II

(Actos no legislativos)

DECISIONES

REGLAMENTO 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

[notificada con el número C(2021) 4800]

(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) El Reglamento (UE) 2016/679 establece las normas que regulan la transferencia de datos personales desde los responsables o encargados del tratamiento en la Unión Europea (UE) a terceros países y organizaciones internacionales, en la medida en que tales transferencias se encuentren comprendidas dentro de su ámbito de aplicación. Las normas relativas a las transferencias internacionales de datos se establecen en el capítulo V de dicho Reglamento, en concreto en sus artículos 44 a 50. Si bien el flujo de datos personales hacia y desde países no pertenecientes a la Unión es esencial para la expansión de la cooperación internacional y el comercio transfronterizo, el nivel de protección de los datos personales en la UE no debe verse menoscabado por transferencias a terceros países ([2]).

(2) A tenor del artículo 45, apartado 3, del Reglamento (UE) 2016/679, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país o una organización internacional garantizan un nivel de protección adecuado. En virtud de esta condición, las transferencias de datos personales a un tercer país pueden producirse sin que sea necesario obtener ninguna autorización adicional, tal como establecen el artículo 45, apartado 1, y el considerando 103, de dicho Reglamento.

(3) Según lo especificado en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación ha de basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que contemple tanto las normas aplicables a los importadores de datos como las limitaciones y garantías en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «esencialmente equivalente» al ofrecido en la Unión Europea [considerando 104 del Reglamento (UE) 2016/679]. La norma con la que se evalúa el nivel de protección «equivalente en lo esencial» es la que establece la legislación de la Unión Europea, en concreto el Reglamento (UE) 2016/679, así como la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) ([3]). En este sentido, también son importantes las referencias sobre adecuación del Comité Europeo de Protección de Datos (CEPD) ([4]).

([1]) DO L 119 de 4.5.2016, p. 1.
([2]) Véase el considerando 101 del Reglamento (UE) 2016/679.
([3]) Véase, más recientemente, el asunto C-311/18, *Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems*, ECLI:EU:C:2020:559.
([4]) Referencias sobre adecuación del Comité Europeo de Protección de Datos, WP 254, rev. 01, disponible en el siguiente enlace: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Tal como ha precisado el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico ([5]). 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 ([6]). Por consiguiente, el nivel de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión. Se trata más bien de determinar si el sistema extranjero ofrece, en su conjunto y por la esencia de los derechos a la protección de los datos y su aplicación, fuerza ejecutiva y supervisión efectivas, el nivel de protección exigido ([7]).

(5) La Comisión ha analizado detenidamente el Derecho y la práctica del Reino Unido. A partir de las conclusiones desarrolladas en los considerandos 8 a 270, la Comisión concluye que el Reino Unido garantiza un nivel adecuado de protección para los datos personales transferidos dentro del ámbito de aplicación del Reglamento (UE) 2016/679 de la Unión Europea al Reino Unido.

(6) Esta conclusión no se refiere a 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 cuarto párrafo, del punto 1, del anexo 2 de la *Data Protection Act* del Reino Unido. La validez e interpretación de la exención de inmigración con arreglo al Derecho del Reino Unido no se ha resulto tras la decisión del Tribunal de Apelación de Inglaterra y Gales, de 26 de mayo de 2021. Si bien se reconoce que los derechos de los interesados pueden, en principio, restringirse con fines de control de la inmigración como «un aspecto importante del interés público», el Tribunal de Apelación ha concluido que la exención de inmigración es, en su forma actual, incompatible con el Derecho del Reino Unido, ya que la medida legislativa carece de disposiciones específicas que establezcan las garantías contempladas en el artículo 23, apartado 2, del Reglamento general de protección de datos del Reino Unido (RGPD del Reino Unido) ([8]). En estas condiciones, deben excluirse del ámbito de aplicación de la presente Decisión las transferencias de datos personales desde la Unión Europea al Reino Unido a las que se puede aplicar la exención de inmigración ([9]). Una vez que se resuelva la incompatibilidad con el Derecho del Reino Unido, se debe volver a evaluar la exención de inmigración, así como la necesidad de mantener la limitación del ámbito de aplicación de la presente Decisión.

(7) La presente Decisión no debe afectar a la aplicación directa del Reglamento (UE) 2016/679 a las organizaciones establecidas en el Reino Unido en las que se cumplan las condiciones relativas al ámbito territorial de dicho Reglamento, establecidas en su artículo 3.

2. **NORMAS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES**

2.1. **Marco constitucional**

(8) El Reino Unido es una democracia parlamentaria que tiene un monarca constitucional como jefe de Estado. Tiene un Parlamento soberano, que es supremo frente a todas las demás instituciones gubernamentales, un poder ejecutivo que se deriva del Parlamento y rinde cuentas ante él y un poder judicial independiente. El poder ejecutivo adquiere su autoridad de su capacidad para obtener la confianza de la Cámara de los Comunes electa y rinde cuentas ante ambas cámaras del Parlamento, que son responsables de escrutar al Gobierno y debatir y aprobar las leyes.

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

([6]) Maximillian Schrems/Data Protection Commissioner, apartado 74.

([7]) Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo, «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], disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=ES.

([8]) Tribunal de Apelación (Sala de lo Civil), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, apartados 53 a 56. El Tribunal de Apelación revocó la sentencia del Tribunal Superior de Justicia que había evaluado previamente la exención a la luz del Reglamento (UE) 2016/679 (en particular, su artículo 23) y la Carta de los Derechos Fundamentales de la Unión Europea y concluido que la exención era legal [*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562].

([9]) Las transferencias con fines de control de la inmigración en el Reino Unido pueden llevarse a cabo sobre la base de los mecanismos de transferencia previstos en los artículos 46 a 49 del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones aplicables.

(9) El Parlamento del Reino Unido ha delegado la responsabilidad al Parlamento de Escocia, el Parlamento de Gales (*Senedd Cymru*) y la Asamblea de Irlanda del Norte de legislar en Escocia, Gales e Irlanda del Norte sobre asuntos internos que el Parlamento del Reino Unido no se haya reservado para sí. Si bien la protección de datos es una cuestión reservada, es decir, que la misma legislación aplica en todo el país, se delegan otras áreas de política pertinentes para la presente Decisión. Por ejemplo, los sistemas de justicia penal, incluidas las autoridades policiales, de Escocia e Irlanda del Norte se delegan en el Parlamento de Escocia y la Asamblea de Irlanda del Norte, respectivamente. El Reino Unido no tiene una constitución codificada, en el sentido de un documento constitutivo afianzado. Los principios constitucionales del Reino Unido han surgido con el tiempo y proceden, en concreto, de la jurisprudencia y del consenso. Los tribunales han reconocido el valor constitucional de determinadas leyes parlamentarias, como la Carta Magna, la *Bill of Rights* (Declaración de Derechos) de 1689 y la *Human Rights Act* (Ley de Derechos Humanos) de 1998. A través del *common law*, las leyes parlamentarias mencionadas y determinados tratados internacionales, en especial el Convenio Europeo de Derechos Humanos, que el Reino Unido ratificó en 1951, se han desarrollado los derechos fundamentales de las personas como parte de la constitución. En 1987, el Reino Unido también ratificó el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ([10]).

(10) La *Human Rights Act* de 1998 incorpora los derechos recogidos en el Convenio Europeo de Derechos Humanos en el Derecho del Reino Unido. 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, interpretados según 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 ([11]). En concreto, en virtud del artículo 8 del Convenio, solo podrá haber injerencia de la autoridad pública en el ejercicio de este derecho en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

(11) En virtud de la *Human Rights Act* de 1998, cualquier acción de las autoridades públicas debe ser compatible con uno de los derechos del Convenio ([12]). Además, el Derecho primario y el subordinado deben interpretarse y aplicarse de manera compatible con los derechos del Convenio ([13]).

2.2. **El marco de protección de datos del Reino Unido**

(12) El Reino Unido se retiró de la Unión Europea el 31 de enero de 2020. En virtud del 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 ([14]), el Derecho de la Unión se aplicó en el Reino Unido durante el período transitorio hasta el 31 de diciembre de 2020. Antes de la retirada y durante el período transitorio, el marco legislativo sobre la protección de datos personales en el Reino Unido consistía en la legislación pertinente de la UE [en particular, el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([15])] y la legislación nacional, en particular, la *Data Protection Act* de 2018 (DPA de 2018) ([16]) que estableció 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 la Directiva transpuesta (UE) 2016/680.

([10]) Los principios del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal se aplicaron inicialmente en el Derecho del Reino Unido a través de la *Data Protection Act* (Ley de Protección de Datos) de 1984, que fue reemplazada por la *Data Protection Act* (DPA) de 1998, y posteriormente, a su vez, por la DPA de 2018 (como puede leerse en el Reglamento General de Protección de Datos del Reino Unido). Asimismo, el Reino Unido firmó en 2018 el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y, en la actualidad, trabaja en la ratificación del Convenio.

([11]) Artículos 6 y 8 del Convenio Europeo de Derechos Humanos (véase también el anexo 1 a la *Human Rights Act* de 1998).

([12]) Sección 6 de la *Human Rights Act* de 1998.

([13]) Sección 3 de la *Human Rights Act* de 1998.

([14]) 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 2019/C 384 I/01, XT/21054/2019/INIT (DO C 384I de 12.11.2019, p. 1), disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=ES.

([15]) 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), disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES.

([16]) *Data Protection Act* de 2018, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) A fin de preparar la retirada de la UE, el Gobierno del Reino Unido promulgó la *European Union (Withdrawal) Act* (Ley de Retirada de la Unión Europea) de 2018 ([17]), que incorpora la legislación de la Unión directamente aplicable al Derecho del Reino Unido ([18]). Este denominado «Derecho de la Unión conservado» incluye el Reglamento (UE) 2016/679 en su totalidad (incluidos sus considerandos) ([19]). De acuerdo con la *European Union (Withdrawal) Act*, los tribunales del Reino Unido debían interpretar el Derecho de la Unión conservado no modificado de conformidad con 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) ([20]).

(14) En virtud de la *European Union (Withdrawal) Act* de 2018, los ministros del Reino Unido están facultados para introducir una legislación secundaria, por medio de instrumentos jurídicos, para realizar las modificaciones necesarias en el Derecho de la Unión conservado como consecuencia de la retirada del Reino Unido de la UE. Hicieron uso de esa habilitación al adoptar el *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* o *DPPEC Regulations* [Reglamentos en materia de Protección de Datos, Privacidad y Comunicaciones Electrónicas (modificaciones, etc.) (salida de la UE) de 2019] ([21]). Dicha normativa 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 ([22]).

(15) En consecuencia, el marco jurídico sobre la protección de datos personales en el Reino Unido una vez finalizado el período transitorio consiste en:

— el RGPD del Reino Unido, incorporado al Derecho del Reino Unido en virtud de la *European Union (Withdrawal) Act* de 2018 y modificado por la normativa *DPPEC Regulations* ([23]), y

— la DPA de 2018 ([24]), en su versión modificada por la normativa DPPEC Regulations.

(16) Dado que el RGPD del Reino Unido se basa en la legislación de la Unión, las normas en materia de protección de datos en el Reino Unido reflejan fielmente en muchos aspectos las normas correspondientes aplicables dentro de la UE.

(17) Además de los poderes que la *European Union (Withdrawal) Act* de 2018 otorga al secretario de Estado, varias disposiciones de la DPA de 2018 confieren poderes al secretario de Estado para adoptar una legislación secundaria a fin de modificar ciertas disposiciones de dicha normativa o proporcionar normas complementarias y adicionales ([25]). Hasta el momento, el secretario de Estado solo ha ejercido sus poderes en virtud del artículo 137 de la DPA de 2018

([17]) *European Union Withdrawal Act* de 2018, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) La intención y el efecto de la *European Union (Withdrawal) Act* de 2018 es que toda la legislación directa de la Unión que se incorporó al Derecho del Reino Unido al final del período transitorio se incorpore efectivamente al Derecho del Reino Unido, de manera que tuviera un efecto inmediato en el Derecho de la UE antes del final del período transitorio. Véase la Sección 3 de la *European Union (Withdrawal) Act* de 2018.

([19]) Las notas explicativas a la *European Union (Withdrawal) Act* de 2018 especifican que: «Cuando la legislación se convierte en virtud de esta sección, es el texto de la propia legislación el que formará parte de la legislación nacional. Esto incluirá el texto completo de cualquier instrumento de la UE (incluidos sus considerandos)». [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]. Según la información proporcionada por las autoridades del Reino Unido, dado que los considerados no tienen el carácter de normas jurídicas vinculantes, no fue necesario modificarlos de la misma forma en que la normativa *DPPEC Regulations* (*The Data Protection, Privacy and Electronic Communications Regulations*) modificó los artículos del Reglamento (UE) 2016/679.

([20]) Sección 6 de la *European Union (Withdrawal) Act* de 2018.

([21]) La normativa *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations* de 2019 puede consultarse en el siguiente enlace: 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: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Estas modificaciones del Reglamento General de Protección de Datos del Reino Unido (RGPD del Reino) Unido y de la DPA de 2018 son fundamentalmente de carácter técnico, como la eliminación de referencias a los «Estados miembros» o un ajuste de la terminología; por ejemplo, sustituyendo las referencias al Reglamento (UE) 2016/679 por referencias al RGPD del Reino Unido. En algunos casos, se requirieron cambios para reflejar el contexto puramente nacional de las disposiciones; por ejemplo, con respecto a «quién» adopta «normas en materia de adecuación» a los efectos del marco legislativo de protección de datos del Reino Unido (véase la sección 17A de la DPA de 2018), esto es, el secretario de Estado en lugar de la Comisión Europea.

([23]) Anexo *Keeling* al Reglamento General de Protección de Datos del Reino Unido, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) Anexo *Keeling* a la *Data Protection Act* de 2018, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Tales poderes están contenidos, por ejemplo, en las secciones 16 (facultad para hacer, en situaciones específicas y limitadas, exenciones adicionales a disposiciones específicas del RGPD del Reino Unido), 17A (facultad para adoptar normas en materia de adecuación), 212 y 213 (facultad para dar inicio a una legislación y realizar una disposición transitoria) y 211 (facultad para realizar modificaciones menores y consiguientes) de la DPA de 2018.

para adoptar la normativa *Data Protection (Charges and Information) (Amendment) Regulations 2019* [Reglamentos en materia de Protección de Datos (tasas e información) (modificación) de 2019], que establece las circunstancias en las que los responsables del tratamiento deben pagar una tasa anual a la autoridad de protección de datos independiente del Reino Unido, la Oficina del Comisionado de Información del Reino Unido (ICO, por sus siglas en inglés).

(18) Por último, en los códigos de práctica y otras orientaciones aprobadas por la ICO se proporciona más orientación sobre la legislación en materia de protección de datos del Reino Unido. Esta orientación, aunque no es formalmente vinculante desde el punto de vista jurídico, tiene un peso interpretativo y demuestra cómo se aplica la legislación en materia de protección de datos y cómo la hace cumplir la ICO en la práctica. En concreto, las secciones 121 a 125 de la DPA de 2018 requieren que la ICO prepare códigos de práctica sobre intercambio de datos, comercialización directa, diseño adaptado a la edad y protección de datos y periodismo.

(19) En lo que respecta a su estructura y componentes principales, el marco jurídico del Reino Unido que se aplica a los datos transferidos en virtud de la presente Decisión es, por tanto, muy similar al que se aplica en la UE. Esto incluye el hecho de que dicho marco no solo se basa en obligaciones establecidas en el Derecho interno, a las que el Derecho de la Unión ha dado forma, sino también en obligaciones consagradas en el Derecho internacional, en concreto a través de la adhesión del Reino Unido al Convenio Europeo de Derechos Humanos (CEDH) y al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, así como su acatamiento de la jurisdicción del Tribunal Europeo de Derechos Humanos. Estas obligaciones derivadas de los instrumentos internacionales jurídicamente vinculantes son, por tanto, en especial en relación con la protección de datos personales, un elemento especialmente importante del marco jurídico evaluado en la presente Decisión.

2.3. **Ámbito de aplicación material y territorial**

(20) De manera similar al Reglamento (UE) 2016/679, el RGPD del Reino Unido se aplica al tratamiento de datos personales por medios automatizados total o parcialmente, o a otro tratamiento, si los datos personales forman parte de un fichero ([26]). Las definiciones de «datos personales», «interesado» y «tratamiento» del RGPD del Reino Unido son idénticas a las del Reglamento (UE) 2016/679 ([27]). Además, el RGPD del Reino Unido se aplica al tratamiento manual de datos personales no estructurados ([28]) en poder de ciertas autoridades públicas del Reino Unido ([29]), aunque los principios y derechos del RGPD del Reino Unido que no son pertinentes para tales datos personales no se aplican en las secciones 24 y 25 de la DPA de 2018. De manera similar a lo que establece el Reglamento (UE) 2016/679, el RGPD del Reino Unido no se aplica al tratamiento de datos personales por parte de un individuo en el curso de una actividad meramente personal o doméstica ([30]).

(21) El RGPD del Reino Unido extiende su alcance también al tratamiento en el curso de una actividad que, inmediatamente antes del final del período transitorio, quedaba fuera del ámbito de aplicación del Derecho de la Unión (por ejemplo, la seguridad nacional) ([31]), o entraba en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (Disposiciones específicas sobre la Política Exterior y de Seguridad Común) ([32]). Al igual que en el sistema de la UE, el RGPD del Reino Unido no se aplica al tratamiento de datos personales por parte de una autoridad competente para fines de prevención, investigación, detección o enjuiciamiento de infracciones

([26]) Artículo 2, apartados 1 y 5, del RGPD del Reino Unido.

([27]) Artículo 4, apartados 1 y 2, del RGPD del Reino Unido.

([28]) En el artículo 2, apartado 5, letra b), del RGPD del Reino Unido se define el tratamiento manual de datos personales no estructurados como el tratamiento de datos personales que no es el tratamiento de datos personales automatizado o estructurado.

([29]) El artículo 2, apartado 1 *bis*, del RGPD del Reino Unido establece la aplicación del Reglamento también al tratamiento manual de datos personales no estructurados en poder de una autoridad pública de libertad de información. La referencia a autoridades públicas de libertad de información significa cualquier autoridad pública según la definición de la *Freedom of Information Act* de 2000 (Ley de Libertad de Información), o cualquier autoridad pública escocesa según la definición de la *Freedom of Information Act (Scotland)* de 2002 (asp 13). Sección 21, apartado 5, de la DPA de 2018.

([30]) Artículo 2, apartado 2, letra a), del RGPD del Reino Unido.

([31]) Las actividades de seguridad nacional solo entran en el ámbito de aplicación del RGPD del Reino Unido en la medida en que no las lleve a cabo una autoridad competente a efectos de aplicación de la ley, en cuyo caso se aplica la parte 3 de la DPA de 2018, o bien que las lleve a cabo un servicio de inteligencia o se haga en su nombre, cuyas actividades quedan excluidas del ámbito de aplicación del RGPD del Reino Unido y están sujetas a la parte 4 de la DPA de 2018, de conformidad con el artículo 2, apartado 2, letra c), del RGPD del Reino Unido. Por ejemplo, las fuerzas del orden pueden realizar controles de seguridad de un empleado para garantizar que puede confiarse en él para acceder al material de seguridad nacional. A pesar de que la policía es una autoridad competente a efectos de aplicación de la ley, el tratamiento en cuestión no se realiza a tales efectos, por lo que en este caso aplicaría el RGPD del Reino Unido. Véase la sección H del *UK Explanatory Framework for Adequacy Discussions*: *National Security Data Protection and Investigatory Powers Framework* («Marco explicativo del Reino Unido para el debate sobre la adecuación: marco de poderes de investigación y protección de datos de seguridad nacional», documento en inglés), p. 8, en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Artículo 2, apartado 1, letras a) y b), del RGPD del Reino Unido.

penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y su prevención (los denominados «efectos de aplicación de la ley») [dicho tratamiento se rige, en cambio, por la parte 3 de la DPA de 2018, como es el caso de la Directiva (UE) 2016/680 en virtud del Derecho de la Unión], o el tratamiento de datos personales por parte de los servicios de inteligencia (el Servicio de Seguridad, el Servicio de Inteligencia Secreto y el Cuartel General de Comunicaciones del Gobierno), que recoge la parte 4 de la DPA de 2018 ([33]).

(22) El ámbito de aplicación territorial del RGPD del Reino Unido se describe en su artículo 3 ([34]) e incluye el tratamiento de datos personales (independientemente de dónde tenga lugar) en el contexto de las actividades de un establecimiento de un responsable o encargado del tratamiento en el Reino Unido, así como el tratamiento de datos personales de interesados que se encuentran en el Reino Unido, en que las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados o el seguimiento de su comportamiento ([35]). Esto refleja el enfoque adoptado en el artículo 3 del Reglamento (UE) 2016/679.

2.4. **Definiciones de datos personales y de los conceptos de «responsable» o «encargado»**

(23) Las definiciones de «datos personales», «tratamiento», «responsable» y «encargado», así como la definición de «seudonimización», que establece el Reglamento (UE) 2016/679, se han conservado sin modificaciones sustanciales en el RGPD del Reino Unido ([36]). Además, en el artículo 9, apartado 1, del RGPD del Reino Unido se definen las categorías especiales de datos de la misma manera que en el Reglamento (UE) 2016/679 («datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física»). Por su parte, la sección 205 de la DPA de 2018 establece la definición de «datos biométricos» ([37]), «datos relativos a la salud» ([38]) y «datos genéticos» ([39]).

2.5. **Garantías, derechos y obligaciones**

2.5.1. *Licitud y lealtad del tratamiento*

(24) Los datos personales deben tratarse de manera lícita y leal.

(25) En el Derecho del Reino Unido, los principios de licitud, lealtad y transparencia y los fundamentos de la licitud del tratamiento se garantizan a través del artículo 5, apartado 1, letra a), y el artículo 6, apartado 1, del RGPD del Reino Unido, que son idénticos a las disposiciones correspondientes en el Reglamento (UE) 2016/679 ([40]). La sección 8 de

([33]) Artículo 2, apartado 2, letras b) y c), del RGPD del Reino Unido.

([34]) El mismo ámbito de aplicación territorial aplica al tratamiento de datos personales en virtud de la parte 2 de la DPA de 2018, que complementa el RGPD del Reino Unido (sección 207, apartado 1 *bis*).

([35]) Esto implica, en particular, que la DPA de 2018 y, por lo tanto, esta decisión no se aplica a las dependencias de la Corona (Jersey, Guernsey y la Isla de Man) y los territorios de ultramar del Reino Unido, como, por ejemplo, las Islas Malvinas y el territorio de Gibraltar.

([36]) Artículo 4, apartados 1, 2, 5, 7 y 8, del RGPD del Reino Unido.

([37]) «Datos biométricos» son datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

([38]) «Datos relativos a la salud» son datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

([39]) «Datos genéticos» son datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

([40]) De conformidad con el artículo 6, apartado 1, del RGPD del Reino Unido, el tratamiento solo es lícito si y en la medida en que: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

la DPA de 2018 complementa el artículo 6, apartado 1, letra e), al establecer que el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra e), del RGPD del Reino Unido (necesario para el desempeño de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento), incluye el tratamiento de datos personales que son necesarios para la administración de justicia, el ejercicio de una función de cualquiera de las cámaras del Parlamento británico, el ejercicio de una función conferida a una persona por una disposición o por el Estado de Derecho, el ejercicio de una función de la Corona, un cargo del Gobierno del Reino Unido o un departamento gubernamental, o una actividad que apoye o promueva el compromiso democrático.

(26) En relación con el consentimiento (uno de los fundamentos para el tratamiento lícito), el RGPD del Reino Unido también conserva las condiciones previstas en el artículo 7 del Reglamento (UE) 2016/679 sin modificaciones, es decir, que el responsable deberá ser capaz de demostrar que el interesado dio su consentimiento, que deberá presentarse una solicitud de consentimiento por escrito utilizando un lenguaje claro y sencillo, que el interesado tendrá derecho a retirar el consentimiento en cualquier momento y, al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta si la ejecución de un contrato se supedita al consentimiento para el tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. Además, de conformidad con el artículo 8 del RGPD del Reino Unido, en el contexto de la prestación de servicios de la sociedad de la información, el consentimiento de un niño solo es lícito cuando tiene, al menos, trece años. Esto se enmarca dentro del intervalo de edad establecido en el artículo 8 del Reglamento (UE) 2016/679.

2.5.2. *Tratamiento de categorías especiales de datos personales*

(27) Deben preverse garantías específicas cuando se estén tratando «categorías especiales» de datos.

(28) El RGPD del Reino Unido y la DPA de 2018 contienen normas específicas relativas al tratamiento de categorías especiales de datos personales, que se definen en el artículo 9, apartado 1, del RGPD del Reino Unido de la misma forma que en el Reglamento (UE) 2016/679 (véase el considerando 23). De conformidad con el artículo 9 del RGPD del Reino Unido, el tratamiento de categorías especiales de datos personales está, en principio, prohibido salvo que se aplique una excepción específica.

(29) Dichas excepciones (que se enumeran en el artículo 9, apartados 2 y 3, del RGPD del Reino Unido) no presentan ningún cambio sustancial a las recogidas en el artículo 9, apartados 2 y 3, del Reglamento (UE) 2016/679. Salvo que el interesado diera su consentimiento explícito para el tratamiento de dichos datos personales, el tratamiento de categorías especiales de datos personales solo está permitido en circunstancias específicas y limitadas. En la mayoría de los casos, el tratamiento de datos sensibles debe ser necesario para un propósito específico definido en la disposición pertinente [véase el artículo 9, apartado 2, letras b), c), f), g), h), i) y j)].

(30) Además, cuando una excepción en virtud del artículo 9, apartado 2, del RGPD del Reino Unido requiera una autorización por ley o remita al interés público, la sección 10 de la DPA de 2018 junto con el anexo 1 de dicha Ley especifican con más detalle las condiciones que deben cumplirse para que pueda confiarse en las excepciones. Por ejemplo, en el caso del tratamiento de datos sensibles para proteger la «salud pública» [artículo 9, apartado 2, letra i), del RGPD del Reino Unido], la parte 1, párrafo tercero, letra b), del anexo 1 requiere que, además de la evaluación de la necesidad, dicho tratamiento se lleve a cabo «por parte de o bajo la responsabilidad de un profesional de la salud» o «por parte de otra persona que tiene el deber de confidencialidad en virtud de una disposición o del Estado de Derecho», especialmente en virtud del deber de confidencialidad bien establecido del *common law*.

(31) Cuando se traten datos sensibles por razones de un interés público esencial [artículo 9, apartado 2, letra g), del RGPD del Reino Unido], la parte 2, del anexo 1, de la DPA de 2018 proporciona una lista exhaustiva de fines que pueden considerarse de interés público esencial y, para cada uno de dichos fines, establece condiciones adicionales específicas. Por ejemplo, la promoción de la diversidad racial y étnica en los niveles superiores de las organizaciones se reconoce como un interés público esencial. El tratamiento de datos sensibles para este propósito específico está sujeto a requisitos bien definidos, incluido que el tratamiento se lleve a cabo como parte de un proceso de identificación de personas adecuadas para ocupar puestos de dirección, que sea necesario para promover la diversidad racial y étnica y que no sea probable que cause un daño o una angustia importantes al interesado.

(32) La sección 11, apartado 1, de la DPA de 2018 establece las condiciones para que los datos personales se traten en las circunstancias descritas en el artículo 9, apartado 3, del RGPD del Reino Unido vinculadas a la obligación de secreto. Esto incluye circunstancias en las que el tratamiento lo realiza un profesional de la salud o un profesional del ámbito social, o bajo su responsabilidad, o bien lo realiza otra persona que, en las circunstancias, tiene el deber de confidencialidad en virtud de una disposición o del Estado de Derecho.

(33) Además, varias de las excepciones recogidas en el artículo 9, apartado 2, RGPD del Reino Unido requieren garantías adecuadas y específicas para su uso. Las condiciones para el tratamiento previstas en el anexo 1 de la DPA de 2018 establecen distintas garantías en función de la naturaleza del tratamiento y del nivel de riesgo para los derechos y las libertades de los interesados. El anexo 1 establece las condiciones para cada una de las situaciones del tratamiento.

(34) En algunos casos, la DPA de 2018 regula y limita el tipo de datos sensibles que pueden tratarse para el cumplimiento de una base jurídica determinada. Por ejemplo, el párrafo octavo del anexo 1 autoriza el tratamiento de datos sensibles con el fin de promover la igualdad de oportunidades o de trato. Esta condición de tratamiento solo puede utilizarse si los datos revelan un origen racial o étnico, convicciones religiosas o filosóficas, orientación sexual o si se trata de datos relativos a la salud.

(35) En otros casos, la DPA de 2018 limita el tipo de responsable del tratamiento que puede hacer uso de la condición de tratamiento. Por ejemplo, el párrafo vigesimotercero del anexo 1 prevé el tratamiento de datos sensibles en relación con las respuestas de los representantes electos al público. Esta condición de tratamiento solo puede utilizarse cuando el responsable del tratamiento es el representante electo o cuando actúa bajo su autoridad.

(36) En otros casos, la DPA de 2018 establece límites en las categorías de interesados para la condición de tratamiento que pueden utilizarse. Por ejemplo, el párrafo vigesimoprimero del anexo 1 regula el tratamiento de datos sensibles para los sistemas de previsión para la jubilación. Esta condición solo puede utilizarse si el interesado en cuestión es un hermano, progenitor, abuelo/a o bisabuelo/a del afiliado al sistema de previsión para la jubilación.

(37) Además, el responsable del tratamiento, cuando se base en las excepciones recogidas en el artículo 9, apartado 2, del RGPD del Reino Unido que se especifican con más detalle en la sección 10 de la DPA de 2018 junto con el anexo 1 de la DPA, debe redactar en la mayoría de los casos un «documento reglamentario adecuado». Este documento debe describir los procedimientos del responsable para garantizar el cumplimiento de los principios del artículo 5 del RGPD del Reino Unido. Asimismo, debe establecer políticas para la conservación y la supresión de datos, con una indicación del período de conservación probable. Los responsables deben revisar y actualizar este documento según corresponda. El responsable debe conservar el documento reglamentario por un plazo de seis meses después de que finalice el tratamiento y debe ponerlo a disposición de la ICO, previa solicitud ([41]).

(38) De conformidad con el apartado 41, del anexo 1, de la DPA de 2018, el documento reglamentario debe ir siempre acompañado de un registro de las actividades de tratamiento a mayor escala. Este registro debe realizar un seguimiento de los compromisos incluidos en el documento reglamentario, es decir, de si los datos se conservan o se suprimen de acuerdo con las políticas. Si no se están respetando las políticas, entonces el registro debe dar cuenta de los motivos. Asimismo, el registro debe describir cómo el tratamiento cumple con el artículo 6 del RGPD del Reino Unido (licitud del tratamiento) y la condición específica recogida en el anexo 1 de la DPA de 2018, en la que se basa.

(39) Por último, al igual que el Reglamento (UE) 2016/679, el RGPD del Reino Unido también ofrece unas garantías generales para ciertas operaciones de tratamiento de categorías especiales de datos. El artículo 35 del RGPD del Reino Unido requiere una evaluación de impacto relativa a la protección de datos cuando se tratan categorías especiales de datos a gran escala. De conformidad con el artículo 37 del RGPD del Reino Unido, un responsable o encargado del tratamiento debe nombrar un delegado de protección de datos cuyas actividades principales consisten en el tratamiento a gran escala de categorías especiales de datos.

(40) Con respecto a los datos personales que están relacionados con condenas e infracciones penales, el artículo 10 del RGPD del Reino Unido es idéntico al artículo 10 del Reglamento (UE) 2016/679. Permite el tratamiento de datos personales relacionados con condenas e infracciones penales solo bajo la supervisión de las autoridades públicas o cuando el tratamiento lo autorice el Derecho interno que establezca garantías adecuadas para los derechos y libertades de los interesados.

(41) Cuando el tratamiento de datos relacionados con condenas e infracciones penales no se realice bajo la supervisión de las autoridades públicas, la sección 10, apartado 5, de la DPA de 2018 establece que dicho tratamiento solo puede realizarse para las finalidades específicas/en las situaciones específicas establecidas en las partes 1, 2 y 3, del anexo 1, de la DPA de 2018 y su subordinación a los requisitos específicos que se establecen para cada una de estas finalidades/situaciones. Por ejemplo, el tratamiento de datos relacionados con condenas penales pueden realizarlo entidades sin ánimo de lucro, siempre que dicho tratamiento se realice a) en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, y b) siempre que: i) el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y ii) los datos personales no se comuniquen al exterior sin el consentimiento de los interesados.

([41]) Apartados 38 a 40, del anexo 1, de la DPA de 2018.

(42) Además, la parte 3, del anexo 1, de la DPA de 2018 establece circunstancias adicionales en las que pueden emplearse datos relacionados con condenas penales, que corresponden a los fundamentos jurídicos del tratamiento de datos sensibles recogidos en el artículo 9, apartado 2, del Reglamento (UE) 2016/679 y el RGPD del Reino Unido (por ejemplo, consentimiento del interesado; intereses vitales de un individuo en caso de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; si el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; si el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones; etc.).

2.5.3. *Limitación de la finalidad, exactitud, minimización de los datos, limitación del plazo de conservación y seguridad de los datos*

(43) Los datos personales deben tratarse con una finalidad específica y, posteriormente, solo deben utilizarse en la medida en que ello no sea incompatible con la finalidad del tratamiento.

(44) Este principio se recoge en el artículo 5, apartado 1, letra b), del Reglamento (UE) 2016/679 y se ha mantenido sin cambios en el artículo 5, apartado 1, letra b), del RGPD del Reino Unido. Las condiciones sobre un tratamiento compatible adicional de conformidad con el artículo 6, apartado 4, del Reglamento (UE) 2016/679 también se han mantenido sin modificaciones sustanciales en el artículo 6, apartado 4, letras a) a e), del RGPD del Reino Unido.

(45) Por otro lado, los datos deberán ser exactos y, en caso necesario, se mantendrán actualizados. También deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados y, en principio, no deben conservarse más tiempo del necesario en relación con los fines para los que se tratan los datos personales.

(46) En el artículo 5, apartado 1, letras c) a e), del Reglamento (UE) 2016/679 se establecen los principios de minimización de los datos, exactitud y limitación del plazo de conservación, y se mantienen sin modificaciones en el artículo 5, apartado 1, letras c) a e), del RGPD del Reino Unido.

(47) Los datos personales deben también ser tratados de modo que se garantice su seguridad, incluida la protección contra todo tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. A tal fin, los operadores económicos deben adoptar las medidas técnicas u organizativas apropiadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta el estado de la técnica y los costes relacionados.

(48) La seguridad de los datos está consagrada en el Derecho del Reino Unido a través del principio de integridad y confidencialidad en el artículo 5, apartado 1, letra f), del RGPD del Reino Unido y en el artículo 32 del mismo Reglamento, relativo a la seguridad del tratamiento. Estas disposiciones son idénticas a las disposiciones correspondientes del Reglamento (UE) 2016/679. Además, el RGPD del Reino Unido requiere, en virtud de las mismas condiciones que las establecidas en los artículos 33 y 34 del Reglamento (UE) 2016/679, la notificación de una violación de la seguridad de los datos personales a la autoridad de control (artículo 33 del RGPD del Reino Unido) y la comunicación de una violación de la seguridad de los datos personales al interesado (artículo 34 del RGPD del Reino Unido).

2.5.4. *Transparencia*

(49) Los interesados deben ser informados de las principales características del tratamiento de sus datos personales.

(50) Esta condición se garantiza en los artículos 13 y 14 del RGPD del Reino Unido que, además de un principio general de transparencia, establece normas relativas a la información que debe proporcionarse al interesado ([42]). El RGPD del Reino Unido no introduce ninguna modificación sustancial a estas normas en comparación con los artículos correspondientes del Reglamento (UE) 2016/679. Sin embargo, al igual que en el Reglamento (UE) 2016/679, los requisitos de transparencia de dichos artículos están sujetos a varias excepciones que se establecen en la DPA de 2018 (véanse los considerandos 55 a 72).

([42]) En el artículo 13, apartado 1, letra f) y artículo 14, apartado 1, letra f), del RGPD del Reino Unido las referencias a las decisiones de adecuación de la Comisión se han sustituido por referencias a un instrumento equivalente del Reino Unido, es decir, las normas en materia de adecuación que establece la DPA de 2018. Además, en el artículo 14, apartado 5, letras c) y d), del mismo Reglamento las referencias al Derecho de la Unión o de los Estados miembros se han sustituido por una referencia al Derecho interno (como ejemplos de dicho Derecho interno que pueden incluirse en el artículo 14, apartado 5, letra c), el Reino Unido mencionó la sección 7 de la *Scrap Metal Dealers Act* (Ley de comerciantes de chatarra) de 2013 que establece normas para el registro de licencias de chatarra, o la parte 35 de la *Companies Act* (Ley de sociedades) de 2006 que establece las reglas para el registro mercantil. Del mismo modo, un ejemplo de Derecho interno que puede incluirse en el ámbito de aplicación del artículo 14, apartado 5, letra d), podría consistir en legislación que establezca normas sobre el derecho profesional u obligaciones reflejadas en contratos de trabajo o en el deber de confidencialidad del *common law* (como los datos personales tratados por profesionales de la salud, recursos humanos, trabajadores sociales, etc.).

2.5.5. *Derechos individuales*

(51) Los interesados deben tener ciertos derechos que puedan hacer valer 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. Al mismo tiempo, estos derechos pueden estar sujetos a limitaciones, en la medida en que dichas limitaciones sean necesarias y proporcionadas para salvaguardar la seguridad pública u otros objetivos importantes de interés público general.

2.5.5.1. Derechos sustantivos

(52) El RGPD del Reino Unido otorga a las personas los mismos derechos exigibles que el Reglamento (UE) 2016/679. Las disposiciones que garantizan los derechos de las personas se han mantenido sin cambios sustanciales en el RGPD del Reino Unido.

(53) Estos derechos incluyen el derecho de acceso del interesado (artículo 15 del RGPD del Reino Unido), el derecho de rectificación (artículo 16 del RGPD del Reino Unido), el derecho de supresión (artículo 17 del RGPD del Reino Unido), el derecho a la limitación del tratamiento (artículo 18 del RGPD del Reino Unido), la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento (artículo 19 del RGPD del Reino Unido), el derecho a la portabilidad de los datos (artículo 20 del RGPD del Reino Unido) y el derecho de oposición (artículo 21 del RGPD del Reino Unido) ([43]). Este último incluye también el derecho del interesado de oponerse al tratamiento de sus datos personales con fines de mercadotecnia directa, que se recoge en el artículo 21, apartados 2 y 3, del Reglamento (UE) 2016/679. Además, de conformidad con la sección 122 de la DPA de 2018, la ICO debe preparar un código de prácticas en relación con el ejercicio de la mercadotecnia directa, de acuerdo con los requisitos de la legislación en materia de protección de datos [y el Reglamento sobre la privacidad y las comunicaciones electrónicas (Directiva CE) de 2003] y otras orientaciones para promover las buenas prácticas en relación con la mercadotecnia directa que la ICO considere apropiadas. La ICO está desarrollando en estos momentos el código sobre mercadotecnia directa ([44]).

(54) Según lo dispuesto en el artículo 22 del Reglamento (UE) 2016/679, el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en él o le afecte significativamente de modo similar, también se ha mantenido en el RGPD del Reino Unido sin cambios sustanciales. Sin embargo, se ha añadido un nuevo párrafo 3A para indicar que la sección 14 de la DPA de 2018 establece garantías para los derechos, libertades e intereses legítimos de los interesados cuando el tratamiento se realiza de conformidad con el artículo 22, apartado 2, letra b), del RGPD del Reino Unido. Esto solo aplica cuando la base de dicha decisión es una autorización o requisito en virtud del Derecho del Reino Unido, y no aplica cuando la decisión es necesaria en virtud de un contrato o se toma con el consentimiento explícito del interesado. En los casos en los que se aplica la sección 14 de la DPA de 2018, el responsable debe, tan pronto como sea razonablemente posible, notificar por escrito al interesado de que se ha tomado una decisión basada únicamente en el tratamiento automatizado. El interesado tiene derecho a solicitar, en el plazo de un mes a partir de la recepción de la notificación, que el responsable reconsidere la decisión o tome una nueva decisión que no se base únicamente en el tratamiento automatizado. El secretario de Estado está facultado para adoptar garantías adicionales en lo que respecta a las decisiones automatizadas. Esta facultad no se ha ejercido todavía.

2.5.5.2. Limitaciones a los derechos individuales

(55) La DPA de 2018 establece varias limitaciones a los derechos individuales dentro del marco del artículo 23 del RGPD del Reino Unido. En dicho marco no se introducen limitaciones en relación con el derecho de oponerse a la mercadotecnia directa según lo dispuesto en el artículo 21, apartados 2 y 3, del RGPD del Reino Unido, o al derecho a no ser objeto de decisiones automatizadas según lo dispuesto en el artículo 22 del RGPD del Reino Unido.

(56) En los anexos 2 a 4 de la DPA de 2018 se definen las limitaciones en detalle. Las autoridades del Reino Unido explicaron que se rigen por dos principios: el principio de especificidad (adoptando un enfoque muy específico y dividiendo las limitaciones más generales en varias disposiciones más específicas) y el principio de condicionalidad (cada disposición se complementa con garantías en forma de limitaciones o condiciones para evitar abusos) ([45]).

([43]) En el artículo 17, apartado 1, letra e), y apartado 3, letra b), del RGPD del Reino Unido las referencias al Derecho de la Unión o los Estados miembros se han sustituido por una referencia al Derecho interno; como ejemplos de dicho Derecho interno que se incluyen en el artículo 17, apartado 1, letra e), el Reino Unido mencionó la normativa *Education (Pupil Information) (England) Regulations* [Reglamento de educación (información del alumno) (Inglaterra)] de 2006, que requiere que los nombres de los alumnos se supriman de los registros escolares una vez que hayan dejado la escuela, o la sección 34F de la *Medical Act* (Ley médica) de 1983 que establece las normas sobre la supresión de nombres del registro del médico de atención primaria y del registro del especialista.

([44]) El borrador del código de prácticas puede encontrarse en el siguiente enlace: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Sección E del *UK Explanatory Framework for Adequacy Discussions* («Marco explicativo del Reino Unido para el debate sobre la adecuación»): p. 1, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Las limitaciones que se describen en el artículo 23, apartado 1, del RGPD del Reino Unido están pensadas para garantizar que solo se apliquen en circunstancias específicas cuando sea necesario en una sociedad democrática y para que sean proporcionadas al fin legítimo que persiguen. Además, de acuerdo con la jurisprudencia establecida sobre la interpretación de las limitaciones, solo puede aplicarse una exención del régimen de protección de datos en casos particulares y cuando resulte necesario y proporcionado para ello ([46]). Por otro lado, se exige que la evaluación de la necesidad sea «estricta y que requiera que cualquier injerencia en los derechos del sujeto sea proporcional a la gravedad de la amenaza al interés público. Por tanto, el ejercicio implica un análisis de proporcionalidad clásico» ([47]).

(58) Los fines que persiguen estas limitaciones corresponden a los enumerados en el artículo 23 del Reglamento (UE) 2016/679, salvo las limitaciones de seguridad nacional y defensa que, en cambio, regula el artículo 26 de la DPA de 2018, pero que están sujetas a los mismos principios de proporcionalidad y necesidad (véanse los considerandos 63 a 66).

(59) Algunas de las limitaciones, por ejemplo, las que se relacionan con la prevención o detección de la delincuencia, la detención o el enjuiciamiento de los delincuentes, y con la evaluación o recaudación de derechos e impuestos ([48]), autorizan limitaciones a todos los derechos individuales y obligaciones de transparencia (salvo los derechos que se recogen en el artículo 21, apartado 2, y el artículo 22). El alcance de otras limitaciones atañe únicamente a las obligaciones de transparencia y los derechos de acceso, como las limitaciones relacionadas con la prerrogativa de confidencialidad ([49]), el derecho a la libertad ante el requisito de proporcionar información que conduciría a la autoincriminación ([50]), y la financiación corporativa, en particular la prevención de las operaciones con información privilegiada ([51]). Pocas de las limitaciones permiten una restricción a la obligación del responsable del tratamiento de comunicar una violación de la seguridad de los datos al interesado y a los principios de limitación de la finalidad y licitud, lealtad y transparencia del tratamiento ([52]).

(60) Algunas de las limitaciones se aplican automáticamente «en su totalidad» a un cierto tipo de tratamiento de datos personales (por ejemplo, la aplicación de las obligaciones de transparencia y derechos individuales se excluye cuando los datos personales se tratan con el fin de evaluar la idoneidad de una persona para una función jurisdiccional o cuando los datos personales los trata un tribunal o individuo que actúa en el ejercicio de su función judicial).

(61) Sin embargo, en la mayoría de los casos, el apartado pertinente del anexo 2 de la DPA de 2018 especifica que la limitación se aplica solo cuando (y en la medida en que) la aplicación de las disposiciones «podría perjudicar» el objetivo legítimo perseguido por dicha limitación: por ejemplo, las disposiciones enumeradas en el RGPD del Reino Unido no se aplican a los datos personales tratados para la prevención o detección de la delincuencia, la detención o el enjuiciamiento de los delincuentes, o la evaluación o recaudación de derechos e impuestos «en la medida en que la aplicación de esas disposiciones podría perjudicar» cualquiera de estas cuestiones ([53]).

(62) Los tribunales del Reino Unido han interpretado reiteradamente que la apreciación «podría perjudicar» representa «una posibilidad muy significativa y relevante de perjuicio para los intereses públicos identificados» ([54]). Por consiguiente, una restricción sujeta al criterio del perjuicio real y concreto solo puede invocarse si, y en la medida en que exista, una posibilidad muy significativa y relevante de que la concesión de un determinado derecho perjudique el interés público en juego. Corresponde al responsable del tratamiento evaluar caso por caso si se cumplen estas condiciones ([55]).

(63) Además de las restricciones que recoge el anexo 2 de la DPA de 2018, la sección 26 de la DPA ofrece una exención que puede aplicarse a determinadas disposiciones del RGPD del Reino Unido y de la propia DPA cuando esa exención es necesaria a fin de salvaguardar la seguridad nacional o con fines de defensa. Esta exención se aplica a los

([46]) *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.

([47]) *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), apartado 43. En relación con esto, véase también *Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), apartado 80.

([48]) Apartado 2, del anexo 2, de la DPA de 2018.

([49]) Apartado 19, del anexo 2, de la DPA de 2018.

([50]) Apartado 20, del anexo 2, de la DPA de 2018.

([51]) Apartado 21, del anexo 2, de la DPA de 2018.

([52]) Por ejemplo, solo se permiten restricciones al derecho a la notificación de una violación de la seguridad de los datos en relación con la delincuencia y la fiscalidad (apartado 2, del anexo 2, de la DPA de 2018), el privilegio parlamentario (apartado 13, del anexo 2, de la DPA de 2018) y el tratamiento para fines de expresión académica, artística o literaria (apartado 26, del anexo 2, de la DPA de 2018).

([53]) Apartado 2, del anexo 2, de la DPA de 2018.

([54]) *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), apartado 100, y *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), apartado 43.

([55]) *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, apartado 31.

principios de protección de datos (salvo el principio de licitud), las obligaciones de transparencia, los derechos del interesado, la obligación de notificar una violación de la seguridad de los datos, las normas sobre transferencias internacionales, algunos de los deberes y poderes de la ICO y las reglas sobre recursos, responsabilidades y sanciones, salvo la disposición sobre las condiciones generales para imponer multas administrativas establecidas en el artículo 83 del RGPD del Reino Unido y la disposición sobre sanciones en el artículo 84 del RGPD. Además, la sección 28 de la DPA de 2018 modifica la aplicación del artículo 9, apartado 1 para permitir el tratamiento de categorías especiales de datos recogidas en el artículo 9, apartado 1, del RGPD del Reino Unido en la medida en que el tratamiento se realice para salvaguardar la seguridad nacional o para fines de defensa, y con las garantías adecuadas para los derechos y libertades de los interesados ([56]).

(64) La exención solo puede aplicarse en la medida en que sea necesaria para salvaguardar la seguridad nacional o la defensa. Como también ocurre con las demás exenciones previstas por la DPA de 2018, el responsable del tratamiento debe considerarla y acogerse a ella caso por caso. Además, cualquier aplicación de la exención debe cumplir con las normas sobre derechos humanos (amparadas por la *Human Rights Act* de 1998), según las cuales cualquier injerencia en los derechos a la privacidad debe ser necesaria y proporcionada en una sociedad democrática ([57]).

(65) Esta interpretación de la exención es confirmada por la ICO que ha emitido una guía detallada sobre la aplicación de la exención de seguridad nacional y defensa, dejando claro que debe ser considerada y aplicada por el controlador caso por caso ([58]). En particular, la guía hace hincapié en que «no es una exención general» y que, para invocarla, «no es suficiente que los datos se traten con fines de seguridad nacional». Por el contrario, el responsable del tratamiento que se acoja a ella debe «demostrar que existe una posibilidad real de que haya un efecto adverso en la seguridad nacional» y, cuando proceda se espera que «aporte [a la ICO] pruebas de por qué utilizó esta exención». La guía contiene una lista de comprobación y una serie de ejemplos para aclarar las condiciones en las que se puede invocar dicha exención.

(66) Por lo tanto, el hecho de que los datos se traten con fines de seguridad nacional o defensa no es suficiente por sí solo para la aplicación de la exención. En la práctica, un responsable del tratamiento debe considerar las consecuencias reales para la seguridad nacional si tuviera que cumplir con la disposición específica de protección de datos. La exención solo puede aplicarse a aquellas disposiciones concretas para las que se haya determinado que, en efecto, plantean el riesgo y debe aplicarse de la manera más restrictiva posible ([59]).

(67) El Tribunal de Información confirmó este planteamiento ([60]). En el asunto *Baker v Secretary of State for the Home Department* («*Baker v Secretary of State*»), se determinó que era ilícito aplicar la exención de seguridad nacional como exención general a las solicitudes de acceso recibidas por parte de los servicios de inteligencia. En su lugar, la exención debía aplicarse caso por caso, valorando cada solicitud sobre la base de su fundamento y teniendo en cuenta el derecho de las personas al respeto de su vida privada ([61]).

([56]) Según la información proporcionada por las autoridades del Reino Unido, cuando el tratamiento se realice en el contexto de la seguridad nacional, los responsables aplicarán normalmente garantías y medidas de seguridad mejoradas al mismo, poniendo de manifiesto la naturaleza sensible del tratamiento. Las garantías adecuadas dependerán de los riesgos que plantee el tratamiento que se esté realizando. Estas podrían incluir restricciones de acceso a los datos para que solo puedan acceder las personas autorizadas con la habilitación de seguridad adecuada, restricciones estrictas para el intercambio de datos y la aplicación del más alto nivel de seguridad a los procedimientos de conservación y manejo.

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

([58]) Véase la guía de la ICO sobre la excepción de seguridad y defensa nacional, disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) Según un ejemplo facilitado por las autoridades del Reino Unido, si un presunto terrorista que está sometido a una investigación activa por parte del MI5 hiciera una solicitud de acceso al Home Office (Ministerio del Interior) (por ejemplo, porque está involucrado en un litigio con este organismo en cuestiones de inmigración), sería necesario evitar una comunicación al interesado de cualquier dato que el MI5 pueda haber compartido con el Home Office en relación con investigaciones en curso que podrían perjudicar fuentes, métodos o técnicas sensibles o conducir a un aumento de la amenaza planteada por dicho individuo. En tales circunstancias, es probable que se alcance el umbral para aplicar la exención recogida en la sección 26 y que se requiera una exención de comunicación de la información para salvaguardar la seguridad nacional. Sin embargo, si el Home Office también hubiera tenido datos personales sobre la persona que no estaban relacionados con la investigación del MI5 y esa información hubiera podido proporcionarse sin riesgo de daño a la seguridad nacional, entonces no habría podido aplicarse la exención de seguridad nacional al considerar la comunicación de información al individuo. La ICO está preparando en estos momentos una guía sobre cómo los responsables del tratamiento deben abordar el uso de la exención de la sección 26. Se espera que la guía se publique a finales de marzo de 2021.

([60]) El Tribunal de Información se estableció para atender los recursos relativos a la protección de datos en virtud de la *Data Protection Act* de 1984. En 2010 este Tribunal pasó a formar parte del Tribunal de Primera Instancia de lo Contencioso-Administrativo (Sala de Asuntos Generales), como parte de la reforma del sistema de tribunales del Reino Unido.

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

2.5.6. *Limitaciones para los datos personales tratados con fines periodísticos, artísticos, académicos y literarios, así como con fines de archivo e investigación*

(68) El artículo 85, apartado 2, del RGPD del Reino Unido permite que los datos personales tratados con fines periodísticos, artísticos, académicos y literarios estén exentos de varias disposiciones del propio RGPD. La parte 5, del anexo 2, de la DPA de 2018 establece las exenciones del tratamiento para estos fines. Establece exenciones de los principios de protección de datos (excepto el principio de integridad y confidencialidad), los fundamentos jurídicos para el tratamiento (incluidas categorías especiales de datos y datos relacionados con condenas penales, etc.), las condiciones para el consentimiento, las obligaciones de transparencia, los derechos de los interesados, la obligación de notificación de violaciones de la seguridad de los datos, y el requisito de consultar a la ICO antes del tratamiento de alto riesgo, y las normas sobre transferencias internacionales ([62]). En este sentido, el RGPD del Reino Unido no difiere de forma importante del Reglamento (UE) 2016/679, que en su artículo 85 también prevé la posibilidad de eximir el tratamiento realizado con fines periodísticos y fines de expresión académica, artística o literaria de una serie de requisitos del propio Reglamento. Las disposiciones de la DPA de 2018, en especial la parte 5, del anexo 2, son compatibles con el RGPD del Reino Unido.

(69) La ponderación básica que debe realizarse en virtud del artículo 85 del RGPD del Reino Unido se refiere a si una exención a las normas de protección de datos mencionadas en el considerando 68 es «necesaria para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información» ([63]). De conformidad con la parte 5, párrafo vigesimosexto, puntos 2 y 3, del anexo 2, de la DPA de 2018, el Reino Unido aplica una evaluación de «creencia razonable» para lograr el equilibrio necesario. Para que pueda justificarse una exención, el responsable del tratamiento debe creer razonablemente que i) la publicación es de interés público; y ii) que la aplicación de la disposición pertinente del Reglamento (UE) 2016/679 sería incompatible con fines periodísticos, artísticos, académicos o literarios. Tal como confirma la jurisprudencia ([64]), la evaluación de la «creencia razonable» tiene un componente tanto subjetivo como objetivo: no basta con que el responsable del tratamiento demuestre que él/ella mismo/a creía que el cumplimiento era incompatible. Su creencia debe ser razonable, es decir, debe compartirla una persona de carácter razonable que conozca los hechos pertinentes. Por tanto, el responsable debe actuar con la debida diligencia al formarse su creencia para poder demostrar el carácter razonable de la misma. De acuerdo con las aclaraciones facilitadas por las autoridades del Reino Unido, la evaluación de «creencia razonable» debe realizarse caso por caso (exención por exención) ([65]). Si se cumplen las condiciones, entonces la exención se considera necesaria y proporcionada con arreglo al Derecho del Reino Unido.

(70) En virtud de la sección 124 de la DPA de 2018, la ICO preparará un código de práctica en materia de protección de datos y periodismo. La preparación del código está en curso en estos momentos. En el marco de la *Data Protection Act* de 1998 se ha emitido una orientación acerca de esta cuestión que destaca principalmente

([62]) Véase el artículo 85 del RGPD del Reino Unido y la parte 5, párrafo vigesimosexto, punto 9, del anexo 2, de la DPA de 2018.

([63]) De conformidad con la parte 5, párrafo vigesimosexto, punto 2, del anexo 2, de la DPA de 2018, la exención se aplica al tratamiento de datos personales que se realiza con fines especiales (fines periodísticos, académicos, artísticos y literarios) si dicho tratamiento se lleva a cabo con miras a la publicación por parte de una persona de material periodístico, académico, artístico o literario, y el responsable del tratamiento cree razonablemente que la publicación de ese material sería de interés público. Al determinar si una publicación sería de interés público, el responsable debe tener en cuenta la especial relevancia del interés público en la libertad de expresión e información. Además, el responsable debe tener en cuenta los códigos de práctica o las directrices pertinentes para la publicación en cuestión (las directrices editoriales de la BBC, el Código de radiodifusión de la Ofcom y el Código de Práctica de los editores). Por otro lado, para que pueda aplicarse una exención, el responsable debe creer razonablemente que el cumplimiento de la disposición pertinente sería incompatible con los fines especiales (párrafo vigesimosexto, punto 3, del anexo 2, de la DPA de 2018).

([64]) La sentencia en el asunto *NT1* v. *Google* [2018] EWHC 799 (QB), apartado 102, abordó un debate sobre si el responsable de los datos tenía una creencia razonable de que la publicación era de interés público y que el cumplimiento de las disposiciones pertinentes era incompatible con los fines especiales. El tribunal declaró que la sección 32, apartado 1, letras b) y c) de la *Data Protection Act* de 1998 tenía un elemento subjetivo y otro objetivo: el responsable debe demostrar la creencia de que la publicación sería de interés público y que esta creencia es objetivamente razonable; debe demostrar también la creencia subjetiva de que el cumplimiento de la disposición para la que se solicita la exención sería incompatible con el fin especial en cuestión.

([65]) En la decisión de la ICO de multar a True Visions Productions, que se tomó en virtud de la *Data Protection Act* de 1998, se incluye un ejemplo de cómo se aplica la evaluación de «creencia razonable». La ICO aceptó que el responsable del medio de comunicación tenía la creencia subjetiva de que el cumplimiento del primer principio de protección de datos (lealtad y licitud) era incompatible con los fines periodísticos. Sin embargo, la ICO no aceptó que esta creencia fuera objetivamente razonable. En el siguiente enlace está disponible la decisión de la ICO: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

que, para acogerse a esta exención, no basta con declarar que el cumplimiento supondría un inconveniente para las actividades periodísticas, sino que debe haber un argumento claro de que la disposición en cuestión presenta un obstáculo para el ejercicio del periodismo responsable ([66]). El regulador de telecomunicaciones del Reino Unido, OFCOM, y la BBC también han publicado en sus directrices editoriales ([67]) una serie de orientaciones sobre la aplicación del criterio de interés público y la ponderación del interés público con el interés de una persona en la privacidad. Las directrices ofrecen principalmente ejemplos de información que puede considerarse de interés público, y explican la necesidad de poder demostrar que el interés público rebasa los derechos de privacidad en las circunstancias concretas del caso.

(71) De manera similar a lo que establece el artículo 89 del Reglamento (UE) 2016/679, los datos personales tratados con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos también pueden estar exentos de una serie de disposiciones enumeradas en el propio RGPD ([68]). Por lo que respecta a los fines de investigación y estadísticos, puede haber exenciones a las disposiciones del RGPD del Reino Unido relacionadas con la confirmación del tratamiento y el acceso a los datos y las garantías para las transferencias a terceros países; el derecho de rectificación; la limitación y la retirada del tratamiento. Por lo que respecta al archivo en interés público, también puede haber exenciones a la obligación de notificación en relación con la rectificación o supresión de datos personales o la restricción del tratamiento y al derecho a la portabilidad de los datos.

(72) En virtud de la parte 6, párrafos vigesimoséptimo, punto 1, y vigesimoctavo, punto 1, del anexo 2, de la DPA de 2018, las exenciones a las disposiciones enumeradas del RGPD del Reino Unido son posibles cuando la aplicación de las disposiciones «impediría o perjudicaría gravemente la consecución» de los fines en cuestión ([69]).

(73) Dada su relevancia para el ejercicio efectivo de los derechos individuales, cualquier novedad pertinente en relación con la interpretación y aplicación en la práctica de las exenciones antes señaladas (además de la relativa al mantenimiento de un control efectivo de la inmigración, como se explica en el considerando 6), en particular, cualquier evolución de la jurisprudencia y de las orientaciones y medidas de ejecución de la OIC, se tendrá debidamente en cuenta en el contexto de la supervisión continua de la presente Decisión ([70]).

2.5.7. *Limitaciones a las transferencias ulteriores*

(74) 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 no debe verse comprometido por la transferencia ulterior de dichos datos a destinatarios que se encuentran en un tercer país. Estas «transferencias ulteriores» que constituyen, desde el punto de vista del responsable o encargado del tratamiento del Reino Unido, transferencias internacionales desde el Reino Unido, solo deberían estar permitidas cuando el destinatario ulterior fuera del Reino Unido esté, por su parte, sujeto a normas que aseguren un nivel de protección similar al garantizado en el ordenamiento jurídico del Reino Unido. Por este motivo, la aplicación de las normas del RGPD del Reino Unido y de la DPA de 2018 sobre transferencias internacionales de datos personales es un factor importante para garantizar la continuidad de la protección en el caso de datos personales que se transfieren de la UE al Reino Unido en virtud de la presente Decisión.

([66]) De conformidad con las orientaciones, las organizaciones deben poder explicar por qué el cumplimiento de la disposición pertinente de la *Data Protection Act* de 1998 es incompatible con los fines del periodismo. En concreto, los responsables del tratamiento deben sopesar el efecto perjudicial que tendría el cumplimiento en el ejercicio del periodismo con el efecto perjudicial que tendría el incumplimiento sobre los derechos del interesado. Si un periodista puede lograr sus objetivos editoriales de tal forma que cumpla con las disposiciones comunes de la DPA, entonces debe hacerlo. Las organizaciones deben poder justificar su uso de la restricción con respecto a todas las disposiciones que no hayan cumplido. *Data protection and journalism: a guide for the media* («Protección de datos y periodismo: una guía para los medios de comunicación», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Algunos ejemplos de interés público incluirían revelar o detectar delitos, proteger la salud o la seguridad públicas, exponer afirmaciones engañosas hechas por personas u organizaciones o comunicar incompetencias que afecten al público. Véanse las directrices de la OFCOM en el siguiente enlace: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf y las directrices editoriales de la BBC en el siguiente enlace: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Véase el artículo 89 del RGPD del Reino Unido y la parte 6, párrafos vigesimoséptimo, punto 2, y vigesimoctavo, punto 2, del anexo 2, de la DPA de 2018.

([69]) Esto está sujeto al requisito de que los datos personales se traten de acuerdo con el artículo 89, apartado 1, del RGPD del Reino Unido, complementado por la sección 19 de la DPA de 2018.

([70]) Véanse los considerandos 281 a 287.

(75) En los artículos 44 a 49 del RGPD del Reino Unido se establece el régimen sobre transferencias internacionales de datos personales desde el Reino Unido, complementado por la DPA de 2018; dicho régimen es en esencia idéntico a las normas establecidas en el capítulo V del Reglamento (UE) 2016/679 ([71]). Las transferencias de datos personales a un tercer país u organización internacional solo pueden realizarse sobre la base de normas en materia de adecuación [el equivalente en el Reino Unido a una decisión de adecuación en virtud del Reglamento (UE) 2016/679], o en ausencia de dichas normas, cuando el responsable o encargado del tratamiento haya proporcionado las garantías adecuadas de conformidad con el artículo 46 del RGPD del Reino Unido. En ausencia de normas en materia de adecuación o garantías apropiadas, una transferencia solo puede realizarse sobre la base de las derogaciones establecidas en el artículo 49 del RGPD del Reino Unido.

(76) Las normas en materia de adecuación dictadas por el secretario de Estado pueden estipular que un tercer país (o un territorio o un sector dentro de un tercer país), una organización internacional, o una descripción ([72]) de dicho país, territorio, sector u organización asegura un nivel adecuado de protección de datos personales. Al evaluar la idoneidad del nivel de protección, el secretario de Estado debe tener en cuenta exactamente los mismos elementos que la Comisión debe evaluar con arreglo al artículo 45, apartado 2, letras a) a c), del Reglamento (UE) 2016/679, interpretado junto con el considerando 104 del mismo Reglamento y la jurisprudencia de la Unión conservada. Esto significa que, al evaluar el nivel adecuado de protección de un tercer país, el criterio pertinente será si ese tercer país en cuestión garantiza un nivel de protección «esencialmente equivalente» al garantizado en el Reino Unido.

(77) Por lo que respecta al procedimiento, las normas en materia de adecuación están sujetas a los requisitos de procedimiento «generales» previstos en la sección 182 de la DPA de 2018. 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 ([73]). 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 ([74]).

(78) De conformidad con la sección 17B, apartado 1, de la DPA de 2018, las normas en materia de adecuación deben revisarse a intervalos de no más de cuatro años y el secretario de Estado debe, de manera continua, supervisar las novedades en terceros países y organizaciones internacionales que podrían afectar las decisiones para adoptar normas en materia de adecuación, o para modificar o derogar tales normas. Cuando el secretario de Estado tenga conocimiento de que un país u organización concretos ya no garantiza un nivel adecuado de protección de los datos personales debe, en la medida necesaria, modificar o derogar las normas y celebrar consultas con el tercer país u organización internacional en cuestión para remediar la falta de un nivel de protección adecuado. Estos aspectos procedimentales reflejan también los requisitos correspondientes del Reglamento (UE) 2016/679.

([71]) Con la excepción del artículo 48 del Reglamento (UE) 2016/679, que el Reino Unido ha optado por no incluir en el RGPD del Reino Unido. A este respecto, cabe recordar, en primer lugar, que como aclara el TJUE (*Maximillian Schrems contra Data Protection Commissioner*, apartados 73 a 74) y reconoce el CEPD (documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos, p. 3), para considerar que se garantiza un nivel de protección adecuado, se aplica la norma del nivel de protección «esencialmente equivalente», no idéntico. Por tanto, como explica el CEPD en su documento relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos, «el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación». A este respecto, es importante señalar que, si bien el ordenamiento jurídico del Reino Unido no contiene formalmente una disposición idéntica al artículo 48, el mismo efecto está garantizado por otras disposiciones y principios jurídicos, es decir, que en respuesta a una solicitud de datos personales por parte de un tribunal o una autoridad administrativa de un tercer país, los datos personales solo pueden transferirse a ese tercer país si existe un acuerdo internacional en virtud del cual se reconoce o ejecuta la resolución judicial o la decisión administrativa del tercer país en el Reino Unido, o si se basa en uno de los mecanismos de transferencia previstos en el capítulo V del RGPD del Reino Unido. En concreto, para hacer cumplir una resolución judicial extranjera, los tribunales del Reino Unido deben poder acogerse al *common law* o un estatuto que permita su aplicabilidad. Sin embargo, ni la *common law* (véase *Adams and Others* v *Cape Industries Plc.*, [1990] 2 W.L.R. 657) ni los estatutos prevén la ejecución de resoluciones judiciales extranjeras que requieran la transferencia de datos sin un acuerdo internacional. En consecuencia, en ausencia de tal acuerdo internacional, las solicitudes de datos no pueden ejecutarse en virtud del Derecho del Reino Unido. Además, las transferencias de datos personales a terceros países, incluso a petición de un tribunal o autoridad administrativa extranjera, permanecen sujeta a las restricciones establecidas en el capítulo V del RGPD del Reino Unido, que son idénticas a las disposiciones correspondientes del Reglamento (UE) 2016/679, y por lo tanto, requieren invocar uno de los motivos de transferencia contemplados en el capítulo V de conformidad con las condiciones específicas a las que está sujeto en virtud de dicho capítulo.

([72]) Las autoridades del Reino Unido aclararon que la descripción de un país u organización internacional se refiere a una situación en la que sería necesario realizar una resolución específica y parcial de adecuación con restricciones específicas (por ejemplo, normas en materia de adecuación en relación con tan solo ciertos tipos de transferencias de datos).

([73]) 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 UK, 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.

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

(79) En ausencia de normas en materia de adecuación, pueden realizarse transferencias internacionales cuando el responsable o encargado del tratamiento haya proporcionado las garantías adecuadas de acuerdo con el artículo 46 del RGPD del Reino Unido. Estas garantías son similares a las que establece el artículo 46 del Reglamento (UE) 2016/679. Incluyen instrumentos jurídicamente vinculantes y exigibles entre autoridades u organismos públicos, normas corporativas vinculantes ([75]), cláusulas tipo de protección de datos, códigos de conducta aprobados, mecanismos de certificación aprobados y, con la autorización de la ICO, cláusulas contractuales entre responsables (o encargados del tratamiento) o acuerdos administrativos entre las autoridades públicas. Sin embargo, desde un punto de vista procedimental, las normas se han modificado para actuar dentro del marco del Reino Unido; en particular, y de conformidad con la DPA de 2018, las cláusulas tipo de protección de datos pueden ser adoptadas por el secretario de Estado (sección 17C) o la ICO (sección 119A).

(80) En ausencia de una decisión de adecuación o de garantías adecuadas, una transferencia únicamente puede realizarse sobre la base de las excepciones establecidas en el artículo 49 del RGPD del Reino Unido ([76]). El RGPD del Reino Unido no introduce ningún cambio sustancial a estas excepciones en comparación con las normas correspondientes del Reglamento (UE) 2016/679. De conformidad con el RGPD del Reino Unido, así como con arreglo al Reglamento (UE) 2016/679, solo se puede apelar a determinadas excepciones si la transferencia es ocasional ([77]). Además, en sus directrices sobre transferencias internacionales, la ICO aclara que: «Solo debe utilizarlas como verdaderas "excepciones" de la norma general de que no debe realizarse una transferencia restringida a menos que esté cubierta por una decisión de adecuación o existan las garantías adecuadas» ([78]). En relación con las transferencias que son necesarias por razones importantes de interés público [artículo 49, apartado 1, letra d) del Reglamento (UE) 2016/679], el secretario de Estado puede adoptar regulaciones para especificar circunstancias en las que una transferencia de datos personales a un tercer país u organización internacional es o no es necesaria por razones importantes de interés público. Además, el secretario de Estado puede limitar mediante regulación la transferencia de una categoría de datos personales a un tercer país u organización internacional donde la transferencia no puede realizarse sobre la base de normas en materia de adecuación, y cuando el secretario de Estado considere que la limitación es necesaria por razones importantes de interés público. Hasta la fecha no se ha adoptado ninguna regulación de este tipo.

(81) Este marco para las transferencias internacionales entró en vigor al final del período transitorio ([79]). Sin embargo, el párrafo cuarto, del anexo 21, de la DPA de 2018 (introducido por la normativa *DPPEC Regulations*) establece que, a partir del final del período transitorio, ciertas transferencias de datos personales deben tratarse como si estuvieran basadas en normas en materia de adecuación. Dichas transferencias incluyen transferencias a un Estado del EEE, el territorio de Gibraltar, una institución, organismo, oficina o agencia de la UE establecidos por el Tratado de la Unión Europea o sobre la base del mismo, y a terceros países que fueron objeto de una decisión de adecuación de la UE al final del período transitorio. En consecuencia, las transferencias a estos países pueden seguir realizándose como antes de la retirada del Reino Unido de la UE. Al final del período transitorio, el secretario de Estado tuvo que iniciar una revisión de estas decisiones de adecuación para un período de cuatro años, es decir, hasta finales de diciembre de 2024. Según la aclaración proporcionada por las autoridades del Reino Unido, a pesar de que el

([75]) El RGPD del Reino Unido conserva las normas recogidas en el artículo 47 del Reglamento (UE) 2016/679, sujetas únicamente a modificaciones para ajustarlas al contexto nacional; por ejemplo, sustituyendo las referencias a la autoridad de control competente por la ICO, eliminando la referencia al mecanismo de coherencia (apartado 1) y suprimiendo todo el apartado 3.

([76]) En virtud del artículo 49 del RGPD del Reino Unido, las transferencias solo son posibles si se cumple alguna de las condiciones siguientes: a) el interesado ha dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas; b) la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; c) la transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; d) la transferencia es necesaria por razones importantes de interés público; e) la transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones; f) la transferencia es necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; g) la transferencia se realiza desde un registro público que, con arreglo al Derecho interno, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho interno para la consulta. Además, cuando ninguna de las condiciones anteriores sea aplicable, una transferencia solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento ha evaluado todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ha ofrecido garantías adecuadas con respecto a la protección de datos personales.

([77]) El considerando 111 del RGPD del Reino Unido especifica que las transferencias en relación con un contrato o una reclamación solo se podrán llevar a cabo cuando sean ocasionales.

([78]) Las directrices sobre transferencias internacionales de la ICO están disponibles en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Durante un período máximo de seis meses, que finaliza a más tardar el 30 de junio de 2021, la aplicabilidad de este nuevo marco debe interpretarse a la luz 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 (L 444/14 de 31.12.2020) disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22020A1231(01)&from=ES.

secretario de Estado debe llevar a cabo esta revisión para finales de diciembre de 2024, las disposiciones transitorias no incluyen una disposición de caducidad y las disposiciones transitorias pertinentes no perderán su vigencia automáticamente en caso de que no se complete la revisión para finales de diciembre de 2024.

(82) Por último, en lo que respecta a la evolución futura del régimen de transferencias internacionales del Reino Unido, a través de la adopción de nuevas normas de adecuación, la celebración de acuerdos internacionales o el desarrollo de otros mecanismos de transferencia, la Comisión seguirá de cerca la situación, evaluará si los diferentes mecanismos de transferencia se utilizan de forma que se garantice la continuidad de la protección y adoptará, en su caso, las medidas adecuadas para abordar los posibles efectos adversos para dicha continuidad (véanse los considerandos 278 a 287). Dado que la UE y el Reino Unido comparten normas similares sobre transferencias internacionales, se espera que las divergencias problemáticas también puedan evitarse mediante la cooperación y el intercambio de información y experiencias, incluso entre la ICO y el CEPD.

2.5.8. *Responsabilidad proactiva*

(83) De conformidad con el principio de responsabilidad proactiva, las entidades que traten datos están obligadas a adoptar las medidas técnicas y organizativas apropiadas para cumplir de manera efectiva con sus obligaciones en materia de protección de datos y deben demostrar el respeto de estas obligaciones, en particular ante la autoridad de control competente.

(84) El principio de responsabilidad proactiva previsto en el Reglamento (UE) 2016/679 se ha mantenido en el artículo 5, apartado 2, del RGPD del Reino Unido sin cambios sustanciales, y lo mismo aplica al artículo 24 sobre la responsabilidad del responsable del tratamiento, al artículo 25 sobre la protección de datos desde el diseño y por defecto, y al artículo 30 sobre el registro de las actividades de tratamiento. También se han mantenido sin cambios los artículos 35 y 36 concernientes a la evaluación de impacto relativa a la protección de datos y la consulta previa de la autoridad de control. Asimismo, los artículos 37 a 39 del Reglamento (UE) 2016/679 relativos a la designación y las tareas de los delegados de protección de datos se han mantenido sin cambios importantes en el RGPD del Reino Unido. Por otro lado, en el RGPD del Reino Unido también se han mantenido las disposiciones recogidas en los artículos 40 y 42 del Reglamento (UE) 2016/679 sobre los códigos de conducta y certificación ([80]).

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

2.6.1. *Supervisión independiente*

(85) Con el fin de garantizar un nivel adecuado de protección de los datos en la práctica, debe existir una autoridad de control independiente encargada de supervisar las normas en materia de protección de datos y hacerlas cumplir. Esta autoridad debe actuar con total independencia e imparcialidad en el desempeño de sus funciones y en el ejercicio de sus competencias.

(86) En el Reino Unido, la autoridad encargada de la supervisión y el cumplimiento de las normas del RGPD del Reino Unido y de la DPA de 2018 es el/la Information Commissioner. El/la Information Commissioner es una persona jurídica unipersonal: una entidad jurídica independiente constituida por una sola persona física. El/la Information Commissioner cuenta con el apoyo de una oficina en su trabajo (la ICO). El 31 de marzo de 2020, la ICO contaba con 768 empleados fijos ([81]). El departamento que ampara a la ICO es el Departamento de Cultura, Medios de Comunicación y Deporte del Reino Unido ([82]).

(87) La independencia del cargo de Information Commissioner se determina explícitamente en el artículo 52 del RGPD del Reino Unido, que no presenta cambios importantes en relación con el artículo 52, apartados 1 a 3, del Reglamento (UE) 2016/679. El/la Information Commissioner debe actuar con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el RGPD del Reino Unido, ser ajeno/a a toda

([80]) Cuando corresponda, estas referencias se sustituyen por referencias a las autoridades del Reino Unido. Por ejemplo, en la sección 17 de la DPA de 2018, la ICO o el organismo nacional de acreditación del Reino Unido pueden acreditar a una persona que cumpla los requisitos establecidos en el artículo 43 del RGPD del Reino Unido para supervisar el cumplimiento de una certificación.

([81]) *Annual Report and Financial Statements 2019-2020* («Informe anual y estados financieros 2019-2020», documento en inglés) de la ICO, disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Un contrato de gestión regula la relación entre ambos. En concreto, las responsabilidades principales del Departamento de Cultura, Medios de Comunicación y Deporte como departamento «patrocinador», incluyen: garantizar que la ICO cuenta con los fondos y los recursos adecuados; representar los intereses de la ICO ante el Parlamento y otros departamentos gubernamentales; garantizar la existencia de un marco nacional sólido de protección de datos; y ofrecer asesoramiento y apoyo a la ICO sobre cuestiones corporativas, como cuestiones de patrimonio, arrendamientos y adjudicación de contratos públicos (el contrato de gestión 2018-2021 está disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

influencia externa, ya sea directa o indirecta, en relación con dichos poderes y funciones, y no solicitará ni admitirá ninguna instrucción. Asimismo, se abstendrá de cualquier acción que sea incompatible con sus funciones y no participará, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

(88) En el anexo 12 de la DPA de 2018 se establecen las condiciones para el nombramiento y la destitución del/de la Information Commissioner. El nombramiento para el cargo de Information Commissioner lo realiza Su Majestad por recomendación del Gobierno, en virtud de una competencia justa y abierta. El/la candidato/a debe contar con las cualificaciones, capacidades y competencias necesarias. De conformidad con lo dispuesto en el *Governance Code on Public Appointments* ([83]), un grupo consultivo de evaluación elabora una lista de posibles candidatos. Antes de que el secretario de Estado del Departamento de Cultura, Medios de Comunicación y Deporte tome su decisión, el Select Committee of Parliament (comité selecto del Parlamento) correspondiente debe realizar un escrutinio previo al nombramiento. La posición del comité se hace pública ([84]).

(89) El/la Information Commissioner ocupa el cargo por un período de hasta siete años y no es posible nombrar a una persona Information Commissioner más de una vez. El/la Information Commissioner puede ser destituido/a de su cargo por decisión de Su Majestad en respuesta a un discurso de ambas cámaras del Parlamento ([85]). No es posible presentar una solicitud de destitución del/de la Information Commissioner ante ninguna de las cámaras del Parlamento salvo que un secretario de Estado haya presentado un informe que indique su convencimiento de que el/la Information Commissioner es culpable de una falta grave o de que ya no cumple las condiciones requeridas para el desempeño de las funciones del cargo ([86]).

(90) La financiación de la ICO procede de tres fuentes: i) tasas por protección de datos que los responsables del tratamiento pagan, y que establecen las regulaciones del secretario de Estado ([87]) [*Data Protection (Charges and Information) Regulations* de 2018], y ascienden al 85-90 % del presupuesto anual de la oficina ([88]); ii) subvención del Gobierno a la ICO, que se emplea principalmente para financiar los costes operativos de la ICO en lo que respecta a las funciones no relacionadas con la protección de datos ([89]); y iii) tasas por servicios ofrecidos ([90]). Actualmente no se cobra ninguna de estas tasas.

(91) Las funciones generales de la ICO en relación con el tratamiento de datos personales al que aplica el RGPD del Reino Unido se establecen en el artículo 57 de dicho Reglamento, que reflejan estrechamente las normas correspondientes del Reglamento (UE) 2016/679. Entre sus funciones se encuentra el control de la aplicación del RGPD del Reino Unido, la promoción de la sensibilización del público, la gestión de las reclamaciones presentadas por los interesados, la realización de investigaciones, etc. Además, la sección 115 de la DPA de 2018 establece otras funciones generales de la ICO, que incluyen el deber de asesorar al Parlamento, el Gobierno y otras instituciones y organismos sobre las medidas legislativas y administrativas relacionadas con la protección de los derechos y libertades de las personas en relación con el tratamiento de los datos personales, y la facultad de emitir, por iniciativa propia o previa solicitud, dictámenes al Parlamento, al Gobierno u otras instituciones y organismos, así como al público, sobre cualquier cuestión relacionada con la protección de los datos personales. A fin de mantener la independencia del poder judicial, la ICO no está autorizada para ejercer sus funciones en relación con el

([83]) *Governance Code on Public Appointments* («Código de gobernanza sobre nombramientos públicos», documento en inglés), disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) *Second Report of Session 2015-2016* («Segundo informe de sesión 2015-2016», documento en inglés) del Comité de Cultura, Medios de Comunicación y Deporte en la Cámara de los Comunes, disponible en el siguiente enlace: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) Un «discurso» es una moción que se presenta ante el Parlamento y cuyo fin es que el/la monarca esté al tanto de las opiniones del Parlamento sobre una cuestión en particular.

([86]) Párrafo tercero, punto 3, del anexo 12, de la DPA de 2018.

([87]) Sección 137 de la DPA de 2018, véase el considerando 17.

([88]) Las secciones 137 y 138 de la DPA de 2018 contienen una serie de garantías que aseguran una fijación de las tasas en un nivel adecuado. En concreto, la sección 137, apartado 4, enumera las cuestiones que el secretario de Estado debe tener en cuenta al adoptar regulaciones que especifiquen la cuantía que deben pagar las distintas organizaciones. Por otro lado, la sección 138, apartado 1, y la sección 182, de la DPA de 2018 también contienen una disposición legal para que el secretario de Estado, antes de adoptar las regulaciones, consulte a la ICO y a otros representantes de las personas que puedan verse afectadas por ellas, de modo que pueda tenerse en cuenta su opinión. Además, con arreglo a la sección 138, apartado 2, de la DPA de 2018, la ICO debe supervisar el funcionamiento de la normativa relativa a las tasas y puede presentar propuestas al secretario de Estado para realizar modificaciones en dicha normativa. Por último, salvo que la normativa se adopte únicamente para tener en cuenta un aumento del índice de precios de venta al público (en cuyo caso estará sujeta al procedimiento de resolución negativa), está sujeta al procedimiento de resolución afirmativa y no podrá adoptarse hasta que se haya aprobado por resolución de cada una de las cámaras del Parlamento.

([89]) El contrato de gestión especificó que «el secretario de Estado puede realizar pagos a la ICO con dinero proporcionado por el Parlamento con arreglo al párrafo noveno, del anexo 12, de la DPA de 2018. Tras consultar con la ICO, el Departamento de Cultura, Medios de Comunicación y Deporte pagará a la ICO cantidades adecuadas (la subvención) para cubrir sus costes administrativos y para el ejercicio de sus funciones en relación con una serie de tareas específicas, incluida la libertad de información» (Contrato de gestión 2018-2021, apartado 1, punto 12; véase la nota a pie de página 82).

([90]) Véase la sección 134 de la DPA de 2018.

tratamiento de datos personales por parte de una persona en el ejercicio de su función judicial o de un tribunal que actúe en el ejercicio de su función judicial. Sin embargo, la supervisión del poder judicial está a cargo de organismos especializados (véanse los considerandos 99 a 103).

2.6.2. *Ejecución, incluidas sanciones*

(92) Los poderes de la ICO se establecen en el artículo 58 del RGPD del Reino Unido, que no introduce cambios sustanciales en relación con el artículo correspondiente del Reglamento (UE) 2016/679. La DPA de 2018 establece normas adicionales sobre la forma de ejecución de estos poderes. En concreto, la ICO dispone de poderes para: a) ordenar al responsable y al encargado del tratamiento (y, en determinadas circunstancias, a cualquier otra persona), que faciliten información necesaria mediante un aviso de información («aviso de información») ([91]); b) llevar a cabo investigaciones y auditorías dando un aviso de evaluación, que puede requerir que el responsable o encargado del tratamiento permita a la ICO entrar en instalaciones específicas, inspeccionar o examinar documentos o equipos, entrevistar a las personas que tratan los datos personales en nombre del responsable, etc. («aviso de evaluación») ([92]); c) obtener el acceso a documentos, etc. de los responsables y encargados del tratamiento y acceder a sus instalaciones de acuerdo con la sección 154 de la DPA de 2018 («poderes de entrada e inspección»); d) ejercer poderes correctivos mediante advertencias y sanciones o dar órdenes mediante un aviso de ejecución, que requiera que los responsables/encargados del tratamiento adopten o se abstengan de adoptar medidas específicas, incluida la orden al responsable o encargado de llevar a cabo alguna de las acciones especificadas en el artículo 58, apartado 2, letras c) a g) y letra j), del RGPD del Reino Unido («aviso de ejecución») ([93]); e) emitir multas administrativas en forma de aviso de sanción («aviso de sanción») ([94]). Este último también puede emitirse en caso de que una autoridad pública no haya cumplido con las disposiciones del RGPD del Reino Unido ([95]).

(93) La política de acción reguladora de la ICO establece las circunstancias en virtud de las cuales emitirá un aviso de información, de evaluación, de ejecución o de sanción ([96]). Un aviso de ejecución que se emite en respuesta a una infracción por parte de un responsable o encargado del tratamiento solo puede imponer los requisitos que la ICO considere adecuados con el fin de remediar dicha infracción. Pueden emitirse avisos de ejecución y sanción a un responsable o encargado del tratamiento en relación con violaciones del capítulo II del RGPD del Reino Unido (principios relativos al tratamiento), los artículos 12 a 22 (derechos del interesado), los artículos 25 a 39 (obligaciones por parte del responsable y el encargado del tratamiento) y los artículos 44 a 49 (transferencias internacionales) del RGPD del Reino Unido. También puede darse un aviso de ejecución a un responsable del tratamiento que ha incumplido el requisito de pagar una tasa en las regulaciones establecidas con arreglo a la sección 137 de la DPA de 2018. Además, un organismo de supervisión, en virtud del artículo 41, o un proveedor de servicios de certificación pueden recibir un aviso de ejecución si no cumplen con sus obligaciones con arreglo al RGPD del Reino Unido. Asimismo, puede darse un aviso de sanción a una persona que no haya cumplido con un aviso de información, de evaluación o de ejecución.

(94) El aviso de sanción requiere que la persona pague a la ICO la cuantía especificada en el aviso. Para determinar si debe emitirse un aviso de sanción a una persona, así como para determinar la cuantía de dicha sanción, la ICO debe tener en cuenta las cuestiones enumeradas en el artículo 83, apartados 1 y 2, del RGPD del Reino Unido, que son idénticas a las correspondientes del Reglamento (UE) 2016/679 ([97]). Con arreglo al artículo 83, apartados 4 y 5, del RGPD del Reino Unido la cuantía máxima de las multas administrativas en caso de incumplimiento de las obligaciones indicadas en dichas disposiciones es de 8,7 millones o 17,5 millones de libras esterlinas, respectivamente. Si se trata de una empresa, la ICO puede también imponer multas como porcentaje del volumen de negocio total anual global, cuando este sea superior. Al igual que en las disposiciones equivalentes del Reglamento (UE) 2016/679, estas cuantías se establecen en el 2 y el 4 % en el artículo 83, apartados 4 y 5, respectivamente. En caso de

([91]) Sección 142 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 143 de la DPA de 2018).
([92]) Sección 146 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 147 de la DPA de 2018).
([93]) Sección 149 a 151 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 152 de la DPA de 2018).
([94]) Sección 155 de la DPA de 2018 y artículo 83 del RGPD del Reino Unido.
([95]) Ello se deduce de la sección 155, apartado 1, de la DPA de 2018 leída en conjunto con las secciones 149, apartados 2 y 5, y 156, apartado 4, de la misma Ley, que restringe la emisión de avisos de sanción únicamente con respecto a los *Crown Estate Commissioners* y los responsables del tratamiento de la Casa Real de conformidad con la sección 209, apartado 4, de dicha Ley.
([96]) Política de acción reguladora de la ICO, disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Incluyendo la naturaleza y gravedad de la infracción (teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido); la intencionalidad o negligencia en la infracción; cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; el grado de responsabilidad del responsable o encargado del tratamiento (habida cuenta de las medidas técnicas u organizativas que el responsable o el encargado del tratamiento haya aplicado); toda infracción anterior cometida por el responsable o el encargado del tratamiento; el grado de cooperación con la ICO; las categorías de los datos de carácter personal afectados por la infracción; y cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

incumplimiento de un aviso de información, de evaluación o de ejecución, la cuantía máxima de la sanción que puede imponerse mediante un aviso de sanción es la cuantía mayor de 17,5 millones de libras esterlinas o, en el caso de una empresa, el 4 % del volumen de negocio total anual global.

(95) El RGPD del Reino Unido, junto con la DPA de 2018, también ha reforzado otros poderes de la ICO. Por ejemplo, la ICO ahora puede realizar auditorías obligatorias en relación con todos los responsables y encargados del tratamiento mediante el recurso a los avisos de evaluación, mientras que con arreglo a la legislación anterior, la *Data Protection Act* de 1998, la ICO solo tenía esta facultad en relación con el Gobierno central y las organizaciones de la salud, mientras que los demás organismos debían aceptar la auditoría previamente.

(96) Desde la introducción del Reglamento (UE) 2016/679, la ICO atiende en torno a 40 000 reclamaciones de interesados al año ([98]) y, además, lleva a cabo unas 2 000 investigaciones *ex officio* ([99]). La mayoría de las reclamaciones están relacionadas con los derechos de acceso y comunicación de los datos. Tras sus investigaciones, la ICO está tomando medidas de ejecución en una amplia gama de sectores. En concreto, según el último informe anual de la ICO (2019-2020) ([100]), se emitieron 54 avisos de información, 8 avisos de evaluación, 7 avisos de ejecución, 4 amonestaciones, 8 enjuiciamientos y 15 multas durante el período de notificación ([101]).

(97) Esto incluye varias sanciones monetarias importantes impuestas en virtud del Reglamento (UE) 2016/679 y la DPA de 2018. En concreto, la ICO multó en octubre de 2020 a una compañía aérea británica con 20 millones de libras esterlinas por una violación de la seguridad de los datos que afectó a más de 400 000 clientes. A finales de octubre de 2020, una cadena hotelera internacional recibió una multa de 18,4 millones de libras esterlinas por no mantener seguros los datos personales de millones de clientes y, en noviembre de 2020, un proveedor de servicios británico que vendía entradas para eventos en línea recibió una multa de 1,25 millones de libras esterlinas por no proteger la información de pago de los clientes ([102]).

(98) Además de los poderes de ejecución de la ICO descritos en el considerando 92, ciertas violaciones de la legislación en materia de protección de datos constituyen infracciones y, por tanto, pueden estar sujetas a sanciones penales (sección 196 de la DPA de 2018). Esto aplica, por ejemplo, a la obtención o comunicación de datos personales intencionalmente o a causa de una imprudencia sin el consentimiento del responsable del tratamiento, la comunicación de datos personales a otra persona sin el consentimiento del responsable del tratamiento ([103]), la desanonimización de información basada en datos personales anonimizados sin el consentimiento del responsable del tratamiento encargado de anonimizar los datos personales ([104]), obstaculizar de manera intencionada a la ICO para ejercer sus poderes en relación con la inspección de datos personales con arreglo a las obligaciones internacionales ([105]), realizar declaraciones falsas en respuesta a un aviso de información o destruir información en relación con avisos de información y evaluación ([106]).

([98]) De acuerdo con la información facilitada por las autoridades del Reino Unido, durante el período contemplado en el informe anual de la ICO 2019-2020 no se encontró ninguna infracción en aproximadamente el 25 % de los casos; en aproximadamente el 29 % de los casos se pidió al interesado que planteara su preocupación al responsable del tratamiento por primera vez, a que esperara la respuesta del responsable o a que entablara un diálogo continuo con el responsable; en alrededor del 17 % de los casos no se encontró ninguna infracción, pero se ofreció asesoramiento al responsable del tratamiento; en aproximadamente el 25 % de los casos, la ICO encontró una infracción y ofreció asesoramiento al responsable del tratamiento o bien se solicitó al responsable del tratamiento que adoptara ciertas medidas; en aproximadamente el 3 % de los casos se determinó que la reclamación no estaba contemplada en el Reglamento (UE) 2016/679; y alrededor del 1 % de los casos se remitieron a otra autoridad de protección de datos en el marco del Comité Europeo de Protección de Datos.

([99]) La ICO puede iniciar esas investigaciones basándose en la información recibida de una variedad de fuentes, incluidas notificaciones de violación de la seguridad de los datos personales, referencias de otras autoridades públicas del Reino Unido o autoridades extranjeras de protección de datos, y reclamaciones de individuos u organizaciones de la sociedad civil.

([100]) *Annual Report and Financial Statements 2019-2020* («Informe anual y estados financieros 2019-2020», documento en inglés) de la ICO (véase la nota a pie de página 81).

([101]) De acuerdo con el informe anual anterior, que cubre el período 2018-2019, la ICO emitió 22 avisos de sanción con arreglo a la DPA de 1998 durante el período de notificación, con multas por un total de 3 010 610 de libras esterlinas, incluidas dos multas de 500 000 libras esterlinas (el máximo permitido con arreglo a la DPA de 1998). Cabe señalar que, en 2018, la ICO llevó a cabo una investigación sobre el uso de análisis de datos con fines políticos tras las revelaciones de Cambridge Analytica. Las conclusiones de la investigación se recogieron en un informe en materia de políticas, un conjunto de recomendaciones, una multa de 500 000 libras esterlinas contra Facebook y un aviso de ejecución a Aggregate IQ, un corredor de datos canadiense, que ordenaba a la compañía que borrara los datos personales que tenía sobre ciudadanos y residentes del Reino Unido [véase el «Informe anual y estados financieros 2018-2019» de la ICO (documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf].

([102]) Para un resumen de las acciones de ejecución emprendidas, consulte el sitio web de la ICO, disponible en el siguiente enlace: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Sección 170 de la DPA de 2018.

([104]) Sección 171 de la DPA de 2018.

([105]) Sección 119 de la DPA de 2018.

([106]) Secciones 144 y 148 de la DPA de 2018.

2.6.3. *Supervisión del poder judicial*

(99) La supervisión del tratamiento de datos personales por parte de los tribunales y el poder judicial es doble. Cuando el titular de un cargo judicial o un tribunal no actúa en el ejercicio de su función judicial, la ICO se encarga de la supervisión. Cuando el responsable del tratamiento actúa en el ejercicio de su función judicial, la ICO no puede ejercer sus funciones de supervisión ([107]) y, en consecuencia, organismos especiales realizan la supervisión. Esto refleja el enfoque adoptado en Reglamento (UE) 2016/679 (artículo 55, apartado 3).

(100) En el segundo escenario, para los tribunales de Inglaterra y Gales y los Tribunales de Primera Instancia y Tribunales Superiores de Inglaterra y Gales, dicha supervisión la proporciona, en particular, el Judicial Data Protection Panel (Sala Jurisdiccional de Protección de Datos) ([108]). Además, el Lord Chief Justice y el Senior President of Tribunals emitieron un aviso de privacidad ([109]) que establece cómo los tribunales de Inglaterra y Gales tratan los datos personales para las funciones jurisdiccionales. Los poderes judiciales de Irlanda del Norte ([110]) y Escocia ([111]) emitieron una notificación similar.

(101) Además, en Irlanda del Norte, el Lord Chief Justice de Irlanda del Norte nombró a un juez del Tribunal Superior como Data Supervisory Judge (juez supervisor de datos) ([112]). Asimismo, se han emitido unas directrices para el poder judicial de Irlanda del Norte sobre qué hacer en caso de pérdida o posible pérdida de datos y el proceso para abordar cualquier problema que surja a raíz de ello ([113]).

(102) En Escocia, el Lord President designó un juez supervisor de datos (Data Supervisory Judge) para investigar cualquier queja por motivos de protección de datos. Esta medida se establece en las normas sobre reclamaciones judiciales, que reflejan las establecidas para Inglaterra y Gales ([114]).

(103) Por último, en el Tribunal Supremo del Reino Unido se designa a uno de los magistrados para supervisar la protección de datos.

2.6.4. *Acciones administrativas y judiciales*

(104) A fin de garantizar una protección adecuada y, en particular, el respeto de los derechos individuales, deben reconocerse al interesado acciones administrativas y judiciales efectivas, incluida la indemnización por daños y perjuicios.

([107]) Sección 117 de la DPA de 2018.

([108]) El Judicial Data Protection Panel es responsable de brindar asesoramiento y formación al poder judicial. También atiende las reclamaciones de los interesados en relación con el tratamiento de los datos personales por parte de tribunales y personas físicas que actúan en el ejercicio de su función judicial. El fin del Judicial Data Protection Panel es proporcionar los medios a través de los cuales pueda resolverse cualquier reclamación. Si un reclamante no está satisfecho con una decisión del Judicial Data Protection Panel y ofrece pruebas adicionales, este último podría reconsiderar su decisión. Si bien el Judicial Data Protection Panel no impone sanciones económicas, si considera que existe un incumplimiento suficientemente grave de la DPA de 2018, puede remitirlo a la Judicial Conduct Investigation Office (Oficina de Investigaciones de Conducta Judicial), que investigará la reclamación. Si la denuncia se sostiene, es competencia del Lord Chancellor y del Lord Chief Justice (o un juez superior autorizado para actuar en su nombre) decidir qué acción debe tomarse contra el titular del cargo. Las consecuencias incluyen, en orden de gravedad: asesoramiento profesional, aviso de carácter formal y amonestación y, en última instancia, destitución del cargo. Si una persona no está satisfecha con la forma en que la Judicial Conduct Investigation Office ha investigado la reclamación, puede presentar una reclamación adicional ante el Appointments and Conduct Ombudsman (Defensor del Pueblo en materia de Nombramientos y Conducta) (véase https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). El Ombudsman tiene el poder de solicitar a la Judicial Conduct Investigation Office que vuelva a investigar una reclamación y puede proponer que se pague una indemnización al reclamante cuando crea que ha sufrido daños como consecuencia de una mala administración.

([109]) El aviso de privacidad emitido por el Lord Chief Justice y el Senior President of Tribunals está disponible en el siguiente enlace: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) El aviso de privacidad emitido por el Lord Chief Justice de Irlanda del Norte está disponible en el siguiente enlace: https://judiciaryni.uk/data-privacy.

([111]) El aviso de privacidad para los tribunales escoceses está disponible en el siguiente enlace: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) El Data Supervisory Judge ofrece asesoramiento al poder judicial e investiga las infracciones o reclamaciones vinculadas con el tratamiento de datos personales por parte de los tribunales o personas físicas que actúan en ejercicio de su función judicial.

([113]) Cuando la reclamación o la infracción se consideren graves, se remitirá al Judicial Complaints Officer (oficial de quejas judiciales) para una investigación en profundidad con arreglo al código de práctica sobre reclamaciones del Lord Chief Justice de Irlanda del Norte. El resultado de dicha reclamación puede incluir: ninguna acción adicional, asesoramiento, formación o tutorías, aviso informal, aviso formal, aviso terminante, restricción de la práctica o remisión a un tribunal ordinario. El código de práctica sobre reclamaciones emitido por el Lord Chief Justice de Irlanda del Norte está disponible en el siguiente enlace: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([114]) Cualquier reclamación que cuente con un fundamento sólido la investiga el Data Supervisory Judge y se remite al Lord President, quien tiene el poder de emitir un consejo, una advertencia formal o una amonestación si lo considera necesario (existen normas equivalentes para los miembros del tribunal, disponibles en el siguiente enlace: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) En primer lugar, todo interesado tiene derecho a presentar una reclamación ante la ICO si considera que, en relación con los datos personales que le conciernen, existe una infracción del RGPD del Reino Unido ([115]). El RGPD del Reino Unido mantiene sin cambios las normas que establece el artículo 77 del Reglamento (UE) 2016/679 en relación con ese mismo derecho. Lo mismo aplica al artículo 57, apartado 1, letra f), y al apartado 2, del RGPD del Reino Unido, que establece las funciones de la ICO en relación con la tramitación de las reclamaciones. Tal como se describe en los considerandos 92 a 98, la ICO tiene el poder de evaluar la conformidad del responsable y el encargado del tratamiento con el RGPD del Reino Unido y la DPA de 2018, y de exigirles que adopten o se abstengan de adoptar las medidas necesarias en caso de incumplimiento e imponer multas.

(106) En segundo lugar, el RGPD del Reino Unido y la DPA de 2018 otorgan el derecho a la tutela judicial contra la ICO. Con arreglo al artículo 78, apartado 1, del RGPD del Reino Unido, un individuo tiene derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de la ICO que le concierna. En el contexto del control jurisdiccional, el juez examina la decisión impugnada en la reclamación y valora si la ICO ha actuado de manera lícita. Además, en virtud del artículo 78, apartado 2, del RGPD del Reino Unido, si la ICO no da curso a una reclamación presentada por el interesado ([116]), el reclamante tiene acceso a la tutela judicial. Este puede solicitar a un Tribunal de Primera Instancia que ordene a la ICO tomar las medidas adecuadas para responder a la reclamación, o para informar al reclamante sobre el progreso de la misma ([117]). Por otro lado, toda persona a la que la ICO haya hecho entrega de uno de los avisos mencionados anteriormente (de información, evaluación, ejecución o sanción) puede apelar ante un Tribunal de Primera Instancia ([118]). Si el tribunal considera que la decisión de la ICO no cumple con la ley o que la ICO debería haber ejercido su facultad de apreciación de manera diferente, entonces el tribunal debe permitir la apelación o sustituir cualquier otro aviso o decisión que la ICO pudiera haber dado o adoptado.

(107) En tercer lugar, todo individuo tiene derecho a emprender acciones judiciales contra los responsables y encargados del tratamiento directamente ante los tribunales, de conformidad con el artículo 79 del RGPD del Reino Unido y la sección 167 de la DPA de 2018. Si, en una solicitud por parte de un interesado, un tribunal está convencido de que ha habido una infracción de los derechos del interesado en virtud de la legislación en materia de protección de datos, el tribunal puede ordenar al responsable, en relación con el tratamiento (o un encargado que actúe en nombre de ese responsable del tratamiento), que tome las medidas especificadas en la resolución o que se abstenga de tomar las medidas especificadas en la misma.

(108) Además, con arreglo al artículo 82 del RGPD del Reino Unido y la sección 168 de la DPA de 2018, toda persona que haya sufrido daños y perjuicios materiales o inmateriales como resultado de una infracción del RGPD del Reino Unido tiene derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. Las normas relativas a la indemnización y la responsabilidad recogidas en el artículo 82, apartados 1 a 5, del RGPD del Reino Unido son idénticas a las normas correspondientes del Reglamento (UE) 2016/679. Con arreglo a la sección 168 de la DPA de 2018, los daños y perjuicios inmateriales incluyen también la ansiedad. En virtud del artículo 80 del RGPD del Reino Unido, el interesado tiene también derecho a dar mandato a un organismo u organización representante para presentar en su nombre la reclamación ante la ICO (con arreglo al artículo 77 del RGPD del Reino Unido) y a ejercer los derechos mencionados en los artículos 78 (derecho a la tutela judicial efectiva contra la ICO), 79 (derecho a la tutela judicial efectiva contra el responsable o encargado del tratamiento) y 82 (derecho a indemnización y responsabilidad) del RGPD del Reino Unido en su nombre.

(109) En cuarto lugar, y además de las vías de reparación descritas previamente, toda persona que considere que las autoridades públicas han violado sus derechos, incluidos los derechos a la privacidad y la protección de datos, puede obtener una reparación ante los tribunales del Reino Unido en virtud de la *Human Rights Act* de 1998 ([119]). Una persona física que alegue que una autoridad pública ha actuado (o se propone actuar) de una manera que es incompatible con un derecho del Convenio Europeo de Derechos Humanos y, por lo tanto, ilícita en virtud del artículo 6, apartado 1, de la *Human Rights Act* de 1998, puede iniciar un procedimiento contra dicha autoridad en el tribunal correspondiente, o apelar a los derechos de que se trate en cualquier procedimiento judicial cuando sea (o vaya a ser) víctima del acto ilícito.

(110) Si el tribunal determina que un acto de una autoridad pública es ilícito, puede conceder dicha compensación o reparación o dictar sentencia, dentro de sus facultades, según lo considere justo y adecuado ([120]). El tribunal también puede declarar que una disposición de la legislación primaria es incompatible con uno de los derechos del Convenio.

([115]) Artículo 77 del RGPD del Reino Unido.

([116]) La sección 166 de la DPA de 2018 se refiere, en particular, a las siguientes situaciones: a) la ICO no toma las medidas adecuadas para responder a la reclamación, b) la ICO no proporciona al reclamante información sobre el progreso de la reclamación, o sobre el resultado de la misma, antes de que finalice el período de tres meses que comienza en el momento en que la ICO recibe la reclamación, o c) si la valoración de la reclamación por parte de la ICO no concluye durante ese período y, por lo tanto, no facilita al reclamante dicha información durante un período posterior de tres meses.

([117]) Artículo 78, apartado 2, del RGPD del Reino Unido y sección 166 de la DPA de 2018.

([118]) Artículo 78, apartado 1, del RGPD del Reino Unido y sección 162 de la DPA de 2018.

([119]) Sección 7, apartado 1, de la *Human Rights Act* de 1998. Con arreglo a la sección 7, apartado 7, de esta misma Ley, una persona es víctima de un acto ilícito solo si también pudiera considerarse víctima a efectos del artículo 34 del Convenio Europeo de Derechos Humanos en caso de iniciarse un procedimiento ante el Tribunal Europeo de Derechos Humanos en relación con dicho acto ilícito.

([120]) Sección 8, apartado 1, de la *Human Rights Act* de 1998.

(111) Por último, una vez agotados los recursos nacionales, una persona puede obtener una reparación ante el Tribunal Europeo de Derechos Humanos por violaciones de los derechos garantizados por el Convenio Europeo de Derechos Humanos.

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

(112) La Comisión evaluó también el marco jurídico del Reino Unido para la recogida y el uso posterior de los datos personales que las autoridades públicas del Reino Unido transfieren a operadores comerciales del Reino Unido en interés público, en particular a efectos de control de la aplicación del Derecho penal y de seguridad nacional (en lo sucesivo, denominado «acceso gubernamental»). A la hora de evaluar si, con arreglo a la presente Decisión, las condiciones en las que el acceso del Gobierno a los datos transferidos al Reino Unido cumpliría la prueba de «equivalencia esencial» de conformidad con el artículo 45, apartado 1, del Reglamento (UE) 2016/679, según la interpretación del Tribunal de Justicia de la Unión Europea a la luz de la Carta de los Derechos Fundamentales, la Comisión tuvo en cuenta, en particular, los siguientes criterios.

(113) En primer lugar, cualquier limitación al derecho a la protección de datos personales debe estar prevista por la ley y la base jurídica que permite la injerencia en este derecho debe definir por sí misma el alcance de la limitación al ejercicio del derecho en cuestión ([121]).

(114) En segundo lugar, a fin de satisfacer el requisito de proporcionalidad, según el cual las excepciones y limitaciones a la protección de datos personales deben aplicarse únicamente en la medida en que sea estrictamente necesario en una sociedad democrática para lograr objetivos específicos de interés general equivalentes a los reconocidos por la Unión, la legislación del tercer país en cuestión que permite la interferencia debe establecer normas claras y precisas que regulen el alcance y la aplicación de dichas medidas e imponer salvaguardias mínimas para que las personas cuyos datos se hayan transferido dispongan de garantías suficientes para proteger de manera efectiva sus datos personales contra un posible riesgo de abuso ([122]). En particular, la legislación debe indicar en qué circunstancias y en qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos ([123]), así como someter el cumplimiento de tales requisitos a una supervisión independiente ([124]).

(115) En tercer lugar, esta legislación debe ser jurídicamente vinculante en virtud del Derecho interno y estos requisitos jurídicos no solo deben ser vinculantes para las autoridades, sino también exigibles ante los tribunales contra las autoridades del tercer país en cuestión ([125]). En concreto, los interesados deben tener la posibilidad de emprender acciones legales ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión ([126]).

3.1. **Marco jurídico general**

(116) Como ejercicio de poder por parte de una autoridad pública, el acceso del Gobierno en el Reino Unido debe llevarse a cabo con pleno respeto de la ley. El Reino Unido ha ratificado el Convenio Europeo de Derechos Humanos (véase el considerando 9) y todas las autoridades públicas del Reino Unido deben actuar de conformidad con el Convenio ([127]). El artículo 8 del Convenio establece que cualquier injerencia en la vida privada debe estar prevista por la ley, en interés de uno de los objetivos establecidos en el artículo 8, apartado 2, y proporcionada a la luz de ese objetivo. Asimismo, el artículo 8 exige que la injerencia sea «previsible», es decir, que tenga una base jurídica clara y accesible, y que la ley contenga las garantías adecuadas para evitar abusos.

(117) Además, en su jurisprudencia, el Tribunal Europeo de Derechos Humanos especifica que cualquier injerencia en el derecho a la privacidad y la protección de datos debe estar sujeta a un sistema de supervisión eficaz, independiente e imparcial que debe brindar un juez u otro organismo independiente ([128]) (por ejemplo, una autoridad administrativa o una instancia parlamentaria).

([121]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 174 y 175, y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véase también el asunto C-623/17 Privacy International/Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 65 (ECLI:EU:C:2020:790) y los asuntos acumulados C-511/18, C-512/18 y C-520/18 La Quadrature du Net y otros/Premier ministre y otros, apartado 175 (ECLI:EU:C:2020:791).

([122]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 176 y 181, y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véase también Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 68, y La Quadrature du Net y otros, apartado 132.

([123]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 176. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véase también Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 68, y La Quadrature du Net y otros, apartado 132.

([124]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 179.

([125]) Véase Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartados 181 y 182.

([126]) Véase Maximillian Schrems contra Data Protection Commissioner, apartado 95, y Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 194. En ese sentido, el TJUE ha destacado en particular que el cumplimiento del artículo 47 de la Carta de los Derechos Fundamentales, que garantiza el derecho a la tutela judicial efectiva ante un juez independiente e imparcial, «contribuye al nivel de protección exigido dentro la Unión Europea [y] debe ser constatado por la Comisión antes de adoptar una decisión de adecuación en virtud del artículo 45, apartado 1, del Reglamento (UE) 2016/679» (Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, apartado 186).

([127]) Sección 6 de la *Human Rights Act* de 1998.

([128]) Tribunal Europeo de Derechos Humanos, sentencia 5029/71, caso Klass y otros contra Alemania, apartados 17 a 51.

(118) Por otro lado, las personas deben disponer de una tutela judicial efectiva, y el Tribunal Europeo de Derechos Humanos ha aclarado que el recurso debe ofrecerlo un organismo independiente e imparcial que haya adoptado su propio reglamento interno, integrado por miembros que deben ostentar o haber ostentando un alto cargo judicial o ser abogados con experiencia, y que no debe haber una carga probatoria que deba superarse para presentar una demanda ante él. Al realizar el examen de las reclamaciones de las personas físicas, el organismo independiente e imparcial debe tener acceso a toda la información pertinente, incluidos los materiales restringidos. Por último, debe contar con los poderes para subsanar el incumplimiento ([129]).

(119) El Reino Unido ratificó también el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y firmó el Protocolo que modifica dicho Convenio en 2018 ([130]). El artículo 9 del Convenio establece que las excepciones a los principios generales de protección de datos (artículo 5, calidad de los datos), las normas que rigen las categorías especiales de datos (artículo 6, categorías particulares de datos) y los derechos del interesado (artículo 8, garantías complementarías para la persona concernida) solo son admisibles cuando dicha excepción está prevista por la ley de la Parte y constituye una medida necesaria en una sociedad democrática en interés de proteger la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la represión de infracciones penales, o para proteger al interesado o los derechos y libertades de otras personas ([131]).

(120) Por lo tanto, a través de la pertenencia al Consejo de Europa, la adhesión al Convenio Europeo de Derechos Humanos y el acatamiento de la jurisdicción del Tribunal Europeo de Derechos Humanos, el Reino Unido está sujeto a una serie de obligaciones, consagradas en el Derecho internacional, que enmarcan su sistema de acceso gubernamental sobre la base de principios, garantías y derechos individuales similares a los que garantiza el Derecho de la Unión y que son de aplicación en los Estados miembros. Tal como se destaca en el considerando 19, la adhesión continuada a dichos instrumentos es, por tanto, un elemento de especial importancia para la evaluación en la que se basa la presente Decisión.

(121) Además, la DPA de 2018 garantiza derechos y garantías específicos de protección de datos cuando los datos los tratan las autoridades públicas, incluidas las autoridades encargadas de garantizar el cumplimiento de la ley y los cuerpos nacionales de seguridad.

(122) En particular, el régimen para el tratamiento de datos personales en el ámbito penal se establece en la parte 3 de la DPA de 2018, que se promulgó a fin de adoptar la Directiva (UE) 2016/680. La parte 3 de la DPA de 2018 se aplica al tratamiento de datos personales 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 ([132]).

(123) En la sección 30 de la DPA de 2018 se define el concepto de «autoridad competente» como una persona incluida en el anexo 7 de la DPA, así como cualquier otra persona en la medida en que dicha persona tenga funciones estatutarias a efectos de la aplicación de la ley ([133]). Tal como se explica más adelante (véase el considerando 139), algunas autoridades competentes (por ejemplo, la National Crime Agency) pueden, en determinadas condiciones, ejercer los poderes previstos en la Investigatory Powers Act de 2016 (Ley de poderes de investigación, «IPA de 2016»). En este caso, además de las garantías establecidas en la parte 3 de la DPA de 2018, se aplicarán las garantías que establece la IPA de 2016. Los servicios de inteligencia (el Servicio de Inteligencia Secreto, el Servicio de Seguridad y el Cuartel General de Comunicaciones del Gobierno) no son «autoridades competentes» ([134]) con arreglo a la parte 3 de la DPA de 2018 y, por tanto, las normas previstas en ella no tienen aplicación en ninguna de sus actividades. Una parte específica de la DPA de 2018 (parte 4) trata sobre el tratamiento de datos personales por parte de los servicios de inteligencia (para más información, véase el considerando 125).

([129]) Tribunal Europeo de Derechos Humanos, sentencia 26839/05, caso Kennedy contra el Reino Unido, apartados 167 y 190.

([130]) Para más información sobre el Convenio Europeo de Derechos Humanos y su incorporación al Derecho del Reino Unido a través de la *Human Rights Act* de 1998, así como sobre el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, véase el considerando 9.

([131]) De igual manera, con arreglo al artículo 11 del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, las restricciones a ciertos derechos y obligaciones específicos del Convenio con fines de seguridad nacional o la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales solo son permisibles cuando dichas restricciones están previstas por la ley, respetan la esencia de los derechos y libertades fundamentales y constituyen una medida necesaria y proporcionada en una sociedad democrática. Las actividades de tratamiento con fines de seguridad nacional y defensa también deben someterse a una investigación y supervisión independientes y efectivas, de conformidad con la legislación nacional de la Parte respectiva del Convenio.

([132]) Sección 31 de la DPA de 2018.

([133]) Las autoridades competentes enumeradas en el anexo 7 no solo incluyen a las autoridades policiales, sino también a todos los departamentos gubernamentales ministeriales del Reino Unido, así como otras autoridades con funciones de investigación (p. ej., el Commissioner for Her Majesty's Revenue and Customs, la National Crime Agency, la Welsh Revenue Authority, la Competition and Markets Authority o Her Majesty's Land Register), agencias encargadas de perseguir la delincuencia, otras agencias de justicia penal y otros titulares u organizaciones que llevan a cabo actividades de aplicación de la ley (entre ellos, el anexo 7 de la DPA de 2018 enumera a los directores de la fiscalía, el director de la fiscalía de Irlanda del Norte o la ICO).

([134]) Sección 30, apartado 2, de la DPA de 2018.

(124) De manera similar a la Directiva (UE) 2016/680, la parte 3 de la DPA 2018 establece los principios de licitud y lealtad ([135]), limitación de la finalidad ([136]), minimización de los datos ([137]), exactitud ([138]), limitación del plazo de conservación ([139]) y seguridad ([140]). La legislación impone obligaciones específicas de transparencia ([141]) y otorga a las personas el derecho de acceso ([142]), rectificación y supresión ([143]) y el derecho a no estar sujeto a decisiones automatizadas ([144]). También se solicita a las autoridades competentes que apliquen la protección de datos desde el diseño y por defecto, que mantengan los registros de las actividades de tratamiento y, para determinadas operaciones de tratamiento, que lleven a cabo evaluaciones de impacto relativas a la protección de datos, previa consulta a la ICO ([145]). Con arreglo a la sección 56 de la DPA de 2018, también deben demostrar el cumplimiento de estas obligaciones. Además, están obligadas a aplicar medidas adecuadas para garantizar la seguridad del tratamiento ([146]) y están sujetas a obligaciones específicas en caso de una violación de la seguridad de los datos, incluida la notificación de dichas violaciones de la seguridad a la ICO y a los interesados ([147]). Al igual que en la Directiva (UE) 2016/680, también existe el requisito de que el responsable del tratamiento (salvo que sea un tribunal u otra autoridad judicial que actúe en el ejercicio de su función judicial) designe un delegado de protección de datos ([148]) que ayude al responsable del tratamiento en el cumplimiento de sus obligaciones y en el seguimiento de dicho cumplimiento ([149]). Por otro lado, la legislación impone requisitos específicos para las transferencias internacionales de datos personales con fines de aplicación de la ley a terceros países u organizaciones internacionales para garantizar la continuidad de la protección ([150]). En la misma fecha que la presente Decisión, la Comisión ha adoptado una decisión de adecuación sobre la base del artículo 36, apartado 3, de la Directiva (UE) 2016/680, al concluir 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 garantiza un nivel de protección esencialmente equivalente al que garantiza la Directiva (UE) 2016/680.

(125) La parte 4 de la DPA de 2018 se aplica a todo tratamiento de datos personales por parte de los servicios de inteligencia o realizado en su nombre. En concreto, establece los principios fundamentales de la protección de datos (licitud, lealtad y transparencia ([151]); limitación de la finalidad ([152]); minimización de los datos ([153]); exactitud ([154]); limitación del plazo de conservación ([155]) y seguridad ([156])), impone condiciones sobre el tratamiento de categorías especiales de datos ([157]), establece los derechos de los interesados ([158]), requiere la protección de datos desde el

([135]) Sección 35 de la DPA de 2018.
([136]) Sección 36 de la DPA de 2018.
([137]) Sección 37 de la DPA de 2018.
([138]) Sección 38 de la DPA de 2018.
([139]) Sección 39 de la DPA de 2018.
([140]) Sección 40 de la DPA de 2018.
([141]) Sección 44 de la DPA de 2018.
([142]) Sección 45 de la DPA de 2018.
([143]) Secciones 46 y 47 de la DPA de 2018.
([144]) Secciones 49 y 50 de la DPA de 2018.
([145]) Secciones 56 a 65 de la DPA de 2018.
([146]) Sección 66 de la DPA de 2018.
([147]) Secciones 67 y 68 de la DPA de 2018.
([148]) Secciones 69 a 71 de la DPA de 2018.
([149]) Secciones 67 y 68 de la DPA de 2018.
([150]) Parte 3, capítulo 5, de la DPA de 2018.
([151]) En virtud de la sección 86, apartado 6, de la DPA de 2018, para determinar la lealtad y la transparencia del tratamiento, debe tenerse en cuenta el método por el cual se obtienen los datos. En este sentido, el requisito de lealtad y transparencia se cumple si los datos se obtienen de una persona que está legalmente autorizada u obligada a proporcionarlos.
([152]) En virtud de la sección 87 de la DPA de 2018, los fines del tratamiento deben ser determinados, explícitos y legítimos. Los datos no pueden tratarse de una manera incompatible con los fines para los que se recogen. Con arreglo a la sección 87, apartado 3, de la DPA de 2018, solo se permite el tratamiento compatible adicional de datos personales si el responsable del tratamiento está autorizado por ley para tratar los datos para ese fin específico y si el tratamiento es necesario y proporcionado para dicho fin adicional. El tratamiento debe considerarse compatible cuando consiste en el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, y está sujeto a las garantías adecuadas (artículo 87, apartado 4, de la DPA de 2018).
([153]) Los datos personales deben ser adecuados, pertinentes y no excesivos (sección 88 de la DPA de 2018).
([154]) Los datos personales deben ser exactos y, si fuera necesario, actualizados (sección 89 de la DPA de 2018).
([155]) Los datos personales no deben conservarse más tiempo del necesario (sección 90 de la DPA de 2018).
([156]) El sexto principio de protección de datos es que los datos personales deben tratarse de una manera que incluya la adopción de medidas de seguridad adecuadas en relación con los riesgos que derivan del tratamiento de los mismos. Los riesgos incluyen (pero no se limitan a) acceso accidental o no autorizado, o la destrucción, pérdida, alteración o comunicación de datos personales (sección 91 de la DPA de 2018). La sección 107 también dispone que 1) cada responsable del tratamiento aplique medidas de seguridad adecuadas a los riesgos que derivan del tratamiento de datos personales y 2) en el caso de tratamiento automatizado, todos los responsables y encargados del tratamiento deben adoptar medidas preventivas o atenuantes basadas en una evaluación de riesgos.
([157]) Sección 86, apartado 2, letra b), y anexo 10, de la DPA de 2018.
([158]) Parte 4, capítulo 3, de la DPA de 2018, en particular los derechos: de acceso, de rectificación y supresión, a oponerse al tratamiento y a no ser objeto de decisiones automatizadas, a intervenir en la toma de decisiones automatizadas y a estar informado sobre la toma de decisiones. Además, el responsable del tratamiento debe brindar al interesado información en relación con el tratamiento de sus datos personales. Tal como se explica en las orientaciones de la ICO sobre el tratamiento por parte de los servicios de inteligencia, las personas pueden ejercer todos sus derechos (incluida una solicitud de rectificación) presentando una reclamación a la ICO o dirigiéndose a un tribunal (véanse las orientaciones de la ICO para el tratamiento por parte de los servicios de inteligencia, disponibles en el siguiente enlace https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

diseño ([159]) y regula las transferencias internacionales de datos personales ([160]). Recientemente, la ICO ha publicado orientaciones detalladas sobre el tratamiento por parte de los servicios de inteligencia, en la parte 4 de la DPA de 2018 ([161]).

(126) Al mismo tiempo, la sección 110 de la DPA de 2018 prevé una exención de las disposiciones especificadas en la parte 4 de esta Ley ([162]) cuando dicha exención sea necesaria para salvaguardar la seguridad nacional. Es posible acogerse a esta exención sobre la base de un análisis caso por caso ([163]). Tal como aclararon las autoridades del Reino Unido y como confirma la jurisprudencia, el «responsable del tratamiento debe tener en cuenta las consecuencias reales para la seguridad nacional o la defensa en caso de tener que cumplir con la disposición de protección de datos en cuestión, así como si podría cumplir razonablemente con la norma habitual sin perjudicar a la seguridad nacional o la defensa» ([164]). La ICO es la encargada de supervisar si la exención se ha utilizado adecuadamente o no ([165]).

(127) Además, en relación con la posibilidad de restringir la aplicación de las disposiciones específicas antes mencionadas, con arreglo a la sección 111 de la DPA de 2018, con el fin de proteger la «seguridad nacional», un responsable del tratamiento puede solicitar un certificado firmado por un ministro del Gabinete o por el fiscal general que certifique que una restricción de tales derechos constituye una medida necesaria y proporcionada para la protección de la seguridad nacional ([166]).

(128) El Gobierno del Reino Unido ha publicado una guía para ayudar a los responsables del tratamiento cuando deban considerar si deben solicitar un certificado de seguridad nacional con arreglo a la DPA de 2018, que destaca en particular que cualquier limitación a los derechos de los interesados para salvaguardar la seguridad nacional debe ser proporcionada y necesaria ([167]). Todos los certificados de seguridad nacional deben publicarse en el sitio web de la ICO ([168]).

([159]) Sección 103 de la DPA de 2018.

([160]) Sección 109 de la DPA de 2018. Es posible realizar transferencias de datos personales a organizaciones internacionales o países fuera del Reino Unido solo si la transferencia es una medida necesaria y proporcionada que se realiza para los fines de las funciones estatutarias del responsable del tratamiento, o para otros fines previstos en secciones específicas de la *Security Service Act* (Ley del servicio de seguridad) de 1989 y la *Intelligence Services Act* (Ley de servicios de inteligencia) de 1994.

([161]) Orientaciones de la ICO, véase la nota a pie de página 158.
Sección 30 de la DPA de 2018 y anexo 7 de la misma Ley.

([162]) La sección 110, apartado 2, de la DPA de 2018 enumera las disposiciones para las cuales es posible una exención. Esto incluye los principios de protección de datos (salvo el principio de licitud), los derechos del interesado, la obligación de informar a la ICO sobre una violación de la seguridad de los datos, los poderes de inspección de la ICO de acuerdo con las obligaciones internacionales, algunos de los poderes de ejecución de la ICO, las disposiciones que tipifican como delito determinadas violaciones de la protección de datos, y las disposiciones vinculadas a fines especiales de tratamiento, como fines periodísticos y fines de expresión académica y artística.

([163]) Véase *Baker v Secretary of State*, nota a pie de página 61.

([164]) Sección H del *UK Explanatory Framework for Adequacy Discussions*: *National Security Data Protection and Investigatory Powers Framework*, pp. 15 y 16 (véase la nota a pie de página 31). Véase también el asunto *Baker v Secretary of State* (véase la nota a pie de página 61), en el que el tribunal anuló un certificado de seguridad nacional emitido por el Home Secretary que confirmaba la aplicación de la excepción de seguridad nacional, sobre la base de que no había razón para establecer una excepción general a la obligación de responder a las solicitudes de acceso y que permitir tal excepción en toda circunstancia sin un análisis caso por caso excede lo que se considera necesario y proporcionado para la protección de la seguridad nacional.

([165]) Véase el memorando de entendimiento entre la ICO y UKIC, según el cual «cuando la ICO reciba una reclamación por parte de un interesado, la ICO querrá asegurarse de que el problema se ha manejado correctamente y, en su caso, que se ha hecho un uso adecuado de la aplicación de cualquier posible exención». Apartado 16 del memorando de entendimiento entre la ICO y la UK Intelligence Community (Comunidad de Inteligencia del Reino Unido), disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) La DPA de 2018 ha suprimido la posibilidad de emitir un certificado con arreglo a la sección 28, apartado 2, de la Data Protection Act de 1998. Sin embargo, la posibilidad de emitir «antiguos certificados» aún existe en la medida en que haya un recurso histórico en virtud de la Data Protection Act de 1998 (véase el apartado 17 de la parte 5 del anexo 20 de la DPA de 2018). Sin embargo, esta posibilidad parece ser excepcional y solo se aplicará a casos limitados, como, por ejemplo, cuando un interesado impugne el uso de la exención de seguridad nacional en relación con el tratamiento por parte de una autoridad pública que haya llevado a cabo el tratamiento con arreglo a la DPA de 1998. Cabe señalar que en estos casos, se aplicará la sección 28 de la DPA de 1998 en su totalidad, incluida, por tanto, la posibilidad de que el interesado impugne el certificado ante el Tribunal.

([167]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional en virtud de la *Data Protection Act* de 2018, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf Según la aclaración facilitada por las autoridades del Reino Unido, si bien un certificado es una prueba concluyente de que la exención es aplicable, con respecto a los datos o al tratamiento descritos en el certificado, esto no elimina el requisito de que el responsable del tratamiento valore si existe la necesidad de acogerse a la exención caso por caso.

([168]) De acuerdo con la sección 130 de la DPA de 2018, la ICO puede decidir no publicar el texto o parte del texto del certificado si fuese en contra del interés de la seguridad nacional, fuese contrario al interés público o pudiese poner en peligro la seguridad de una persona. Sin embargo, en estos casos, la ICO publicará el hecho de que el certificado ha sido emitido.

(129) El certificado debe tener una duración determinada de no más de cinco años, de modo que el poder ejecutivo pueda revisarlo periódicamente ([169]). En el certificado deben figurar los datos personales o las categorías de datos personales sujetos a la exención, así como las disposiciones de la DPA de 2018 a las que se aplica la exención ([170]).

(130) Es importante señalar que los certificados de seguridad nacional no prevén un motivo adicional para restringir los derechos de protección de datos por razones de seguridad nacional. En otras palabras, el responsable o encargado del tratamiento solo puede acogerse a un certificado cuando haya concluido que es necesario acogerse a la exención de seguridad nacional que, como se explicó anteriormente, debe aplicarse caso por caso ([171]). Aun en el caso de que un certificado de seguridad nacional se aplique al asunto en cuestión, la ICO puede investigar si el amparo en la exención de seguridad nacional estaba justificado en un caso específico ([172]).

(131) Cualquier persona directamente afectada por la emisión de un certificado puede apelar ante el Tribunal Superior ([173]) contra el certificado ([174]) o, cuando el certificado identifique datos mediante una descripción general, impugnar la aplicación del certificado a datos específicos ([175]). El tribunal revisará la decisión de emisión del certificado y decidirá si existían motivos razonables para su emisión ([176]). Puede tener en cuenta una amplia gama de cuestiones, incluida la necesidad, la proporcionalidad y la licitud, considerando el impacto en los derechos de los interesados y sopesando la necesidad de salvaguardar la seguridad nacional. Como resultado de ello, el tribunal puede determinar que el certificado no se aplica a los datos personales específicos objeto de la apelación ([177]).

(132) Un conjunto diferente de posibles restricciones se refiere a las que se aplican, con arreglo al anexo 11 de la DPA de 2018, a determinadas disposiciones de la parte 4 de dicha Ley ([178]) para salvaguardar otros objetivos importantes de interés público general o intereses protegidos como, por ejemplo, el privilegio parlamentario, la prerrogativa de confidencialidad, la conducción de procedimientos judiciales o la eficacia de combate de las fuerzas armadas ([179]). La aplicación de estas disposiciones está exenta para ciertas categorías de información («basadas en la clase») o exenta en la medida en que la aplicación de las disposiciones pueda perjudicar el interés protegido («basadas en el perjuicio») ([180]). Solo es posible apelar a las exenciones basadas en el perjuicio en la medida en que la aplicación de

([169]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 15, véase la nota a pie de página 167.

([170]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 5, véase la nota a pie de página 167.

([171]) Véase la nota a pie de página 164.

([172]) La sección 102 de la DPA de 2018 establece que el responsable del tratamiento debe poder demostrar su cumplimiento con la DPA de 2018. Esto implica que un servicio de inteligencia tendría que demostrar a la ICO que, al ampararse en la exención, se tuvieron en cuenta las circunstancias específicas del caso. La ICO también publica un registro de los certificados de seguridad nacional, que puede consultarse en el siguiente enlace: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) El Tribunal Superior es el tribunal competente para atender las apelaciones contra las decisiones de los tribunales administrativos inferiores y tiene competencia específica para las apelaciones directas contra las decisiones de ciertos órganos gubernamentales.

([174]) Sección 111, apartado 3, de la DPA de 2018.

([175]) Sección 111, apartado 5, de la DPA de 2018.

([176]) En *Baker v Secretary of State* (véase la nota a pie de página 61), el Tribunal de Información anuló un certificado de seguridad nacional emitido por el Home Secretary sobre la base de que no había razón para establecer una excepción general a la obligación de responder a las solicitudes de acceso y que permitir tal excepción en toda circunstancia sin un análisis caso por caso excede lo que se considera necesario y proporcionado para la protección de la seguridad nacional.

([177]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 25, véase la nota a pie de página 167.

([178]) Esto incluye: i) los principios de protección de datos recogidos en la parte 4, excepto por el requisito de licitud del tratamiento con arreglo al primer principio y el hecho de que el tratamiento debe cumplir una de las condiciones pertinentes establecidas en los anexos 9 y 10; ii) los derechos de los interesados; y iii) los deberes relacionados con la denuncia de violaciones de la seguridad de los datos a la ICO.

([179]) La parte 4 de la DPA de 2018 contempla el marco jurídico que se aplica a todos los tipos de tratamiento de datos personales por parte de los servicios de inteligencia (y no solo al ejercicio de sus funciones relacionadas con la seguridad nacional). Por consiguiente, la parte 4 también se aplica cuando los servicios de inteligencia traten datos, por ejemplo, a efectos de la gestión de recursos humanos, en el contexto de un litigio o de contratación pública. Las restricciones mencionadas en el anexo 11 están pensadas principalmente para aplicarse en estos otros contextos. Por ejemplo, en el contexto de un litigio con un empleado, se puede recurrir a la restricción a efectos de «procedimientos judiciales», o, en el contexto de la contratación pública, se puede recurrir a la restricción a efectos de «negociación», etc. Esto se refleja en las orientaciones de la ICO sobre el tratamiento por parte de los servicios de inteligencia, que mencionan la negociación como un acuerdo entre una agencia de inteligencia y un antiguo empleado que reclama derechos laborales como un ejemplo para la aplicación de las restricciones mencionadas en el anexo 11 (véase la nota a pie de página 161). Asimismo, cabe señalar que las mismas restricciones están disponibles para otras autoridades públicas de conformidad con el anexo 2 de la parte 2 de la DPA de 2018.

([180]) De acuerdo con el marco explicativo del Reino Unido, las excepciones que están «basadas en la clase» son: i) información sobre el otorgamiento de honores y dignidades de la Corona; ii) la prerrogativa de confidencialidad; iii) referencias confidenciales de empleo, formación o educación; y iv) exámenes escritos y calificaciones de exámenes. Las excepciones «basadas en el perjuicio» se relacionan con las siguientes cuestiones: i) prevención o detección de la delincuencia; detención y enjuiciamiento de los delincuentes; ii) privilegio parlamentario; iii) procedimientos judiciales; iv) la eficacia de combate de las fuerzas armadas de la Corona; v) el bienestar económico del Reino Unido; vi) negociaciones con el interesado de los datos; vii) fines de investigación científica e histórica o fines estadísticos; viii) fines de archivo en interés público. Sección H del *UK Explanatory Framework for Adequacy Discussions: National Security*, p. 13; véase la nota a pie de página 31.

las disposiciones de protección de datos enumeradas pueda perjudicar el interés específico en cuestión. Por tanto, el uso de una exención siempre debe justificarse haciendo referencia al perjuicio pertinente que probablemente se produciría en el caso en cuestión. En cuanto a las exenciones basadas en la clase, solo puede apelarse a ellas en relación con la categoría de información específica y estrechamente definida para la que se concede la exención. Estas son similares, en cuanto a su fin y efecto, a varias de las excepciones al RGPD del Reino Unido (con arreglo al anexo 2 de la DPA de 2018) que, a su vez, reflejan las previstas en el artículo 23 del Reglamento (UE) 2016/679.

(133) De lo anterior se desprende que las limitaciones y las condiciones están establecidas con arreglo a las disposiciones jurídicas aplicables del Reino Unido, así como de acuerdo con la interpretación que los tribunales y la ICO hacen de ellas, para garantizar que estas exenciones y restricciones permanezcan dentro de los límites de lo que es necesario y proporcionado para proteger la seguridad nacional.

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

(134) El Derecho del Reino Unido impone una serie de limitaciones al acceso y uso de datos personales a efectos de control de la aplicación del Derecho penal, y proporciona mecanismos de supervisión y reparación en este ámbito que se ajustan a los requisitos mencionados en los considerandos 113 a 115 de la presente Decisión. Las condiciones en las que puede tener lugar dicho acceso y las garantías aplicables al uso de estos poderes se precisan en detalle en las siguientes secciones.

3.2.1. *Base jurídica y limitaciones/garantías aplicables*

(135) De conformidad con el principio de licitud garantizado con arreglo a la sección 35 de la DPA de 2018, el tratamiento de datos personales para cualquiera de los fines de aplicación de la ley es lícito solo si se basa en la ley y si el interesado ha dado su consentimiento para el tratamiento para dicho fin ([181]) o el tratamiento es necesario para la realización de una tarea que una autoridad competente lleva a cabo a tal efecto.

3.2.1.1. Órdenes de registro y órdenes de entrega

(136) En el marco jurídico del Reino Unido, la recogida de datos personales de operadores económicos, incluidos los operadores que procesarían datos transferidos desde la UE en virtud de la presente decisión de adecuación, a efectos de control de la aplicación del Derecho penal, está permitida sobre la base de órdenes de registro ([182]) y órdenes de entrega ([183]).

(137) Las órdenes de registro las emite un tribunal, por lo general previa solicitud del agente investigador. Estas órdenes permiten que un agente entre en las instalaciones para buscar material o personas pertinentes para su investigación y que retenga cualquier cosa para la que se haya autorizado una búsqueda, incluidos los documentos o materiales pertinentes que contengan datos personales ([184]).

([181]) El uso del consentimiento no parece pertinente en un escenario de adecuación, ya que en una situación de transferencia los datos no los habrá recopilado directamente, sobre la base del consentimiento, una autoridad encargada de garantizar el cumplimiento de la ley del Reino Unido de un interesado de la UE.

([182]) Para la base jurídica pertinente, véanse la sección 8 y ss. de la *Police and Criminal Evidence Act* (Ley de pruebas policiales y penales) (PACE) de 1984 (para Inglaterra y Gales), la sección 10 y ss. de la *Police and Criminal Evidence Order (Northern Ireland)* de 1989 y para Escocia se obtiene en virtud del *common law* [véase la sección 46 de la *Criminal Justice (Scotland) Act* de 2016] y la sección 23B de la *Criminal Law (Consolidation) (Scotland)*. Para la orden de registro emitida después del arresto, la base jurídica es la sección 18 de la PACE de 1984 (para Inglaterra y Gales), las secciones 20 y ss. de la *Police and Criminal Evidence Order (Northern Ireland)* de 1989 y para Escocia se obtiene en virtud del *common law* [véase la sección 46 de la *Criminal Justice (Scotland) Act* de 2016]. Las autoridades del Reino Unido aclararon que las órdenes de registro las emite un tribunal, previa solicitud del agente investigador. Estas permiten al agente acceder a las instalaciones para buscar material o personas pertinentes para su investigación; la ejecución de la orden a menudo requerirá la ayuda de un agente de policía.

([183]) Cuando la investigación está relacionada con blanqueo de capitales (incluidos procesos de decomiso y recuperación civil), la base jurídica pertinente para solicitar una orden de entrega son la sección 345 y ss. para Inglaterra, Gales e Irlanda del Norte y la sección 380 y ss. de la *Proceeds of Crime Act* de 2002 para Escocia. Cuando la investigación está relacionada con otras cuestiones distintas al blanqueo de capitales, puede presentarse una solicitud de orden de entrega con arreglo a la sección 9 y el anexo 1 de la PACE de 1984 para Inglaterra y Gales, y la sección 10 y ss. de la *Police and Criminal Evidence Order (Northern Ireland)* de 1989 para Irlanda del Norte. En el caso de Escocia, las órdenes de producción se obtienen con arreglo al *common law* [véase la sección 46 de la *Criminal Justice Act (Scotland)* de 2016] y la sección 23B de la *Criminal Law (Consolidation) (Scotland)*. Las autoridades del Reino Unido aclararon que una orden de entrega requiere que la persona que figura en ella produzca o dé acceso al material que está en su posesión o bajo su control (véase el apartado 4, del anexo 1, de la PACE de 1984).

([184]) Por ejemplo, las secciones 8 y 18 de la PACE de 1984 contienen poderes para la incautación y el decomiso de cualquier cosa para la que se haya autorizado una búsqueda.

Las órdenes de entrega, que también debe emitirlas un tribunal, requieren que la persona que figura en ella produzca o dé acceso al material que está en su posesión o bajo su control. El solicitante debe justificar ante el tribunal por qué es necesaria la orden, así como por qué es de interés público. Hay varios poderes estatutarios que permiten la emisión de órdenes de registro y de entrega. Cada disposición tiene su propio conjunto de condiciones legales que deben cumplirse para que sea posible emitir una orden de registro ([185]) o una orden de entrega ([186]).

(138) Las órdenes de entrega y las órdenes de registro pueden impugnarse mediante un control jurisdiccional ([187]). En términos de garantías, todas las autoridades encargadas de garantizar el cumplimiento del Derecho penal que entran en el ámbito de aplicación de la parte 3 de la DPA de 2018 solo pueden acceder a los datos personales (lo que constituye una forma de tratamiento) de acuerdo con los principios y requisitos

([185]) Estas dos secciones de la PACE de 1984 regulan, respectivamente, el poder de un juzgado de paz para autorizar una orden judicial y de un agente de policía para registrar una propiedad. En el caso de la sección 8, antes de emitir una orden judicial, el juzgado de paz debe estar convencido de que existen motivos razonables para creer que: i) se ha cometido un delito grave; ii) hay material en las instalaciones cuyo valor es probablemente significativo (ya sea por sí mismo o junto con otro material) para la investigación del delito; iii) es probable que el material sea evidencia pertinente; iv) no consta ni incluye elementos sujetos a la prerrogativa de confidencialidad, material excluido o material de procedimiento especial; y v) no sería posible lograr la entrada a las instalaciones sin el uso de una orden judicial. En el caso de la sección 18, permite que un agente de policía registre las instalaciones de una persona arrestada por un delito grave en busca de material, que no sea material sujeto a la prerrogativa de confidencialidad, si tiene motivos razonables para sospechar que hay pruebas en las instalaciones que se relacionan con ese delito u otro delito grave similar o vinculado. El registro debe limitarse a descubrir ese material y debe autorizarlo, por escrito, un agente de policía que tenga, al menos, el rango de inspector, salvo que sea necesario para la investigación del delito. En tal caso, después de que se haya realizado el registro debe informarse tan pronto como sea posible a un agente de policía que tenga, al menos, el rango de inspector. Deben documentarse los motivos del registro y la naturaleza de las pruebas solicitadas. Por otro lado, las secciones 15 y 16 de la PACE de 1984 ofrecen garantías legales que deben seguirse al solicitar una orden de registro. La sección 15 especifica los requisitos aplicables para obtener una orden de registro (incluido el contenido de la solicitud presentada por el agente y el hecho de que la orden debe especificar, entre otras cosas, el acto normativo en virtud del cual se emite e identificar, tanto como sea posible, los artículos y personas a buscar y las instalaciones a registrar). La sección 16 rige cómo debe llevarse a cabo una búsqueda con arreglo a una orden judicial (por ejemplo: la sección 16, apartado 5, establece que el agente que ejecuta la orden debe proporcionar al ocupante una copia de la misma; la sección 16, apartado 11, requiere que la orden, una vez ejecutada, se conserve por un período de doce meses; la sección 16, apartado 12, otorga al ocupante el derecho de inspeccionar la orden durante ese período, si así lo desea). Estas secciones ayudan a garantizar el cumplimiento del artículo 8 del Convenio Europeo de Derechos Humanos [véase, por ejemplo, Kent Pharmaceuticals v Director of the Serious Fraud Office, 2002, EWHC 3023 (QB) en (30) por Lord Woolf CJ]. El resultado de un incumplimiento de estas garantías es que la búsqueda se declare ilícita [los ejemplos incluyen R (Brook) v Preston Crown Court, 2018, EWHC 2024 (Admin), (2018) ACD 95; R (Superior Import / Export Ltd) v Revenue and Customs Commissioners, 2017, EWHC 3172 (Admin), (2018) Lloyd's Rep FC 115; y R (F) v Blackfriars Crown Court, 2014, EWHC 1541 (Admin)]. Las secciones 15 y 16 de la PACE de 1984 se complementan con el código B de la PACE, un Código de prácticas que rige el ejercicio de los poderes policiales para registrar instalaciones.

([186]) Por ejemplo, cuando se emite una orden de entrega con arreglo a la Proceeds of Crime Act de 2002, además de la necesidad de tener motivos razonables para cumplir con las condiciones establecidas en la sección 346, apartado 2, de dicha Ley, debe haber motivos razonables de que la persona está en posesión o control del material así especificado y de que este material tiene un valor probablemente significativo. Además, otro requisito para emitir una orden de entrega es que debe haber motivos razonables para creer que el hecho de que el material se produzca o se dé acceso al mismo es en interés público, teniendo en cuenta a) el beneficio que probablemente devengaría para la investigación si se obtiene el material; y b) las circunstancias en virtud de las cuales la persona figura en la solicitud como persona en posesión o control del material que contiene su información. De igual manera, un tribunal que considere una solicitud para una orden de entrega con arreglo al anexo 1 de la PACE de 1984 debe estar convencido de que se cumplen las condiciones específicas. En particular, el anexo 1 de la PACE establece dos conjuntos alternativos separados de condiciones, de las cuales debe cumplirse una para que un juez pueda emitir una orden de entrega. El primer conjunto de condiciones requiere que el juez tenga motivos razonables para creer i) que se ha cometido un delito grave; ii) que el material que se busca en las instalaciones consiste o incluye un procedimiento especial pero no material excluido; iii) que el material tiene un valor probablemente significativo para la investigación, ya sea por sí solo o junto con otro material; iv) y es probable que constituya una prueba importante; v) ya se han intentado, o no se han intentado, otros métodos para obtener el material porque seguramente fracasarían; y vi) una vez se ha valorado el beneficio para la investigación y las circunstancias bajo las cuales el individuo está en posesión o control del material, es de interés público que se produzca el material o se dé acceso al mismo. El segundo conjunto de condiciones requiere que: i) haya material en las instalaciones que consista en un procedimiento especial o material excluido; i) hubiera podido emitirse una orden de registro para el material si no hubiera sido por la prohibición de registros realizados sobre la base de la legislación adoptada por la PACE para procedimientos especiales, material excluido o material sujeto al secreto profesional; y iii) hubiera sido adecuado hacerlo.

([187]) El control jurisdiccional es el procedimiento jurídico por el cual pueden ser impugnadas en el Tribunal Superior las decisiones de un organismo público. Los tribunales revisan la decisión que se ha impugnado y deciden si es defendible que esta sea jurídicamente defectuosa, teniendo en consideración conceptos/principios del Derecho público. Los motivos fundamentales para el control jurisdiccional son, a saber, la ilegalidad, la irracionalidad, la incorrección procesal, las expectativas legítimas y los derechos humanos. Después de un control jurisdiccional exitoso, un tribunal puede ordenar varios recursos diferentes. El más común es una orden de anulación (que anularía o cancelaría la decisión original, es decir, la decisión de emitir una orden de registro), y en algunas circunstancias esto también puede incluir la adjudicación de una compensación financiera. En la publicación del departamento jurídico del Gobierno del Reino Unido *Judge Over Your Shoulder – a guide to good decision-making* («Juzgar con la mayor dedicación: una guía para una buena toma de decisiones», documento en inglés), disponible en el siguiente enlace, hay más información sobre el control jurisdiccional en el Reino Unido: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

establecidos en la DPA de 2018 (véanse los considerandos 122 y 124). Por lo tanto, una solicitud que haya realizado cualquier autoridad encargada de garantizar el cumplimiento de la ley debe cumplir con el principio según el cual los fines del tratamiento deben ser determinados, explícitos y legítimos ([188]) y que los datos personales tratados por una autoridad competente deben ser pertinentes para ese propósito y no excesivos ([189]).

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

(139) Con el fin de prevenir o detectar solo delitos graves ([190]), ciertas autoridades encargadas de garantizar el cumplimiento de la ley, por ejemplo, la National Crime Agency o el jefe de policía ([191]), pueden utilizar poderes de investigación selectiva con arreglo a la IPA de 2016. En este caso, además de las garantías establecidas en la parte 3 de la DPA de 2018, se aplicarán las garantías que establece la IPA de 2016. 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), conservación de datos de comunicaciones (parte 4 de la IPA de 2016) e interferencia de equipos específicos (parte 5 de la IPA de 2016). La interceptación cubre la captación del contenido de una comunicación ([192]), mientras que la captación y la conservación de los datos de comunicaciones no tienen como objetivo obtener el contenido de la comunicación, sino la información relativa al «quién», «cuándo», «dónde» y «cómo» de la comunicación. Esto cubre, por ejemplo, el tiempo y la duración de una comunicación, el número de teléfono o la dirección de correo electrónico del remitente y el destinatario de la comunicación y, algunas veces, la ubicación de los dispositivos desde los que se realizó la comunicación, el suscriptor a un servicio telefónico o una facturación desglosada ([193]). La interferencia de equipos es un conjunto de técnicas que se utilizan para obtener una variedad de datos de los equipos, que incluyen ordenadores, tabletas y teléfonos inteligentes, así como cables y dispositivos de almacenamiento ([194]).

(140) Los poderes de interceptación selectiva también pueden utilizarse cuando «sea necesario a efectos de la aplicación de las disposiciones de un instrumento de asistencia mutua de la UE o un acuerdo internacional de asistencia mutua» (la denominada «orden de asistencia mutua» ([195])). Las órdenes de asistencia mutua solo se otorgan en relación con el fin de interceptación, no con la adquisición de datos de comunicaciones ni con la interferencia de equipos. Estos poderes específicos los regula la IPA de 2016 ([196]) que, junto con la *Regulation of Investigatory Powers Act* de 2000 (RIPA) para Inglaterra, Gales e Irlanda del Norte y la *Regulation of Investigatory Powers (Scotland) Act* de 2000 (RIPSA) para Escocia, establecen la base jurídica y establecen las limitaciones y garantías aplicables para el uso de tales poderes. La IPA de 2016 establece también el régimen para el uso de los poderes de investigación masiva de datos, aunque las autoridades encargadas de garantizar el cumplimiento de la ley no pueden hacer uso de ellos (solo están disponibles para los servicios de inteligencia pueden hacer uso de ellos) ([197]).

([188]) Sección 36, apartado 1, de la DPA de 2018.
([189]) Sección 37 de la DPA de 2018.
([190]) La sección 263, apartado 1, de la *Investigatory Powers Act* (IPA) (Ley de poderes de investigación) de 2016 establece que «delito grave» significa un delito por el que podría esperarse razonablemente que un adulto, que no tenía una condena previa, sea condenado a prisión por un período de tres años o más, o si la conducta implica el uso de la violencia conduciría a una ganancia económica sustancial, o bien si se trata de la conducta de un gran número de personas. Además, a efectos de la captación de comunicaciones con arreglo a la parte 4 de la IPA de 2016, la sección 87, apartado 10B de esta Ley establece que «delito grave» significa un delito por el que puede imponerse una pena de prisión de doce meses o más por una infracción cometida por una persona que no es una persona física, o bien que implique, como parte integrante de la misma, el envío de una comunicación o una violación de la privacidad de una persona.
([191]) En particular, las siguientes autoridades encargadas de garantizar el cumplimiento de la ley pueden solicitar una orden de interceptación selectiva: el director general de la National Crime Agency, el Commissioner of Police of the Metropolis, el Chief Constable of the Police Service of Northern Ireland, el Chief Constable of the Police Service of Scotland, el Commissioner for Her Majesty's Revenue and Customs, el Chief of Defence Intelligence y una persona que sea una autoridad competente de un país o territorio fuera del Reino Unido a los efectos de un instrumento de asistencia mutua de la UE o de un acuerdo internacional de asistencia mutua (sección 18, apartado 1, de la IPA de 2016).
([192]) Véase la sección 4 de la IPA de 2016.
([193]) Véase la sección 261, apartado 5, de la IPA de 2016 y el código de práctica sobre adquisición masiva de datos de comunicaciones, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf (apartado 2.9).
([194]) *Code of Practice on Equipment Interference*, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf (apartado 2.2).
([195]) Una orden de asistencia mutua autoriza a una autoridad del Reino Unido a brindar ayuda a una autoridad fuera del territorio del Reino Unido para la interceptación y la comunicación del material interceptado a dicha autoridad, con arreglo a un instrumento internacional de asistencia mutua (sección 15, apartado 4, de la IPA de 2016).
([196]) 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.
([197]) Sección 138, apartado 1, sección 158, apartado 1, sección 178, apartado 1, y sección 199, apartado 1, de la IPA de 2016.

(141) Para ejercer estos poderes, las autoridades deben obtener una orden ([198]) emitida por una autoridad competente ([199]) y aprobada por un comisionado judicial independiente ([200]) (el llamado procedimiento de «doble bloqueo»). Para obtener dicha orden debe realizarse un examen de necesidad y proporcionalidad ([201]). Dado que estos poderes de investigación selectiva que proporciona la IPA de 2016 son los mismos que los disponibles para las agencias de seguridad nacional, las condiciones, limitaciones y garantías aplicables a dichos poderes se tratan en detalle en la sección sobre acceso y el uso de datos personales por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional (véanse el considerando 177 y siguientes).

3.2.2. *Uso ulterior de la información recogida*

(142) 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») está sujeto a ciertas condiciones.

(143) De manera similar a lo que se establece en el artículo 4, apartado 2, de la Directiva (UE) 2016/680, la sección 36, apartado 3, de la DPA de 2018 permite que los datos personales recogidos por una autoridad competente con fines de aplicación de la ley puedan tratarse posteriormente (ya sea por parte del responsable original del tratamiento o por parte de otro responsable) para cualquier otro fin de aplicación de la ley, siempre que el responsable del tratamiento esté autorizado por ley para tratar datos para dicho fin y el tratamiento sea necesario y proporcionado para ese otro fin ([202]). En este caso, todas las garantías que establece la parte 3 de la DPA de 2018, recogidas en los considerandos 122 y 124, se aplican al tratamiento que realiza la autoridad receptora.

(144) En el ordenamiento jurídico del Reino Unido, distintas leyes permiten explícitamente este intercambio. En particular, i) la *Digital Economy Act* (Ley de economía digital) de 2017 permite el intercambio entre autoridades públicas para varios fines, por ejemplo, en caso de cualquier tipo de fraude contra el sector público que implique una pérdida o un riesgo de pérdida para las autoridades públicas ([203]), o en caso de una deuda con una autoridad pública o la Corona ([204]); ii) la *Crime and Courts Act* (Ley de delincuencia y tribunales) de 2013, que permite el intercambio de información con la National Crime Agency (NCA) ([205]) para combatir, investigar y perseguir la delincuencia organizada y grave; iii) la *Serious Crime Act* (Ley de delitos graves) de 2007 permite a las autoridades públicas comunicar información a organizaciones de lucha contra el fraude con fines de prevención del fraude ([206]).

(145) Estas leyes establecen explícitamente que el intercambio de información debe respetar los principios establecidos en la DPA de 2018. Además, el College of Policing ha emitido una práctica profesional autorizada sobre intercambio de información ([207]) para ayudar a la policía a cumplir con sus

([198]) La parte 2, capítulo 2, de la IPA de 2016 establece un número limitado de casos en los que puede realizarse una interceptación sin una orden judicial. Esto incluye: interceptación con el consentimiento del remitente o el destinatario, interceptación con fines administrativos o de ejecución, interceptación que se realice en determinadas instituciones (centros penitenciarios, hospitales psiquiátricos y centros de internamiento de inmigrantes), así como interceptación realizada con arreglo a un acuerdo internacional pertinente.

([199]) 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 la sección 106 de la IPA de 2016.

([200]) 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 (para más información, véase el considerando 162 y siguientes).

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

([202]) Sección 36, apartado 3, de la DPA de 2018.

([203]) Sección 56 de la *Digital Economy Act* de 2017, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) Sección 48 de la *Digital Economy Act* de 2017.

([205]) Sección 7 de la *Crime and Courts Act* de 2013, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) Sección 68 de la *Serious Crime Act* de 2007, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) La práctica profesional autorizada sobre intercambio de información está disponible en el siguiente enlace: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

obligaciones de protección de datos en virtud del RGPD del Reino Unido, la DPA y la *Human Rights Act* de 1998. El cumplimiento del intercambio con el marco jurídico de protección de datos aplicable está, por supuesto, sujeto a control jurisdiccional ([208]).

(146) Además, de manera similar a lo que dispone el artículo 9 de la Directiva (UE) 2016/680, la DPA de 2018 establece que los datos personales recogidos para cualquier propósito de aplicación de la ley pueden tratarse para un fin distinto siempre que dicho tratamiento esté autorizado por la ley ([209]).

(147) Este tipo de intercambio de datos cubre dos posibles escenarios: 1) cuando una autoridad encargada del cumplimiento del Derecho penal comparte datos con una autoridad que no está encargada del cumplimiento del Derecho penal que no es un servicio de inteligencia (como, por ejemplo, una autoridad financiera o fiscal, una autoridad de competencia, una oficina de servicio social para menores, etc.); y 2) cuando una autoridad encargada del cumplimiento del Derecho penal comparte datos con un servicio de inteligencia. En el primer escenario, el tratamiento de datos personales quedará dentro del alcance del RGPD del Reino Unido, así como de la parte 2 de la DPA de 2018. La Comisión ha evaluado las garantías que proporcionan el RGPD del Reino Unido y la parte 2 de la DPA de 2018 en los considerandos 12 a 111 y ha llegado a la conclusión de que el Reino Unido garantiza un nivel adecuado de protección de los datos personales que se transfieren, en el ámbito del Reglamento (UE) 2016/679, desde la Unión Europea al Reino Unido.

(148) En el segundo escenario, en relación con el intercambio con fines de seguridad nacional de datos recopilados por parte de una autoridad encargada del cumplimiento del Derecho penal con un servicio de inteligencia, la base jurídica que autoriza dicho intercambio es la sección 19 de la *Counter Terrorism Act* (Ley contra el terrorismo) de 2008 (CTA 2008) ([210]). Con arreglo a la CTA 2008, cualquier persona puede dar información a cualquiera de los servicios de inteligencia con el propósito de cumplir con cualquiera de las funciones de ese servicio, incluida la «seguridad nacional».

(149) Por lo que respecta a las condiciones en virtud de las cuales pueden compartirse datos con fines de seguridad nacional, la *Intelligence Services Act* ([211]) y la *Security Service Act* ([212]) limitan la capacidad de los servicios de inteligencia para obtener datos a lo que se considera necesario para el desempeño de sus funciones estatutarias. Los organismos encargados del cumplimiento de la ley que deseen compartir datos con los servicios de inteligencia deberán tener en cuenta una serie de factores/limitaciones, además de las funciones estatutarias de los organismos, que se establecen en la *Intelligence Services Act* y la *Security Service Act* ([213]). La sección 20 de la CTA de 2008 deja claro que cualquier intercambio de datos con arreglo a la sección 19 debe seguir cumpliendo con la legislación en materia de protección de datos, lo que significa que se aplican todas las limitaciones y requisitos recogidos en la parte 3 de la DPA de 2018. Además, dado que las autoridades competentes son autoridades públicas a efectos de la *Human Rights Act* de 1998, deben garantizar que actúan de conformidad con los derechos del Convenio Europeo de Derechos Humanos, incluido su artículo 8. Estas limitaciones garantizan que todo intercambio de datos entre los organismos encargados del cumplimiento de la ley y los servicios de inteligencia cumpla con la legislación en materia de protección de datos y con el Convenio Europeo de Derechos Humanos.

([208]) Véase, por ejemplo, el asunto *M, R v the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), en el que se solicitó al Tribunal Superior que considerara el intercambio de datos entre la policía y una asociación para la reducción de la delincuencia empresarial (BCRP, por sus siglas en inglés), una organización facultada para administrar sistemas de aviso de exclusión, que prohíben a las personas entrar en los locales comerciales de sus miembros. El tribunal revisó el intercambio de datos, que se estaba realizando con arreglo a un acuerdo con el fin de proteger al público y prevenir la delincuencia y, finalmente, concluyó que la mayoría de los aspectos del intercambio de datos eran lícitos, excepto en relación con cierta información confidencial compartida entre la policía y la BCRP. Otro ejemplo es el asunto *Cooper v NCA* [2019] EWCA Civ 16, en el que el Tribunal de Apelación confirmó el intercambio de datos entre la policía y la Serious Organised Crime Agency (SOCA), un cuerpo de seguridad que actualmente forma parte de la NCA.

([209]) Sección 36, apartado 4, de la DPA de 2018.

([210]) *Counter Terrorism Act* de 2008, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) *Intelligence Services Act* de 1994, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) *Security Service Act* de 1989, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) La sección 2, apartado 2, de la *Intelligence Services Act* de 1994 dispone que «El director del servicio de inteligencia será responsable de la eficiencia de ese servicio y será su deber asegurar a) que existan acuerdos para garantizar que el servicio de inteligencia no obtiene ninguna información, excepto en la medida necesaria para el debido desempeño de sus funciones, y que no comunique ninguna información salvo en la medida en que sea necesario: i) para dicho fin; ii) en interés de la seguridad nacional; iii) a efectos de prevenir o detectar delitos graves; o iv) a efectos de cualquier procedimiento penal; y b) que el servicio de inteligencia no toma ninguna medida para promover los intereses de ningún partido político del Reino Unido», mientras que la sección 2, apartado 2, de la *Security Service Act* de 1989 establece que «El director general será responsable de la eficiencia del servicio y será su deber asegurar a) que existen acuerdos para garantizar que el servicio no obtiene ninguna información, excepto en la medida necesaria para el debido desempeño de sus funciones, y que no comunica información, salvo en la medida en que sea necesario para tal fin o a efectos de prevenir o detectar delitos graves, o bien a efectos de cualquier procedimiento penal; y b) que el servicio no toma medidas para promover los intereses de ningún partido político; y c) que existen acuerdos, establecidos con el director general de la National Crime Agency, para coordinar las actividades del servicio en virtud de la sección 1, apartado 4, de esta Ley con las actividades de las fuerzas policiales, la National Crime Agency y otros organismos encargados del cumplimiento de la ley».

(150) En los casos en los que una autoridad competente tiene la intención de intercambiar datos personales, tratados en virtud de la parte 3 de la DPA de 2018, con las autoridades encargadas del cumplimiento de la ley de un tercer país se aplican requisitos específicos ([214]). En concreto, dichas transferencias pueden realizarse cuando se basan en normas en materia de adecuación adoptadas por el secretario de Estado o, en ausencia de tales regulaciones, deben asegurarse las garantías adecuadas. La sección 75 de la DPA de 2018 establece que existen garantías adecuadas cuando las establece un instrumento jurídico que vincula al destinatario, o cuando el responsable del tratamiento, una vez que ha evaluado todas las circunstancias que rodean las transferencias de ese tipo de datos personales al tercer país u organización internacional, llega a la conclusión de que existen las garantías adecuadas para proteger los datos.

(151) Si una transferencia no se basa en una norma en materia de adecuación o en garantías adecuadas, entonces solo puede realizarse en determinas circunstancias específicas, denominadas «circunstancias especiales» ([215]). Este es el caso cuando la transferencia es necesaria: a) para proteger los intereses vitales del interesado o de otra persona; b) para salvaguardar intereses legítimos del interesado; c) para prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro o de un tercer país; d) en un caso concreto a efectos de aplicación de la ley; o e) en un caso concreto con fines jurídicos (como en relación con procedimientos legales o para obtener asesoramiento jurídico). Cabe señalar que los supuestos d) y e) no se aplican si los derechos y libertades del interesado prevalecen sobre el interés público en la transferencia. Este conjunto de circunstancias corresponde a las situaciones y condiciones específicas que se califican como «excepciones» con arreglo al artículo 38 de la Directiva (UE) 2016/680.

(152) Por otro lado, la IPA de 2016 impone garantías adicionales cuando se entrega a un tercer país material adquirido por parte de las autoridades encargadas del cumplimiento de la ley en virtud de una orden que autoriza el uso de interceptación o interferencia de equipos. En concreto, este tipo de comunicación, que se denomina «comunicación internacional», solo se permite si la autoridad emisora considera que existen acuerdos específicos adecuados que limitan el número de personas a las que se comunican los datos y la medida en que se comunica o se pone a disposición cualquier material, así como la medida en que se copia el material y el número de copias realizadas. Además, la autoridad emisora puede considerar que son necesarios acuerdos apropiados para garantizar que se destruye cada copia realizada de cualquier parte de ese material tan pronto como dejen de existir motivos pertinentes para conservarla (si no se destruye antes) ([216]).

(153) Por último, en el futuro podrían realizarse transferencias ulteriores del Reino Unido a los Estados Unidos sobre la base del Acuerdo entre el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte y el Gobierno de los Estados Unidos de América sobre el acceso a datos electrónicos con el fin de combatir delitos graves (el «Acuerdo entre el Reino Unido y EE. UU.» o «el Acuerdo») ([217]), celebrado en octubre de 2019 ([218]). Si bien el Acuerdo entre el Reino Unido y EE. UU. todavía no ha entrado en vigor en el momento de la adopción de la presente Decisión, su probable entrada en vigor puede afectar a las transferencias ulteriores a Estados Unidos de datos transferidos primero al Reino Unido sobre la base de esta Decisión. Más concretamente, los datos transferidos desde la UE a proveedores de servicios en el Reino Unido podrían estar sujetos a órdenes para la producción de pruebas electrónicas emitidas por las autoridades competentes de Estados Unidos encargadas del cumplimiento de la ley, y que podrían aplicarse en el Reino Unido en virtud de dicho Acuerdo, una vez que entre en vigor. Por estos motivos, es pertinente para la presente Decisión la evaluación de las condiciones y garantías en virtud de las cuales pueden emitirse y ejecutarse dichas órdenes.

([214]) Véase la parte 3, capítulo 5, de la DPA de 2018.

([215]) Sección 76 de la DPA de 2018.

([216]) Secciones 54 y 130 de la IPA de 2016. Las autoridades emisoras deben valorar la necesidad de imponer garantías específicas al material entregado a autoridades extranjeras, a fin de asegurarse de que los datos están sujetos a garantías en términos de conservación, destrucción y comunicación similares a los que establecen las secciones 53 y 129 de la IPA de 2016.

([217]) 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.

([218]) Este es el primer acuerdo alcanzado bajo la *Clarifying Lawful Overseas Use of Data Act* (CLOUD) de los Estados Unidos. La *Cloud Act* es una ley federal de los Estados Unidos que se adoptó el 23 de marzo de 2018 y que aclara, a través de una enmienda de la *Stored Communications Act* de 1986, que los proveedores de servicios de Estados Unidos están obligados a cumplir con las órdenes estadounidenses de comunicación de datos de contenido y datos sin contenido, independientemente de dónde se conserven dichos datos. La Cloud Act también permite la celebración de acuerdos ejecutivos con gobiernos extranjeros, sobre la base de los cuales los proveedores de servicios de Estados Unidos podrían entregar datos de contenido directamente a estos gobiernos extranjeros (el texto de la Cloud Act está disponible en el siguiente enlace: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) En este sentido, cabe señalar que, en primer lugar, en lo que respecta a su alcance material, el Acuerdo solo es aplicable a delitos que sean punibles con una pena máxima de encarcelación de, al menos, tres años (definido como «delito grave») ([219]), incluyendo «actividad terrorista». En segundo lugar, que los datos tratados en la otra jurisdicción pueden obtenerse en virtud de este Acuerdo solo como consecuencia de una «Orden [...] sujeta a control o supervisión, con arreglo al Derecho interno de la Parte emisora, por parte de un tribunal, juez, magistrado u otra autoridad independiente antes o durante el proceso con respecto a la ejecución de la Orden» ([220]). En tercer lugar, que cualquier orden debe «basarse en requisitos para una justificación razonable basada en hechos articulables y creíbles, particularidad, licitud y gravedad en relación con la conducta sometida a investigación» ([221]) y «estar dirigida a cuentas específicas, así como identificar a una persona, cuenta, dirección, dispositivo personal o cualquier otro identificador específico» ([222]). En cuarto lugar, que los datos obtenidos en virtud de este Acuerdo se benefician de protecciones equivalentes a las garantías específicas que brinda el denominado «Acuerdo marco UE-EE. UU.» ([223]), un acuerdo integral de protección de datos firmado en diciembre de 2016 por la UE y los Estados Unidos y que establece las garantías y derechos aplicables a las transferencias de datos en el ámbito de la cooperación policial, y que se incorporan todas en este Acuerdo por referencia *mutatis mutandis* para tener en cuenta, en particular, la naturaleza específica de las transferencias (es decir, transferencias de operadores privados a las autoridades encargadas de garantizar el cumplimiento de la ley, en lugar de transferencias entre las propias autoridades encargadas de garantizar el cumplimiento de la ley) ([224]). El Acuerdo entre el Reino Unido y EE. UU. establece específicamente que se aplicarán protecciones equivalentes a las que brinda el Acuerdo marco UE-EE. UU. «a toda la información personal producida durante la ejecución de órdenes sujetas al Acuerdo para producir protecciones equivalentes» ([225]).

(155) Los datos transferidos a las autoridades de los Estados Unidos en virtud del Acuerdo entre el Reino Unido y EE. UU. deberían beneficiarse de las mismas protecciones que brinda un instrumento legislativo de la UE, con las adaptaciones necesarias para reflejar la naturaleza de las transferencias en cuestión. Las autoridades del Reino Unido han confirmado, además, que las protecciones del Acuerdo marco se aplicarán a toda la información personal producida o conservada en virtud del Acuerdo, independientemente de la naturaleza o el tipo de organismo que realiza la solicitud (p. ej., tanto las autoridades policiales federales como estatales de los Estados Unidos), por lo que debe proporcionarse una protección equivalente en todos los casos. Sin embargo, las autoridades del Reino Unido también han aclarado que los detalles de la aplicación completa de las garantías de protección de datos todavía están sujetos a conversaciones entre el Reino Unido y los Estados Unidos. En el contexto de las conversaciones con los servicios de la Comisión Europea en torno a la presente decisión, las autoridades del Reino Unido confirmaron que el Acuerdo solo entrará en vigor cuando estén satisfechas de que su aplicación cumple con las obligaciones jurídicas previstas en el mismo, incluida la claridad con respecto al cumplimiento de las normas de protección de datos para cualquier dato solicitado en virtud de este Acuerdo. Dado que una posible entrada en vigor del Acuerdo puede afectar al nivel de protección valorado en la presente Decisión, el Reino Unido debe comunicar a la Comisión Europea, tan pronto como esté disponible y, en cualquier caso, antes de la entrada en vigor del Acuerdo, cualquier información y aclaración futura sobre la forma en que los Estados Unidos cumplirán con sus obligaciones en virtud del Acuerdo, a fin de garantizar un seguimiento adecuado de esta decisión en virtud de artículo 45, apartado 4, del Reglamento (UE) 2016/679. Se prestará especial atención a la aplicación y adaptación de las protecciones del Acuerdo marco al tipo específico de transferencias contempladas por el Acuerdo entre el Reino Unido y EE. UU.

(156) De manera más general, cualquier desarrollo pertinente en lo que respecta a la entrada en vigor y la aplicación del Acuerdo se tendrá debidamente en cuenta en el contexto del seguimiento continuo de esta decisión, en especial en lo que respecta a las consecuencias necesarias que deban extraerse en caso de haber indicios de que ya no se garantiza un nivel de protección esencialmente equivalente.

3.2.3. *Supervisión*

(157) Dependiendo de los poderes que emplean las autoridades competentes al tratar datos personales con fines de aplicación de la ley (ya sea en el marco de la DPA de 2018 o la IPA de 2016), diferentes organismos garantizan la supervisión del uso de estos poderes. En concreto, la ICO supervisa el tratamiento de datos personales cuando entra

([219]) Artículo 1, apartado 14, del Acuerdo.

([220]) Artículo 5, apartado 2, del Acuerdo.

([221]) Artículo 5, apartado 1, del Acuerdo.

([222]) Artículo 4, apartado 5, del Acuerdo. Se aplica una normal adicional y más estricta a la interceptación en tiempo real: las órdenes deben tener una duración limitada, que no será superior a lo razonablemente necesario para cumplir con los propósitos de la orden, y solo se emitirán si la misma información no puede obtenerse razonablemente mediante un método menos intrusivo (artículo 5, apartado 3, del Acuerdo).

([223]) 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), disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.

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

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

dentro del ámbito de la parte 3 de la DPA de 2018 ([226]). La Investigatory Powers Commissioner's Office (IPCO) ([227]) garantiza la supervisión judicial e independiente sobre el uso de los poderes de investigación en virtud de la IPA de 2016 (esta parte se aborda en los considerandos 250 a 255). Además, el Parlamento y otros órganos garantizan una supervisión adicional.

3.2.3.1 Supervisión de la parte 3 de la DPA de 2018

(158) En el anexo 13 de la DPA de 2018 se establecen las funciones generales de la ICO, cuya independencia y organización se detallan en el considerando 87, en relación con el tratamiento de datos personales que entran en el ámbito de aplicación de la parte 3 de dicha Ley. La labor principal de la ICO es la supervisión y el cumplimiento de la parte 3 de la DPA de 2018, así como promover la sensibilización del público, asesorar al Parlamento, al Gobierno y a otras instituciones y organismos. A fin de mantener la independencia del poder judicial, la ICO no está autorizada para ejercer sus funciones en relación con el tratamiento de datos personales por parte de una persona en el ejercicio de su función judicial o de un tribunal que actúe en el ejercicio de su función judicial. En estas circunstancias, otros organismos ejercerían las funciones de supervisión, como se explica en los considerandos 99 a 103.

(159) La ICO tiene competencias generales de investigación, corrección, autorización y asesoramiento en relación con el tratamiento de datos personales que entra en el ámbito de la parte 3 de la DPA. En particular, la ICO tiene competencias para notificar al responsable o al encargado del tratamiento acerca de una supuesta infracción de la parte 3 de la DPA de 2018, emitir advertencias o sanciones a un responsable o encargado del tratamiento que haya infringido las disposiciones de la parte 3 de la Ley, así como para emitir por propia iniciativa o previa solicitud dictámenes al Parlamento, al Gobierno u otras instituciones y organismos, así como al público sobre cualquier tema relacionado con la protección de datos personales ([228]).

(160) Además, la ICO tiene competencias para emitir avisos de información ([229]), de evaluación ([230]) y de ejecución ([231]), así como la competencia para acceder a los documentos de responsables y encargados del tratamiento, acceder a sus instalaciones ([232]) y emitir multas administrativas en forma de avisos de sanción ([233]). La política de acción reguladora de la ICO establece las circunstancias en virtud de las cuales emitir un aviso de información, de evaluación, de ejecución o de sanción ([234]) [véase también el considerando 93 y los considerandos 101 y 102 de la decisión de adecuación de la Directiva (UE) 2016/680].

(161) Según sus últimos informes anuales (2018-2019 ([235]), 2019-2020 ([236])), la ICO ha llevado a cabo una serie de investigaciones y ha adoptado medidas de ejecución con respecto al tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento de la ley. Por ejemplo, la ICO realizó una investigación y publicó un dictamen en octubre de 2019 sobre el uso de la tecnología de reconocimiento facial con fines de aplicación de la ley en lugares públicos. La investigación se centró, en concreto, en el uso de capacidades de reconocimiento facial en directo por parte de la policía de Gales del Sur y la Policía Metropolitana de Londres. La ICO investigó también la «Gangs Matrix» ([237]) de la Policía Metropolitana de Londres y encontró una serie de infracciones graves de la ley de protección de datos que probablemente debilitarían la confianza del público en la matriz y en cómo se estaban utilizando los datos. En noviembre de 2018, la ICO emitió un aviso de ejecución y, posteriormente, la Policía Metropolitana de Londres tomó las medidas necesarias para aumentar la seguridad y la responsabilidad, y para garantizar el uso de los datos de manera proporcional. Otro ejemplo de una medida de ejecución en esta área es la multa de 325 000 libras esterlinas emitida por

([226]) Sección 116 de la DPA de 2018.
([227]) Véase la IPA de 2016 y, en particular, la parte 8, capítulo 1.
([228]) Apartado 2, anexo 13, de la DPA de 2018.
([229]) Que solicitan al responsable o encargado del tratamiento (y, en determinadas circunstancias, a cualquier otra persona) que proporcione la información necesaria (sección 142 de la DPA de 2018).
([230]) Que permiten realizar investigaciones y auditorías, que pueden requerir que el responsable o encargado del tratamiento permita a la ICO la entrada a instalaciones específicas, inspeccionar o examinar documentos o equipos y entrevistar a personas que tratan datos personales en nombre del responsable (sección 146 de la DPA de 2018).
([231]) Que permiten el ejercicio de poderes correctivos, lo que requiere que los responsables/encargados del tratamiento tomen o se abstengan de adoptar medidas específicas (sección 149 de la DPA de 2018).
([232]) Sección 154 de la DPA de 2018.
([233]) Sección 155 de la DPA de 2018.
([234]) Política de acción reguladora de la ICO, véase la nota a pie de página 96.
([235]) *Annual Report and Financial Statements 2018-2019* («Informe anual y estados financieros 2018-2019», documento en inglés) de la ICO; véase la nota a pie de página 101.
([236]) *Annual Report and Financial Statements 2019-2020* («Informe anual y estados financieros 2019-2020», documento en inglés) de la ICO; véase la nota a pie de página 82.
([237]) Una base de datos que registraba inteligencia relacionada con presuntos miembros de bandas y víctimas de delitos relacionados con bandas.

la ICO en mayo de 2018 contra el Crown Prosecution Service, por perder múltiples DVD sin cifrar que contenían grabaciones de entrevistas policiales. La ICO realizó llevó también a cabo investigaciones sobre temas más amplios; por ejemplo, en el primer semestre de 2020 sobre el uso de la extracción de teléfonos móviles con fines policiales y sobre el tratamiento de los datos de las víctimas por parte de la policía. Además, la ICO está investigando en estos momentos un caso que implica el acceso por parte de las autoridades encargadas de garantizar el cumplimiento de la ley a datos en poder de una entidad del sector privado, Clearview AI Inc. ([238]).

(162) Además de los poderes de ejecución de la ICO mencionados en los considerandos 160 y 161, ciertas violaciones de la legislación en materia de protección de datos constituyen infracciones y, por tanto, pueden estar sujetas a sanciones penales (sección 196 de la DPA de 2018). Esto aplica, por ejemplo, a la obtención, comunicación o conservación de datos personales sin el consentimiento del responsable del tratamiento y a facilitar la comunicación de datos personales a otra persona sin el consentimiento del responsable del tratamiento ([239]); a la desanonimización de información basada en datos personales anonimizados sin el consentimiento del responsable del tratamiento encargado de la anonimización de los datos personales ([240]); y a obstaculizar de forma intencionada a la ICO para ejercer sus poderes en relación con la inspección de datos personales con arreglo a las obligaciones internacionales ([241]), realizar declaraciones falsas en respuesta a un aviso de información o destruir información en relación con avisos de información y evaluación ([242]).

3.2.3.2. Otros organismos de supervisión en el ámbito penal

(163) Además de la ICO, existen varios organismos de supervisión en el ámbito penal con mandatos específicos pertinentes en cuestiones de protección de datos. Por ejemplo, el Commissioner for the Retention and Use of Biometric Material ([243]) (Comisionado para la Retención y Uso de Material Biométrico) y el Surveillance Camera Commissioner ([244]) (Comisionado de Cámaras de Vigilancia).

3.2.3.3. Supervisión del Parlamento en el ámbito penal

(164) El Home Affairs Select Committee (Comité Selecto de Asuntos Internos) garantiza la supervisión parlamentaria en el ámbito de la aplicación de la ley. Este Comité está formado por once miembros del Parlamento, procedentes de los tres partidos políticos mayoritarios. El Comité tiene la labor de examinar el gasto, la administración y la política del Ministerio del Interior y los organismos públicos asociados, en concreto, la policía y la NCA, cuyo trabajo el Comité puede examinar específicamente ([245]).

([238]) Véase la declaración de la ICO en el siguiente enlace: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) Sección 170 de la DPA de 2018.

([240]) Sección 171 de la DPA de 2018.

([241]) Sección 119, apartado 6, de la DPA de 2018.

([242]) Durante el ejercicio fiscal que abarca el período comprendido entre el 1 de abril de 2019 y el 31 de marzo de 2020, las investigaciones de la ICO dieron lugar a cuatro amonestaciones y ocho enjuiciamientos. Estos casos se procesaron con arreglo a la sección 55 de la *Data Protection Act* de 1998, la sección 77 de la *Freedom of Information Act* de 2000 y la sección 170 de la *Data Protection Act* de 2018. En el 75 % de los casos, los demandados se declararon culpables negando la necesidad de juicios prolongados, con los consiguientes costes asociados. [*Annual Report and Financial Statements 2019-2020* («Informe anual y estados financieros 2019-2020», documento en inglés) de la ICO; véase la nota a pie 87, página 40].

([243]) El Biometrics Commissioner fue establecido por la *Protection of Freedoms Act* (Ley de protección de las libertades) de 2012 (véase https://www.legislation.gov.uk/ukpga/2012/9/contents). El comisionado, entre otras funciones, decide si las autoridades policiales pueden retener o no registros de perfiles de ADN y huellas dactilares obtenidos de personas arrestadas pero no acusadas de un delito clasificado (sección 63G de la PACE de 1984). Además, el comisionado tiene la responsabilidad general de revisar la conservación y el uso de ADN y huellas dactilares, así como la conservación por motivos de seguridad nacional (sección 20, apartado 2, de la *Protection of Freedom Act* de 2012). El Comisionado se nombra conforme a lo dispuesto en el *Code for Public Appointments* («Código para nombramientos públicos», disponible en el siguiente enlace: https://www.gov.uk/government/publications/governance-code-for-public-appointments) y las condiciones de su nombramiento dejan claro que solo puede ser destituido de su cargo por decisión del Home Secretary en un conjunto de circunstancias estrechamente definido; estas incluyen el incumplimiento de sus obligaciones por un período de tres meses, una condena por delito penal o el incumplimiento de las condiciones de su nombramiento.

([244]) El Surveillance Camera Commissioner fue establecido por la *Protection of Freedoms Act* de 2012 y tiene la función de fomentar el cumplimiento del código de prácticas en materia de cámaras de vigilancia, revisar el funcionamiento de este código y asesorar a los ministros sobre la necesidad de modificar el código. El comisionado se nombra de conformidad con las mismas normas que los Biometrics Commissioners y goza de los mismos poderes, recursos y protección contra la expulsión.

([245]) Véase https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/.

(165) El Comité puede, dentro de los límites de su competencia, elegir su propio tema de investigación, incluidos casos específicos, siempre que el tema no esté pendiente de resolución judicial. El Comité también puede buscar pruebas escritas y orales de una amplia gama de grupos e individuos relevantes. Redacta informes sobre sus conclusiones y emite recomendaciones al Gobierno ([246]). El Gobierno debe responder a cada una de las recomendaciones de los informes, y debe hacerlo en un plazo de sesenta días ([247]).

(166) En el área de la vigilancia, el Comité también ha elaborado un informe relativo a la *Regulation of Investigatory Powers Act* (RIPA) de 2000 ([248]), que concluyó que la RIPA de 2000 no era adecuada para su propósito. Este informe se tuvo en cuenta durante la sustitución de partes importantes de la RIPA 2000 con partes de la IPA 2016. En el sitio web del Comité puede encontrarse una lista completa de las consultas ([249]).

(167) En Escocia, las tareas del Home Affairs Select Committee las lleva a cabo el Justice Subcommittee on Policing, y en Irlanda del Norte el Committee for Justice ([250]).

3.2.4. *Acciones administrativas y judiciales*

(168) Por lo que respecta al tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento de la ley, los mecanismos de reparación están disponibles en la parte 3 de la DPA de 2018 y en la IPA de 2016, así como en la *Human Rights Act* de 1998.

(169) Esta serie de mecanismos ofrecen a los interesados acciones administrativas y judiciales efectivas que les permiten, en particular, garantizar sus derechos, en especial el derecho a acceder a sus datos personales o a obtener la rectificación o supresión de dichos datos.

(170) En primer lugar, con arreglo a la sección 165 de la DPA de 2018, un interesado tiene el derecho a presentar una reclamación ante la ICO si considera que, en relación con datos personales que le conciernen, existe una infracción de la parte 3 de la DPA de 2018 ([251]). La ICO tiene la facultad de evaluar el cumplimiento del responsable y el encargado del tratamiento con la DPA de 2018, exigirles que adopten las medidas necesarias en caso de incumplimiento e imponer multas.

([246]) Los comités selectos, incluido el Home Affairs Select Committee, están sujetos a los Standing Orders (o reglamentos) de la Cámara de los Comunes. Estos *Standing Orders* son las normas, acordadas por la Cámara de los Comunes, que rigen los asuntos de práctica ordinaria del Parlamento. El mandato de los comités selectos es amplio, con el apartado 1 de la *Standing Order* 152, que establece que «se nombrarán comités selectos para examinar los gastos, la administración y la política de los principales departamentos gubernamentales, como se establece en el apartado 2 de este Reglamento, y de los organismos públicos asociados». Esto permite al Home Affairs Select Committee examinar cualquier política que pertenezca al Ministerio del Interior, lo que incluye políticas (y la legislación vinculada) sobre poderes de investigación. Además, el apartado 4 de la *Standing Order* 152 aclara que los comités tienen varios poderes, incluida la capacidad de solicitar a las personas que presenten pruebas o documentos sobre un tema en particular, y también que elaboren informes. Las consultas actuales y previas del Comité están disponibles en el siguiente enlace: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Los poderes del Home Affairs Select Committee en Inglaterra y Gales se definen en las *Standing Orders* de la Cámara de los Comunes, disponibles en el siguiente enlace: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Disponible en el siguiente enlace: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Disponible en el siguiente enlace: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Las normas del Justice Subcommittee on Policing de Escocia están disponibles en el siguiente enlace https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx y las normas del Committee of Justice de Irlanda del Norte pueden consultarse en el siguiente enlace. http://www.niassembly.gov.uk/assembly-business/standing-orders/.

([251]) El último informe anual de la ICO ofrece un desglose de la naturaleza de las reclamaciones recibidas y resueltas. En concreto, el número de reclamaciones recibidas por «antecedentes penales» asciende al 6 % del total de las reclamaciones recibidas (con un aumento del 1 % en comparación con el ejercicio anterior). El informe muestra también que la mayoría de las reclamaciones se relacionan con solicitudes de acceso de los sujetos (46 % sobre el número total de reclamaciones, con un aumento del 8 % en comparación con el ejercicio anterior) (*Annual Report and Financial Statements 2019-2020* de la ICO, p. 55; véase la nota a pie de página 88).

(171) En segundo lugar, la DPA de 2018 establece el derecho a la tutela judicial contra la ICO si esta no maneja adecuadamente una reclamación presentada por el interesado. En concreto, si la ICO no «procesa» ([252]) una reclamación presentada por el interesado, el reclamante tiene acceso a la tutela judicial, ya que puede apelar ante un Tribunal de Primera Instancia ([253]) para que ordene a la ICO que adopte las medidas adecuadas para responder a la reclamación o para informar al reclamante sobre el progreso de la misma ([254]). Por otro lado, toda persona a la que la ICO entregue cualquiera de los avisos mencionados con anterioridad (aviso de información, de evaluación, de ejecución o de sanción) puede apelar ante un Tribunal de Primera Instancia. Si el tribunal considera que la decisión de la ICO no cumple con la ley o que la ICO debería haber ejercido su facultad de apreciación de manera diferente, entonces el tribunal debe permitir la apelación o sustituir cualquier otro aviso o decisión que la ICO pudiera haber dado o adoptado ([255]).

(172) En tercer lugar, toda persona tiene derecho a emprender acciones judiciales contra los responsables y encargados del tratamiento directamente ante los tribunales. En concreto, con arreglo a la sección 167 de la DPA de 2018, un interesado puede obtener una reparación ante el tribunal por una infracción de su derecho en virtud de la legislación en materia de protección de datos y el tribunal puede, mediante una orden, solicitar al responsable del tratamiento que adopte (o se abstenga de adoptar) cualquier medida en relación con el tratamiento para cumplir con la DPA de 2018. Además, con arreglo a la sección 169 de la DPA de 2018, toda persona que haya sufrido daños debido a una violación de un requisito de la legislación en materia de protección de datos (incluida la parte 3 de la DPA de 2018), que no sea el RGPD del Reino Unido, tiene derecho a una compensación por dicho daño por parte del responsable o el encargado del tratamiento, salvo que el responsable o el encargado del tratamiento demuestre que el responsable o el encargado del tratamiento no son de ninguna manera responsables del hecho que dio lugar al daño. El daño incluye tanto las pérdidas económicas como los daños que no implican pérdidas económicas, por ejemplo, la ansiedad.

(173) Por último, cualquier persona, en la medida en que considere que cualquier autoridad pública ha violado sus derechos, incluidos los derechos a la privacidad y la protección de los datos, puede obtener una reparación ante los tribunales del Reino Unido en virtud de la *Human Rights Act* de 1998 ([256]) y, después de agotar los recursos nacionales, una persona, una organización no gubernamental y grupos de personas pueden obtener una reparación ante el Tribunal Europeo de Derechos Humanos por violaciones de los derechos reconocidos por el Convenio Europeo de Derechos Humanos ([257]) (véase el considerando 111).

3.2.4.1. Mecanismos de reparación disponibles en virtud de la IPA de 2016

(174) Las personas físicas pueden obtener una reparación por violaciones de la IPA de 2016 ante el Investigatory Powers Tribunal (Tribunal de Poderes de Investigación). Las vías de reparación disponibles con arreglo a la IPA de 2016 se describen en los considerandos 263 a 269 siguientes.

([252]) La sección 166 de la DPA de 2018 se refiere, en particular, a las siguientes situaciones: a) la ICO no toma las medidas adecuadas para responder a la reclamación, b) la ICO no proporciona al reclamante información sobre el progreso de la reclamación, o sobre el resultado de la misma, antes de que finalice el período de tres meses que comienza en el momento en que la ICO recibe la reclamación, o c) si la valoración de la reclamación por parte de la ICO no concluye durante ese período y, por lo tanto, no facilita al reclamante dicha información durante un período posterior de tres meses.

([253]) El Tribunal de Primera Instancia es el tribunal competente para tratar recursos contra las decisiones adoptadas por los organismos reguladores del gobierno. En el caso de la decisión de la ICO, la sala competente es la Sala de Asuntos Generales, que tiene jurisdicción sobre todo el Reino Unido.

([254]) Sección 166 de la DPA de 2018. Un ejemplo de acciones exitosas contra la ICO ante el tribunal incluye un caso en el que la ICO acusó recibo de una reclamación de un interesado pero no indicó qué procedimiento pretendía adoptar y, por lo tanto, se le ordenó confirmar, en el plazo de veintiún días naturales, si iba a investigar las reclamaciones y, de ser así, a informar al reclamante sobre el progreso de la investigación con una frecuencia no inferior a veintiún días naturales a partir de entonces (la sentencia aún está pendiente de publicarse); y un caso en el que el Tribunal de Primera Instancia consideró que no estaba claro si la respuesta de la ICO a una reclamante podía considerarse efectivamente el «resultado» de la reclamación [véase el asunto *Susan Milne v The Information Commissioner* (2020), sentencia disponible en el siguiente enlace: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Secciones 162 y 163 de la DPA de 2018.

([256]) Véase, por ejemplo, el asunto *Brown v Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724, en el que se concedieron 9 000 libras esterlinas en concepto de daños en virtud de la DPA de 1998 y la *Human Rights Act* de 1998 por la obtención ilícita y el uso indebido de información personal, y el asunto *R (on the application of Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, en el que el Tribunal de Apelación declaró ilícito el despliegue de un sistema de reconocimiento facial por parte de la policía de Gales, dado que infringía el artículo 8 del Convenio Europeo de Derechos Humanos y la evaluación de impacto relativa a la protección de datos realizada por el responsable del tratamiento no respetaba la DPA de 2018.

([257]) El artículo 34 del Convenio Europeo de Derechos Humanos establece que «El Tribunal podrá conocer de una demanda presentada por cualquier persona física, organización no gubernamental o grupo de particulares que se considere víctima de una violación por una de las Altas Partes Contratantes de los derechos reconocidos en el Convenio o sus Protocolos. Las Altas Partes Contratantes se comprometen a no poner traba alguna al ejercicio eficaz de este derecho».

3.3. **Acceso a los datos y uso de los mismos por parte de las autoridades públicas del Reino Unido con fines de seguridad nacional**

(175) En el ordenamiento jurídico del Reino Unido, los servicios de inteligencia facultados para recopilar información electrónica en poder de los responsables o encargados del tratamiento por motivos de seguridad nacional, en situaciones que sean pertinentes para un escenario de adecuación, son el Servicio de Seguridad (MI5) ([258]), el Servicio de Inteligencia Secreto (SIS) ([259]) y el Cuartel General de Comunicaciones del Gobierno ([260]) (GCHQ) ([261]).

3.3.1. *Base jurídica, limitaciones y garantías*

(176) En el Reino Unido, los poderes de los servicios de inteligencia se establecen en la IPA de 2016 y la RIPA de 2000, que, junto con la DPA de 2018, define el alcance material y personal de estos poderes, así como las limitaciones y garantías para su uso. En las siguientes secciones se evalúan en detalle estos poderes, así como las limitaciones y garantías que les son aplicables.

3.3.1.1. Poderes de investigación ejercidos en el contexto de la seguridad nacional

(177) La IPA de 2016 proporciona el marco jurídico para el uso de los poderes de investigación, esto es, el poder de interceptación, de acceso a datos de comunicación y de realizar interferencias de equipos. La IPA de 2016 introduce una prohibición general y tipifica como delito el uso de técnicas que permitan el acceso al contenido de comunicaciones, el acceso a los datos de comunicaciones o la interferencia de equipos sin autorización legal ([262]). Esto se refleja en el hecho de que el uso de estos poderes de investigación solo es lícito cuando se lleva a cabo sobre la base de una orden judicial o una autorización ([263]).

(178) La IPA de 2016 establece normas detalladas que rigen el alcance y la aplicación de cada poder de investigación, así como sus limitaciones y garantías específicas. Se aplican diferentes normas en función del tipo de poder de investigación (interceptación de comunicaciones, adquisición y conservación de datos de comunicaciones e

([258]) El MI5 se encuentra bajo la autoridad de la Secretaria de Estado del Ministerio del Interior. La *Security Service Act* de 1989 establece las funciones del MI5: proteger la seguridad nacional (incluida la protección contra amenazas de espionaje, terrorismo y sabotaje, de actividades de agentes de potencias extranjeras y de acciones destinadas a derrocar o socavar la democracia parlamentaria por medios políticos, industriales o violentos), salvaguardar el bienestar económico del Reino Unido contra amenazas externas y actividades de apoyo de las fuerzas policiales y otros organismos encargados del cumplimiento de la ley en la prevención y detección de delitos graves.

([259]) El SIS se encuentra bajo la autoridad del secretario de Estado para las Relaciones Exteriores y sus funciones se establecen en la *Intelligence Services Act* de 1994. Sus funciones son obtener y proporcionar información relacionada con las acciones o intenciones de personas fuera de las Islas Británicas y realizar otras tareas relacionadas con las acciones o intenciones de dichas personas. Estas funciones solo pueden ejercerse en interés de la seguridad nacional, en interés del bienestar económico del Reino Unido o en apoyo de la prevención y la detección de delitos graves.

([260]) El GCHQ se encuentra bajo la autoridad del secretario de Estado para las Relaciones Exteriores y sus funciones se establecen en la *Intelligence Services Act* de 1994. Dichas funciones son a) realizar un seguimiento, hacer uso o interferir en las emisiones electromagnéticas y de otro tipo y los equipos que producen tales emisiones, obtener y proporcionar información derivada o relacionada con dichas emisiones o equipos y derivada de material encriptado; b) ofrecer asesoramiento y asistencia sobre idiomas, en especial la terminología utilizada para asuntos técnicos y criptografía y otros asuntos relacionados con la protección de la información, a las fuerzas armadas, al gobierno u otras organizaciones o personas que se consideren apropiadas. Estas funciones solo pueden ejercerse en interés de la seguridad nacional, en interés del bienestar económico del Reino Unido en relación con las acciones o intenciones de personas fuera de las Islas Británicas o en apoyo de la prevención y la detección de delitos graves.

([261]) Otros organismos públicos que ejercen funciones pertinentes para la seguridad nacional son la Defence Intelligence, el National Security Council y el National Security Secretariat, la Joint Intelligence Organisation y el Joint Intelligence Committee. Sin embargo, ni la Joint Intelligence Organisation ni el Joint Intelligence Committee pueden hacer uso de los poderes de investigación en virtud de la IPA de 2016, mientras que la Defence Intelligence tiene un alcance limitado para el uso de sus poderes.

([262]) La prohibición se aplica tanto a las redes de comunicación públicas como privadas, así como al servicio postal público cuando la interceptación se realiza en el Reino Unido. La prohibición no se aplica al responsable del tratamiento de la red privada cuando se le ha dado consentimiento expreso o implícito para llevar a cabo la interceptación (sección 3 de la IPA de 2016).

([263]) En casos específicos limitados, es posible la interceptación legal sin una orden judicial, esto es, cuando la interceptación se realiza con el consentimiento del remitente o el destinatario (sección 44 de la IPA de 2016), en caso de fines administrativos o de ejecución limitados (sección 45 a 48 de la IPA de 2016), en determinadas instituciones especiales (secciones 49 a 51 de la IPA de 2016) y de acuerdo con las solicitudes en el extranjero (sección 52 de la IPA de 2016).

interferencia de equipos) ([264]) y en función de si el poder se ejerce sobre un objetivo específico o de forma masiva. En la sección específica más adelante se describen con detalle el alcance, las garantías y las limitaciones de cada medida prevista en la IPA de 2016.

(179) Además, la IPA de 2016 se complementa con una serie de códigos de práctica estatutarios, emitidos por el secretario de Estado, aprobados por ambas cámaras del Parlamento ([265]) y aplicables en todo el país, que ofrecen orientación adicional sobre el uso de estos poderes ([266]). Si bien los interesados pueden basarse directamente en las disposiciones establecidas en la IPA de 2016 para ejercer sus derechos, el apartado 5, anexo 7, de la IPA de 2016 especifica que los códigos de práctica son admisibles como prueba en procesos civiles y penales, y que el tribunal o la autoridad de control puede tener en cuenta cualquier incumplimiento de los códigos al determinar la pertinencia de un asunto en un proceso judicial ([267]). En el contexto de su evaluación de la «calidad de la ley» de la legislación anterior del Reino Unido en el ámbito de la vigilancia, la RIPA de 2000, la Gran Sala del Tribunal Europeo de Derechos Humanos reconoció expresamente la importancia de los códigos de práctica del Reino Unido y aceptó que sus disposiciones pudiesen tenerse en cuenta al evaluar la previsibilidad de la legislación que permite la vigilancia ([268]).

(180) Cabe señalar entonces que los poderes selectivos (interceptación selectiva ([269]), captación de datos de comunicaciones ([270]), conservación de datos de comunicaciones ([271]) e interferencia de equipos específicos ([272])) están disponibles para las agencias de seguridad nacional y ciertas autoridades encargadas de garantizar el cumplimiento de la ley ([273]), mientras que solo los servicios de inteligencia pueden hacer uso de poderes masivos (es decir, interceptación masiva ([274]), adquisición masiva de datos de comunicaciones ([275]), interferencia masiva de equipos ([276]) y conjuntos de datos personales masivos ([277])).

(181) En el momento de decidir qué poder de investigación debe usarse, el servicio de inteligencia debe cumplir con los «deberes generales en relación con la privacidad» enumerados en la sección 2, apartado 2, letra a), de la IPA de 2016, que incluyen una evaluación de la necesidad y la proporcionalidad. En concreto, con arreglo a esta

([264]) Por ejemplo, en lo que respecta al alcance de tales medidas, en virtud de las partes 3 y 4 (conservación y adquisición de datos de comunicaciones), el alcance de la medida está estrictamente vinculado a la definición de «operadores de telecomunicaciones», cuyos datos sobre los usuarios están sujetos a la medida. Otro ejemplo puede darse en relación con el uso de los poderes «masivos». En este caso, el alcance de estos poderes se limita a las «comunicaciones enviadas o recibidas por personas fuera de las Islas Británicas».

([265]) El anexo 7 de la IPA de 2016 determina el alcance de los códigos de práctica, el procedimiento que debe seguirse para su emisión, las normas para la revisión de los mismos y el efecto de los códigos.

([266]) Los códigos de práctica con arreglo a la IPA de2016 están disponibles en el siguiente enlace: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Los tribunales usan los códigos de práctica para evaluar la licitud de la conducta de las autoridades. Véase, por ejemplo el asunto *Dias v Cleveland Police*, [2017] UKIPTrib15_586-CH, en el que el Investigatory Powers Tribunal hizo referencia a pasajes específicos del *Code of Practice on Communication Data* («Código de práctica sobre datos de comunicación», documento en inglés) para comprender la definición del motivo de «prevención o detección de delitos o de prevención del desorden» utilizado para solicitar la adquisición de datos de comunicaciones. El código se incluyó en el razonamiento para determinar si ese motivo se utilizó incorrectamente. El tribunal llegó a la conclusión de que las conductas impugnadas eran ilícitas. Los tribunales hicieron también una evaluación del nivel de garantías disponibles en los códigos; véase, por ejemplo, el asunto *Just for Law Kids v Secretary of State for the Home Department* [2019] EWHC 1772 (Admin), en el que el Tribunal Superior determinó que la legislación primaria y secundaria junto con la guía interna proporcionaban garantías suficientes; o el asunto *(National Council for Civil Liberties) v Secretary of State for the Home Department & Others* [2019] EWHC 2057 (Admin), en el que el Tribunal Superior determinó que tanto la IPA de 2016 como el *Code of Practice on Equipment Interference* («Código de práctica sobre interferencias en equipos», documento en inglés) contenían disposiciones suficientes en cuanto a la necesidad de especificidad de las garantías.

([268]) En el asunto *Big Brother Watch*, la Gran Sala del Tribunal Europeo de Derechos Humanos señaló que «el código de la ICO es un documento público aprobado por ambas cámaras del Parlamento, que el Gobierno publica en línea y en versión impresa, y que debe ser tenido en cuenta tanto por quienes ejercen funciones de interceptación como por los tribunales» (véanse los apartados 93 y 94 más arriba). Como consecuencia, esta Corte ha aceptado que sus disposiciones podrían tenerse en cuenta al evaluar la previsibilidad de la RIPA (véase el asunto Kennedy v. the United Kingdom, citado con anterioridad, apartado 157). Por consiguiente, la Corte aceptaría que el Derecho nacional era debidamente "accesible"». [Véase Tribunal Europeo de Derechos Humanos (Gran Sala), *Big Brother Watch and others v United Kingdom*, solicitudes 58170/13, 62322/14 y 24960/15, de 25 de mayo de 2021, apartado 366].

([269]) Parte 2 de la IPA de 2016.

([270]) Parte 3 de la IPA de 2016.

([271]) Parte 4 de la IPA de 2016.

([272]) Parte 5 de la IPA de 2016.

([273]) Para consultar la lista de las autoridades encargadas de garantizar el cumplimiento de la ley pertinentes que pueden aplicar poderes de investigación selectivos en virtud de la IPA de 2016, véase la nota a pie de página (139).

([274]) Sección 136 de la IPA de 2016.

([275]) Sección 158 de la IPA de 2016.

([276]) Sección 176 de la IPA de 2016.

([277]) Sección 199 de la IPA de 2016.

disposición, una autoridad pública que tenga la intención de hacer uso de un poder de investigación debe valorar i) si lo que se busca lograr por medio de la orden, autorización o aviso podría lograrse razonablemente por otros medios menos intrusivos; ii) si el nivel de protección que se aplicará en relación con cualquier obtención de información en virtud de la orden, autorización o aviso es mayor debido a la sensibilidad particular de esa información; iii) el interés público en la integridad y seguridad de los sistemas de telecomunicaciones y los servicios postales, y iv) cualquier otro aspecto de interés público en la protección de la privacidad ([278]).

(182) La forma en que deben aplicarse estos criterios, y la forma en que se evalúa su cumplimiento como parte de la autorización del uso de tales poderes por parte del secretario de Estado y los comisionados judiciales independientes, se especifica con más detalle en los códigos de práctica correspondientes. En concreto, el uso de cualquiera de estos poderes de investigación debe ser siempre «proporcional al objetivo que se pretende alcanzar [lo que] implica equilibrar la gravedad de la intrusión en la privacidad (y otras consideraciones establecidas en la sección 2, apartado 2) frente a la necesidad de la actividad en términos de investigación, operativos o de capacidad». Esto significa, en particular, que «debe ofrecer una perspectiva realista de la obtención del beneficio esperado y no debe ser desproporcionado o arbitrario» y «[ninguna] interferencia con la privacidad debe considerarse proporcionada si la información que se busca podría obtenerse razonablemente por otros medios menos intrusivos» ([279]). Más concretamente, el cumplimiento del principio de proporcionalidad debe evaluarse atendiendo a los siguientes criterios: «i) el alcance de la injerencia propuesta en la privacidad frente al objetivo que se pretende alcanzar; ii) cómo y por qué los métodos que se adoptarán causarán la menor injerencia posible a la persona y a los demás; iii) si la actividad supone un uso adecuado de la Ley y una forma razonable, tras haber tenido en cuenta todas las alternativas razonables, de lograr el objetivo que se pretende alcanzar; iv) qué otros métodos, según corresponda, no se aplicaron o se han utilizado pero se consideran insuficientes para cumplir los objetivos operativos sin el uso del poder de investigación propuesto» ([280]).

(183) En la práctica, como explicaron las autoridades del Reino Unido, esto garantiza, en primer lugar, que un servicio de inteligencia establezca el objetivo operativo (delimitando así la recogida; por ejemplo, un fin de lucha contra el terrorismo internacional en un área geográfica específica) y, en segundo lugar, sobre la base de ese objetivo operativo, tendrá que valorar qué opción técnica (por ejemplo, interceptación selectiva o masiva, interferencia de equipos o adquisición de datos de comunicaciones) es la más proporcionada (es decir, la menos intrusiva para la privacidad; véase la sección 2, apartado 2, de la IPA de 2016) al objetivo que se pretende alcanzar y que, por lo tanto, puede autorizarse con arreglo a una de las bases jurídicas disponibles.

(184) Cabe señalar que el Relator Especial sobre el derecho a la privacidad de las Naciones Unidas, Joseph Cannataci, también señaló y acogió esta dependencia de los estándares de necesidad y proporcionalidad, y afirmó, en relación con el sistema que establece la IPA de 2016, que «[l]os procedimientos establecidos tanto dentro de los servicios de inteligencia como dentro de los organismos encargados de garantizar el cumplimiento de la ley parecen requerir sistemáticamente una consideración de la necesidad y proporcionalidad de una medida u operación de vigilancia antes de que se recomiende su autorización, así como su revisión de acuerdo con los mismos motivos» 2016 ([281]). Asimismo, observó que en su reunión con representantes de las autoridades encargadas de garantizar el cumplimiento de la ley y las agencias de seguridad nacional «[él] recibió una opinión consensuada de que el derecho a la privacidad debe ser una consideración primordial para cualquier decisión relacionada con las medidas de vigilancia. Todos comprendieron y valoraron la necesidad y la proporcionalidad como principios primordiales a tener en cuenta».

([278]) El *Code of Practice on Interception of Communications* («Código de práctica sobre interceptación de comunicaciones», documento en inglés) establece que otros elementos de la evaluación de proporcionalidad son: «i) el alcance de la injerencia propuesta en la privacidad frente al objetivo que se pretende alcanzar; ii) cómo y por qué los métodos que se adoptarán causarán la menor injerencia posible a la persona y a los demás; iii) si la actividad supone un uso adecuado de la Ley y una forma razonable, tras haber tenido en cuenta todas las alternativas razonables, de lograr el objetivo que se pretende alcanzar; iv) qué otros métodos, según corresponda, no se aplicaron o se han utilizado, pero se consideran insuficientes para cumplir los objetivos operativos sin el uso del poder de investigación propuesto». *Code of Practice on Interception of Communications*, apartado 4.16, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Véase *Code of Practice on Interception of Communications*, apartados 4.12 y 4.15, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf .

([280]) Véase *Code of Practice on Interception of Communications*, apartado 4.16.

([281]) *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* («Declaración de fin de misión del Relator Especial sobre el derecho a la privacidad al concluir su misión en el Reino Unido de Gran Bretaña e Irlanda del Norte», documento en inglés), disponible en el siguiente enlace: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, apartado 1.a.

(185) Los criterios específicos para la emisión de las distintas órdenes, así como las limitaciones y garantías que establece la IPA de 2016 en relación con cada poder de investigación, se detallan en los considerandos 186 a 243.

3.3.1.1.1. Interceptación y examen selectivos

(186) Hay tres tipos de órdenes de interceptación selectiva: la orden de interceptación selectiva ([282]), la orden de examen selectivo y la orden de asistencia mutua ([283]). En la parte 2, capítulo 1, de la IPA de 2016 se establecen las condiciones para la obtención de estas órdenes y las garantías pertinentes.

(187) Una orden de interceptación selectiva autoriza la interceptación de las comunicaciones que se describen en la orden durante su transmisión y la obtención de otros datos pertinentes para esas comunicaciones ([284]), incluidos datos secundarios ([285]). Una orden de examen selectivo autoriza a una persona a realizar una selección para el examen del contenido interceptado obtenido en virtud de una orden de interceptación masiva ([286]).

(188) Toda orden judicial con arreglo a la parte 2 de la IPA de 2016 puede emitirla el secretario de Estado ([287]) y ser aprobada por un comisionado judicial ([288]). En todos los casos, la duración de cualquier tipo de orden selectiva está limitada a seis meses ([289]), y se aplican normas específicas relativas a su modificación ([290]) y renovación ([291]).

(189) Antes de emitir una orden, el secretario de Estado debe realizar una evaluación de necesidad y proporcionalidad ([292]). En concreto, para una orden de interceptación selectiva y una orden de examen selectivo, el secretario de Estado debe verificar si la medida es necesaria con base en uno de los siguientes motivos: en interés de la seguridad nacional; la prevención o detección de un delito grave; en interés del bienestar económico del Reino Unido ([293]), en la medida en que esos intereses también sean pertinentes para los intereses de la seguridad nacional ([294]). Por otro lado, solo puede emitirse una orden de asistencia mutua (véase el considerando 139) si el secretario de Estado considera que existen circunstancias equivalentes a aquellas en las que emitiría una orden judicial con el propósito de prevenir o detectar delitos graves ([295]).

(190) Además, el secretario de Estado debe evaluar si la medida es proporcional al objetivo que se pretende alcanzar ([296]). La evaluación de la proporcionalidad de las medidas solicitadas debe tener en cuenta los deberes generales en relación con la privacidad que establece la sección 2, apartado 2, de la IPA de 2016, en particular la necesidad de evaluar si el objetivo que se pretende alcanzar con la orden, autorización o aviso podría lograrse razonablemente

([282]) Sección 15, apartado 2, de la IPA de 2016.
([283]) Sección 15, apartado 4, de la IPA de 2016.
([284]) Sección 15, apartado 2, de la IPA de 2016.
([285]) Los datos secundarios son datos adjuntos o asociados de forma lógica a la comunicación interceptada, que pueden separarse de ella de forma lógica y, si estuvieran separados, no revelarían nada de lo que razonablemente podría considerarse el significado (si lo hubiera) de la comunicación. Algunos ejemplos de datos secundarios incluyen las configuraciones de encaminadores o cortafuegos, o el período de tiempo que un encaminador ha estado activo en una red cuando forma parte, está conectado o está asociado de forma lógica a la comunicación interceptada. Para más información, véase la definición en la sección 16 de la IPA de 2016 y el *Code of Practice on Interception of Communication*, apartado 2.19; véase la nota a pie de página 278.
([286]) Este examen se realiza como una excepción de la sección 152, apartado 4, de la IPA de 2016, que establece la prohibición de buscar las comunicaciones de personas que se encuentran en las Islas Británicas. Véase el considerando 229.
([287]) El Scottish Minister autoriza la orden cuando está relacionada con una actividad delictiva grave en Escocia (véanse las secciones 21 y 22 de la IPA de 2016), mientras que el secretario de Estado puede designar a un funcionario de alto rango para emitir una orden de asistencia mutua cuando parezca que la interceptación implicará a una persona o unas instalaciones ubicadas fuera del Reino Unido (sección 40 de la IPA de 2016).
([288]) Secciones 19 y 23 de la IPA de 2016.
([289]) Sección 32 de la IPA de 2016.
([290]) Sección 39 de la IPA de 2016. Las personas prescritas pueden realizar modificaciones limitadas a las órdenes judiciales con arreglo a las condiciones establecidas en la IPA de 2016. La persona que emitió la orden puede cancelarla en cualquier momento. Por otro lado, deberá hacerlo si la orden ya no es necesaria por ningún motivo pertinente o si la conducta autorizada por la orden ya no es proporcional al objetivo que se pretende alcanzar.
([291]) Sección 33 de la IPA de 2016. La decisión de renovar una orden debe aprobarla un comisionado judicial.
([292]) Sección 19 de la IPA de 2016.
([293]) En relación con la noción de «intereses del bienestar económico del Reino Unido, en la medida en que esos intereses también son pertinentes para la seguridad nacional», la Gran Sala del Tribunal Europeo de Derechos Humanos consideró que en *Big Brother Watch and others v United Kingdom* (véase la nota a pie de página 268 más arriba), apartado 371, esta noción se centraba lo suficiente en la seguridad nacional. Si bien la conclusión del Tribunal en este caso estaba relacionada con el uso de esta noción en la RIPA de 2000, se utiliza la misma noción en la IPA de 2016.
([294]) Sección 20, apartado 2, de la IPA de 2016.
([295]) Sección 20, apartado 3, de la IPA de 2016.
([296]) Sección 19, apartado 1, letra b), apartado 2, letra b) y apartado 3, letra b), de la IPA de 2016.

por otros medios menos intrusivos y si el nivel de protección que debe aplicarse en relación con cualquier obtención de información en virtud de la orden es mayor debido a la sensibilidad particular de esa información (véase el considerando 181).

(191) Para ello, el secretario de Estado deberá tener en cuenta todos los elementos de la solicitud que facilite la autoridad que la presenta, en particular los relacionados con las personas a interceptar y la relevancia de la medida para la investigación. Dichos elementos se detallan en el *Code of Practice on Interception of Communications* y deben describirse con un cierto grado de especificidad ([297]). Además, la sección 17 de la IPA de 2016 requiere que cualquier orden que se emita con arreglo al capítulo 2 de dicha sección debe nombrar o describir a la persona específica o grupo de personas, organización o instalaciones que se interceptarán (el «objetivo»). Las órdenes de interceptación selectiva y las órdenes de examen selectivo también pueden estar relacionadas con un grupo de personas, más de una persona o una organización, o con más de un conjunto de instalaciones (también se denominan «órdenes temáticas») ([298]). En estos casos, la orden debe describir el fin o actividad común que comparte el grupo de personas o la operación/investigaciones y nombrar o describir tantas personas/organizaciones o conjunto de instalaciones, cuando sea razonablemente factible ([299]). Por último, todas las órdenes que se emiten con arreglo a la parte 2 de la IPA de 2016 deben especificar las direcciones, números, aparatos, factores o combinación de factores que se utilizarán para identificar las comunicaciones ([300]). A este respecto, el *Code of Practice on Interception of Communications* especifica que, en caso de una orden de interceptación selectiva y de una orden de examen selectivo, «la orden debe especificar (o describir) los factores o la combinación de factores que se utilizarán para identificar las comunicaciones. Cuando las comunicaciones deban identificarse por referencia a un número de teléfono (por ejemplo), el número se especificará plasmándose en su totalidad. Pero cuando, para identificar las comunicaciones, vayan a utilizarse selectores de conexión a Internet muy complejos o que cambian continuamente, esos selectores deberán describirse tanto como sea posible» ([301]).

(192) Una garantía importante en este contexto es que la evaluación realizada por el secretario de Estado para la emisión de una orden debe aprobarla un comisionado judicial independiente ([302]), que comprobará en particular si la decisión de emitir la orden cumple con los principios de necesidad y proporcionalidad ([303]) (acerca de la condición y función de los comisionados judiciales véanse los considerandos 251 a 256). La IPA de 2016 aclara también que, al realizar dicha comprobación, el comisionado judicial debe aplicar los mismos principios que aplicaría un tribunal en una solicitud de revisión judicial ([304]). Esto garantiza que, en cada caso, y antes de que se produzca el acceso a los datos, un organismo independiente compruebe sistemáticamente el cumplimiento del principio de necesidad y proporcionalidad.

(193) La IPA de 2016 prevé pocas excepciones específicas y estrictas para llevar a cabo interceptaciones selectivas sin una orden. Los casos limitados se detallan en la ley ([305]) y, salvo el caso basado en el «consentimiento» del remitente/destinatario, los llevan a cabo personas (organismos públicos o privados) distintas a las agencias de seguridad nacional. Además, este tipo de interceptaciones se llevan a cabo para fines distintos de la recopilación de «inteligencia» ([306]) y, para algunas de ellas, es muy improbable que la recogida pueda tener lugar en el contexto de un

([297]) La información solicitada incluye los detalles sobre la información previa (descripción de las personas/organizaciones/conjunto de instalaciones y la comunicación a interceptar) y cómo la obtención de dicha información beneficiará a la investigación, así como una descripción de la conducta a autorizar. En caso de que no sea posible describir a las personas/organizaciones/instalaciones, se incluirá una explicación de por qué no fue posible o de por qué solo se hizo una descripción general (*Code of Practice on Interception of Communications*, apartados 5.32 y 5.34; véase la nota a pie de página 278).

([298]) Sección 17, apartado 2, de la IPA de 2016. Véase también *Code of Practice on Interception of Communications*, apartado 5.11 y ss.; véase la nota a pie de página 278.

([299]) Sección 31, apartados 4 y 5, de la IPA de 2016.

([300]) Sección 31, apartado 8, de la IPA de 2016.

([301]) *Code of Practice on Interception of Communications*, apartados 5.37 y 5.38; véase la nota a pie de página 278.

([302]) No se requiere la aprobación de un comisionado judicial cuando el secretario de Estado considera que existe una necesidad urgente de emitir la orden (sección 19, apartado 1, de la IPA de 2016). Sin embargo, debe informarse al comisionado judicial en un breve plazo de tiempo, y este debe decidir si aprueba o no la orden. Si no la aprueba, entonces la orden deja de tener validez (secciones 24 y 25 de la IPA de 2016).

([303]) Sección 23, apartado 1, de la IPA de 2016.

([304]) Sección 23, apartado 2, de la IPA de 2016.

([305]) Véanse las secciones 44 a 51 de la IPA de 2016 y la sección 12 del *Code of Practice on Interception of Communications* (véase la nota a pie de página 278).

([306]) Este es el caso, por ejemplo, cuando se necesita una interceptación en prisión o en un hospital psiquiátrico (para comprobar la conducta de una persona detenida o de un paciente) o por un operador postal o de telecomunicaciones, por ejemplo para detectar contenidos abusivos.

escenario de «transferencia» (por ejemplo, en caso de interceptación realizada en un hospital psiquiátrico o en prisión). Teniendo en cuenta la naturaleza del organismo al que se aplican estos casos específicos (distinto de las agencias de seguridad nacional), se aplicarán todas las garantías previstas en la parte 2 de la DPA de 2018 y en el RGPD del Reino Unido, incluida la supervisión de la ICO y los mecanismos de reparación disponibles. Por otra parte, además de las garantías proporcionadas por la DPA de 2018, en algunos casos, la IPA de 2016 también prevé la supervisión *ex post* de la IPCO ([307]).

(194) Cuando se lleva a cabo una interceptación, se aplican limitaciones y garantías adicionales relacionadas con la condición específica de la persona o personas interceptadas ([308]). Por ejemplo, la interceptación de artículos sujetos a la prerrogativa de confidencialidad solo está autorizada cuando se dan circunstancias excepcionales y apremiantes; la persona que emite la orden debe tener en cuenta el interés público en la confidencialidad de los artículos sujetos a tal prerrogativa, así como la existencia de requisitos específicos para el manejo, conservación y comunicación de dicho material ([309]).

(195) Además, la IPA de 2016 dispone garantías específicas relacionadas con la seguridad, la conservación y la comunicación, que el secretario de Estado debe tener en cuenta antes de emitir una orden selectiva ([310]). En concreto, la sección 53, apartado 5, de la IPA de 2016, establece que toda copia de cualquier material recogido con arreglo a la orden se conserve de manera segura y se destruya tan pronto como ya no existan motivos pertinentes para conservarlo, mientras que la sección 53, apartado 2, de la IPA de 2016 requiere que el número de personas a las que se comunique el material y la medida en que se comunique, se ponga a disposición o se copie debe limitarse al mínimo necesario para los fines jurídicos.

(196) Por último, cuando el material que ha sido interceptado, ya sea por medio de una orden de interceptación selectiva o de una orden de asistencia mutua, debe entregarse a un tercer país («comunicación internacional»), la IPA de 2016 dispone que el secretario de Estado debe asegurarse de que hay acuerdos en vigor que garanticen la existencia de garantías similares en materia de seguridad, conservación y comunicación en ese tercer país ([311]). Además, la sección 109, apartado 2, de la DPA de 2018 establece que los servicios de inteligencia solo pueden transferir datos personales fuera del territorio del Reino Unido si la transferencia constituye una medida necesaria y proporcionada a efectos de las funciones estatutarias del responsable del tratamiento o para otros fines dispuestos en la sección 2, apartado 2, letra a), de la *Security Service Act* de 1989 o en la sección 2, apartado 2, letra a), y la sección 4, apartado 2, letra a), de la *Intelligence Services Act* de 1994 ([312]). Es importante señalar que estos requisitos también se aplican en los casos en que se recurra a la exención de seguridad nacional con arreglo a la sección 110 de la DPA de 2018, ya que esa sección no menciona la sección 109 de la DPA de 2018 como una de las disposiciones que pueden no aplicarse si se requiere una exención de determinadas disposiciones con el fin de salvaguardar la seguridad nacional.

3.3.1.1.2 Adquisición y conservación selectivas de los datos de comunicaciones

(197) 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 variedad de autoridades públicas, incluidos los organismos encargados de garantizar el cumplimiento de la ley y los servicios de inteligencia. La parte 4 de la IPA de 2016 prevé la conservación de datos de comunicaciones, mientras que la parte 3 prevé la adquisición selectiva de datos de comunicaciones. Las partes 3 y 4 de la IPA de 2016 también establecen limitaciones específicas sobre el uso de estos poderes y disponen garantías específicas.

([307]) Véase, *a contrario*, la sección 229, apartado 4, de la IPA.

([308]) Las secciones 26 a 29 de la IPA de 2016 introducen limitaciones para la obtención de órdenes de interceptación y de examen selectivos en relación con la interceptación de comunicaciones enviadas por, o destinadas a, una persona que es miembro del Parlamento (cualquier Parlamento del Reino Unido), la interceptación de artículos sujetos a la prerrogativa de confidencialidad, la interceptación de comunicaciones que la autoridad de interceptación crea que serán comunicaciones que contienen material periodístico confidencial y cuando el propósito de la orden es identificar o confirmar una fuente de información periodística.

([309]) Sección 26 de la IPA de 2016.

([310]) Sección 19, apartado 1, de la IPA de 2016.

([311]) Sección 54 de la IPA de 2016. Las garantías relativas a la divulgación de material a autoridades extranjeras se especifican con más detalle en los códigos de práctica: véanse, en particular, los apartados 9.26 y ss. y 9.87 del *Code of Practice on the Interception of Communications* y los apartados 9.33 y ss. y 9.41 del *Code of Practice on Equipment Interference* (véase la nota a pie de página 278).

([312]) Estos fines son: para el Servicio de Seguridad, la prevención o detección de delitos graves o cualquier procedimiento penal [sección 2, apartado 2, letra a), de la *Security Service Act* de 1989]; para el Servicio de Inteligencia Secreto, el interés de la seguridad nacional, la prevención o detección de delitos graves o cualquier procedimiento penal [sección 2, apartado 2, letra a), de la *Intelligence Services Act* de 1994]; y para el Cuartel General de Comunicaciones del Gobierno, cualquier procedimiento penal [sección 4, apartado 2, letra a), de la *Intelligence Services Act* de 1994]. Véanse también las notas explicativas sobre la DPA de 2018, disponibles en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) 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. La adquisición y la conservación de datos de comunicaciones, a diferencia de la interceptación de datos, no están destinadas a obtener el contenido de las comunicaciones, sino a obtener información como el abonado a un servicio telefónico o una facturación desglosada. Esto podría 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 ([313]).

(199) Cabe señalar que la conservación y adquisición de datos de comunicaciones, por lo general, no se referirá a los datos personales de interesados de la UE transferidos al Reino Unido en virtud de la presente Decisión. La obligación de conservar o comunicar datos de comunicaciones, con arreglo a las partes 3 y 4 de la IPA de 2016, cubre los datos recogidos por los operadores de telecomunicaciones en el Reino Unido directamente de los usuarios de un servicio de telecomunicaciones ([314]). Este tipo de tratamiento «de cara al cliente» generalmente no implica una transferencia sobre la base de esta Decisión, es decir, una transferencia de un responsable/encargado del tratamiento en la UE a un responsable/encargado del tratamiento en el Reino Unido.

(200) Sin embargo, en aras de la exhaustividad, en los siguientes considerandos se analizan las condiciones y garantías que rigen estos regímenes de adquisición y conservación.

(201) Como premisa, cabe señalar que la conservación y la adquisición selectiva de datos de comunicaciones están a disposición tanto de las agencias de seguridad nacional como de determinadas autoridades encargadas de garantizar el cumplimiento de la ley ([315]). Las condiciones para exigir la conservación o la adquisición de datos de comunicaciones pueden variar en función del motivo para solicitar la medida, a saber, a efectos de seguridad nacional o de aplicación de la ley.

(202) En particular, si bien el nuevo régimen ha introducido el requisito general de una autorización *ex ante* por parte de un organismo independiente, que se aplicará en todos los casos en que se conserven o adquieran datos de comunicaciones (a efectos de aplicación de la ley o de seguridad nacional), a raíz de la sentencia *Tele2/Watson* del Tribunal de Justicia de la Unión Europea ([316]), se han introducido garantías específicas cuando la medida se solicita a efectos de aplicación de la ley. En particular, cuando se solicite la conservación o la adquisición de datos de comunicaciones a efectos de aplicación de la ley, la autorización *ex ante* siempre debe ser otorgada por el Investigatory Powers Commissioner. Este no siempre es el caso cuando la medida se solicita a efectos de seguridad nacional, ya que, como se describe a continuación, en algunos casos, este tipo de medidas puede ser autorizado por otra «persona encargada de la autorización». Además, el nuevo régimen ha elevado a «delitos graves» el umbral para el que puede permitirse la conservación y la adquisición de datos de comunicaciones ([317]).

([313]) Los datos de comunicaciones se definen en la sección 261, apartado 5, de la IPA de 2016. Los datos de comunicaciones se dividen en «datos de eventos» (cualquier dato que identifique o describa un evento, sea o no por referencia a su ubicación, en o por medio de un sistema de telecomunicaciones en el que el evento consista en una o varias entidades que participan en una actividad específica en un momento concreto) y «datos de la entidad» (cualquier dato que a) tenga que ver con i) una entidad, ii) una asociación entre un servicio de telecomunicaciones y una entidad, o iii) una asociación entre cualquier parte de un sistema de telecomunicaciones y una entidad; b) consista en, o incluya, datos que identifiquen o describan a la entidad (ya sea por referencia o no a la ubicación de la entidad); y c) no constituya datos de eventos).

([314]) Esto se desprende de la definición de datos de comunicaciones proporcionada en la sección 261, apartado 5, de la IPA de 2016, según la cual los datos de comunicaciones los mantiene u obtiene un operador de telecomunicaciones, y se refieren bien al usuario de un servicio de telecomunicaciones y están relacionados con la provisión de este servicio, o bien están incluidos en, incluidos como parte de, adjuntos o vinculados de forma lógica a una comunicación (véanse también los apartados 2.22 a 2.33 del *Code of Practice on Communications Data*, disponible en el siguiente enlace https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf). Además, la definición de «operador de telecomunicaciones» proporcionada en la sección 261, apartado 10, de la IPA de 2016 establece que un operador de telecomunicaciones es una persona que ofrece o proporciona un servicio de telecomunicaciones a personas en el Reino Unido o que controla o proporciona un sistema de telecomunicaciones que está (total o parcialmente) en el Reino Unido o que se controla desde el Reino Unido. Estas definiciones ponen en claro que las obligaciones con arreglo a la IPA de 2016 no pueden imponerse a los operadores de telecomunicaciones cuyos equipos no se encuentran en el Reino Unido o no se controlan desde el Reino Unido, y que no ofrecen o proporcionan servicios a personas en el Reino Unido (véase también el apartado 2.1 del *Code of Practice on Communications Data*). Si los abonados de la UE (ya se encuentren en la UE o en el Reino Unido) hicieran uso de los servicios en el Reino Unido, cualquier comunicación relacionada con la prestación de este servicio sería recopilada directamente por el proveedor del servicio en el Reino Unido en lugar de estar sujeta a una transferencia desde la UE.

([315]) Las autoridades pertinentes se enumeran en el anexo 4 de la IPA de 2016 e incluyen a las fuerzas policiales, los servicios de inteligencia, algunos ministerios y departamentos del Gobierno, la National Crime Agency, Her Majesty's Revenue and Customs, la Competition and Markets Authority, el/la Information Commissioner, ambulancias, bomberos y servicios de salvamento y autoridades, por ejemplo, en el área de la salud y la seguridad alimentaria.

([316]) Asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB/Post- och telestyrelsen y Secretary of State for the Home Department/Tom Watson y otros (ECLI:EU:C:2016:970).

([317]) Véase la sección 61.7, letra b), para la adquisición de datos de comunicaciones, y la sección 87.10A para la conservación de los datos de comunicaciones.

i) *Autorización para la obtención de datos de comunicaciones*

(203) De conformidad con la parte 3 de la IPA de 2016, las autoridades públicas pertinentes están autorizadas para obtener datos de comunicaciones de un operador de telecomunicaciones o de cualquier persona capaz de obtener y comunicar dichos datos. La autorización puede no permitir la interceptación del contenido de las comunicaciones ([318]) y deja de tener efecto al cabo de un mes ([319]), con la posibilidad de ser renovada sujeta a una autorización adicional ([320]). La adquisición de datos de comunicaciones requiere una autorización del Investigatory Powers Commissioner ([321]) (para más información sobre la condición y los poderes del Investigatory Powers Commissioner, véanse los considerandos 250 a 251). Este es siempre el caso cuando una autoridad encargada de garantizar el cumplimiento de la ley solicita la adquisición de datos de comunicaciones. Sin embargo, de acuerdo con la sección 61 de la IPA de 2016, cuando los datos se adquieren en interés de la seguridad nacional o el bienestar económico del Reino Unido, siempre que sean pertinentes para la seguridad nacional, o cuando la solicitud la realiza un miembro de un servicio de inteligencia con arreglo a la sección 61, apartado 7, letra b) ([322]), la adquisición puede autorizarla de manera alternativa ([323]) el Investigatory Powers Commissioner o un funcionario de alto rango designado ([324]). El funcionario designado debe ser independiente de la investigación u operación en cuestión y tener conocimientos prácticos de los principios y la legislación en materia de derechos humanos, específicamente los principios de necesidad y proporcionalidad ([325]). La decisión adoptada por el funcionario designado estará sujeta a una supervisión *ex post* por parte del Investigatory Powers Commissioner (véase el considerando 254) para más información sobre las funciones de supervisión *ex post* del Investigatory Powers Commissioner].

(204) La autorización para adquirir datos de comunicaciones se basa en una evaluación de la necesidad y proporcionalidad de la medida. En concreto, la necesidad de la medida se evalúa a la luz de los motivos enumerados en la legislación ([326]). Teniendo en cuenta el carácter específico de esta medida, también debe ser necesaria para una investigación u operación específica ([327]). En el Code of Practice on Communication Data se establecen requisitos adicionales sobre la evaluación de la necesidad de las medidas ([328]). En particular, el código dispone que la solicitud presentada por la autoridad solicitante debe identificar tres elementos mínimos para justificar la necesidad de dicha solicitud: i) el evento bajo investigación, como un crimen o la ubicación de una persona vulnerable desaparecida; ii) la persona cuyos datos se buscan, como puede ser un sospechoso, testigo o desaparecido, y cuál es su vinculación con el hecho; y iii) los datos de comunicaciones buscados, como un número telefónico o una dirección IP, y cómo se relacionan estos datos con la persona y el evento ([329]).

(205) Además, la adquisición de datos de comunicaciones debe ser proporcional al objetivo que se pretende alcanzar ([330]). El *Code of Practice on Interception of Communications* especifica que, al realizar dicha evaluación, la persona encargada de la autorización debe realizar un ejercicio de equilibrio entre «el alcance de la interferencia con los derechos y libertades de una persona frente a un beneficio específico para la investigación u operación que realiza una autoridad pública pertinente en interés público» y que, teniendo en cuenta todas las consideraciones de un caso

([318]) Sección 60A, apartado 6, de la IPA de 2016.

([319]) Este período se reduce a tres días cuando la autorización se concede por razones de urgencia (sección 65, apartado 3A, de la IPA de 2016).

([320]) De conformidad con la sección 65 de la IPA de 2016, la autorización renovada tendrá una duración de un mes a partir de la fecha de vencimiento de la autorización actual. La persona que concede la autorización puede anularla en cualquier momento si considera que ya no se cumplen los requisitos necesarios.

([321]) Sección 60A, apartado 1, de la IPA de 2016. La Office for Communications Data Authorisations desempeña esta función en nombre del Investigatory Powers Commissioner (véase el *Code of Practice on Communication Data*, apartado 5.6).

([322]) La solicitud con arreglo a la sección 61, apartado 7, letra b), de la IPA de 2016 se realiza para «un fin delictivo aplicable», lo que significa, de acuerdo con la sección 61, apartado 7A, de la IPA de 2016: «cuando los datos de las comunicaciones sean total o parcialmente datos de eventos, el fin de prevenir o detectar delitos graves; en todos los demás casos, el fin de prevenir o detectar delitos o prevenir desórdenes».

([323]) El *Code of Practice on Communication Data* especifica que «Cuando pueda presentarse una solicitud relacionada con la seguridad nacional en virtud de la sección 60A o 61, la decisión sobre qué vía de autorización es la más adecuada en un caso determinado es competencia de cada una de las autoridades públicas. Las autoridades públicas que deseen utilizar la ruta designada por el funcionario de alto rango deben tener directrices claras sobre cuándo es apropiada esta ruta de autorización» (apartado 5.19 del *Code of Practice on Communication Data,* disponible en la siguiente dirección: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) La sección 70, apartado 3, de la IPA de 2016 proporciona la definición de «funcionario designado», que varía según la autoridad pública pertinente (como establece el anexo 4 de la IPA de 2016).

([325]) En el *Code of Practice on Communication Data* (apartados 4.12 a 4.17, véase la nota a pie de página 323) se ofrecen más detalles sobre la independencia del funcionario de alto rango designado.

([326]) Los motivos son: i) la seguridad nacional; ii) la prevención o detección de delitos o la prevención de desórdenes (en el caso de «datos de eventos» solo delitos graves); iii) en interés del bienestar económico del Reino Unido, en la medida en que esos intereses también sean pertinentes para los intereses de la seguridad nacional; iv) en interés de la seguridad pública; v) con el fin de prevenir la muerte o lesiones, o cualquier daño a la salud física o mental de una persona, o de mitigar cualquier lesión o daño a la salud física o mental de una persona; vi) ayudar en investigaciones sobre presuntos errores judiciales o vii) identificar a una persona fallecida o que no es posible identificar debido a una determinada condición (sección 61, apartado 7, de la IPA de 2016).

([327]) Sección 60A, apartado 1, letra b), de la IPA de 2016.

([328]) Apartado 3.3 y ss. del *Code of Practice on Communications Data*; véase la nota a pie de página 323.

([329]) Apartado 3.13 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323.

([330]) Sección 60, apartado 1, letra c), de la IPA de 2016.

particular, «una injerencia en los derechos de un individuo puede no estar justificada, debido a que el impacto adverso en los derechos de otro individuo o grupo de individuos es demasiado serio». Además, para evaluar específicamente la proporcionalidad de la medida, el código enumera una serie de elementos que deben incluirse en la solicitud presentada por la autoridad solicitante ([331]). Debe prestarse también especial atención al tipo de datos de comunicación (datos de «entidad» o «eventos» ([332])) que van a adquirirse y debe darse preferencia al uso de una categoría de datos menos intrusiva ([333]). El *Code of Practice on Interception of Communications* contiene también instrucciones específicas para autorizaciones que involucran datos de comunicaciones de personas en profesiones particulares (como médicos, abogados, periodistas, parlamentarios o ministros religiosos) ([334]), y que están sujetos a garantías adicionales ([335]).

ii) *Avisos que exigen la conservación de datos de comunicaciones*

(206) La parte 4 de la IPA de 2016 establece las normas relativas a la conservación de datos de comunicaciones y, en específico, los criterios que permiten al secretario de Estado emitir un aviso de conservación ([336]). Las garantías que introduce la IPA de 2016 se son las mismas cuando los datos se conservan con fines de aplicación de la ley o en interés de la seguridad nacional.

(207) La emisión de dichos avisos de conservación 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 ([337]). 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 del IPA de 2016, y descrita en los considerandos 203 a 205.

(208) El ejercicio de la facultad de exigir la conservación de determinados datos está sujeto a una serie de limitaciones y garantías. El secretario de Estado puede emitir un aviso de conservación a uno o varios operadores ([338]) solo cuando considere que el requisito de conservación de los datos es necesario para uno de los fines jurídicos ([339]) y es proporcional al objetivo que se pretende alcanzar ([340]). Como

([331]) La información que debe incluirse tiene que contener: i) un resumen de cómo la obtención de datos beneficiará a la investigación u operación; ii) una explicación de la relevancia de los períodos de tiempo solicitados, en especial cómo estos períodos son proporcionales al evento bajo investigación; iii) una explicación de cómo se justifica el nivel de intrusión cuando se toma en consideración el beneficio que los datos brindarán a la investigación (esta justificación debe incluir la consideración de si se podrían realizar investigaciones menos intrusivas para lograr el objetivo); iv) una observación de los derechos del individuo (en particular el derecho a la privacidad y, en los casos pertinentes, a la libertad de expresión) y una ponderación de estos derechos con el beneficio de la investigación; v) detalles de qué intrusión colateral puede producirse y cómo los períodos de tiempo solicitados impactan en la intrusión colateral (apartados 3.22 a 3.26 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([332]) Véase la nota a pie de página 313.

([333]) Cuando se buscan datos de comunicación más intrusivos (es decir, datos de eventos), el código especifica que es más adecuado adquirir primero datos de la entidad o adquirir directamente datos de eventos en casos limitados de urgencia específica (apartados 6.10 a 6.14 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([334]) Apartados 8.8 a 8.44 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323.

([335]) El código especifica que «la persona encargada de la autorización debe tener especial cuidado al considerar dichas solicitudes, incluida una consideración adicional de si podría haber consecuencias no deseadas de las mismas, así como si la solicitud sirve mejor al interés público» (apartado 8.8 del Code of Practice on Interception of Communications). Además, deben mantenerse registros para este tipo de solicitudes, y en la siguiente inspección deben marcarse dichas solicitudes para que el Investigatory Powers Commissioner las tenga en consideración (apartado 8.10 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([336]) Secciones 87 a 89 de la IPA de 2016.

([337]) En virtud de la sección 90 de la IPA de 2016, un operador de telecomunicaciones que ha recibido un aviso de conservación puede solicitar una revisión al secretario de Estado que la emitió.

([338]) De conformidad con la sección 87, apartado 2, letra a) de la IPA de 2016, un aviso de conservación puede referirse «a un operador específico o a cualquier descripción de operadores».

([339]) Los fines son i) el interés de la seguridad nacional; ii) el fin delictivo aplicable (como se define en la sección 87.10A de la IPA de 2016); iii) el interés del bienestar económico del Reino Unido, en la medida en que dicho interés sea también pertinente para los intereses de la seguridad nacional; iv) en interés de la seguridad pública; v) el fin de prevenir la muerte o lesiones, o cualquier daño a la salud física o mental de una persona, o de mitigar cualquier lesión o daño a la salud física o mental de una persona; o vi) ayudar en investigaciones sobre presuntos errores judiciales (sección 87 de la IPA).

([340]) Sección 87 de la IPA de 2016. Además, de acuerdo con el Código de práctica pertinente, para poder evaluar la proporcionalidad del aviso de conservación, se aplican los criterios establecidos en la sección 2, apartado 2, de la IPA de 2016, en particular el requisito de evaluar si el objetivo que se pretende alcanzar con el aviso podría lograrse razonablemente con medios menos intrusivos. De manera similar a la evaluación de la proporcionalidad en la adquisición de datos de comunicaciones, el *Code of Practice on Interception of Communications* aclara que dicha evaluación implica el «equilibrio entre el alcance de la interferencia con el derecho de un individuo al respeto de su vida privada y un beneficio específico para el investigación» (apartado 16.3 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

especifica la IPA de 2016 ([341]), antes de emitir un aviso de conservación, el secretario de Estado debe tener en cuenta: los beneficios probables del aviso ([342]); una descripción de los servicios de telecomunicaciones; la conveniencia de limitar los datos que se conservarán por referencia a la ubicación o descripciones de las personas a las que se prestan los servicios de telecomunicaciones ([343]); el número probable de usuarios (si se conoce) de cualquier servicio de telecomunicaciones al que se refiere el aviso ([344]); la viabilidad técnica de cumplir con el aviso; el coste probable de cumplir con el aviso, y cualquier otro efecto que el aviso tenga en el operador de telecomunicaciones (o descripción de los operadores) al que hace referencia ([345]). Como se explica en detalle en el capítulo 17 del *Code of Practice on Interception of Communications*, todos los avisos de conservación deben especificar cada tipo de datos que deben conservarse y cómo ese tipo de datos cumple con las evaluaciones necesarias para la conservación.

(209) En todos los casos (tanto a efectos de seguridad nacional como de aplicación de la ley), la decisión del secretario de Estado de emitir el aviso de conservación debe ser aprobada por un comisionado judicial independiente, con arreglo al denominado «procedimiento de doble llave», quien debe comprobar, en particular, si el aviso de conservación de los datos de comunicaciones pertinentes es necesario y proporcionado para uno o varios de los fines jurídicos ([346]).

3.3.1.1.3 Interferencia de equipos

(210) La interferencia de equipos consiste en un conjunto de técnicas que se utilizan para obtener una variedad de datos procedentes de equipos ([347]), que incluyen ordenadores, tabletas y teléfonos inteligentes, así como cables y dispositivos de almacenamiento de datos ([348]). La interferencia de equipos permite obtener tanto el contenido de las comunicaciones como los datos del equipo ([349]).

(211) Con arreglo a la sección 13, apartado 1, de la IPA de 2016, las interferencias de equipos por parte de un servicio de inteligencia requieren una autorización mediante orden judicial de acuerdo con el procedimiento de «doble bloqueo» establecido por la IPA de 2016, siempre que exista una «conexión con las Islas Británicas» ([350]). Según las aclaraciones

([341]) Véase la sección 88 de la IPA de 2016.

([342]) Los beneficios pueden ser reales y vigentes o previstos, y deben ser concernientes a los propósitos jurídicos para los cuales la conservación de los datos es posible (apartado 17.17 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([343]) Estas consideraciones incluirán la determinación de si el alcance geográfico total del aviso de conservación es necesario y proporcionado, así como si es necesario y proporcionado incluir o excluir cualquier descripción particular de personas (apartado 17.17 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([344]) Esto ayudará al secretario de Estado a valorar tanto el nivel de intrusión en la privacidad de los clientes como también los beneficios probables de los datos que se conservarán (apartado 17.17 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 323).

([345]) Sección 88 de la IPA de 2016.

([346]) Sección 89 de la IPA de 2016.

([347]) De conformidad con la sección 135, apartado 1, y la sección 198, apartado 1, de la IPA de 2016, «equipo» comprende los equipos que producen emisiones electromagnéticas, acústicas o de otro tipo y cualquier dispositivo que pueda utilizarse en conexión con dichos equipos.

([348]) *Code of Practice on Equipment Interference*, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf (apartado 2.2).

([349]) Los datos de equipos se definen en la sección 100 de la IPA de 2016 como datos del sistema y datos que a) están comprendidos en, incluidos como parte de, adjuntos o asociados lógicamente con una comunicación (ya sea por parte del remitente o de otro modo) o cualquier otro elemento de información; b) pueden separarse lógicamente del resto de la comunicación o del elemento de información, y c) si estuvieran separados de esta manera, no revelarían ninguna cosa que pudiera considerarse razonablemente como el significado (si lo hubiera) de la comunicación o el elemento de información.

([350]) Para que el requisito de la orden judicial sea obligatorio, la sección 13, apartado 1, de la IPA de 2016 también requiere que la conducta del servicio de inteligencia constituya una o varias infracciones con arreglo a las secciones 1 a 3A de la *Computer Misuse Act* de 1990, que sería el caso en la gran mayoría de las circunstancias (véanse los apartados 3.32 y 3.6 a 3.9 del *Code of Practice on Equipment Interference*). De conformidad con la sección 13, apartado 2, de la IPA de 2016, existe una «conexión con las Islas Británicas» si a) alguna de las conductas se llevase a cabo en las Islas Británicas (independientemente de la ubicación de los equipos que serán o que podrían ser interferidos), b) el servicio de inteligencia cree que cualquiera de los equipos que serán o que podrían ser interferidos, está o podría estar en las Islas Británicas en algún momento mientras se produce la interferencia, o c) el propósito de la interferencia es obtener: i) comunicaciones enviadas por, o enviadas a, una persona que está, o que el servicio de inteligencia cree que está, por el momento en las Islas Británicas, ii) información privada relacionada con un individuo que está, o que el servicio de inteligencia cree que está, por el momento en las Islas Británicas, o iii) datos de equipos que forman parte de, o están conectados con, comunicaciones o información privada contemplada en los subpárrafos i) o ii).

proporcionadas por las autoridades del Reino Unido, en situaciones en las que los datos se transfieran de la UE al Reino Unido dentro del alcance de la presente Decisión, siempre habrá una «conexión con las Islas Británicas» y, por lo tanto, cualquier interferencia de equipos que cubriera dichos datos estaría sujeta al requisito de autorización obligatoria de la sección 13, apartado 1, de la IPA de 2016 ([351]).

(212) En la parte 5 de la IPA de 2016 se establecen las normas sobre las garantías de interferencia selectiva de equipos. De manera similar a la interceptación selectiva, la interferencia selectiva de equipos debe estar relacionada con un «objetivo» específico, que debe reflejarse en la orden judicial ([352]). El asunto y el tipo de equipo que se interferirá determinan los detalles sobre cómo debe identificarse un «objetivo». En concreto, la sección 115, apartado 3, de la IPA de 2016 especifica los elementos que deben incluirse en la orden (p. ej. el nombre de la persona u organización y la descripción de la ubicación) dependiendo, por ejemplo, de si la interferencia está relacionada con un equipo que pertenece, lo utiliza o está en posesión de una persona específica, una organización o un grupo de personas, si se encuentra en una ubicación específica, etc. ([353]). Los fines para los cuales pueden emitirse órdenes de interferencia selectiva de equipos dependen de la autoridad pública que las solicite ([354]).

(213) De manera similar a la interceptación selectiva, la autoridad emisora debe tener en cuenta si la medida es necesaria para lograr un fin específico, así como si es proporcional al objetivo que se pretende alcanzar ([355]). Además, también debe considerar si hay garantías en relación con la seguridad, la conservación y la comunicación, así como en relación con la «comunicación internacional» ([356]) (véase el considerando 196).

(214) La orden debe aprobarla un comisionado judicial, salvo en caso de urgencia ([357]). En este último caso, es necesario informar al comisionado judicial de que se ha emitido una orden y este debe aprobarla en un plazo de tres días hábiles. El caso de que el comisionado no apruebe la orden, esta dejará de tener efecto y no podrá renovarse ([358]). Además, el comisionado está facultado para exigir que se suprima cualquier dato obtenido en virtud de la orden ([359]). El hecho de que se emita una orden con urgencia no afecta a la supervisión *ex post* (véanse los considerandos 244 a 255) ni las posibilidades para que las personas busquen reparación (véanse los considerandos 260 a 270). Las personas pueden presentar un recurso ante la ICO o presentar una reclamación con respecto a cualquier presunta conducta ante el Investigatory Powers Tribunal (Tribunal de Poderes de Investigación) del modo habitual. En todos los casos, la prueba que aplica el comisionado judicial a la hora de decidir si aprueba o no una orden es el examen de necesidad y proporcionalidad aplicable a las solicitudes de interceptación selectiva ([360]) (véase el considerando 192).

([351]) En aras de la exhaustividad, debe tenerse en cuenta que incluso en situaciones en las que no hay una «conexión con las Islas Británicas» y, por lo tanto, el recurso a las interferencias de equipos no está sujeto al requisito de autorización obligatoria que impone la sección 13, apartado 1, de la IPA de 2016, un servicio de inteligencia que tiene intención de llevar a cabo una actividad para la que pueda obtener una orden de interferencia masiva de equipos debe obtener dicha autorización como una cuestión de política (véase el apartado 3.24 del *Code of Practice on Equipment Interference*). Incluso cuando una interferencia de equipos contemplada en la IPA de 2016 no esté requerida por ley ni se obtenga lícitamente como una cuestión de política, las acciones de los servicios de inteligencia están sujetas a una serie de condiciones y limitaciones con arreglo a la sección 7 de la *Intelligence Services Act* de 1994. Esto incluye, en particular, la exigencia de una autorización por parte del secretario de Estado, quien debe cerciorarse de que cualquier acción no exceda lo necesario para el adecuado desempeño de las funciones del servicio de inteligencia.

([352]) La sección 115 de la IPA de 2016 regula el contenido de las órdenes, puntualizando que deben incluir el nombre o descripción de las personas, organizaciones, ubicación o grupo de personas que constituyen el «objetivo», una descripción de la naturaleza de la investigación y una descripción de las actividades para las que se emplean el/los equipo(s). Asimismo, debe describir el tipo de equipo(s) y la conducta que la persona a quien se dirige la orden está autorizada a adoptar.

([353]) Véase también el apartado 5.7 del *Code of Practice on Equipment Interference*, nota a pie de página 348.

([354]) Las agencias de seguridad nacional pueden solicitar una orden de interferencia de equipos cuando sea necesario por motivos de seguridad nacional, con el fin de detectar delitos graves o en interés del bienestar económico del Reino Unido, siempre y cuando dichos intereses también sean pertinentes para los intereses de la seguridad nacional (secciones 102 y 103 de la IPA de 2016). En función de la agencia de que se trate, puede solicitarse una orden de interferencia de equipos con el propósito de hacer cumplir la ley cuando sea necesario para detectar o prevenir un delito grave o con el fin de prevenir la muerte o lesiones, o cualquier daño a la salud física o mental de una persona, o de mitigar cualquier lesión o daño a la salud física o mental de una persona (véase la sección 106, apartados 1 y 3, de la IPA 2016).

([355]) Sección 102, apartado 1, de la IPA de 2016.

([356]) Secciones 129 a 131 de la IPA de 2016.

([357]) Sección 109 de la IPA de 2016.

([358]) Sección 109, apartado 4, de la IPA de 2016.

([359]) Sección 110, apartado 3, letra b), de la IPA de 2016. De conformidad con el apartado 5.67 del *Code of Practice on Equipment Interference*, la urgencia se determina en función de si sería razonablemente viable solicitar la aprobación del comisionado judicial para emitir la orden en el tiempo disponible para satisfacer una necesidad operativa o de investigación. Las órdenes urgentes deben pertenecer a una de las siguientes categorías, o a ambas: i) amenaza inminente para la vida o daños graves, por ejemplo, si una persona ha sido secuestrada y se considera que su vida corre peligro inminente; o ii) una oportunidad de recogida de datos o de investigación con un tiempo limitado para actuar —por ejemplo, un envío de drogas de clase A está a punto de entrar en el Reino Unido y los organismos encargados de hacer cumplir la ley desean una cobertura de los autores de delitos graves para llevar a cabo detenciones. Véase la nota a pie de página 348.

([360]) Sección 108 de la IPA de 2016.

(215) Por último, las garantías específicas aplicables a la interceptación selectiva se aplican también a la interferencia de equipos en lo que respecta a la duración, renovación y modificación de la orden judicial, así como a la interceptación de miembros del Parlamento, de elementos sujetos a la prerrogativa de confidencialidad y de material periodístico (véase el considerando 193 para más información).

3.3.1.1.4 Ejercicio de poderes masivos

(216) La parte 6 de la IPA de 2016 regula los poderes masivos. Por su parte, los códigos de práctica ofrecen más información sobre el uso de los poderes masivos. Si bien no existe una definición en el Derecho del Reino Unido de «poderes masivos», en el contexto de la IPA de 2016 se ha descrito como la recogida y conservación de grandes cantidades de datos adquiridos por el Gobierno a través de varios medios (es decir, los poderes de interceptación masiva, adquisición masiva, interferencia masiva de equipos y conjuntos de datos personales masivos) y a los que las autoridades pueden acceder posteriormente. Esta descripción se precisa al contrastarla con lo que no son «poderes masivos»: no equivale a la denominada «vigilancia masiva» sin limitaciones ni garantías. Por el contrario, como se explica a continuación, incorpora limitaciones y garantías diseñadas para asegurar que el acceso a los datos no se haga de forma indiscriminada o injustificada ([361]). En concreto, solo puede hacerse uso de los poderes masivos si se establece un vínculo entre la medida técnica que un servicio de inteligencia nacional pretende utilizar y el objetivo operativo para el que se solicita dicha medida.

(217) Además, los poderes masivos están disponibles solamente para los servicios de inteligencia y siempre están sujetos a una orden emitida por el secretario de Estado y aprobada por un comisionado judicial. Al escoger los medios para recopilar datos, debe tenerse en cuenta si el objetivo en cuestión puede alcanzarse por «medios menos intrusivos» ([362]). Este enfoque deriva del marco de la legislación que se basa en el principio de proporcionalidad y, por lo tanto, prioriza la recogida selectiva sobre la recogida masiva.

3.3.1.1.4.1 Interceptación masiva e interferencia masiva de equipos

(218) El régimen para la interceptación masiva se recoge en la parte 6, capítulo 1, de la IPA de 2016, mientras que la parte 6, capítulo 3, regula la interferencia masiva de equipos. Estos regímenes son, en esencia, los mismos, por lo que las condiciones y las garantías adicionales aplicables a las correspondientes órdenes se analizan en conjunto.

i) *Condiciones y criterios para la emisión de una orden judicial*

(219) Las órdenes de interceptación masiva se limitan a la interceptación de comunicaciones producidas en el curso de su transmisión, enviada o recibida por personas que se encuentran fuera de las Islas Británicas ([363]), las denominadas «comunicaciones internacionales» ([364]), así como otros datos pertinentes y la posterior selección

([361]) De acuerdo con el apartado 1.9 del informe sobre poderes masivos presentado por Lord David Anderson, revisor independiente de la legislación en materia de terrorismo antes de la aprobación de la IPA de 2016, «debe quedar claro que la recogida y conservación de datos en masa no equivale a la denominada 'vigilancia masiva'». Cualquier sistema jurídico que se precie incorporará limitaciones y garantías diseñadas precisamente para garantizar que el acceso a los almacenes de datos sensibles […] no se dé de forma indiscriminada o injustificada. Dichas limitaciones y garantías existen ciertamente en el proyecto de ley». Lord David Anderson, *Report of the bulk power review* («Informe de revisión de los poderes masivos» documento en inglés), agosto de 2016 (el subrayado es mío), disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Sección 2.2 de la IPA de 2016. Véase, por ejemplo, el apartado 4.11 del *Code of Practice on Bulk Acquisition of Communications Data*, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) La denominación «Islas Británicas» incluye al Reino Unido, las Islas del Canal y la Isla de Man, y se definen en el anexo 1 de la *Interpretation Act* de 1978, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Con arreglo a la sección 136 de la IPA de 2016, «comunicaciones internacionales» significa: i) comunicaciones enviadas por personas que se encuentran fuera de las Islas Británicas, o ii) comunicaciones recibidas por personas que se encuentran fuera de las Islas Británicas. Según han confirmado las autoridades del Reino Unido, este régimen también cubre las comunicaciones entre dos personas que se encuentran fuera de las Islas Británicas. La Gran Sala del Tribunal Europeo de Derechos Humanos, en el asunto *Big Brother Watch and others v United Kingdom* (véase la nota a pie de página 279 más arriba), apartado 376, declaró, con respecto a una limitación similar (relativa a las «comunicaciones externas») de las comunicaciones que pueden captarse mediante interceptación masiva en virtud de la RIPA de 2000, que estaba lo suficientemente delimitada y era lo suficientemente previsible.

para examen del material interceptado ([365]). Una orden de interferencia masiva de equipos ([366]) autoriza al destinatario a asegurar la interferencia con cualquier equipo con el fin de obtener comunicaciones internacionales (incluyendo cualquier elemento que comprenda voz, música, sonidos, imágenes visuales o datos de cualquier descripción), datos de equipos (datos que habilitan o facilitan el funcionamiento de un servicio postal; un sistema de telecomunicaciones; o un servicio de telecomunicaciones) o cualquier otro tipo de información ([367]).

(220) El secretario de Estado puede emitir una orden masiva solo en respuesta a una solicitud realizada por un director de un servicio de inteligencia ([368]). Una orden que autorice una interceptación masiva o una interferencia masiva de equipos debe emitirse solo si es necesario para el interés de la seguridad nacional y para un fin adicional de prevención o detección de delitos graves, o en interés del bienestar económico del Reino Unido cuando sea pertinente para la seguridad nacional ([369]). Además, la sección 142, apartado 7, de la IPA de 2016 establece que una orden de interceptación masiva debe incluir más detalles que la simple referencia a los «intereses de la seguridad nacional», el «bienestar económico del Reino Unido» y la «prevención y lucha contra la delincuencia grave», y que debe establecerse un vínculo entre la medida que va a solicitarse y uno o varios fines operativos que deberán incluirse en la orden.

(221) La elección del fin operativo es el resultado de un proceso a varios niveles. La sección 142, apartado 4, de la IPA de 2016 dispone que los fines operativos que se precisen en la orden judicial deben especificarse también en una lista que mantendrán los directores de los servicios de inteligencia, como fines que ellos consideran que constituyen fines operativos para los cuales puede seleccionarse para examen el contenido interceptado o los datos secundarios obtenidos en virtud de órdenes de interceptación masiva. El secretario de Estado debe aprobar la lista de fines operativos. El secretario de Estado solo puede conceder dicha aprobación si está convencido de que el propósito operativo se especifica con un mayor nivel de detalle que los motivos generales para autorizar la orden (seguridad nacional o seguridad nacional y bienestar económico o prevención de delitos graves) ([370]). Al final de cada período pertinente de tres meses, el secretario de Estado debe entregar una copia de la lista de fines operativos al Intelligence and Security Committee (Comité de Inteligencia y Seguridad) del Parlamento. Por último, el primer ministro debe revisar la lista de fines operativos, por lo menos, una vez al año ([371]). Como señaló el Tribunal Superior, «[n]o deben tomarse por garantías insignificantes, ya que junto construyen un intrincado conjunto de modos de rendición de cuentas que involucran al Parlamento y a miembros del Gobierno al más alto nivel» ([372]).

(222) Dichos fines operativos también limitan el alcance selección del material de interceptación para la etapa de examen. La selección para examen de cualquier material recogido en virtud de la orden masiva debe justificarse a la luz del(los) fin(es) operativo(s). Como explicaron las autoridades del Reino Unido, esto significa que el secretario de Estado debe evaluar ya en la etapa de solicitud de la orden las disposiciones prácticas en relación con el examen, proporcionando detalles suficientes para cumplir con los deberes estatutarios en virtud de las secciones 152 y 193 de la IPA de 2016 ([373]). Los detalles que se proporcionen al secretario de Estado en relación con dichas disposiciones deberían incluir, por ejemplo, información (cuando corresponda) sobre cómo las disposiciones de filtrado pueden variar a lo largo del tiempo en que una orden tendrá validez ([374]). Para más información sobre el proceso y las garantías aplicadas en las fases de filtrado y examen, véase el considerando 229.

([365]) Sección 136, apartado 4, de la IPA de 2016. De acuerdo con la aclaración recibida por parte de las autoridades del Reino Unido, la interceptación masiva puede emplearse, por ejemplo, para identificar amenazas previamente desconocidas a la seguridad nacional del Reino Unido por medio del filtrado y análisis del material interceptado con el fin de identificar comunicaciones que contengan datos valiosos (sección H del *UK Explanatory Framework for Adequacy Discussions*: *National security*, p. 27; véase la nota a pie de página 29). Como explicaron las autoridades del Reino Unido, estos instrumentos pueden emplearse para establecer vínculos entre temas de interés conocidos, así como para buscar rastros de la actividad de personas que pueden no ser conocidos aún pero que emergen en el curso de una investigación, y para identificar patrones de actividad que pueden indicar una amenaza para el Reino Unido.

([366]) Con arreglo a la sección 13, apartado 1, de la IPA de 2016, el uso de interferencias de equipos por parte de un servicio de inteligencia requiere de una orden judicial que provea una autorización en virtud de la IPA de 2016, siempre que exista una «conexión con las Islas Británicas»; véase el considerando 211.

([367]) Sección 176 de la IPA de 2016. Una orden para la interferencia masiva de equipos no puede autorizar una conducta que (salvo que se haga con la debida autoridad legal) constituya una interceptación ilícita (excepto en relación con una comunicación almacenada). De acuerdo con el *UK Explanatory Framework for Adequacy Discussions*, la información obtenida podría ser necesaria para la identificación de temas de interés y serían, por lo general, operaciones adecuadas a gran escala (sección H del *UK Explanatory Framework for Adequacy Discussions*: *National security*, p. 28; véase la nota a pie de página 29).

([368]) Sección 138, apartado 1, y sección 178, apartado 1, de la IPA de 2016.

([369]) Sección 138, apartado 2, y sección 178, apartado 2, de la IPA de 2016.

([370]) De acuerdo con las aclaraciones facilitadas por las autoridades del Reino Unido, un fin operativo puede limitar el alcance de la medida a la existencia de una amenaza en un área geográfica concreta.

([371]) Sección 142, apartados 4 a 10, de la IPA de 2016.

([372]) Tribunal Superior de Inglaterra y Gales, *Liberty*, [2019] EWHC 2057 (Admin), apartado 167.

([373]) Las secciones 152 y 193 de la IPA de 2016 requieren que: a) la selección para examen se lleve a cabo únicamente para los fines operativos especificados en la orden, b) la selección para examen sea necesaria y proporcionada en todas las circunstancias, y c) la selección para examen no infrinja la prohibición de selección de material e identificación de comunicaciones enviadas por o destinadas a personas que se sabe que se encuentran en las Islas Británicas en ese momento.

([374]) Véase el apartado 6.6 del *Code of Practice on Interception of Communications*, nota a pie de página 278.

(223) Un poder masivo solo puede autorizarse si es proporcional al objetivo que se pretende alcanzar ([375]). Como se especifica en el *Code of Practice on Interception of Communications*, cualquier evaluación de la proporcionalidad implica «equilibrar la seriedad de la intrusión en la privacidad (y otras consideraciones establecidas en la sección 2, apartado 2) con la necesidad de la actividad en términos de investigación, operatividad y capacidad. La conducta autorizada debe ofrecer una perspectiva realista de generar el beneficio esperado y no debe ser desproporcionada ni arbitraria» ([376]). Como ya se ha indicado, en la práctica esto significa que la evaluación de la proporcionalidad se basa en una prueba de equilibrio entre el objetivo que se pretende alcanzar [«fin(es) operativo(s)»] y las opciones técnicas disponibles (p. ej., interceptación, interferencia de equipos y adquisición de datos de comunicaciones, selectivas o masivas), dando preferencia a los medios menos intrusivos (véanse los considerandos 181 y 182). Cuando más de una medida es adecuada para el objetivo, entonces debe optarse por los medios menos intrusivos.

(224) Una garantía adicional en la evaluación de la proporcionalidad de la medida solicitada queda garantizada por el hecho de que el secretario de Estado debe recibir la información pertinente necesaria para realizar debidamente su evaluación. En concreto, el *Code of Practice on Interception of Communications* y el *Code of Practice on Equipment Interference* requieren que la solicitud presentada por la autoridad pertinente indique la información previa asociada a la solicitud, la descripción de las comunicaciones que se interceptarán y los operadores de telecomunicaciones requeridos para ayudar, la descripción de la conducta que se autorizará, los fines operativos y una explicación de por qué la conducta es necesaria y proporcionada ([377]).

(225) Por último, y un paso importante, es que la decisión del secretario de Estado de emitir la orden debe ser aprobada por un comisionado judicial independiente, que deberá valorar la evaluación de la necesidad y proporcionalidad de la medida propuesta utilizando los mismos principios que utilizaría un tribunal en una solicitud de control jurisdiccional ([378]). Más concretamente, el comisionado judicial revisará las conclusiones del secretario de Estado en cuanto a si la orden es necesaria y si la conducta es proporcionada a la luz de los principios establecidos en la sección 2, apartado 2, de la IPA de 2016 (deberes generales en relación con la privacidad). Asimismo, el comisionado judicial revisará las conclusiones del secretario de Estado en relación con si cada uno de los fines operativos especificados en la orden es un fin para el cual es, o puede ser, necesaria la selección. Si el comisionado judicial se niega a aprobar la decisión de emitir una orden, el secretario de Estado podrá entonces: i) aceptar la decisión y, por lo tanto, no emitir la orden; o ii) remitir el asunto al Investigatory Powers Commissioner para una decisión (salvo que el Investigatory Powers Commissioner haya tomado la decisión original) ([379]).

ii) *Garantías adicionales*

(226) La IPA de 2016 ha introducido límites adicionales en torno a la duración, renovación y modificación de las órdenes masivas. La orden debe tener una duración máxima de seis meses y cualquier decisión de renovación o modificación (excepto modificaciones menores) de la orden también debe aprobarla un comisionado judicial ([380]). El *Code of Practice on Interception of Communications* y el *Code of Practice on Equipment Interference* establecen que un cambio en los fines operativos de la orden se considera una modificación mayor de la misma ([381]).

([375]) Sección 138, apartado 1, letras b) y c), y sección 178, apartado 1, letras b) y c), de la IPA de 2016.

([376]) Apartado 4.10 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 278.

([377]) Apartado 6.20 del *Code of Practice on Interception of Communications*, véase la nota a pie de página 278; y apartado 6.13 del *Code of Practice on Equipment Interference*, véase la nota a pie de página 348.

([378]) Sección 138, apartado 1, letra g), y sección 178, apartado 1, letra f), de la IPA de 2016. El Tribunal Europeo de Derechos Humanos ha identificado, en particular, que la autorización previa por parte de un organismo independiente constituye una garantía importante contra el abuso en el contexto de la interceptación masiva. Tribunal Europeo de Derechos Humanos (Gran Sala), *Big Brother Watch and others v United Kingdom*, (véase la nota a pie de página 269 más arriba), apartados 351 y 352. Es importante tener en cuenta que esta sentencia se refería al marco jurídico anterior (RIPA de 2000), que no contenía algunas de las garantías (incluida la autorización previa por parte de un comisionado judicial independiente) introducidas por la IPA de 2016.

([379]) Sección 159, apartados 3 y 4, de la IPA de 2016.

([380]) Secciones 143 a 146 y 184 a 188, de la IPA de 2016. En caso de una modificación urgente, el secretario de Estado puede realizar la modificación sin aprobación, pero debe informar al comisionado judicial y el comisionado debe entonces decidir si aprueba o rechaza la modificación (sección 147 de la IPA de 2016). Las órdenes deben cancelarse cuando ya no sean necesarias o proporcionadas o cuando el examen del contenido interceptado, los metadatos u otros datos obtenidos en virtud de la orden ya no sean necesarios para ninguno de los fines operativos especificados en la orden (sección 148 y 189 de la IPA de 2016).

([381]) Apartados 6.44 a 6.47 del *Code of Practice on Interception of Communications*, véase la nota a pie de página 278; y apartado 6.48 del *Code of Practice on Equipment Interference*, véase la nota a pie de página 348.

(227) De manera similar a lo que se estipula para la interceptación selectiva, la parte 6 de la IPA de 2016 establece que el secretario de Estado debe asegurarse de que estén vigentes los acuerdos para ofrecer garantías sobre la conservación y comunicación del material obtenido en virtud de la orden ([382]), así como para las comunicaciones internacionales ([383]). En concreto, la sección 150, apartado 5, y la sección 191, apartado 5, de la IPA de 2016 requieren que toda copia hecha de cualquier material recogido en virtud de la orden judicial se almacene de forma segura y se destruya tan pronto como ya no existan motivos pertinentes para retenerla, mientras que la sección 150, apartado 2, y la sección 191, apartado 2 requieren que el número de personas a quienes se comunica el material y la medida en que se comunica, se pone a disposición o se copia cualquier material debe limitarse al mínimo necesario para los fines estatutarios ([384]).

(228) Por último, cuando el material que ha sido interceptado, ya sea mediante una interceptación masiva o una interferencia masiva de equipos, debe entregarse a un tercer país («comunicación internacional»), la IPA de 2016 dispone que el secretario de Estado debe asegurarse de que hay acuerdos en vigor que garanticen la existencia de garantías similares en materia de seguridad, conservación y comunicación en ese tercer país ([385]). Además, la sección 109 de la DPA de 2018 establece requisitos específicos para las transferencias internacionales de datos personales por parte de los servicios de inteligencia a terceros países u organizaciones internacionales, y no permite las transferencias de datos personales a un país o territorio fuera del Reino Unido o a una organización internacional, a menos que la transferencia sea necesaria y proporcionada a efectos de las funciones estatutarias del responsable del tratamiento o para otros fines dispuestos en la sección 2, apartado 2, letra a), de la *Security Service Act* de 1989 o en la sección 2, apartado 2, letra a), y la sección 4, apartado 2, letra a), de la *Intelligence Services Act* de 1994 ([386]). Es importante señalar que estos requisitos también se aplican en los casos en que se recurra a la exención de seguridad nacional con arreglo a la sección 110 de la DPA de 2018, ya que esa sección no menciona la sección 109 de la DPA de 2018 como una de las disposiciones que pueden no aplicarse si se requiere una exención de determinadas disposiciones con el fin de salvaguardar la seguridad nacional.

(229) Una vez que se ha aprobado la orden y que los datos se han recogido de forma masiva, estos quedarán sujetos a una selección antes de ser examinados. La fase de selección y examen está sujeta a una evaluación de la proporcionalidad adicional que lleva a cabo el analista, quien define los criterios de selección sobre la base de los propósitos operativos incluidos en la orden (y las disposiciones de filtrado que puedan existir). Como establecen las secciones 152 y 193 de la IPA, al emitir la orden, el secretario de Estado debe asegurarse de que existan disposiciones para garantizar que la selección del material se lleve a cabo solo para los fines operativos especificados y que sea necesaria y proporcionada en todas las circunstancias. En este sentido, las autoridades del Reino Unido aclararon que el material que se intercepta de forma masiva se selecciona, en primer lugar, mediante un filtrado automatizado con el objetivo de descartar datos que probablemente no sean de interés para la seguridad nacional. Los filtros variarán de tanto en tanto (a medida que cambien los patrones, tipos y protocolos del tráfico de internet) y dependerán de la tecnología y del contexto operativo. Una vez superada esta fase, solo podrán seleccionarse datos para examen si resultan pertinentes para los fines operativos que aparecen reflejados en la orden ([387]). Las garantías previstas por la IPA de 2016 para el examen del material recogido se aplican a todo tipo de datos (tanto contenidos interceptados como datos secundarios) ([388]). Las secciones 152 y 193 de la IPA de 2016 también establecen una prohibición general para la selección del material a examinar que se refiera a conversaciones enviadas por o destinadas a personas que se encuentran en las Islas Británicas. Si las autoridades desean examinar este material, tendrán que enviar una solicitud para una orden de examen selectivo en virtud de las partes 2 y 4 de la IPA de 2016, que emitirá el secretario de Estado y deberá aprobar un comisionado judicial ([389]). Si una persona selecciona para examen de forma deliberada contenido interceptado, incumpliendo de esta forma los requisitos establecidos en la legislación ([390]), incurre en un delito ([391]).

([382]) Sección 156 de la IPA de 2016.
([383]) Secciones 150 y 191 de la IPA de 2016.
([384]) La Gran Sala del Tribunal Europeo de Derechos Humanos, en el asunto*Big Brother Watch and others v United Kingdom* (véase la nota a pie de página 268 más arriba), confirmó el sistema de garantías adicionales para la conservación, el acceso y la divulgación previsto en la RIPA de 2000, véanse los apartados 392 a 394 y 402 a 405. La IPA de 2016 prevé el mismo sistema de garantías.
([385]) Secciones 151 y 192 de la IPA de 2016.
([386]) Para más información al respecto, véase la nota a pie de página 312.
([387]) A este respecto, el código relativo a la interceptación de comunicaciones especifica que «Estos sistemas de tratamiento tratan datos de los enlaces o señales de comunicaciones que la autoridad de interceptación ha elegido interceptar. Posteriormente, se aplica cierto grado de filtrado al tráfico en esos enlaces y señales, diseñado para seleccionar tipos de comunicaciones que contengan datos potencialmente valiosos, mientras se descartan aquellas comunicaciones que tienen menos probabilidades de contener datos valiosos. Como resultado de este proceso de filtrado, que variará en función del sistema de tratamiento, se descartará automáticamente una parte significativa de las comunicaciones en estos enlaces y señales. Es posible que, con posterioridad, se realicen búsquedas más complejas para obtener más comunicaciones que contengan posiblemente datos de gran valor y que se relacionen con las funciones estatutarias de la agencia. Cuando se cumplan las condiciones de necesidad y proporcionalidad, estas comunicaciones pueden seleccionarse para su examen con arreglo a uno o varios de los fines operativos especificados en la orden. Tan solo los elementos que no se han filtrado pueden ser seleccionados potencialmente para su examen por parte de personas autorizadas» (apartado 6.6 del *Code of Practice on Interception of Communications*; véase la nota a pie de página 278).
([388]) Véase la sección 152, apartado 1, letras a) y b), de la IPA de 2016, según la cual el examen de ambos tipos de datos (contenidos interceptados y datos secundarios) debe llevarse a cabo únicamente para el fin especificado y ser necesario y proporcionado en toda circunstancia.
([389]) Este tipo de orden no es necesario cuando los datos relacionados con las personas que se encuentran en las Islas Británicas son «datos secundarios» [véase la sección 152, apartado 1, letra c), de la IPA de 2016].
([390]) Secciones 152 y 193 de la IPA de 2016.
([391]) Secciones 155 y 196 de la IPA de 2016.

(230) La evaluación realizada por el analista sobre la selección del material está sujeta a una supervisión *ex post* por parte del comisionado judicial, que evalúa el cumplimiento de las garantías específicas establecidas en la IPA de 2016 para la fase de examen ([392]) (véase también el considerando 229). El comisionado judicial debe someter a revisión continua (incluso mediante procesos de auditoría, inspección e investigación) el ejercicio por parte de las autoridades públicas de los poderes de investigación recogidos en la IPA de 2016 ([393]). A este respecto, el *Code of Practice on Interception of Communications* y el *Code of Practice on Equipment Interference* especifican que la agencia debe mantener registros con fines de posteriores exámenes y auditorías, y que estos registros deben describir por qué es necesario y proporcionado el acceso al material por parte de personas autorizadas, así como los fines operativos aplicables ([394]). Por ejemplo, en su informe anual de 2018, la Investigatory Powers Commissioner Office ([395]) concluyó que las justificaciones registradas por los analistas para el examen de cierto material recogido de forma masiva cumplían con el estándar de proporcionalidad requerido, proporcionando suficientes detalles acerca de los motivos de sus «consultas» en relación con el objetivo que se pretendía alcanzar ([396]). En su informe de 2019, la IPCO, en relación con los poderes masivos, declaró claramente su intención de continuar las inspecciones de las interceptaciones masivas, incluido un examen detallado de los selectores y criterios de búsqueda ([397]). Asimismo, seguirá examinando cuidadosamente, caso por caso, la elección de las medidas de vigilancia (específicas frente a masivas) tanto durante el examen de las solicitudes de órdenes en virtud del procedimiento de doble bloqueo como en las inspecciones ([398]). Este seguimiento ulterior se tendrá debidamente en cuenta en el contexto del seguimiento por parte de la Comisión de esta Decisión a que se hace referencia en los considerandos 281 a 284.

3.3.1.1.4.2 Adquisición masiva de datos de comunicaciones

(231) La parte 6, capítulo 2, de la IPA de 2016 regula las órdenes de adquisición masiva de datos que autorizan al destinatario a exigir a un operador de telecomunicaciones la comunicación u obtención de cualquier dato de comunicaciones en posesión de este último. Estas órdenes autorizan también a la autoridad solicitante a seleccionar los datos para la fase posterior de examen. Al igual que sucede con la conservación y adquisición selectivas de datos de comunicaciones (véase el considerando 199), la adquisición masiva de datos de comunicaciones normalmente no afecta a los datos personales de interesados de la UE transferidos en virtud de la presente Decisión al Reino Unido. La obligación de comunicar datos de comunicaciones, con arreglo a la parte 6, capítulo 2, de la IPA de 2016, cubre los datos recogidos por los operadores de telecomunicaciones en el Reino Unido directamente de los usuarios de un servicio de telecomunicaciones ([399]). Este tipo de tratamiento «de cara al cliente» generalmente no implica una transferencia sobre la base de esta Decisión, es decir, una transferencia de un responsable/encargado del tratamiento en la UE a un responsable/encargado del tratamiento en el Reino Unido.

(232) Sin embargo, en aras de la exhaustividad, a continuación se describen las condiciones y garantías que rigen la adquisición masiva de datos de comunicaciones.

([392]) Secciones 152 y 193 de la IPA de 2016.
([393]) Sección 229 de la IPA de 2016.
([394]) Apartado 6.74 del *Code of Practice on Interception of Communications*, véase la nota a pie de página 278 y apartado 6.78 del *Code of Practice on Equipment Interference*, véase la nota a pie de página 348.
([395]) La Investigatory Powers Commissioner Office se constituyó en virtud de la sección 238 de la IPA de 2016 para proporcionar al comisionado judicial el personal, el alojamiento, los equipos y otras instalaciones y servicios necesarios para el desempeño de sus funciones (véase el considerando 251).
([396]) El informe anual de 2018 de la Investigatory Powers Commissioner Office especificó que las justificaciones registradas por los analistas del Cuartel General de Comunicaciones del Gobierno «cumplieron con el estándar requerido y tuvieron en cuenta la proporcionalidad de sus consultas de datos masivos con suficiente detalle». Apartado 6.22 del informe anual de 2018 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 464.
([397]) Apartado 7.6 del informe anual de 2019 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 463.
([398]) Apartado 10.22 del informe anual de 2019 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 463.
([399]) Esto se desprende de la definición de datos de comunicaciones proporcionada en la sección 261, apartado 5, de la IPA de 2016, según la cual los datos de comunicaciones los mantiene u obtiene un operador de telecomunicaciones, y se refieren bien al usuario de un servicio de telecomunicaciones y están relacionados con la provisión de este servicio, o bien están incluidos en, incluidos como parte de, adjuntos o vinculados de forma lógica a una comunicación (véanse también los apartados 2.15 a 2.22 del *Code of Practice on Bulk Acquisition of Communications Data*, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf). Además, la definición de «operador de telecomunicaciones» proporcionada en la sección 261, apartado 10, de la IPA de 2016 establece que un operador de telecomunicaciones es una persona que ofrece o proporciona un servicio de telecomunicaciones a personas en el Reino Unido o que controla o proporciona un sistema de telecomunicaciones que está (total o parcialmente) en el Reino Unido o que se controla desde el Reino Unido. Estas definiciones ponen en claro que las obligaciones con arreglo a la IPA de 2016 no pueden imponerse a los operadores de telecomunicaciones cuyos equipos no se encuentran en el Reino Unido o no se controlan desde el Reino Unido, y que no ofrecen o proporcionan servicios a personas en el Reino Unido (véase también el apartado 2.2 del *Code of Practice on Bulk Acquisition of Communications Data*). Si los abonados de la UE (ya se encuentren en la UE o en el Reino Unido) hicieran uso de los servicios en el Reino Unido, cualquier comunicación relacionada con la prestación de este servicio sería recopilada directamente por el proveedor del servicio en el Reino Unido en lugar de estar sujeta a una transferencia desde la UE.

(233) La IPA de 2016 sustituye a la legislación en materia de adquisición masiva de datos de comunicaciones que fue objeto de la sentencia del TJUE en el asunto de *Privacy International*. La legislación involucrada en ese asunto del TJUE fue derogada y el nuevo régimen establece condiciones y garantías específicas que aplican a la autorización de la medida.

(234) En concreto, a diferencia del régimen anterior, en virtud del cual el secretario de Estado podía hacer uso únicamente de su criterio para autorizar la medida ([400]), la IPA de 2016 requiere que el secretario de Estado emita una orden judicial solo si la medida es necesaria y proporcionada. En la práctica, esto significa que debe existir un vínculo entre el acceso a los datos y el fin que se pretende alcanzar ([401]). En concreto, el secretario de Estado tendrá que valorar la existencia de un vínculo entre la medida solicitada y uno o varios «fin(es) operativo(s)» indicado(s) en la orden (véase el considerando 219) con respecto a la evaluación de la proporcionalidad; el Código de práctica pertinente especifica que «el secretario de Estado debe tener en cuenta si el objetivo que se pretende alcanzar con la orden judicial podría lograrse razonablemente por otros medios menos intrusivos [sección 2, apartado 2, letra a), de la IPA]. Por ejemplo, obtener la información requerida a través de un poder menos intrusiva, como puede ser la adquisición específica de datos de comunicaciones» ([402]).

(235) Para realizar dicha evaluación, el secretario de Estado se apoyará en la información que los directores de los servicios de inteligencia ([403]) deben presentar en su solicitud, como son las razones por las que la medida se considera necesaria para alguna de las bases estatutarias y las razones por las que el objetivo que se pretende alcanzar no puede lograrse razonablemente por otros medios menos intrusivos ([404]). Además, los fines operativos limitan el alcance por el que pueden seleccionarse los datos obtenidos en virtud de la orden para examen ([405]). Como se especifica en el Código de práctica pertinente, los fines operativos deben describir un requisito claro y contener detalles suficientes para demostrar al secretario de Estado que los datos adquiridos solo pueden seleccionarse para examen por razones específicas ([406]). De hecho, el secretario de Estado tendrá que asegurarse, antes de emitir la orden, de que existen disposiciones específicas para garantizar que solo se seleccione el material que se ha considerado necesario para examen en aras de un fin operativo y un fin estatutario, y que dicho material sea proporcionado y necesario en todas las circunstancias. Este requisito específico, que se refleja en las secciones 158 y 172 ([407]) de la IPA de 2016, relativo a la evaluación previa de la necesidad y proporcionalidad de los criterios empleados a efectos de la selección de los datos representa otra importante novedad del régimen que introdujo la IPA de 2016, en comparación con el régimen anterior.

(236) La IPA de 2016 introdujo también la obligación para el secretario de Estado de asegurarse de que, antes de emitir una orden para la adquisición masiva de datos de comunicaciones, existan limitaciones específicas en materia de seguridad, conservación y comunicación de los datos de carácter personal recogidos ([408]). En el caso de las comunicaciones internacionales, también se aplican las garantías (que se describen en el considerando 227) para la interceptación masiva y la interferencia masiva de equipos ([409]). En la legislación pertinentes también se establecen límites adicionales sobre la duración ([410]), renovación ([411]) y modificación de las órdenes masivas ([412]).

(237) Cabe señalar que, por lo que respecta a los demás poderes masivos, antes de emitir la orden, el secretario de Estado debe obtener la aprobación de un comisionado judicial ([413]). Esta es una característica clave del régimen establecido por la IPA de 2016.

([400]) La sección 94, apartado 1, de la *Telecommunication Act* de 1984 disponía que el secretario de Estado podía emitir «instrucciones de carácter general que el secretario de Estado considere necesarias o convenientes en interés de la seguridad nacional [...]» (véase la nota a pie de página 451).

([401]) Véase el asunto *Privacy International*, apartado 78.

([402]) Véase el apartado 4.11 del *Code of Practice on Bulk Acquisition of Communications Data* (véase la nota a pie de página 399414).

([403]) Solo los directores de los servicios de inteligencia pueden solicitar una orden de adquisición masiva, en concreto: i) el director general del Servicio de Seguridad; ii) el director del Servicio de Inteligencia Secreto; o iii) el director del Cuartel General de Comunicaciones del Gobierno (véanse las secciones 158 y 263 de la IPA de 2016).

([404]) Véase el apartado 4.5 del *Code of Practice on Bulk Acquisition of Communications Data* (véase la nota a pie de página 399).

([405]) De acuerdo con la sección 161 de la IPA de 2016, los fines operativos que se precisan en la orden deben ser también los que se especifican en una lista que mantendrán los directores de los servicios de inteligencia (la «lista de fines operativos»), como fines que ellos consideran que constituyen fines operativos para los cuales pueden seleccionarse para examen datos de comunicaciones obtenidos en virtud de órdenes de adquisición masiva.

([406]) Véase el apartado 6.6 del *Code of Practice on Bulk Acquisition of Communications Data* (véase la nota a pie de página 399).

([407]) La sección 172 de la IPA de 2016 requiere que se establezcan garantías específicas para la fase de filtrado y selección para el examen de la comunicación adquirida de forma masiva. Además, un examen deliberado que infrinja estas garantías constituye un delito penal (véase la sección 173 de la IPA de 2016).

([408]) Sección 171 de la IPA de 2016.

([409]) Sección 171, apartado 9, de la IPA de 2016.

([410]) Sección 162 de la IPA de 2016.

([411]) Sección 163 de la IPA de 2016.

([412]) Secciones 164 a 166 de la IPA de 2016.

([413]) Sección 159 de la IPA de 2016.

(238) El Investigatory Powers Commissioner realiza una supervisión *ex post* del procedimiento de examen del material (datos de comunicaciones) adquirido de forma masiva (véase el considerando 254). A este respecto, la IPA de 2016 introdujo el requisito de que el analista de inteligencia que lleva a cabo el examen registre, antes de seleccionar los datos para examen, la razón por la que el examen propuesto es necesario y proporcionado para un fin operativo específico ([414]). En el informe anual de 2019 de la Investigatory Powers Commissioner Office se constató, en relación con la práctica del Cuartel General de Comunicaciones del Gobierno y del MI5 que «el papel crítico de los datos de comunicaciones masivos en el rango de actividades realizadas en el Cuartel General de Comunicaciones del Gobierno estaba bien articulado en los casos que inspeccionamos. Tuvimos en consideración la naturaleza de los datos solicitados y los requisitos de inteligencia declarados y quedamos satisfechos de que la documentación demostrara que su enfoque era necesario y proporcionado ([415]). Las justificaciones registradas del MI5 eran satisfactorias y cumplían con los principios de necesidad y proporcionalidad» ([416]).

3.3.1.1.4.3 Conservación y examen de conjuntos de datos personales masivos

(239) Las órdenes de conjuntos de datos personales masivos ([417]) autorizan a los servicios de inteligencia a conservar y examinar conjuntos de datos que contengan datos personales relativos a una serie de individuos. Según las aclaraciones facilitadas por las autoridades del Reino Unido, el análisis de estos conjuntos de datos puede ser «la única manera de que la UK Intelligence Community avance en sus investigaciones e identifique a los terroristas a partir de una pista de inteligencia muy limitada, o cuando sus comunicaciones se hayan ocultado deliberadamente» ([418]). Hay dos tipos de órdenes: por un lado, las «órdenes de conjuntos de datos personales masivos de clase» ([419]), que se refieren a una categoría de conjuntos de datos determinada, esto es, conjuntos de datos que son similares en cuanto a su contenido y uso propuesto y que plantean consideraciones similares en cuanto a, por ejemplo, el grado de intrusión y sensibilidad y la proporcionalidad del uso de los datos, lo que permite al secretario de Estado valorar la necesidad y proporcionalidad de adquirir todos los datos dentro de la clase pertinente de una sola vez. Por ejemplo, una orden de conjuntos de datos personales masivos de clase puede cubrir conjuntos de datos de viajes que se relacionan con rutas similares ([420]). Y, por otro lado, «órdenes selectivas de conjuntos de datos personales masivos» ([421]), que se refieren a un conjunto de datos específico, como puede ser un conjunto de datos de un tipo de información nuevo o inusual que no pertenece al ámbito de una orden de datos personales masivos de una clase existente, o un conjunto de datos que se refiere a tipos específicos de datos personales ([422]) y que, por lo tanto, requieren garantías adicionales ([423]). Las disposiciones de la IPA de 2016 relativas a los conjuntos de datos personales masivos permiten que estos conjuntos de datos se examinen y conserven solo cuando la medida resulte necesaria y proporcionada ([424]), y siempre de conformidad con las obligaciones generales relacionadas con la privacidad ([425]).

(240) La facultad de emitir órdenes de conjuntos de datos personales masivos está sujeta al procedimiento de «doble bloqueo»: la evaluación de la necesidad y la proporcionalidad de la medida la realiza, en primer lugar, el secretario de Estado y, a continuación, el comisionado judicial ([426]). El secretario de Estado debe valorar la naturaleza y el alcance del tipo de orden judicial que se solicita, la categoría de datos en cuestión y el número de conjuntos de datos personales masivos que probablemente pertenezcan al ámbito del tipo concreto de orden judicial ([427]). Asimismo, como se especifica en el *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, deben mantenerse registros detallados que están, además, sujetos a auditoría por parte del Investigatory Powers Commissioner ([428]). La conservación y el examen de conjuntos de datos personales masivos fuera de los límites de la IPA de 2016 constituye un delito penal ([429]).

([414]) Apartado 8.6 del informe anual de 2019 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 463.
([415]) Apartado 10.4 del informe anual de 2019 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 463.
([416]) Apartado 8.37 del informe anual de 2019 de la Investigatory Powers Commissioner Office; véase la nota a pie de página 463.
([417]) Sección 200 de la IPA de 2016.
([418]) Sección H del *UK Explanatory Framework for Adequacy Discussions*: *National Security*, p. 34; véase la nota a pie de página 29.
([419]) Sección 204 de la IPA de 2016.
([420]) Apartado 4.7 del *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets* («Código de práctica sobre la conservación y el uso de conjuntos de datos personales masivos por parte de los servicios de inteligencia», documento en inglés), disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Sección 205 de la IPA de 2016.
([422]) Como, por ejemplo, los datos personales sensibles. Véase la sección 202 de la IPA de 2016 y los apartados 4.21 y 4.12 del *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*; consúltese la nota a pie de página 469.
([423]) El secretario de Estado debe considerar de manera individual las solicitudes para una orden selectiva de conjuntos de datos personales masivos, es decir, en relación con un conjunto de datos específico. En virtud de la sección 205 de la IPA de 2016, el servicio de inteligencia está obligado a incluir en su solicitud para órdenes selectivas de conjuntos de datos personales masivos una explicación detallada de la naturaleza y alcance del material en cuestión, así como una lista de los «fines operativos» para los que el servicio de inteligencia pertinente desea examinar los conjuntos de datos personales (cuando se solicite una orden de conservación y examen, en lugar de una orden de solo conservación). En cambio, a la hora de emitir una orden de conjuntos de datos personales masivos de clase, el secretario de Estado valora la categoría completa de conjuntos de datos.
([424]) Secciones 204 y 205 de la IPA de 2016.
([425]) Sección 2 de la IPA de 2016.
([426]) Secciones 204 y 205 de la IPA de 2016.
([427]) Apartado 5.2 del *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*; véase la nota a pie de página 420.
([428]) Apartados 8.1 a 8.15 del *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*; véase la nota a pie de página 420.
([429]) Sección H del *UK Explanatory Framework for Adequacy Discussions*: *National Security*, p. 34; véase la nota a pie de página 29.

3.3.2. *Uso ulterior de la información recogida*

(241) Los datos personales tratados con arreglo a la parte 4 de la DPA de 2018 no deben tratarse de una manera que sea incompatible con el fin para el que se recogieron ([430]). La DPA de 2018 dispone que el responsable del tratamiento puede tratar los datos para otro fin distinto de aquel para el que se recogieron, siempre y cuando sea compatible con el fin original y siempre que el responsable del tratamiento esté autorizado por ley para tratar dichos datos y que el tratamiento sea necesario y proporcionado ([431]). Además, la *Security Service Act* de 1989 y la *Intelligence Services Act* de 1994 especifican que los directores de los servicios de inteligencia tienen el deber de garantizar que no se obtenga ni se comunique ninguna información, salvo en la medida necesaria para el desempeño adecuado de las funciones de la agencia o para los demás fines limitados y específicos recogidos en las disposiciones pertinentes ([432]).

(242) Además, la sección 109 de la DPA de 2018 establece requisitos específicos para las transferencias internacionales de datos personales por parte de los servicios de inteligencia a terceros países u organizaciones internacionales. Con arreglo a esta disposición, no se permiten las transferencias de datos personales a un país o territorio fuera del Reino Unido o a una organización internacional, a menos que la transferencia sea necesaria y proporcionada a efectos de las funciones estatutarias del responsable del tratamiento o para otros fines dispuestos en la sección 2, apartado 2, letra a), de la *Security Service Act* de 1989 o en la sección 2, apartado 2, letra a), y la sección 4, apartado 2, letra a), de la *Intelligence Services Act* de 1994 ([433]). Es importante señalar que estos requisitos también se aplican en los casos en que se recurra a la exención de seguridad nacional con arreglo a la sección 110 de la DPA de 2018, ya que esa sección no menciona la sección 109 de la DPA de 2018 como una de las disposiciones que pueden no aplicarse si se requiere una exención de determinadas disposiciones con el fin de salvaguardar la seguridad nacional.

(243) Por otra parte, como subraya la ICO en sus orientaciones sobre el tratamiento por parte de los servicios de inteligencia, además de las garantías previstas en la parte 4 de la DPA de 2018, una agencia de inteligencia, al compartir datos con un organismo de inteligencia de un tercer país, también está sujeta a las garantías previstas en otras medidas legislativas que se le apliquen para garantizar que los datos personales se obtengan, compartan y traten de manera lícita y responsable ([434]). Por ejemplo, la IPA de 2016 establece garantías adicionales con respecto a las transferencias a un tercer país del material recogido mediante interceptación selectiva ([435]), interferencia selectiva de equipos ([436]), interceptación masiva ([437]), adquisición masiva de datos de comunicaciones ([438]) e interferencia masiva de equipos ([439]) (la denominada «comunicación internacional»). En particular, la autoridad que emite la orden debe asegurarse de que existen disposiciones para garantizar que el tercer país que recibe los datos limite el número de personas que ven el material, el alcance de la comunicación y el número de copias realizadas de cualquier material al mínimo necesario para los fines autorizados establecidos en la IPA de 2016 ([440]).

3.3.3. *Supervisión*

(244) Varios organismos supervisan el acceso del Gobierno por motivos de seguridad nacional. La ICO supervisa el tratamiento de datos personales a la luz de la DPA de 2018 (para obtener más información sobre la independencia, la función de nombramiento y los poderes de la ICO, consulte los considerandos 85 a 98), mientras que la supervisión judicial e independiente sobre el uso de los poderes de investigación en virtud de la IPA de 2016 le corresponde al Investigatory Powers Commissioner. El Investigatory Powers Commissioner supervisa el uso de los

([430]) Sección 87, apartado 1, de la DPA de 2018.

([431]) Sección 87, apartado 3, de la DPA de 2018. Si bien los responsables del tratamiento pueden estar exentos de este principio, de conformidad con la sección 110 de la DPA de 2018, en la medida en que dicha exención sea necesaria para salvaguardar la seguridad nacional, la exención debe evaluarse caso por caso y puede recurrirse a ella solo en la medida en que la aplicación de una disposición concreta tuviera consecuencias negativas para la seguridad nacional (véase el considerando 132). Los certificados de seguridad nacional para los servicios de inteligencia del Reino Unido (disponibles en el siguiente enlace https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) no cubren la sección 87, apartado 3, de la DPA de 2018. Además, dado que cualquier tratamiento para un fin distinto debe estar autorizado por ley, los servicios de inteligencia deben contar con una base jurídica clara para el tratamiento ulterior.

([432]) Para más información al respecto, véase la nota a pie de página 312.

([433]) Véase la nota a pie de página 312.

([434]) Orientaciones de la ICO sobre el tratamiento por parte de los servicios de inteligencia (véase la nota a pie de página 161).

([435]) Sección 54 de la IPA de 2016.

([436]) Sección 130 de la IPA de 2016.

([437]) Sección 151 de la IPA de 2016.

([438]) Sección 171, apartado 9, de la IPA de 2016.

([439]) Sección 192 de la IPA de 2016.

([440]) Las disposiciones deben incluir medidas para garantizar que toda copia que se realice de cualquiera de estos materiales se almacene de forma segura durante el tiempo de conservación. El material obtenido en virtud de la orden y toda copia que se realice de cualquiera de estos materiales deben destruirse tan pronto como ya no existan motivos pertinentes para su conservación (véanse la sección 150, apartados 2 y 5, y la sección 151, apartado 2, de la IPA de 2016). Cabe señalar que se ha comprobado que garantías similares, previstas en el marco jurídico anterior (RIPA de 2000), cumplen los requisitos establecidos por el Tribunal Europeo de Derechos Humanos para el intercambio de material obtenido mediante interceptación masiva con Estados extranjeros u organizaciones internacionales [Tribunal Europeo de Derechos Humanos (Gran Sala), *Big Brother Watch and others v United Kingdom*, (véase la nota a pie de página 279 más arriba), apartados 362 y 399].

poderes de investigación contemplados en la IPA de 2016 por parte de las autoridades encargadas de garantizar el cumplimiento de la ley y de las autoridades nacionales de seguridad. La supervisión política está garantizada por el Intelligence Service Committee del Parlamento.

3.3.3.1 Supervisión en virtud de la parte 4 de la DPA de 2018

(245) La ICO supervisa el tratamiento de datos personales que realizan los servicios de inteligencia en virtud de la parte 4 de la DPA de 2018 ([441]).

(246) En el anexo 13 de la DPA de 2018 se establecen las funciones generales de la ICO en relación con el tratamiento de datos personales por parte de los servicios de inteligencia que entran en el ámbito de aplicación de la parte 4 de dicha Ley. Estas funciones incluyen, pero no se limitan a, el control de la aplicación de la parte 4 de la DPA de 2018; la promoción de la sensibilización del público; asesorar al Parlamento, al Gobierno y otras instituciones sobre medidas legislativas y administrativas; la promoción del conocimiento por parte de los responsables y encargados del tratamiento de sus obligaciones; proporcionar información a un interesado sobre el ejercicio de los derechos del interesado; realizar investigaciones; etc.

(247) Con arreglo a la parte 3 de la DPA de 2018, la ICO tiene poderes para notificar a los responsables del tratamiento de una presunta infracción y para emitir avisos de la probabilidad de que un tratamiento infrinja las normas, así como de sancionar cuando se confirma una infracción. También puede emitir avisos de ejecución y de sanción por el incumplimiento de una determinada disposición de la DPA ([442]). Sin embargo, a diferencia de lo que disponen otras partes de la DPA de 2018, la ICO no puede entregar un aviso de evaluación a una autoridad nacional de seguridad ([443]).

(248) Además, la sección 110 de la DPA de 2018 establece una excepción al uso de ciertos poderes de la ICO cuando resulta necesario para salvaguardar la seguridad nacional. Esto incluye el poder de la ICO de emitir (cualquier tipo de) avisos con arreglo a la DPA (avisos de información, evaluación, ejecución y sanción), la facultad de realizar inspecciones de conformidad con las obligaciones internacionales, los poderes de entrada e inspección y las normas sobre infracciones ([444]). Como se explica en el considerando 126, estas excepciones se aplican solo si resulta necesario y proporcionado, y siempre caso por caso.

(249) La ICO y los servicios de inteligencia del Reino Unido han firmado un memorando de entendimiento ([445]) que establece un marco para la cooperación en varias cuestiones, incluidas las notificaciones de violación de la seguridad de los datos y el manejo de las reclamaciones de los interesados. En concreto, el memorando establece que, cuando se reciba una reclamación, la ICO evaluará el uso adecuado de la aplicación de cualquier exención relacionada con la seguridad nacional. El servicio de inteligencia de que se trate debe enviar las respuestas a las consultas realizadas por la ICO en el contexto del examen de reclamaciones individuales en un plazo de veinte días hábiles, utilizando los canales seguros apropiados si se trata de información clasificada. Desde abril de 2018 hasta la fecha, la ICO ha recibido veintiuna reclamaciones de personas físicas sobre los servicios de inteligencia. Cada una de estas reclamaciones se evaluó y se comunicaron al interesado las conclusiones ([446]).

([441]) Sección 116 de la DPA de 2018.

([442]) De conformidad con el párrafo segundo, anexo 13, de la DPA de 2018, pueden emitirse avisos de ejecución y sanción a un responsable o encargado del tratamiento en relación con incumplimientos de la parte 4, capítulo 2, de la DPA de 2018 (principios del tratamiento), con una disposición de la parte 4 de la DPA de 2018 que confiere derechos a un interesado, con un requisito para comunicar una violación de la seguridad de los datos a la ICO con arreglo a la sección 108 de la DPA 2018, y con los principios para las transferencias de datos personales a terceros países, países que no han ratificado el Convenio Europeo de Derechos Humanos y organizaciones internacionales en la sección 109 de la DPA de 2018 (véase el considerando para más información sobre los avisos de ejecución y sanción 92).

([443]) En virtud de la sección 147, apartado 6, de la DPA de 2018, la ICO no puede emitir un aviso de evaluación a un organismo que esté especificado en la sección 23, apartado 3, de la *Freedom of Information Act* de 2000. Esto incluye al Servicio de Seguridad (MI5), el Servicio de Inteligencia Secreto (MI6) y el Cuartel General de Comunicaciones del Gobierno.

([444]) Las disposiciones que pueden quedar exentas son: sección 108 (comunicación de una violación de la seguridad de los datos a la ICO), sección 119 (inspecciones de conformidad con las obligaciones internacionales); secciones 142 a 154 y anexo 15 (avisos de la ICO y poderes de entrada e inspección); y secciones 170 a 173 (infracciones relacionadas con los datos personales). Además de las disposiciones en relación con el tratamiento por parte de los servicios de inteligencia en el párrafo primero, letras a) y g), y párrafo segundo, del anexo 13 (otras funciones generales de la ICO).

([445]) Memorando de entendimiento entre la Information Commission's Office y la UK Intelligence Community (Comunidad de Inteligencia del Reino Unido); véase la nota a pie de página 165.

([446]) En siete de estos casos, la ICO aconsejó al reclamante que planteara su preocupación al responsable del tratamiento (este es el caso cuando una persona ha planteado una preocupación a la ICO, pero debería haberla planteado en primer lugar al responsable del tratamiento), en otro de los casos la ICO brindó asesoramiento general al responsable del tratamiento (esto se hace cuando las acciones del responsable del tratamiento no parecen haber incumplido la legislación, pero una mejora de las prácticas podría haber evitado que se planteara la preocupación ante la ICO), y en los otros trece casos no se requirió ninguna acción por parte del responsable del tratamiento (esto sucede cuando las preocupaciones planteadas por el individuo entran en el ámbito de la DPA de 2018 porque están relacionadas con el tratamiento de información personal, pero en función de la información proporcionada no parece que el responsable del tratamiento haya incumplido la legislación).

3.3.3.2. Supervisión del uso de los poderes de investigación en virtud de la IPA de 2016

(250) De acuerdo con la parte 8 de la IPA de 2016, el Investigatory Powers Commissioner es el encargado de supervisar el uso de los poderes de investigación. Este órgano está asistido por otros comisionados judiciales, a los que se hace referencia de forma conjunta como «comisionados judiciales» ([447]). La IPA de 2016 establece las garantías que protegen la independencia de los comisionados judiciales. Los comisionados judiciales deben ocupar o haber ocupado un alto cargo judicial (es decir, deben ser o haber sido miembros de los tribunales de mayor rango) ([448]) y, como cualquier miembro del poder judicial, gozan de independencia respecto al Gobierno ([449]). De conformidad con la sección 227 de la IPA de 2016, el primer ministro es quien nombra al Investigatory Powers Commissioner y al número de comisionados judiciales que considere necesario. Todos los comisionados, ya sean miembros actuales o antiguos del poder judicial, solo pueden ser nombrados sobre la base de una recomendación conjunta de los tres Chief Justices de Inglaterra y Gales, Escocia e Irlanda del Norte y el Lord Chancellor ([450]). El secretario de Estado debe proporcionar al Investigatory Powers Commissioner personal, alojamiento, equipos y otras instalaciones y servicios que pueda necesitar ([451]). El mandato de los comisionados es de tres años y pueden ser reelegidos ([452]). Como garantía adicional de su independencia, los comisionados judiciales solo pueden ser destituidos de su cargo sujeto a condiciones estrictas que impongan un umbral elevado: ya sea por el primer ministro en las circunstancias específicas enumeradas de forma exhaustiva en la sección 228, apartado 5, de la IPA de 2016 (como pueden ser quiebra o encarcelamiento), o si cada una de las cámaras del Parlamento ha ratificado una resolución que aprueba la destitución ([453]).

(251) La Investigatory Powers Commissioner y los comisionados judiciales reciben apoyo en sus funciones de la Investigatory Powers Commissioner's Office (IPCO). El personal de la IPCO incluye un equipo de inspectores, expertos juristas y técnicos internos y un grupo consultivo en materia de tecnología que ofrecen asesoramiento de expertos. Como ocurre con cada uno de los comisionados judiciales, la independencia de la IPCO está protegida. La IPCO es un organismo independiente del Home Office, es decir, que recibe financiación del Home Office pero lleva a cabo sus funciones de forma independiente ([454]).

(252) En la sección 229 de la IPA de 2016 ([455]) se establecen las funciones principales de los comisionados judiciales. En particular, los comisionados judiciales tienen un amplio poder de aprobación previa, que forma parte de las garantías que introdujo la IPA de 2016 en el marco jurídico del Reino Unido. Los comisionados judiciales son los encargados de aprobar las garantías en relación con la interceptación selectiva, la interferencia de equipos, los conjuntos de datos personales masivos, la adquisición masiva de datos de comunicaciones, así como los avisos de conservación de datos de comunicaciones ([456]). El Investigatory Powers Commissioner también debe emitir siempre una autorización previa para la adquisición de datos de comunicaciones con fines de aplicación de la ley ([457]). Si un comisionado se niega a aprobar una orden judicial, el secretario de Estado puede apelar al Investigatory Powers Commissioner, cuya decisión es definitiva.

([447]) De conformidad con la sección 227, apartados 7 y 8, de la IPA de 2016, el Investigatory Powers Commissioner es un comisionado judicial, y el Investigatory Powers Commissioner y los demás comisionados judiciales se denominan, de forma conjunta, «comisionados judiciales». Actualmente hay quince comisionados judiciales.

([448]) Con arreglo a la parte 3, sección 60, apartado 2, de la *Constitutional Reform Act* de 2005, un «alto cargo judicial» significa el cargo de juez de cualquiera de los siguientes tribunales: i) el Tribunal Supremo del Reino Unido; ii) el Tribunal de Apelación (Inglaterra y Gales); iii) Tribunal Superior de Inglaterra y Gales; iv) el Tribunal Superior de Justicia de Escocia; v) el Tribunal de Apelación de Irlanda del Norte; vi) el Tribunal Superior de Justicia de Irlanda del Norte; o como Lord of Appeal in Ordinary.

([449]) La independencia del poder judicial se basa en las convenciones y está ampliamente reconocida desde la *Act of Settlement* de 1701.

([450]) Sección 227, apartado 3, de la IPA de 2016. De acuerdo con la sección 227, apartado 4, letra e), de la IPA de 2016, os comisionados judiciales también deben ser recomendados por el Investigatory Powers Commissioner.

([451]) Sección 238 de la IPA de 2016.

([452]) Sección 227, apartado 2, de la IPA de 2016.

([453]) El proceso de destitución es igual al proceso de destitución de otros jueces en el Reino Unido (véase, por ejemplo, la sección 11, apartado 3, de la de *Senior Courts Act* 1981 y la sección 33 de la *Constitutional Reform Act* de 2005, que también requieren una resolución previa aprobación de ambas cámaras del Parlamento). Hasta la fecha, ningún comisionado judicial ha sido destituido de su cargo.

([454]) Un organismo independiente es una organización o agencia que recibe financiación del gobierno, pero que puede actuar de forma independiente (para una definición completa y más información sobre los organismos independientes, consúltese el manual del Gabinete del Reino Unido acerca de la clasificación de los organismos públicos, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf y el primer informe de la sesión 2014-2015 del Public Administration Select Committee de la Cámara de los Comunes, disponible en el siguiente enlace: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) De conformidad con el artículo 229 de la IPA de 2016, el comisionado judicial dispone de amplios poderes de supervisión que también abarcan la supervisión de la conservación y divulgación de los datos recopilados por los servicios de inteligencia.

([456]) Las decisiones en torno a la aprobación de una decisión del secretario de Estado de emitir una orden judicial atañen a los propios comisionados jurídicos. Si un comisionado se niega a aprobar una orden judicial, el secretario de Estado puede apelar al Investigatory Powers Commissioner, cuya decisión es definitiva.

([457]) Siempre es necesaria la autorización del Investigatory Powers Commissioner cuando se adquieren datos de comunicaciones con fines de aplicación de la ley (sección 60A de la IPA de 2016). Cuando los datos de comunicaciones se adquieren con fines de seguridad nacional, la autorización puede concederla el Investigatory Powers Commissioner o, alternativamente, un funcionario de alto rango designado de la autoridad pública pertinente (véanse las secciones 61 y 61A de la IPA de 2016 y el considerando 203).

(253) El Relator Especial sobre el derecho a la privacidad de las Naciones Unidas acogió con gran satisfacción el establecimiento de los comisionados judiciales con la IPA de 2016, ya que «todas las solicitudes, de carácter más sensible o intrusivo, para realizar vigilancias debe autorizarlas tanto un ministro del Gabinete como la Investigatory Powers Commissioner's Office». En particular, destacó que «este elemento de control jurisdiccional (a través de la función del Investigatory Powers Commissioner) asistido por un equipo de inspectores experimentados y expertos en tecnología con mejores recursos es una de las garantías nuevas más importantes introducidas por el IPA», que sustituyó a un sistema previamente fragmentado de autoridades de supervisión y complementa el papel del Intelligence and Security Committee del Parlamento y del Investigatory Powers Tribunal ([458]).

(254) Además, el Investigatory Powers Commissioner tiene poderes para realizar una supervisión *ex post*, incluso mediante auditoría, inspección e investigación, del uso de los poderes de investigación con arreglo a la IPA de 2016 ([459]), y algunos poderes y funciones adicionales previstos en la legislación pertinente ([460]). Los resultados de la supervisión *ex post* se incluyen en el informe que el Investigatory Powers Commissioner debe elaborar anualmente y presentar al primer ministro ([461]), y que debe publicarse y presentarse al Parlamento ([462]) El informe contiene estadísticas e información relevante 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, así como la aplicación de las garantías en relación con elementos sujetos a la prerrogativa de confidencialidad, material periodístico confidencial y fuentes de información periodística, información sobre las disposiciones adoptadas y los fines operativos empleados en el contexto de las órdenes masivas. Por último, en el informe anual de la IPCO se especifica en qué ámbito se han ofrecido recomendaciones a las autoridades públicas y cómo estas se han abordado ([463]).

(255) De acuerdo con la sección 231 de la IPA de 2016, si el Investigatory Powers Commissioner tiene conocimiento de algún error pertinente cometido por las autoridades públicas en el uso de sus poderes de investigación, deberá informar al interesado cuando considere que el error es grave y que es de interés público para la persona ser informado/a ([464]). En particular, la sección 231 de la IPA de 2016 especifica que, cuando se informe a una persona de un error, el Investigatory Powers Commissioner debe proporcionar información sobre cualquier derecho que deba ejercer ante el Investigatory Powers Tribunal, y brindar los detalles que el Investigatory Powers Commissioner considere necesarios para el ejercicio de tales derechos y cuando exista un interés público para la comunicación en cuestión ([465]).

([458]) *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* («Declaración de fin de misión del Relator Especial sobre el derecho a la privacidad al concluir su misión en el Reino Unido de Gran Bretaña e Irlanda del Norte», documento en inglés); véase la nota a pie de página 281).

([459]) Sección 229 de la IPA de 2016. Los poderes de investigación e información del comisionado judicial se establecen en la sección 235 de la IPA de 2016.

([460]) Estos incluyen medidas de vigilancia en virtud de la RIPA de 2000, el ejercicio de funciones con arreglo a la parte 3 de la *Police Act* (Ley de las fuerzas policiales) de 1997 (autorización de acción con respecto a la propiedad) y el ejercicio por parte del secretario de Estado de funciones en virtud de las secciones 5 a 7 de la *Intelligence Services Act* (Ley de los servicios de inteligencia) de 1994 (órdenes de interferencia con radiotelegrafía, entrada e interferencia con la propiedad (sección 229 de la IPA de 2016).

([461]) Sección 230 de la IPA de 2016. El Investigatory Powers Commissioner también puede informar al primer ministro por iniciativa propia sobre cualquier asunto relacionado con sus funciones. Por otro lado, el Investigatory Powers Commissioner también debe informar al primer ministro cuando así lo solicite y este último puede indicar al Investigatory Powers Commissioner que revise cualquier función de los servicios de Inteligencia.

([462]) Algunas partes pueden quedar excluidas si su publicación fuera contraria a la seguridad nacional.

([463]) Por ejemplo, en el informe anual de 2019 de la IPCO (apartado 6.38 del informe) se menciona que se recomendó al MI5 modificar su política de conservación de conjuntos de datos personales masivos, ya que debería haber adoptado un enfoque en el que se consideró la proporcionalidad de la conservación para todos los campos de conservación de conjuntos de datos personales masivos y para cada conjunto de datos personales masivos conservado. A finales de 2018, la IPCO no estaba convencida de que se estuviera siguiendo esta recomendación y el informe de 2019 explicaba que el MI5 estaba entonces introduciendo un nuevo proceso para cumplir con este requisito. El informe anual de 2019 (apartado 8.22 del informe) menciona también que se proporcionaron una serie de recomendaciones al Cuartel General de Comunicaciones del Gobierno relativas a la presentación de informes sobre la proporcionalidad de sus consultas en materia de datos masivos. El informe confirma que a finales de 2018 se habían realizado mejoras en este aspecto. Informe anual de 2019 de la Investigatory Powers Commissioner's Office, disponible en el siguiente enlace: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Además, cada inspección realizada por la IPCO de una autoridad pública se concluye con un informe que se presenta a la autoridad e incluye las recomendaciones derivadas de dicha inspección. Después, la IPCO inicia cada inspección posterior con una revisión de las recomendaciones anteriores de la última inspección y, en el nuevo informe de inspección, se refleja si se han aplicado o se siguen aplicando las recomendaciones anteriores.

([464]) Un error se considera «grave» cuando el Investigatory Powers Commissioner estima que ha causado un perjuicio o daño significativo a la persona en cuestión (sección 231, apartado 2, de la IPA de 2016). En 2018, se informó de veintidós errores, de los cuales ocho se consideraron graves y, en consecuencia, se informó de ellos al interesado. Véase el anexo C del informe anual de 2018 de la Investigatory Powers Commissioner Office (véase https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). En 2019, fueron catorce los errores hallados que se consideraron graves. Véase el anexo C del informe anual de 2019 de la Investigatory Powers Commissioner Office (véase la nota a pie de página 463).

([465]) La sección 231 de la IPA de 2016 especifica que cuando se informa a una persona de un error, el Investigatory Powers Commissioner debe brindar los detalles que considere necesarios para el ejercicio de tales derechos, teniendo en cuenta, en especial, la medida en que la comunicación de los detalles sería contraria al interés público o perjudicial para la prevención o detección de delitos graves, el bienestar económico del Reino Unido o el desempeño continuado de las funciones de cualquiera de los servicios de inteligencia.

3.3.3.3 Supervisión parlamentaria de los servicios de inteligencia

(256) La supervisión parlamentaria por parte del Intelligence and Security Committee tiene su fundamente jurídico en la *Justice and Security Act* de 2013 (JSA de 2013) ([466]). Esta Ley establece al Intelligence and Security Committee como un comité del Parlamento del Reino Unido. Desde 2013, el Intelligence and Security Committee ha estado recibiendo poderes de mayor envergadura, en especial la supervisión de las actividades operativas de los servicios de seguridad. En virtud de la sección 2 de la JSA de 2013, el Intelligence and Security Committee tiene la tarea de supervisar los gastos, la administración, la política y las operaciones de las agencias de seguridad nacional. La JSA de 2013 también especifica que el Intelligence and Security Committee puede realizar investigaciones sobre cuestiones operativas cuando estas no estén relacionadas con operaciones en curso ([467]). El memorando de entendimiento entre el primer ministro y el Intelligence and Security Committee ([468]) especifica en detalle los elementos que deben tenerse en cuenta al valorar si una actividad no forma parte de ninguna operación en curso ([469]). El primer ministro puede también solicitar al Intelligence and Security Committee que investigue operaciones en curso y puede revisar la información proporcionada voluntariamente por las agencias de seguridad nacional.

(257) Con arreglo al anexo 1 de la JSA de 2013, el Intelligence and Security Committee puede solicitar a los directores de cualquiera de los tres servicios de inteligencia que comuniquen cualquier información. La agencia debe entonces poner dicha información a disposición, salvo que el secretario de Estado la vete ([470]). De acuerdo con las aclaraciones proporcionadas por las autoridades del Reino Unido, en la práctica se retiene una parte muy marginal de la información que el Intelligence and Security Committee solicita ([471]).

(258) El Intelligence and Security Committee está formado por miembros que pertenecen a una de las dos cámaras del Parlamento y son nombrados por el primer ministro tras consultar con el líder de la oposición ([472]). El Intelligence and Security Committee debe presentar un informe anual al Parlamento sobre el desempeño de sus funciones y otros informes que considere oportunos ([473]). Además, el Intelligence and Security Committee tiene derecho a recibir cada tres meses la lista de fines operativos que se utiliza para examinar el material que se obtiene de forma masiva ([474]). El primer ministro comparte con el Intelligence and Security Committee copias de las investigaciones, inspecciones o auditorías realizadas por el Investigatory Powers Commissioner cuando la cuestión tratada en los informes es pertinente para las competencias estatutarias del Comité ([475]). Por último, el Intelligence and Security Committee puede solicitar al Investigatory Power Commissioner que realice una investigación, y este último debe informar al Comité sobre la decisión de llevar a cabo o no la investigación ([476]).

(259) El Intelligence and Security Committee también proporcionó información sobre el proyecto de ley de la IPA de 2016, que resultó en una serie de enmiendas que ahora se reflejan en la IPA de 2016 ([477]). En concreto, el Intelligence and Security Committee recomendó reforzar las protecciones de la privacidad mediante la introducción de un conjunto

([466]) Como aclararon las autoridades del Reino Unido, la JSA de 2013 amplió el mandato del Intelligence and Security Committee para incluir una labor de supervisión de la comunidad de inteligencia más allá de las tres agencias principales, y permitir la supervisión retrospectiva de las actividades operativas de las agencias en asuntos de gran interés nacional.

([467]) Sección 2 de la JSA de 2013.

([468]) Memorando de entendimiento entre el primer ministro y el Intelligence and Security Committee, disponible en el siguiente enlace: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Apartado 14 del memorando de entendimiento entre el primer ministro y el Intelligence and Security Committee (véase la nota a pie de página 468).

([470]) El secretario de Estado solo puede vetar la comunicación de información por dos motivos: la información es sensible y, por lo tanto, en interés de la seguridad nacional no debe comunicarse al Intelligence and Security Committee; o se trata de información de una naturaleza tal que, si se solicitara al secretario de Estado que la presentara ante un Departmental Select Committee de la Cámara de los Comunes, el secretario de Estado no consideraría (por motivos que no se limitan a la seguridad nacional) oportuno hacerlo (párrafo cuarto, punto 2, del anexo 2, de la JSA de 2013).

([471]) Sección H del *UK Explanatory Framework for Adequacy Discussions*: *National Security*, p. 43; véase la nota a pie de página 31.

([472]) Sección 1 de la JSA de 2013. Los secretarios de Estado no son elegibles como miembros del Comité. Los miembros del Comité mantienen su cargo en el mismo mientras dure la formación del Parlamento durante el cual fueron nombrados. Pueden ser destituidos mediante resolución de la Cámara por la que fueron nombrados, o bien si dejan de ser miembros del Parlamento o asumen el cargo de secretarios de Estado. Los miembros del Intelligence and Security Committee también pueden renunciar.

([473]) En el siguiente enlace pueden encontrarse los informes y declaraciones en línea del Intelligence and Security Committee: https://isc.independent.gov.uk/publications/. En 2015, el Intelligence and Security Committee publicó un informe sobre *Privacy and Security: A modern and transparent legal framework* («Privacidad y seguridad: un marco jurídico moderno y transparente», documento en inglés) (véase: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), en el que consideró el marco jurídico de las técnicas de vigilancia utilizadas por los servicios de inteligencia y emitió una serie de recomendaciones que, posteriormente, se valoraron y se integraron en el anteproyecto de ley *Investigatory Powers Bill*, que se convirtió en la API de 2016. La respuesta del Gobierno al informe de privacidad y seguridad está disponible en el siguiente enlace: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Secciones 142, 161 y 183 de la IPA de 2016.

([475]) Sección 234 de la IPA de 2016.

([476]) Sección 236 de la IPA de 2016.

([477]) Intelligence and Security Committee of Parliament, *Report on the draft Investigatory Powers Bill* («Informe sobre el proyecto de ley *Investigatory Powers Bill*», documento en inglés), disponible en el siguiente enlace: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

de protecciones de la privacidad que aplican a toda la gama de poderes de investigación ([478]). Asimismo, sugirió cambios a las capacidades propuestas relativas a la interferencia de equipos, los conjuntos de datos personales masivos y los datos de comunicaciones, y solicitó otras enmiendas específicas para reforzar las limitaciones y garantías para el uso de los poderes de investigación ([479]).

3.3.4. *Acciones administrativas y judiciales*

(260) En el ámbito del acceso gubernamental con fines de seguridad nacional, los interesados deben tener la posibilidad de emprender acciones legales ante un tribunal imparcial e independiente para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión ([480]). Este órgano jurisdiccional debe tener, en particular, la facultad de adoptar decisiones vinculantes sobre el servicio de inteligencia ([481]). En el Reino Unido, como se explica en los considerandos 261 a 271, una serie de vías de acción judicial brindan a los interesados la posibilidad de perseguir y obtener tales vías de derecho.

3.3.4.1 Mecanismos de reparación disponibles en virtud de la parte 4 de la DPA

(261) En virtud de la sección 165 de la DPA de 2018, un interesado tiene el derecho a presentar una reclamación ante la ICO si considera que, en relación con datos personales que le conciernen, existe una infracción de la parte 4 de dicha Ley. La ICO tiene la facultad de evaluar el cumplimiento del responsable y el encargado del tratamiento con la DPA de 2018, así como de exigirles que adopten medidas oportunas, de ser necesario. Además, en virtud de la parte 4 de la DPA de 2018, las personas físicas tienen derecho a solicitar al Tribunal Superior (o Tribunal Superior de Justicia de Escocia) una orden que requiera que el responsable del tratamiento cumpla con los derechos de acceso a los datos ([482]), a oponerse al tratamiento ([483]) y a la rectificación o supresión de los datos ([484]).

(262) Las personas físicas también tienen derecho a reclamar una indemnización por los daños sufridos debido a la violación de un requisito de la parte 4 de la DPA de 2018 por parte del responsable o del encargado del tratamiento ([485]). Los daños incluyen tanto las pérdidas económicas como los daños que no implican pérdidas económicas, como puede ser la ansiedad ([486]).

3.3.4.2 Mecanismos de reparación disponibles en virtud de la IPA de 2016

(263) Las personas físicas pueden obtener una reparación por violaciones de la IPA de 2016 ante el Investigatory Powers Tribunal.

(264) La RIPA de 2000 establece la creación del Investigatory Powers Tribunal, que es independiente del poder ejecutivo ([487]). En virtud de la sección 65 de la RIPA de 2000, Su Majestad nombra a los miembros de este Tribunal por un período de cinco años. Los miembros del Tribunal pueden ser destituidos de su cargo por decisión de Su Majestad en respuesta a un discurso ([488]) de ambas cámaras del Parlamento ([489]).

([478]) Estos deberes generales en relación con la privacidad se establecen ahora en la sección 2, apartado 2, de la IPA de 2016, que dispone que una autoridad pública que actúa en virtud de la IPA de 2016 debe tener en cuenta si el objetivo que se pretende alcanzar gracias a la orden, autorización o aviso podría lograrse razonablemente por otros medios menos intrusivos, ya sea que 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, el interés público en la integridad y seguridad de los sistemas de telecomunicaciones y los servicios postales, o cualquier otro aspecto de interés público en la protección de la privacidad.

([479]) Por ejemplo, en respuesta a la solicitud del Intelligence and Security Committee, se redujo de cinco a tres días hábiles el número de días que una orden «urgente» puede estar en vigor antes de que el comisionado judicial tenga que aprobarla, y se otorgó al Intelligence and Security Committee el poder de remitir asuntos al Investigatory Powers Commissioner para su investigación.

([480]) Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, punto 194.

([481]) Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, punto 197.

([482]) Sección 94, apartado 11, de la DPA de 2018.

([483]) Sección 99, apartado 4, de la DPA de 2018.

([484]) Sección 100, apartado 1, de la DPA de 2018.

([485]) La sección 169 de la DPA de 2018 admite las reclamaciones de «Una persona que sufre un daño debido a una violación de un requisito de la legislación en materia de protección de datos». De acuerdo con la información proporcionada por las autoridades del Reino Unido, en la práctica, es probable que se presenten reclamaciones o quejas contra los servicios de inteligencia ante el Investigatory Powers Tribunal, que tiene una amplia jurisdicción, es capaz de conceder indemnizaciones por daños y la presentación de reclamaciones ante él no conlleva ningún coste.

([486]) Sección 169, apartado 5, de la DPA de 2018.

([487]) En virtud del anexo 3 de la RIPA de 2000, los miembros deben tener experiencia judicial concreta y pueden ser reelegidos para el cargo.

([488]) Un «discurso» es una moción que se presenta ante el Parlamento y cuyo fin es que el/la monarca esté al tanto de las opiniones del Parlamento sobre una cuestión en particular.

([489]) Párrafo primero, punto 5, del anexo 3, de la RIPA de 2000.

(265) Con arreglo a la sección 65 de la RIPA de 2000, el Investigatory Powers Tribunal es el órgano jurisdiccional apropiado para cualquier reclamación de una persona agraviada por una conducta contemplada en la IPA de 2016, la RIPA de 2000 o cualquier conducta de los servicios de inteligencia ([490]).

(266) De conformidad con la sección 65 de la RIPA de 2000, para que una persona pueda presentar un recurso ante el Investigatory Powers Tribunal («requisito de legitimación») debe creer ([491]) que la conducta de un servicio de inteligencia ha tenido lugar en relación con él/ella, cualquiera de sus bienes, cualquier comunicación enviada por él/ella o a él/ella, o destinada a él/ella, o en relación con su uso de cualquier servicio postal, servicio de telecomunicaciones o sistema de telecomunicaciones ([492]). Además, el reclamante debe creer que la conducta se ha producido en «circunstancias impugnables» ([493]) o que «la han llevado a cabo los servicios de inteligencia o se ha llevado a cabo en su nombre» ([494]). Dado que, en particular, este estándar de «creencia» se ha interpretado de manera bastante difusa ([495]), llevar un caso ante el Investigatory Powers Tribunal está sujeto a requisitos de baja legitimación.

(267) Cuando el Investigatory Powers Tribunal sopesa una reclamación que se ha presentado ante él, es su deber investigar si las personas contra las que se hace alguna acusación en la reclamación tienen alguna implicación respecto al reclamante, así como investigar a la autoridad que presuntamente ha cometido las violaciones y si la presunta conducta efectivamente se ha producido ([496]). En las vistas del Tribunal este debe aplicar, para adoptar su resolución, los mismos principios que aplicaría un tribunal en una solicitud de control jurisdiccional ([497]). Además, los destinatarios de las órdenes o avisos en virtud de la IPA de 2016, y todas las demás personas que ocupen un cargo dentro de la Corona británica, que sean empleados de las fuerzas del orden o formen parte del Police Investigations and Review Commissioner tienen el deber de comunicar o proporcionar al Investigatory Powers Tribunal todos los documentos e información que el Tribunal pueda requerir con el fin de permitirle ejercer sus competencias ([498]).

(268) El Investigatory Powers Tribunal debe notificar al reclamante si ha habido una resolución a su favor o no ([499]). En virtud de la sección 67, apartados 6 y 7, de la RIPA de 2000, el Tribunal tiene la facultad de emitir medidas provisionales y conceder cualquier indemnización u otra medida que considere adecuada. Estas medidas pueden incluir órdenes que anulen o invaliden cualquier orden o autorización y órdenes que requieran la destrucción de cualquier registro de información obtenida en el ejercicio de cualquier tipo de poder conferido por una orden,

([490]) Sección 65, apartado 5, de la RIPA de 2000.

([491]) Sobre el estándar de la valoración de «creencia», véase el asunto *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH, apartado 41. En dicho asunto, el Investigatory Powers Tribunal, haciendo referencia a la jurisprudencia del Tribunal Europeo de Derechos Humanos, sostuvo que la valoración apropiada en relación con la creencia afirmada de que ha habido alguna conducta contemplada en el artículo 68, apartado 5, de la RIPA de 2000 por parte de o en nombre de cualquiera de los servicios de inteligencia, es si existe alguna base para tal creencia, de modo que el individuo pueda afirmar ser víctima de una violación ocasionada por la mera existencia de medidas secretas o legislación que permita medidas secretas, solo si puede demostrar que, debido a su situación personal, corre el riesgo potencial de ser sometido a tales medidas.

([492]) Sección 65, apartado 4, letra a, de la RIPA de 2000.

([493]) Tales circunstancias se refieren a la conducta de las autoridades públicas que tiene lugar con autoridad (por ejemplo, una orden judicial, una autorización/aviso para la adquisición de comunicaciones, etc.), o si las circunstancias son tales que (exista o no dicha autoridad) no hubiera sido adecuado que la conducta se llevara a cabo sin ella o, al menos, sin que se tuviera debidamente en cuenta si hubiera debido buscarse dicha autoridad. Se considera que las conductas autorizadas por un comisionado judicial se han producido en circunstancias impugnables (sección 65, apartado 7ZA, de la RIPA 2000), mientras que se considera que otras conductas que tienen lugar con el permiso de una persona que ocupa un cargo judicial no han tenido lugar en circunstancias impugnables (sección 65, apartados 7 y 8, de la RIPA de 2000).

([494]) De acuerdo con la información facilitada por las autoridades del Reino Unido, el bajo umbral para presentar una reclamación determina que no sea inusual que la investigación del Tribunal resuelva que, de hecho, el reclamante nunca estuvo sometido a investigación por parte de una autoridad pública. El último informe estadístico del Investigatory Powers Tribunal determina que, en 2016, el Tribunal recibió 209 denuncias, de las cuales el 52 % se consideraron insustanciales o abusivas y el 25 % recibieron un resultado de «sin resolución». Las autoridades del Reino Unido aclararon que esto significa que no se utilizaron actividades/poderes encubiertos en relación con el reclamante, o que se utilizaron técnicas encubiertas y el Tribunal determinó que la actividad era lícita. Por otro lado, el 11 % de las reclamaciones se desestimaron, se revocaron o se consideraron inválidas, el 5 % se presentaron fuera de plazo y el 7 % se resolvieron a favor del reclamante. El informe estadístico de 2016 del Investigatory Powers Tribunal está disponible en el siguiente enlace: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Véase el asunto *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. En dicho asunto, el Investigatory Powers Tribunal, haciendo referencia a la jurisprudencia del Tribunal Europeo de Derechos Humanos, sostuvo que la valoración apropiada en relación con la creencia afirmada de que ha habido alguna conducta contemplada en el artículo 68, apartado 5, de la RIPA de 2000 por parte de o en nombre de cualquiera de los servicios de inteligencia, es si existe alguna base para tal creencia, incluido el hecho de que el individuo pueda afirmar ser víctima de una violación ocasionada por la mera existencia de medidas secretas o legislación que permita medidas secretas, solo si puede demostrar que, debido a su situación personal, corre el riesgo potencial de ser sometido a tales medidas (véase el apartado 41, del asunto *Human Rights Watch v Secretary of State*).

([496]) Sección 67, apartado 3, de la RIPA de 2000.

([497]) Sección 67, apartado 2, de la RIPA de 2000.

([498]) Sección 68, apartados 6 y 7, de la RIPA de 2000.

([499]) Sección 68, apartado 4, de la RIPA de 2000.

autorización o aviso, o que de otra manera tenga cualquier autoridad pública en relación con cualquier persona ([500]). Con arreglo a la sección 67A de la RIPA de 2000, las resoluciones del Investigatory Powers Tribunal pueden apelarse, bajo reserva de la autorización concedida por este Tribunal o el tribunal de apelaciones correspondiente.

(269) Por último, cabe señalar que se ha debatido en varias ocasiones el papel del Investigatory Powers Tribunal en el contexto de acciones legales ante el Tribunal Europeo de Derechos Humanos, en particular en el asunto *Kennedy v. the United Kingdom* ([501]) y, más recientemente, en el asunto *Big Brother Watch and others v. United Kingdom* ([502]), en el que el Tribunal Europeo declaró que «el Investigatory Powers Tribunal ofreció un recurso judicial sólido a toda persona que sospechase que sus comunicaciones habían sido interceptadas por los servicios de inteligencia» ([503]).

3.3.4.3 Otros mecanismos de reparación disponibles

(270) Como se explica en los considerandos 109 a 111, los medios de reparación en virtud de la *Human Rights Act* de 1998 y ante el Tribunal Europeo de Derechos Humanos ([504]) también están disponibles en el ámbito de la seguridad nacional. La sección 65, apartado 2, de la RIPA de 2000 otorga al Investigatory Powers Tribunal la jurisdicción exclusiva para todas las reclamaciones de la *Human Rights Act* relacionadas con los servicios de inteligencia ([505]). Tal como apunta el Tribunal Superior «si se ha producido una violación de la *Human Rights Act* sobre los hechos de un caso particular esto puede, en principio, plantearse y juzgarse en un tribunal independiente que puede tener acceso a todo el material pertinente, incluido material secreto. […] También tenemos en cuenta en este contexto que el propio Tribunal está ahora sujeto a la posibilidad de una apelación ante un tribunal de apelaciones apropiado (en Inglaterra y Gales, dicho tribunal sería el Tribunal de Apelación); y que el Tribunal Supremo del Reino Unido ha decidido recientemente que el Tribunal es, en principio, susceptible de control jurisdiccional: véase *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ([506]).

(271) De lo anterior se desprende que cuando las autoridades encargadas de garantizar el cumplimiento de la ley o las autoridades nacionales de seguridad del Reino Unido acceden a datos personales que entran en el ámbito de aplicación de la presente Decisión, dicho acceso se rige por leyes que establecen las condiciones en las que puede realizarse el acceso y garantizan que el acceso y el uso ulterior de los datos se limiten a lo necesario y proporcionado al objetivo perseguido de aplicación de la ley o de seguridad nacional. Además, dicho acceso está sujeto en la mayoría de los casos a la autorización previa por parte de un órgano jurisdiccional, mediante la aprobación de una orden judicial o una orden de entrega y, en todos los casos, está sujeto a supervisión independiente. Una vez que las autoridades públicas han accedido a los datos, su tratamiento, incluido el intercambio y la transferencia ulteriores de los mismos, está sujeto a garantías específicas de protección de datos en virtud de la parte 3 de la DPA de 2018, que refleja las garantías previstas por la Directiva (UE) 2016/680, para su tratamiento por parte de las autoridades encargadas de garantizar el cumplimiento de la ley y la parte 4 de la DPA de 2018 para su tratamiento por parte de los servicios de inteligencia. Por último, los interesados disfrutan en este ámbito de la posibilidad de recurrir a acciones administrativas y judiciales efectivas, incluido el acceso a sus datos o la rectificación o supresión de dichos datos.

(272) Dada la importancia de tales condiciones, limitaciones y garantías a efectos de la presente Decisión, la Comisión seguirá de cerca la aplicación e interpretación de las normas del Reino Unido que regulan el acceso del Gobierno a los datos. Esto incluirá los avances legislativos, reglamentarios y de la jurisprudencia pertinentes, así como las actividades de la ICO y otras autoridades de supervisión en este ámbito. También se prestará especial atención a la

([500]) Un ejemplo de la aplicación de esos poderes es el asunto de *Liberty & Others vs. the Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. El Tribunal resolvió a favor de dos reclamantes porque su comunicación, en un caso, se conservó más allá de los límites establecidos y, en el otro, porque no se siguió el procedimiento de examen tal y como se establece en las normas internas del Cuartel General de Comunicaciones del Gobierno. En el primer caso, el Tribunal ordenó a los servicios de inteligencia la destrucción de las comunicaciones conservadas por más tiempo del correspondiente. En el segundo caso, no se emitió una orden de destrucción porque no se había conservado la comunicación.

([501]) *Kennedy v. the United Kingdom*, véase la nota a pie de página 129.

([502]) Tribunal Europeo de Derechos Humanos, *Big Brother Watch and others v United Kingdom*, (véase la nota a pie de página 268 más arriba), apartados 413 a 415.

([503]) Tribunal Europeo de Derechos Humanos, *Big Brother Watch*, apartado 425.

([504]) Como ilustra, por ejemplo, la reciente sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos en el asunto *Big Brother Watch and others v United Kingdom* (véase la nota a pie de página 279 más arriba), esto permite un control judicial efectivo —similar al que están sujetos los Estados miembros de la UE— por parte de un tribunal internacional sobre el respeto de los derechos fundamentales por las autoridades públicas al acceder a los datos personales. Además, la ejecución de las sentencias del Tribunal Europeo de Derechos Humanos está sujeta a una supervisión específica por parte del Consejo de Europa.

([505]) En *Belhaj & others* [2017] UKSC 3, la resolución de la ilicitud de la interceptación de material sujeto a la prerrogativa de confidencialidad se basó directamente en el artículo 8 del Convenio Europeo de Derechos Humanos (véase la resolución 11).

([506]) Tribunal Superior de Inglaterra y Gales, *Liberty*, [2019] EWHC 2057 (Admin), apartado 170.

ejecución por parte del Reino Unido de las sentencias pertinentes del Tribunal Europeo de Derechos Humanos, incluidas las medidas identificadas en los «planes de acción» y los «informes de acción» presentados al Comité de Ministros en el contexto de la supervisión del cumplimiento de las sentencias del Tribunal.

4. **CONCLUSIÓN**

(273) La Comisión considera que el RGPD del Reino Unido y la DPA de 2018 garantizan 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.

(274) Además, la Comisión estima que, en su conjunto, los mecanismos de supervisión y las vías de reparación previstos en el Derecho del Reino Unido permiten identificar y sancionar en la práctica las infracciones cometidas y ofrecen al interesado remedios legales para obtener acceso a los datos personales que le conciernen y, en su caso, a la rectificación o supresión de los mismos.

(275) 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 transfieren 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 de aplicación de la ley y de seguridad nacional, se limitará a lo estrictamente necesario para lograr el objetivo legítimo en cuestión, y que existe una tutela judicial efectiva contra tal injerencia.

(276) Por lo tanto, a la luz de las conclusiones de la presente Decisión, debe concluirse que el Reino Unido garantiza un nivel adecuado de protección a tenor del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

(277) Esta conclusión se basa tanto en el régimen nacional pertinente del Reino Unido como en sus compromisos internacionales, en particular la adhesión al Convenio Europeo de Derechos Humanos y el acatamiento de la jurisdicción del Tribunal Europeo de Derechos Humanos. Por tanto, la adhesión continuada a dichas obligaciones internacionales es un elemento de especial importancia para la evaluación en la que se basa la presente Decisión.

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

(278) 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 expirado, no hayan 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.

(279) 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 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.

(280) 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 Maximillian Schrems ([507]), 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 de la persona a la privacidad y la protección de los datos, el Derecho nacional debe proporcionarle un recurso legal para presentar esas objeciones ante un tribunal nacional, al que podrá exigirse la presentación de una petición de decisión prejudicial al Tribunal de Justicia ([508]).

([507]) Maximillian Schrems contra Data Protection Commissioner, apartado 65.

([508]) Maximillian Schrems contra Data Protection Commissioner, 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».

6. SUPERVISIÓN, SUSPENSIÓN, DEROGACIÓN O MODIFICACIÓN DE LA PRESENTE DECISIÓN

(281) 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 tras la adopción de la presente Decisión a fin de valorar si esta aún garantiza un nivel de protección esencialmente equivalente. Dicha supervisión es de especial importancia en este caso particular, ya que el Reino Unido administrará y aplicará un nuevo régimen de protección de datos que ya no está sujeto al Derecho de la Unión y que puede transformarse. A ese respecto, se prestará 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 la presente Decisión; a la eficacia del ejercicio de los derechos individuales, incluido cualquier avance pertinente en la legislación y en la práctica con respecto a las excepciones o restricciones 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 basará en, entre otros elementos, los avances de la jurisprudencia y la supervisión de la ICO y otros organismos independientes.

(282) 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 presente Decisión, así como de cualquier evolución en las prácticas relacionadas con el tratamiento de los datos personales evaluados en 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 281.

(283) 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.

(284) Cuando la información disponible, en particular la información resultante de la supervisión de 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.

(285) Si, al expirar dicho plazo determinado, las autoridades competentes del Reino Unido no han adoptado dichas medidas o no han demostrado satisfactoriamente de otro modo que la presente Decisión sigue basándose en un nivel de protección adecuado, la Comisión iniciará 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, esta Decisión.

(286) De manera alternativa, la Comisión iniciará este procedimiento con miras a modificar la Decisión, en particular mediante la imposición de condiciones adicionales para las transferencias de datos o limitando el alcance de la conclusión de adecuación solo a las transferencias de datos para las que se sigue garantizando un nivel adecuado de protección.

(287) Por razones imperiosas de urgencia debidamente justificadas, la Comisión hará uso de la posibilidad 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 Decisión.

7. DURACIÓN Y RENOVACIÓN DE LA PRESENTE DECISIÓN

(288) La Comisión debe tener en cuenta que, una vez finalizado el período transitorio previsto por el acuerdo de retirada, y tan pronto como deje de aplicarse la disposición provisional en virtud del artículo 782 del Acuerdo de Comercio y Cooperación UE-Reino Unido, el Reino Unido administrará, aplicará y ejecutará un nuevo régimen de protección de datos comparable al acuerdo vigente cuando estaba sujeto al Derecho de la Unión. Esto puede implicar, en especial, modificaciones o cambios en el marco de protección de datos evaluado en la presente Decisión, así como otros acontecimientos pertinentes.

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

(290) 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**

(291) El Comité Europeo de Protección de Datos publicó su dictamen ([509]), que se ha tomado en consideración en la elaboración de la presente Decisión.

(292) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado en virtud del artículo 93 del Reglamento (UE) 2016/679,

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. A los 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 del Reglamento (UE) 2016/679, desde la Unión Europea al Reino Unido.

2. La presente Decisión no abarca 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 efectivo de la inmigración de conformidad con el párrafo cuarto, punto 1, anexo 2, de la DPA de 2018.

Artículo 2

Cuando las autoridades de supervisión competentes de los Estados miembros, a fin de proteger a las personas físicas en lo que respecta al tratamiento de sus datos personales, ejerzan sus poderes en virtud del artículo 58 del Reglamento (UE) 2016/679 en relación con las transferencias de datos que pertenecen al ámbito de aplicación establecido en el artículo 1, el Estado miembro en cuestión informará sin demora a la Comisión.

Artículo 3

1. La Comisión realizará un seguimiento continuo de la aplicación del marco jurídico en el que se basa la presente Decisión, incluidas las condiciones en que se realizan las transferencias ulteriores, se ejercen los derechos individuales y las autoridades públicas del Reino Unido tienen acceso a los datos transferidos sobre la base de la presente Decisión, a fin de evaluar si el Reino Unido sigue garantizando un nivel adecuado de protección a tenor del artículo 1.

2. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que la ICO, o cualquier otra autoridad competente del Reino Unido, no garantice el cumplimiento del marco jurídico en el que se basa la presente Decisión.

3. Los Estados miembros y la Comisión se informarán recíprocamente de cualquier indicio de que las injerencias de las autoridades públicas del Reino Unido en el derecho de las personas a la protección de sus datos personales van más allá de lo estrictamente necesario, o de que no existe una tutela judicial efectiva frente a tales injerencias.

4. Siempre que la Comisión tenga indicios de que ya no se garantiza un nivel adecuado de protección, informará a las autoridades competentes del Reino Unido y podrá suspender, derogar o modificar la presente Decisión.

([509]) Dictamen 14/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con el Reglamento (UE) 2016/679 sobre el nivel de protección adecuado de los datos personales en el Reino Unido; disponible en el siguiente enlace: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. La Comisión podrá suspender, derogar o modificar la presente Decisión cuando la falta de cooperación del Gobierno del Reino Unido le impida determinar si la constatación formulada en el artículo 1, apartado 1, se ve afectada.

Artículo 4

La presente Decisión tendrá validez hasta el 27 de junio de 2025, salvo que se prorrogue de conformidad con el procedimiento indicado en el artículo 93, apartado 2, del Reglamento (UE) 2016/679.

Artículo 5

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 28 de junio de 2021.

Por la Comisión
Didier REYNDERS
Miembro de la Comisión