar seis meses antes de que la presente Decisión deje de aplicarse, iniciar el procedimiento para modificar la presente Decisión ampliando su ámbito temporal de aplicación, en principio, por un período adicional de cuatro años. Cualquier acto de ejecución que modifique la presente Decisión se adoptará de conformidad con el procedimiento contemplado en el artículo 93, apartado 2, del Reglamento (UE) 2016/679.

8. **CONSIDERACIONES FINALES**

(133) El Comité Europeo de Protección de Datos publicó su correspondiente dictamen ([181]), que se ha tenido en cuenta en la elaboración de la presente Decisión.

(134) La medida prevista en la presente Decisión se ajusta al dictamen del Comité creado en virtud del artículo 93 del Reglamento (UE) 2016/679.

(135) Procede, por tanto, modificar la Decisión de Ejecución (UE) 2021/1772 en consecuencia.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Queda derogado el artículo 1, apartado 2, de la Decisión de Ejecución (UE) 2021/1772.

Artículo 2

El artículo 4 de la Decisión de Ejecución (UE) 2021/1772 se sustituye por el texto siguiente:

«*Artículo 4*

La presente Decisión tendrá validez hasta el 27 de diciembre de 2031, salvo que se prorrogue de conformidad con el procedimiento indicado en el artículo 93, apartado 2, del Reglamento (UE) 2016/679.».

Artículo 3

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 19 de diciembre de 2025.

Por la Comisión
Michael MCGRATH
Miembro de la Comisión

([181]) Dictamen 26/2025 sobre el proyecto de Decisión de Ejecución de la Comisión Europea con arreglo al Reglamento (UE) 2016/679, relativo a la protección adecuada de los datos personales por parte del Reino Unido, disponible en el siguiente enlace [en inglés] https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.