DECISIÓN DE EJECUCIÓN (UE) 2021/1773 DE LA COMISIÓN

de 28 de junio de 2021

con arreglo a la Directiva (UE) 2016/680 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) 4801]

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo ([1]), y en particular su artículo 36, apartado 3,

Considerando lo siguiente:

1. **INTRODUCCIÓN**

(1) La Directiva (UE) 2016/680 establece las normas para la transferencia de datos personales por parte de las autoridades competentes de la Unión Europea (UE) a terceros países y organizaciones internacionales en la medida en que tales transferencias entren dentro de su ámbito de aplicación. Las normas relativas a las transferencias internacionales de datos por parte de las autoridades competentes se establecen en el capítulo V de la Directiva (UE) 2016/680, en concreto en sus artículos 35 a 40. Si bien el flujo de datos personales hacia y desde países no pertenecientes a la UE es esencial para una cooperación eficaz en materia policial, debe garantizarse que el nivel de protección concedido a los datos personales en la Unión no se ve menoscabado por dichas transferencias ([2]).

(2) A tenor del artículo 36, apartado 3, de la Directiva (UE) 2016/680, 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, pueden realizarse transferencias de datos personales a un tercer país sin necesidad de obtener ninguna autorización adicional (salvo cuando otro Estado miembro del que se obtuvieron los datos tenga que dar su consentimiento para la transferencia), como se establece en el artículo 35, apartado 1, y en el considerando 66, de la Directiva (UE) 2016/680.

(3) Como se precisa en el artículo 36, apartado 2, de la Directiva (UE) 2016/680, la adopción de una decisión de adecuación debe basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país. 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 67 de la Directiva (UE) 2016/680]. La norma con la que se evalúa el nivel de protección «esencialmente equivalente» es la que establece la legislación de la Unión Europea, en concreto la Directiva (UE) 2016/680, 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 ([4]).

(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, el nivel de protección exigido a través del contenido de los derechos de privacidad y de su ejecución, supervisión y cumplimiento efectivos ([7]).

([1]) DO L 119 de 4.5.2016, p. 89.

([2]) Véase el considerando 64 de la Directiva (UE) 2016/680.

([3]) Véase, más recientemente, el asunto C-311/18, *Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems*, ECLI:EU:C:2020:559.

([4]) Véanse las recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal, adoptadas en febrero de 2021, disponibles en el siguiente enlace: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_es.

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

([6]) *Schrems*, apartado 74.

([7]) 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 y 7 [COM(2017) 7], disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=ES.

(5) La Comisión ha analizado detenidamente la legislación y la práctica pertinentes del Reino Unido. A tenor de sus conclusiones, que se exponen a continuación, la Comisión concluye que el Reino Unido garantiza un nivel adecuado de protección de los datos personales transferidos por parte de las autoridades competentes de la Unión, que entran en el ámbito de aplicación de la Directiva (UE) 2016/680, a las autoridades competentes en el Reino Unido dentro del ámbito de aplicación de la parte 3 de la *Data Protection Act* (Ley de protección de datos) de 2018 (DPA de 2018) ([8]).

(6) La presente Decisión tiene como efecto que dichas transferencias puedan realizarse sin necesidad de obtener otro tipo de autorización por un período de cuatro años, sujeto a una posible renovación, y sin perjuicio de las condiciones establecidas en el artículo 35 de la Directiva (UE) 2016/680.

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

2.1. Marco constitucional

(7) El Reino Unido es una democracia parlamentaria. 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 (Cámara de los Comunes y Cámara de los Lores), que son responsables de escrutar al Gobierno y debatir y aprobar las leyes. 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 determinados asuntos internos. Si bien la protección de datos es un asunto reservado al Parlamento británico, 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 funciones policiales (actividades que realizan las autoridades policiales) de Escocia e Irlanda del Norte, se delegan en el Parlamento de Escocia y la Asamblea de Irlanda del Norte respectivamente ([9]).

(8) Si bien el Reino Unido no tiene una constitución codificada, en el sentido de un documento constitutivo afianzado, sus principios constitucionales han surgido con el tiempo y proceden, en particular, de la jurisprudencia y del consenso. Se ha 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 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]).

(9) La *Human Rights Act* de 1998 incorpora los derechos recogidos en el Convenio Europeo de Derechos Humanos al 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 a 18 del Convenio. Esto incluye el derecho al respeto a la vida privada y familiar que, a su vez, incluye el derecho a la protección de los datos, así como el derecho a un proceso equitativo ([11]). En concreto, de acuerdo con el artículo 8 del Convenio Europeo de Derechos Humanos, no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

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

([9]) Sección F del *UK Explanatory Framework for Adequacy Discussions: Law enforcement* («Marco explicativo del Reino Unido para el debate sobre la adecuación: fuerzas y cuerpos de seguridad», documento en inglés), disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([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* de 1984, que fue reemplazada por la *Data Protection Act* 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 actualmente 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).

(10) En virtud de la *Human Rights Act* de 1998, cualquier acción de las autoridades públicas debe ser compatible con uno de los derechos garantizados por el Convenio ([12]). Además, el Derecho primario y el subordinado deben interpretarse y aplicarse de manera compatible con tales derechos ([13]). Cualquier persona, en la medida en que considere que las autoridades públicas han 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 y, después de agotar los recursos nacionales, puede obtener una reparación ante el Tribunal Europeo de Derechos Humanos por violaciones de los derechos reconocidos por el Convenio Europeo de Derechos Humanos.

2.2. **Marco de protección de datos del Reino Unido**

(11) 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 de protección de datos personales del Reino Unido que regía el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y la prevención frente a las amenazas para la seguridad pública, consistía en las partes pertinentes de la *Data Protection Act* de 2018, que incorporó la Directiva (UE) 2016/680.

(12) 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 ([15]), que incorpora la legislación de la Unión directamente aplicable al Derecho del Reino Unido y dispone que la denominada «legislación nacional derivada de la UE» siguiera teniendo efecto una vez finalizado el período transitorio. La parte 3 de la DPA de 2018 ([16]), que incorporó la Directiva (UE) 2016/680, constituye la «legislación nacional derivada de la UE» según la *European Union (Withdrawal) Act*. De acuerdo con la *European Union (Withdrawal) Act*, los tribunales del Reino Unido debían interpretar la «legislación nacional derivada de la UE» no modificada 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) ([17]).

(13) En virtud de la *European Union (Withdrawal) Act*, los secretarios de Estado 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 Unión. La normativa *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] ([18]) ejerció esta facultad. Esta normativa modifica la legislación en materia de protección de datos del Reino Unido, en particular la DPA de 2018, para adaptarla al contexto nacional ([19]).

([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 («acuerdo de retirada»), disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=ES.

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

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

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

([18]) La normativa *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations* de 2019 está disponible 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.

([19]) Las *DPPEC Regulations* realizan una serie de modificaciones de la parte 3 de la DPA de 2018. Muchas de ellas suponen cambios técnicos, como la eliminación de referencias a los «Estados miembros» o a la «Directiva sobre protección de datos en el ámbito penal» [véase, por ejemplo, la sección 48, apartado 8, o la sección 73, apartado 5, letra a), de la DPA de 2018 donde se indica «domestic law» (Derecho interno)], de modo que la parte 3 de la DPA tenga una aplicación eficaz como Derecho interno una vez finalizado el período transitorio. En algunos casos, se requirieron otro tipo de cambios; 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 74A de la DPA de 2018), esto es, el secretario de Estado en lugar de la Comisión Europea.

(14) Por tanto, las normas jurídicas sobre el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención en el Reino Unido tras el período transitorio en virtud del acuerdo de retirada seguirán siendo las normas establecidas en las partes pertinentes de la DPA de 2018, pero en su forma modificada por la normativa *DPPEC Regulations*, en particular en la parte 3 de dicha Ley. El Reglamento General de Protección de Datos del Reino Unido (RGPD del Reino Unido) no se aplica a este tipo de tratamiento.

(15) La parte 3 de la DPA de 2018 establece las normas para el tratamiento de datos personales a efectos de control de la aplicación del Derecho penal, en particular los principios de protección de datos, los fundamentos jurídicos del tratamiento (licitud), los derechos de los interesados, las obligaciones de las autoridades competentes (como responsables del tratamiento) y las restricciones para las transferencias ulteriores. Al mismo tiempo, en las partes 5 y 6 de la DPA de 2018 se proporcionan las normas aplicables sobre supervisión, ejecución y reparación aplicables al ámbito penal.

(16) Por otro lado, a la luz del importante papel que desempeñan las autoridades policiales en el sector del ámbito penal, deben tenerse en cuenta las normas que rigen las funciones policiales. Las funciones policiales están descentralizadas, es decir, se recogen en leyes diferentes que, sin embargo, son a menudo similares en su contenido y regulan las funciones policiales en a) Inglaterra y Gales, b) Escocia e c) Irlanda del Norte ([20]). Además, varios tipos de documentos de orientación ofrecen aclaraciones adicionales sobre cómo deben utilizarse las competencias policiales. Hay tres formas principales de orientación policial: 1) orientación estatutaria emitida en virtud de la legislación, como el *Code of Ethics* ([21]) y el *Code of Practice on the Management of Police Information* (Código de práctica MoPI) ([22]), emitidos en virtud de la *Police Act* (Ley de las fuerzas policiales) de 1996 ([23]), o los códigos PACE ([24]) emitidos en virtud de la *Police and Criminal Evidence Act* (Ley de pruebas policiales y penales) ([25]), 2) *Authorised Professional Practice on the Management of Police Information* (Guía APP sobre la gestión de la información policial) ([26]), emitida por el College of Policing, y 3) directrices operativas (publicadas por las propias fuerzas policiales). El National Police Chiefs Council (un organismo de coordinación de todas las autoridades policiales del Reino Unido) publica una guía operativa que todas las autoridades policiales han respaldado y que, por tanto, es de aplicación a escala nacional ([27]). El objetivo de esta guía es garantizar la coherencia entre las fuerzas policiales en cuanto a la forma en que se gestiona la información ([28]).

(17) El Código de práctica MoPI lo emitió el secretario de Estado en 2005, haciendo uso de los poderes previstos en la sección 39A de la *Police Act* de 1996 ([29]). Todo código de práctica emitido con arreglo a la *Police Act* debe tener la aprobación del secretario de Estado y está sujeto a consulta con la National Crime Agency antes de su presentación ante el Parlamento. La sección 39A, apartado 7, de la *Police Act* requiere que las autoridades policiales tengan

([20]) Para una explicación detallada sobre las autoridades policiales y sus competencias en el Reino Unido, véase: Sección F del *UK Explanatory Framework for Adequacy Discussions*: *Law Enforcement* (véase la nota a pie de página 9).

([21]) *Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales* («Código de práctica para los principios y normas de conducta profesional para las fuerzas policiales de Inglaterra y Gales», documento en inglés), disponible en el siguiente enlace: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; *Police Service Northern Ireland Code of Ethic* («Código de ética del servicio de policía de Irlanda del Norte», documento en inglés), disponible en el siguiente enlace: https://www.nipolicingboard.org.uk/psni-code-ethics; *Code of Ethic for policing in Scotland* («Código de ética para la policía en Escocia», documento en inglés), disponible en el siguiente enlace: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) *Code of Practice on the Management of Police Information* («Código de práctica sobre la gestión de la información policial», disponible en el siguiente enlace: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) *Police Act* de 1996, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Códigos de práctica en virtud de la *Police and Criminal Evidence Act* de 1984, disponibles en el siguiente enlace: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) *Police and Criminal Evidence Act* 1984, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) *Authorised Professional Practice on the Management of Police Information* («Práctica profesional autorizada sobre la gestión de la información policial», documento en inglés), disponible en el siguiente enlace: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) *Data Protection Manual for Police Data Protection Professionals* («Manual de protección de datos para profesionales de las autoridades policiales en el ámbito de la protección de datos», documento en inglés), disponible en el siguiente enlace: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Por ejemplo, el Código de práctica MoPI (véase la nota a pie de página 22) se aplica a la conservación de la información policial operativa (véase el considerando 47 de la presente Decisión).

([29]) Según la información facilitada por las autoridades del Reino Unido, durante el período de las conversaciones en materia de adecuación, el College of Policing estaba redactando un código de práctica para la gestión de la información y los registros, para reemplazar al MoPI. El proyecto de código se publicó para consulta pública el 25 de enero de 2021, y está disponible en el siguiente enlace: https://www.college.police.uk/article/information-records-management-consultation.

debidamente en cuenta los códigos emitidos en virtud de la Ley, por lo que se espera que las autoridades policiales cumplan esta disposición ([30]). Además, las orientaciones no reglamentarias (como la Guía APP sobre la gestión de la información policial) siempre deben ser coherentes con el Código de práctica MoPI, que prevalece sobre ellas ([31]). En cualquier caso, si bien puede haber ciertas situaciones operativas en las que los agentes de policía deban desviarse de esta guía, aún deben cumplir con los requisitos de la parte 3 de la DPA de 2018 ([32]).

(18) La Oficina del Comisionado de Información del Reino Unido (ICO, por sus siglas en inglés) ([33]) proporciona una guía sobre la legislación de protección de datos del Reino Unido para el tratamiento en el ámbito penal (para más información sobre la ICO, véanse los considerandos 93 a 109). A pesar de no ser jurídicamente vinculante, en un asunto judicial, los tribunales estarían obligados a tener en consideración cualquier incumplimiento de la guía, ya que tiene un peso interpretativo y demuestra cómo interpreta y aplica la ICO la legislación de protección de datos en la práctica ([34]).

(19) Por último, como se indica en los considerandos 8 a 10, los organismos del Reino Unido encargados de garantizar el cumplimiento de la ley deben asegurar el cumplimiento del Convenio Europeo de Derechos Humanos y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

(20) En su estructura y componentes principales, el marco jurídico que rige el tratamiento de datos por parte de las autoridades del Reino Unido encargadas de garantizar el cumplimiento del Derecho penal 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**

(21) El ámbito de aplicación material de la parte 3 de la DPA de 2018 coincide con el ámbito de la Directiva (UE) 2016/680, como se explica en el artículo 2, apartado 2, de la DPA. La parte 3 se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, por parte de una autoridad competente.

(22) Además, para entrar en el ámbito de aplicación de la parte 3, el responsable del tratamiento debe ser una «autoridad competente» y el tratamiento debe llevarse a cabo con un «fin de aplicación de la ley». Por lo tanto, el régimen de protección de datos que se analiza en la presente Decisión se aplica a todas las actividades de aplicación de estas autoridades competentes.

(23) 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. 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 (por ejemplo, el Commissioner for Her Majesty's Revenue

([30]) En el asunto *R v the Commission of Police of the Metropolis* [2014] EWCA Civ 585, se confirmó la condición jurídica del Código de práctica MoPI y el Lord Justice, Sir John Laws, declaró que el Metropolitan Police Commissioner está obligado a tener en cuenta el Código de práctica MoPI y la Guía APP sobre la gestión de la información policial a tenor de la sección 39A de la *Police Act* de 1996.

([31]) Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (Cuerpo de Inspectores de la Policía y los Servicios de Bomberos y Salvamento de Su Majestad) somete a control a las autoridades policiales en cuanto a su cumplimiento del Código de práctica MoPI.

([32]) A este respecto, véase la posición del College of Policing sobre el cumplimiento de la Guía APP sobre la gestión de la información policial en relación con todos los elementos de las funciones policiales, que explica que «La Guía APP está autorizada por el organismo profesional para las funciones policiales (el College of Policing) como fuente oficial de la práctica profesional dentro de las fuerzas de policía. Los agentes y el personal de policía deben respetar la Guía APP en el desempeño de sus responsabilidades. No obstante, puede haber circunstancias en las que exista una razón operativa legítima para que un cuerpo de policía se desvíe de la Guía APP, siempre que exista una justificación lógica para hacerlo. Correspondería a dicho cuerpo de policía asumir la responsabilidad de cualquier riesgo local y nacional de operar fuera de las directrices acordadas a escala nacional, y si se produce un incidente o una investigación como consecuencia de ello (por ejemplo, a través de la Independent Office of Police Conduct), el cuerpo policial es responsable de cualquier riesgo», disponible en el siguiente enlace: https://www.app.college.police.uk/faq-page/.

([33]) *Guide to Law Enforcement Processing* («Guía para el tratamiento con fines de aplicación de la ley», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Véase el asunto *Bridges v the Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) en el que, aunque señaló la naturaleza no estatutaria de la guía de la ICO, el Tribunal Superior declaró que «[c]uando se valora si un responsable del tratamiento ha cumplido o no con la obligación que establece la sección 64 (de realizar una evaluación de impacto relativa a la protección de datos en relación con el tratamiento de alto riesgo), un tribunal tendrá en cuenta las orientaciones emitidas por la ICO con respecto a las evaluaciones de impacto relativas a la protección de datos».

and Customs, la Welsh Revenue Authority, la Competition and Markets Authority, Her Majesty's Land Register o la National Crime Agency), 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 ([35]). La parte 3 de la DPA de 2018 también se aplica a los tribunales cuando ejercen sus funciones jurisdiccionales, excepto por la parte relacionada con los derechos del interesado y la supervisión de la ICO ([36]). La lista de autoridades competentes que proporciona el anexo 7 no es definitiva y el secretario de Estado puede actualizarla mediante reglamentos que tengan en cuenta los cambios en la organización de los cargos públicos ([37]).

(24) El tratamiento en cuestión también debe tener un «fin de aplicación de la ley», en el sentido de la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública ([38]). El tratamiento por parte de una autoridad competente no se rige por la parte 3 de la DPA de 2018 cuando no se produce con fines de aplicación de la ley. Este sería el caso, por ejemplo, cuando la Competition and Markets Authority (Autoridad de Competencia y Mercados) investiga casos que no están tipificados como delito (por ejemplo, fusiones entre empresas). En este caso, se aplicaría el RGPD del Reino Unido, junto con la parte 2 de la DPA de 2018, ya que el tratamiento de datos personales por parte de las autoridades competentes se realiza con fines distintos a los de aplicación de la ley. Para determinar qué régimen de protección de datos aplica (parte 3 o parte 2, de la DPA de 2018) al tratamiento de datos personales en cuestión, la autoridad competente, esto es, el responsable del tratamiento, debe valorar si el «fin principal» de dicho tratamiento es uno de los fines de aplicación de la ley previstos en la DPA de 2018.

(25) En lo que respecta al ámbito de aplicación territorial de la parte 3 de la DPA de 2018, la sección 207, apartado 2, establece que la DPA se aplica al tratamiento de datos personales en el contexto de las actividades de una persona que tiene un establecimiento en todo el territorio del Reino Unido. Esto incluye a las autoridades públicas de los territorios de Inglaterra, Gales, Escocia e Irlanda del Norte que se encuentran dentro del ámbito de aplicación material de la parte 3 de la DPA de 2018 ([39]).

2.3.1. *Definición de «datos personales» y de «tratamiento»*

(26) En la sección 3 de la DPA de 2018 se definen los conceptos fundamentales de «datos personales» y de «tratamiento», que se aplican a lo largo de todo el texto de la Ley. Las definiciones siguen de cerca las definiciones correspondientes establecidas en el artículo 3 de la Directiva (UE) 2016/680. Con arreglo a la DPA de 2018, «datos personales» significa toda información sobre una persona física identificada o identificable ([40]). En virtud de la sección 3, apartado 3, de la DPA de 2018 un individuo es identificable cuando es posible identificarlo, directa o indirectamente, a partir de la información, en particular mediante un identificador, como por ejemplo un nombre o un número de identificación, o por referencia a uno o más factores propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. La noción de «tratamiento» se define como una operación o conjunto de operaciones realizadas sobre información, o sobre conjuntos de información, como a) recogida, registro, organización, estructuración o conservación; b) adaptación o modificación; c) extracción, consulta o utilización; d) comunicación por transmisión, difusión o cualquier otra forma de habilitación; e) cotejo o combinación; o f) limitación, supresión o destrucción. Además, la DPA de 2018 define el «tratamiento sensible» como «a) el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical; b) el tratamiento de datos genéticos o biométricos con el objetivo de identificar de manera unívoca a una persona; c) el tratamiento de datos relativos a la salud; d) el tratamiento de datos relativos a la vida sexual o la orientación sexual de una persona» ([41]). A este respecto, la sección 205 de la DPA de 2018 establece la definición de «datos biométricos» ([42]), «datos relativos a la salud» ([43]) y «datos genéticos» ([44]).

([35]) 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.

([36]) Sección 43, apartado 3, de la DPA de 2018.

([37]) Sección 30, apartado 3, de la DPA de 2018. 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 (véase la sección 30, apartado 2, de la DPA de 2018), por lo que la parte 3 de dicha Ley no tiene aplicación en ninguna de sus actividades. Estas actividades corresponden al ámbito de la parte 4 de la DPA de 2018.

([38]) Sección 31 de la DPA de 2018.

([39]) Esto significa que la DPA de 2018 y, por lo tanto, esta decisión no se aplican a las dependencias de la Corona y los territorios de ultramar del Reino Unido, como, por ejemplo, las Islas Malvinas y el territorio de Gibraltar.

([40]) Los datos personales relativos a las personas fallecidas no entran en el ámbito de aplicación de la DPA de 2018.

([41]) Sección 35, apartado 8, de la DPA de 2018.

([42]) «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.

([43]) «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.

([44]) «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.

(27) La sección 32 de la DPA de 2018 aclara las definiciones de «responsable del tratamiento» y «encargado del tratamiento» en el contexto del tratamiento de datos personales con fines de aplicación de la ley siguiendo de cerca las definiciones equivalentes de la Directiva (UE) 2016/680. «Responsable del tratamiento» es la autoridad competente que determina los fines y medios del tratamiento de datos personales. Cuando la ley requiere el tratamiento, el responsable del tratamiento es la autoridad competente a la que la ley impone dicha obligación. El «encargado del tratamiento» es la persona que trata datos personales por cuenta del responsable del tratamiento (distinto a una persona que es un empleado del responsable).

2.4. **Garantías, derechos y obligaciones**

2.4.1. *Licitud y lealtad del tratamiento*

(28) A tenor de la sección 35 de la DPA de 2018, el tratamiento de datos personales debe ser lícito y leal, de una forma similar a lo que estipula el artículo 4, apartado 1, letra a), de la Directiva (UE) 2016/680. En virtud de la sección 35, apartado 2, 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, o el tratamiento es necesario para la realización de una tarea que una autoridad competente lleva a cabo a tal efecto.

2.4.1.1. Tratamiento de acuerdo con la ley

(29) De manera similar a lo que establece el artículo 8 de la Directiva (UE) 2016/680, para garantizar la licitud de un tratamiento contemplado en la parte 3 de la DPA de 2018, dicho tratamiento debe estar «basado en la ley». Tratamiento «lícito» significa autorizado por la ley, por el *common law* o por prerrogativas reales ([45]).

(30) Los poderes de las autoridades competentes se rigen, en general, por estatutos, lo que significa que sus funciones y poderes se establecen claramente en las legislaciones aprobadas por el Parlamento ([46]). En determinados casos, las autoridades policiales, así como otras autoridades competentes enumeradas en el anexo 7 de la DPA de 2018, puede apoyarse en el *common law* para tratar los datos ([47]). El *common law* se ha construido a través de sentencias doctrinales establecidas mediante decisiones de los tribunales. El *common law* es pertinente en el contexto de los poderes de que disponen las autoridades policiales que derivan de esta fuente de derecho, y cuyo deber fundamental es proteger al público mediante la detección y prevención de la delincuencia ([48]). Sin embargo, las

([45]) Notas explicativas a la DPA de 2018, apartado 181, disponibles en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Por ejemplo, la National Crime Agency deriva sus poderes de la *Crime and Courts Act* (Ley de delincuencia y tribunales) de 2013, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2013/22/contents. De manera similar, los poderes de la Food Standards Agency (Agencia de Normas Alimentarias) se recogen en la *Food Standards Act* (Ley de normas alimentarias) de 1999, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1999/28/contents. Otros ejemplos incluyen la *Prosecution of Offenders Act* (Ley de enjuiciamiento de delincuentes) de 1985, que creó el Crown Prosecution Service (ministerio fiscal del Reino Unido) (véase https://www.legislation.gov.uk/ukpga/1985/23/contents); la *Commissioners for Revenue and Customs Act* (Ley de comisionados de ingresos y aduanas) de 2005, que estableció Her Majesty's Revenue and Customs (véase https://www.legislation.gov.uk/ukpga/2005/11/contents); la *Criminal Procedure (Scotland) Act* (Ley de proceso penal de Escocia) de 1995, que creó la Scottish Criminal Cases Review Commission (Comisión de Revisión de Casos Penales de Escocia) (véase https://www.legislation.gov.uk/ukpga/1995/46/contents); la *Justice (Northern Ireland) Act* (Ley de justicia de Irlanda del Norte) de 2002, que estableció el ministerio fiscal de Irlanda del Norte (véase https://www.legislation.gov.uk/ukpga/2002/26/contents) y la Serious Fraud Office (Oficina de Delitos Graves), que se creó y obtuvo sus poderes en virtud de la *Criminal Justice Act* (Ley de justicia penal) de 1987 (véase https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Por ejemplo, según la información facilitada por las autoridades del Reino Unido, dentro del Crown Office and Procurator Fiscal Service, responsable de procesar los casos en Escocia, el Lord Advocate, que es el responsable del sistema de enjuiciamiento de delitos en Escocia, deriva sus poderes para investigar muertes y perseguir delitos del *common law*, mientras que algunas de sus funciones están establecidas en estatutos. Además, la Corona y, por extensión, varios departamentos gubernamentales y ministeriales, también derivan sus poderes de una combinación de legislación, *common law* y prerrogativas leales (estos son poderes del *common law* conferidos a la Corona pero que ejercen los secretarios de Estado).

([48]) Sección F del *UK Explanatory Framework for Adequacy Discussions*: *Law Enforcement*, página 8 (véase la nota a pie de página 9).

autoridades policiales tienen tanto poderes legislativos ([49]) como poderes del *common law* para ejercer ese deber. Siempre que las autoridades policiales tengan un deber estatutario, este sustituye cualquier poder del *common law* ([50]).

(31) Los tribunales han reconocido que la amplitud de los poderes y obligaciones de las autoridades de policía recogidos en el *common law* incluyen «todas las medidas que les parezcan necesarias para mantener la paz, prevenir la delincuencia o proteger la propiedad de daños criminales» ([51]). Los poderes del *common law* no son poderes incondicionales. Están sujetos a una serie de limitaciones, en particular límites que establecen los tribunales ([52]) y la legislación, en concreto la *Human Rights Act* (Ley de derechos humanos) de 1998 y la *Equality Act* (Ley de igualdad) de 2010 ([53]). Además, para las autoridades competentes que tratan datos en virtud de la parte 3 de la DPA de 2018, esto incluye el ejercicio de los poderes recogidos en el *common law* de una forma coherente con los requisitos establecidos en la DPA de 2018 ([54]). Por otro lado, la decisión de realizar cualquier tipo de tratamiento de datos debe tener en cuenta los requisitos de las directrices aplicables, como el Código de práctica MoPI, así como la orientación específica para uno de los territorios del Reino Unido ([55]). El gobierno y las autoridades de policía ejecutivas emiten una serie de documentos de orientación para garantizar que los agentes de policía ejercen sus poderes dentro de los límites establecidos por el *common law* o el estatuto pertinente ([56]).

(32) Las prerrogativas reales representan otro componente de la ley y se refieren a ciertos poderes conferidos por la Corona, y ejecutables por parte del poder ejecutivo, que no se basan en estatutos sino que se derivan de la soberanía del monarca ([57]). Existen muy pocos ejemplos de poderes de prerrogativa que sean pertinentes en el ámbito penal. Estos poderes incluyen, por ejemplo, el marco de asistencia judicial mutua que permite el intercambio de datos por parte de un secretario de Estado con terceros países con fines de aplicación de la ley; la facultad de compartir datos

([49]) Las leyes fundamentales que dotan al régimen de los principales poderes policiales (arresto, registros, autorización de detención ininterrumpida, huellas dactilares, toma de muestras íntimas, órdenes judiciales de interceptación, acceso a datos de comunicaciones, etc.) son: i), para Inglaterra y Gales, la *Police and Criminal Evidence Act* de 1984 (PACE), disponible en el siguiente enlace https://www.legislation.gov.uk/ukpga/1984/60/contents [en su versión modificada por la *Protection of Freedoms Act* (Ley de protección de las libertades) de 2012, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2012/9/contents] y la *Investigatory Powers Act* (IPA) (Ley de poderes de investigación) de 2016, disponible en el siguiente enlace https://www.legislation.gov.uk/ukpga/2016/25/contents); ii) para Escocia, la *Criminal Justice (Scotland) Act* de 2016, disponible en el siguiente enlace https://www.legislation.gov.uk/asp/2016/1/contents y la *Criminal Procedure (Scotland) Act* de 1995, disponible en el siguiente enlace https://www.legislation.gov.uk/ukpga/1995/46/contents; y iii) y para Irlanda del Norte, la *Police and Criminal Evidence (Northern Ireland) Order* (Orden sobre pruebas policiales y penales de Irlanda del Norte) de 1989, disponible en el siguiente enlace https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Las autoridades del Reino Unido han explicado que la supremacía de la ley estatutaria se estableció hace mucho tiempo en el Reino Unido, ya en la sentencia *Entick v Carrington* [1765] EWHC KB J98, que reconocía que había límites en el ejercicio de los poderes por parte del poder ejecutivo y estableció el principio de que los poderes recogidos en el *common law* y los poderes de prerrogativa del monarca y el gobierno están subordinados a la ley del país.

([51]) Véase el asunto *Rice v Connolly* [1966] 2 QB 414.

([52]) Véase el asunto *R(Catt) v Association of Chief police Officers* [2015] AC 1065 en el que, en relación con el poder policial para obtener y conservar la información de un individuo (que había cometido un delito), Lord Sumption sostuvo que en virtud del *common law* las autoridades policiales tienen el poder de obtener y conservar información con fines policiales, es decir, en términos generales para el mantenimiento del orden público y la prevención y detección de la delincuencia. Estos poderes, no obstante, no autorizan métodos intrusivos para obtener información, como la entrada en propiedades privadas o actos (distintos del arresto en virtud de los poderes del *common law*) que constituirían una agresión. El juez consideró que, en este caso, los poderes recogidos en el *common law* eran sobradamente suficientes para autorizar la obtención y conservación del tipo de información pública en cuestión sobre estos recursos.

([53]) *Equality Act* (Ley de igualdad) de 2010, disponible en el siguiente enlace https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Para ver un ejemplo de un caso en el que los poderes policiales recogidos en el *common law* se evalúan en el marco de la DPA de 1998, véase la decisión del Tribunal Superior en *Bridges v the Chief Constable of South Wales Police* (véase la nota a pie de página 33). Véanse también los casos *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 y *Richard v BBC* [2018] EWHC 1837 (Ch).

([55]) Véase, por ejemplo, la guía del servicio de policía de Irlanda del Norte sobre la instrucción del servicio de gestión de registros, disponible en el siguiente enlace: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) La Cámara de los Comunes ha publicado un documento de orientación que establece los poderes clave del *common law* y los poderes estatutarios de las autoridades policiales en Inglaterra y Gales (véase https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Según este documento, si bien los poderes de mantenimiento de «la paz de la Corona» son poderes derivados del *common law*, así como «el uso de la fuerza», los «poderes de detención y registro» siempre se derivan del estatuto. Además, el Gobierno escocés ofrece información en su sitio web sobre los poderes policiales de arresto e interrupción de búsquedas (véase https://www.gov.scot/policies/police/police-powers/).

([57]) De acuerdo con la información facilitada por las autoridades del Reino Unido, los poderes de prerrogativa que ejerce el Gobierno incluyen, por ejemplo, la elaboración y ratificación de tratados, la conducción de la diplomacia y el uso de las fuerzas armadas dentro del Reino Unido para el mantenimiento la paz en apoyo de las fuerzas policiales.

de esta manera no siempre está contemplada en la ley ([58]). Las prerrogativas reales están sujetas a los principios del *common law* ([59]) y subordinadas al estatuto, por lo que están sujetas a los límites que establecen la *Human Rights Act* de 1998 y la DPA de 2018 ([60]).

(33) De manera similar al artículo 8 de la Directiva (UE) 2016/680, el régimen del Reino Unido requiere que, para cumplir con el principio de licitud, las autoridades competentes se aseguren de que, cuando el tratamiento está basado en la ley, también sea «necesario» para llevar a cabo la tarea ejecutada en el ámbito penal. La ICO ofrece orientación en este sentido, aclarando que «debe ser una forma específica y proporcionada de lograr el fin. El fundamento jurídico no se aplicará si puede lograrse razonablemente el fin por otros medios menos intrusivos. No basta con declarar que el tratamiento es necesario porque ha escogido gestionar su negocio de una manera particular. La cuestión es si el tratamiento es necesario para el fin indicado» ([61]).

2.4.1.2. Tratamiento sobre la base del «consentimiento» del interesado

(34) Como se menciona en el considerando 28, la sección 35, apartado 2, de la DPA de 2018 prevé la posibilidad de tratar los datos personales sobre la base del «consentimiento» del interesado.

(35) Sin embargo, el consentimiento no parece ser un fundamento jurídico pertinente para las operaciones de tratamiento contempladas en el ámbito de aplicación de la presente Decisión. De hecho, las operaciones de tratamiento contempladas en la presente Decisión se referirán siempre a datos que ha transferido una autoridad competente de un Estado miembro a una autoridad competente del Reino Unido en virtud de la Directiva (UE) 2016/680. Por tanto, normalmente no implicarán el tipo de interacción directa (recogida) entre una autoridad pública y los interesados que puede basarse en el consentimiento con arreglo a la sección 35, apartado 2, letra a), de la DPA de 2018.

(36) Por tanto, si bien la confianza en el consentimiento no se considera pertinente para la evaluación realizada en virtud de esta Decisión, vale la pena señalar, en aras de la exhaustividad, que en un contexto de aplicación de la ley, el tratamiento nunca se basa únicamente en el consentimiento, dado que una autoridad competente debe estar siempre investida de un poder que le permita tratar los datos ([62]). En concreto, y de manera similar a lo permitido por la Directiva (UE) 2016/680 ([63]), esto significa que el consentimiento sirve como condición adicional para permitir ciertas operaciones limitadas y específicas de tratamiento que, de otro modo, no podrían llevarse a cabo como, por ejemplo, la recogida y el tratamiento de una muestra de ADN de un individuo que no es sospechoso. En este caso, el tratamiento no se llevaría a cabo si no se concede el consentimiento o si se retira ([64]).

([58]) A este respecto, véase la evaluación del régimen de transferencias ulteriores del Reino Unido en los considerados 74 a 87.

([59]) Véase el asunto *Bancoult v Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, en virtud del cual los tribunales sostuvieron que el poder de prerrogativa de dictar decretos ministeriales también estaba sujeto a las causas ordinarias de control jurisdiccional.

([60]) Véase el asunto *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508, en el que el tribunal sostuvo que los poderes de prerrogativa no pueden emplearse cuando haya poderes estatutarios que los sustituyan; el asunto *Laker Airways Ltd v Department of Trade* 1977] QB 643], en el que el tribunal determinó que los poderes de prerrogativa no pueden emplearse para anular la ley estatutaria; el asunto *R v Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, en el que el tribunal sostuvo que los poderes de prerrogativa no pueden emplearse cuando entren en conflicto con la legislación promulgada, aun cuando dicha legislación promulgada no esté aún en vigor; y el asunto *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5, en el que el tribunal confirmó la capacidad de la ley para ajustar y abolir los poderes de prerrogativa. Para un resumen general de la relación entre las prerrogativas reales y el estatuto o los poderes del *common law*, consúltese el documento de orientación de la Cámara de los Comunes, disponible en el siguiente enlace: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) *Guide to Law Enforcement Processing. «What is the first principle about?»* («Guía para el tratamiento con fines de aplicación de la ley. ¿De qué trata el primer principio?», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Esto se desprende del lenguaje de la disposición pertinente de la DPA de 2018, a tenor de la cual el tratamiento de datos personales para cualquiera de los fines de aplicación de la ley solo es lícito si, y en la medida en que, «se base en la ley» y a) el interesado haya dado su consentimiento para el tratamiento con ese fin, o b) el tratamiento sea necesario para el desempeño de una tarea realizada por una autoridad competente con ese fin específico.

([63]) Véanse los considerandos 35 a 37 de la Directiva (UE) 2016/680.

([64]) Las autoridades del Reino Unido explicaron que un ejemplo de cuándo el consentimiento puede ser una base adecuada para el tratamiento sería cuando las autoridades policiales obtienen una muestra de ADN en relación con una persona desaparecida para compararla con un cuerpo, en casos en los que se encuentra un cuerpo. En estas circunstancias, no sería adecuado que las autoridades policiales obligaran al interesado a proporcionar una muestra; en lugar de ello, solicitarían su consentimiento, que se da libremente y puede retirarse en cualquier momento. Si se retirara el consentimiento, los datos ya no podrían tratarse, a menos que se estableciera un nuevo fundamento jurídico para seguir tratando la muestra (por ejemplo, si el interesado se convierte en sospechoso). Otro ejemplo podría surgir cuando una fuerza policial investiga un delito en el que una víctima (puede ser víctima de un robo, un delito sexual, violencia doméstica, familiar de una víctima de homicidio u otra víctima de un delito) podría beneficiarse de una remisión a Victim Support (una organización benéfica independiente que se dedica a apoyar a las personas afectadas por delitos e incidentes traumáticos). En estas circunstancias, las autoridades policiales solo compartirán cierta información personal (como el nombre y los datos de contacto) con Victim Support si cuentan con el consentimiento de la víctima.

(37) En casos que requieren el consentimiento del interesado, este debe ser inequívoco e implicar una clara acción afirmativa ([65]). Las fuerzas policiales deben disponer de una declaración de confidencialidad que incluya, entre otras cosas, la información necesaria relacionada con el uso válido del consentimiento. Además, algunas de ellas publican material adicional sobre cómo cumplen con la legislación de protección de datos, que incluye cómo y cuándo se utilizaría el consentimiento como fundamento jurídico ([66]).

2.4.1.3. Tratamiento sensible

(38) Deben preverse garantías específicas cuando se estén tratando «categorías especiales» de datos. En este sentido, de forma similar a lo que establece el artículo 10 de la Directiva (UE) 2016/680, la parte 3 de la DPA de 2018 dispone garantías más estrictas para el denominado «tratamiento sensible» ([67]).

(39) Según la sección 35, apartado 3, de la DPA de 1998, las autoridades competentes pueden tratar datos sensibles con fines de aplicación de la ley únicamente en dos casos: 1) el interesado ha dado su consentimiento para el tratamiento con fines de aplicación de la ley y, en el momento en que se lleva a cabo el tratamiento, el responsable del tratamiento dispone de un documento reglamentario apropiado ([68]); o 2) el tratamiento es estrictamente necesario para el fin de aplicación de la ley de que se trate y el tratamiento cumple, al menos, una de las condiciones establecidas en el anexo 8 de la DPA de 2018 y, en el momento en que se lleva a cabo el tratamiento, el responsable del tratamiento dispone de un documento reglamentario apropiado ([69]).

(40) Por lo que respecta al primer caso, y como se explica en el considerando 38, la confianza en el consentimiento no se considera pertinente en el tipo de situación de transferencia sujeta a la presente Decisión ([70]).

(41) Cuando el tratamiento de datos sensibles no se basa en el consentimiento, puede realizarse haciendo uso de una de las condiciones enumeradas en el anexo 8 de la DPA de 2018. Estas condiciones se refieren al tratamiento necesario para fines estatutarios; la administración de la justicia; la protección de los intereses vitales del interesado o de otra persona; la protección de los menores y de las personas en situación de riesgo; reclamaciones; actos judiciales;

([65]) No existe una definición específica de «consentimiento» a efectos del tratamiento de datos personales en virtud de la parte 3 de la DPA de 2018. La ICO brindó orientación sobre la noción de «consentimiento» con arreglo a la parte 3 de la DPA de 2018, aclarando que tiene el mismo significado y debe estar en consonancia con la definición proporcionada por el Reglamento (UE) 2016/679, en particular el hecho de que «el consentimiento debe darse de forma libre, específica e informada y debe haber una elección verdadera respecto al consentimiento para el tratamiento de los datos» [*Guide to Law Enforcement Processing*. «*What is the first principle about?*» (véase la nota a pie de página 64) y *Guide to Data Protection on consent* («Guía para la protección de datos respecto al consentimiento», documento en inglés), disponible el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Véase, por ejemplo, la información en el sitio web de la policía de Lincolnshire (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) o el sitio web de la policía de Yorkshire del Oeste (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Sección 35, apartado 8, de la DPA de 2018.

([68]) Sección 35, apartado 4, de la DPA de 2018.

([69]) Sección 35, apartado 5, de la DPA de 2018.

([70]) En aras de la exhaustividad, cabe señalar que cuando el tratamiento se basa en el consentimiento, este debe darse de forma libre, específica e informada y debe haber una elección específica respecto al consentimiento para el tratamiento de los datos. Además, a la hora de realizar el tratamiento sobre la base del consentimiento del interesado, el responsable del tratamiento debe disponer de un «documento reglamentario apropiado». La sección 42 de la DPA de 2018 señala los requisitos que este documento debe cumplir. Deja claro que el documento debe, como mínimo, explicar los procedimientos del responsable del tratamiento para garantizar el cumplimiento de los principios de protección de datos, así como explicar las políticas del responsable en lo que respecta a la conservación y la supresión de datos personales. Con arreglo a la sección 42 de la DPA de 2018, esto significa que el responsable del tratamiento debe presentar un documento que a) explique los procedimientos del responsable del tratamiento para garantizar el cumplimiento de los principios de protección de datos; y b) explicar las políticas del responsable del tratamiento en lo que respecta a la conservación y la supresión de datos personales tratados sobre la base del consentimiento del interesado o aportar una indicación de cuánto tiempo es probable que se conserven dichos datos personales. En particular, el documento reglamentario requiere que el responsable del tratamiento, en el respeto de su deber de registrar las actividades de tratamiento, incluya siempre los elementos mencionados en los puntos a) y b). La ICO publicó un documento de orientación [*Guide to Law Enforcement Processing*. «*Conditions for sensitive processing*» («Guía para el tratamiento en el ámbito de aplicación de la ley: condiciones para el tratamiento sensible», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing] y puede adoptar medidas de ejecución si los responsables del tratamiento no cumplen con estos requisitos. Los tribunales también examinan el documento reglamentario cuando valoran posibles infracciones de la DPA de 2018. Por ejemplo, en el asunto reciente *R (Bridges) v Chief Constable of South Wales Police*, los tribunales revisaron el documento reglamentario del responsable del tratamiento y concluyeron que era adecuado, pero que podría haberse mejorado con un mayor nivel de detalle. Como resultado de ello, la policía de Gales del Sur revisó el documento reglamentario y lo actualizó de acuerdo con la nueva orientación de la ICO (véase la nota a pie de página 33). Además, de conformidad con la sección 42, apartado 3, de la DPA de 2018, el responsable del tratamiento debe revisar periódicamente el documento reglamentario. Por último, como garantía adicional, de conformidad con la sección 42, apartado 4, de la DPA de 2018, el responsable del tratamiento debe mantener un registro ampliado de las actividades de tratamiento, que incluye elementos adicionales en comparación con la obligación general que recae sobre el responsable de mantener registros sobre las actividades de tratamiento, y que se establece en la sección 61 de la DPA de 2018.

prevención del fraude; archivo; cuando el interesado ha hecho manifiestamente públicos los datos personales. Aparte del caso en el que los datos se hacen manifiestamente públicos, todas las condiciones previstas en el anexo 8 están sujetas a la evaluación de la «necesidad estricta». Como aclaró la ICO, «necesidad estricta en este contexto significa que el tratamiento tiene que relacionarse con una necesidad social apremiante, y no se puede lograr razonablemente a través de medios menos intrusivos» ([71]). Además, algunas de las condiciones están también sujetas a restricciones adicionales. Por ejemplo, para poder recurrir a la condición de «fines estatutarios» y a la «condición de salvaguardia» (párrafos primero y cuarto, del anexo 8, de la DPA de 2018) es necesario cumplir una evaluación adicional de interés público esencial. Además, en relación con las condiciones relativas a la protección de los menores (párrafo cuarto, del anexo 8), el interesado también debe tener una edad específica y ser considerado en riesgo. Por otro lado, el responsable del tratamiento solo puede aplicar la condición establecida en el párrafo cuarto, del anexo 8, de la DPA en determinadas circunstancias ([72]). Asimismo, existen restricciones para las condiciones de «actos judiciales» y «prevención del fraude» (párrafos séptimo y octavo del anexo 8, respectivamente). Ambas condiciones aplican exclusivamente a responsables del tratamiento específicos. En el caso de los actos judiciales, solo un tribunal u otra autoridad judicial puede emplear dicha condición, y en el caso de la prevención del fraude tan solo los responsables del tratamiento que son organizaciones de lucha contra el fraude pueden recurrir a esta condición.

(42) Por último, cuando el tratamiento se basa en una de las condiciones enumeradas en el anexo 8 de la DPA de 2018 y de conformidad, respectivamente, con la sección 42 de la DPA de 2018, debe existir un «documento reglamentario apropiado», que explique los procedimientos del responsable del tratamiento para garantizar el cumplimiento de los principios de protección de datos y las políticas del responsable del tratamiento en lo que respecta a la conservación y la supresión de datos personales, y se aplican las obligaciones de registro ampliadas.

2.4.2. *Limitación de la finalidad*

(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. La sección 36 de la DPA de 2018 garantiza este principio de la protección de datos. Esta disposición, de manera similar al artículo 4, apartado 1, letra b), de la Directiva (UE) 2016/680, requiere que a) el fin de aplicación de la ley para el que se recogen los datos personales debe ser determinado, explícito y legítimo, y b) los datos personales así recogidos no deben tratarse de una forma incompatible con el fin para el que se recogieron.

(44) Cuando las autoridades competentes traten datos con fines de aplicación de la ley, esto puede incluir el archivo, la investigación científica o histórica y fines estadísticos ([73]). En estos casos, la DPA de 2018 también aclara que no está permitido el archivo (o el tratamiento con fines de investigación científica o histórica o fines estadísticos) cuando se lleva a cabo de acuerdo con las decisiones adoptadas en relación con un interesado en particular o si es probable que le cause daño o sufrimiento ([74]).

2.4.3. *Exactitud y minimización de los datos*

(45) Los datos deben 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. De manera similar al artículo 4, apartado 1, letras c), d) y e), de la Directiva (UE) 2016/680, estos principios están garantizados en las secciones 37 y 38 de la DPA de 2018. Se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación ([75]) los datos personales

([71]) *Guide to Law Enforcement Processing, «Conditions for sensitive processing»* («Guía para el tratamiento con fines de aplicación de la ley. Condiciones para el tratamiento sensible» documento en inglés) (véase la nota a pie de página 70).

([72]) El tratamiento se realiza sin el consentimiento del interesado cuando: a) el consentimiento para el tratamiento no puede darlo el interesado; b) no puede esperarse razonablemente que el responsable del tratamiento obtenga el consentimiento del interesado para el tratamiento; c) el tratamiento debe realizarse sin el consentimiento del interesado, ya que la obtención del consentimiento del interesado perjudicaría la prestación de la protección a que se refiere el subpárrafo primero, letra a).

([73]) Sección 41, apartado 1, de la DPA de 2018.

([74]) Sección 41, apartado 2, de la DPA de 2018.

([75]) Sección 38, apartado 1, letra b), de la DPA de 2018.

que sean inexactos ([76]) con respecto a los fines de aplicación de la ley para los que son tratados ([77]), y para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros para ninguno de los fines de aplicación de la ley ([78]).

(46) Asimismo, de manera similar al artículo 7 de la Directiva (UE) 2016/680, el régimen de protección de datos del Reino Unido especifica que los datos personales basados en hechos deben, en la medida de lo posible, distinguirse de los datos personales basados en apreciaciones personales ([79]). Cuando sea pertinente, y en la medida de lo posible, debe establecerse una clara distinción entre los datos personales relacionados con las diferentes categorías de interesados, como sospechosos, personas condenadas por una infracción penal, víctimas de una infracción penal y testigos ([80]).

2.4.4. *Limitación de la conservación*

(47) A tenor del artículo 5 de la Directiva (UE) 2016/680, los datos no deben, en principio, conservarse más tiempo del que sea necesario para los fines con los que se tratan. En virtud de la sección 39 de la DPA de 2018, y de manera similar al artículo 5 de la Directiva (UE) 2016/680, está prohibido mantener los datos personales tratados para cualquiera de los fines de aplicación de la ley durante más tiempo del necesario en relación con el fin con el que se tratan. El marco jurídico del Reino Unido requiere que se establezcan límites de tiempo apropiados para la revisión periódica de la necesidad de conservación continuada de datos personales para cualquiera de los fines de aplicación de la ley. En la legislación pertinente y en las orientaciones que rigen las competencias y el funcionamiento de las autoridades policiales se han establecido normas adicionales sobre prácticas relacionadas con la conservación de los datos personales y los plazos aplicables a dicha conservación. Por ejemplo, en Inglaterra y Gales el Código de práctica MoPI del College of Policing, junto con la Guía APP sobre la gestión de la información policial, proporciona un marco para garantizar un proceso consistente de conservación, revisión y eliminación basado en el riesgo para la gestión de la información policial operativa ([81]). Este marco establece expectativas claras en todo el servicio en cuanto a cómo debe crearse, compartirse, utilizarse y gestionarse la información dentro y entre cada una de las fuerzas policiales y con otros organismos ([82]). Se espera que las autoridades policiales respeten el código de práctica, cuyo cumplimiento verifica el Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ([83]).

(48) El servicio de policía de Irlanda del Norte no está obligado por ley a seguir el Código de práctica MoPI. Sin embargo, el marco MoPI que se adaptó en 2011 se complementa con un manual del servicio de policía de Irlanda del Norte ([84]), que establece políticas y procedimientos sobre la forma en que el Código de práctica MoPI se aplica en Irlanda del Norte.

([76]) La sección 205 de la DPA de 2018 define el término «inexactos» como datos personales «incorrectos o engañosos». Las autoridades del Reino Unido han explicado que es típico que los datos relacionados con las investigaciones penales a menudo estén incompletos pero, al margen de eso, pueden ser precisos.

([77]) De acuerdo con el *UK Explanatory Framework for Adequacy Discussions* «esto garantiza que se reconozcan tanto los derechos del interesado como las necesidades operativas de los organismos encargados de garantizar el cumplimiento de la ley. El punto anterior se valoró cuidadosamente durante las etapas de redacción del *Data Protection Bill* (proyecto de ley de protección de datos), ya que pueden existir razones operativas específicas y limitadas por las que no puedan rectificarse los datos. Lo más probable es que esto suceda si los datos personales inexactos en cuestión deben conservarse en su forma original con fines probatorios» [véase la sección F del *UK Explanatory Framework for Adequacy Discussions: Law Enforcement* («Marco explicativo del Reino Unido para el debate sobre la adecuación: fuerzas y cuerpos de seguridad», documento en inglés), página 21, véase la nota a pie de página 9].

([78]) Sección 38, apartado 4, de la DPA de 2018. Además, en virtud de la sección 38, apartado 5, de la DPA de 2018, debe comprobarse la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros. En todas las transmisiones de datos personales se añadirá la información necesaria para que el receptor pueda valorar en qué medida los datos personales son exactos, completos y fiables y en qué medida están actualizados y, si se observara que se hubieran transmitido datos personales incorrectos o se hubieran transmitido ilegalmente, el hecho deberá ponerse en conocimiento del destinatario sin dilación.

([79]) Sección 38, apartado 2, de la DPA de 2018.

([80]) Sección 38, apartado 3, de la DPA de 2018.

([81]) Este marco garantiza la consistencia en la aplicación de la conservación de los datos personales adquiridos. El período de revisión depende de las infracciones, que se dividen en cuatro grupos: 1) ciertas cuestiones de protección pública; 2) otros delitos de violencia sexual e infracciones graves; 3) todas las demás infracciones; 4) varios. En la Guía APP sobre la gestión de la información policial puede encontrarse más información (véase la nota a pie de página 26).

([82]) De acuerdo con la información facilitada por las autoridades del Reino Unido, otras organizaciones son libres de seguir los principios del Código de práctica MoPI si lo desean; por ejemplo, Her Majesty's Revenue and Customs y la National Crime Agency adoptan voluntariamente muchos de los principios de este código de práctica para garantizar la coherencia entre los distintos organismos encargados de garantizar el cumplimiento de la ley. En general, la mayoría de las organizaciones proporcionarán a sus empleados políticas y directrices específicas para todo el personal sobre cómo manejar los datos personales como parte de su función, adaptándolas al contexto de la organización específica. Normalmente, esto también incluye formación obligatoria.

([83]) El Código de práctica MoPI se emitió haciendo uso de los poderes previstos en la *Police Act* de 1996, que permiten al College of Policing emitir códigos de práctica relacionados con el funcionamiento eficaz de las funciones policiales. Todo código de práctica que se redacte en virtud de la *Police Act* debe contar con la aprobación del secretario de Estado y está sujeto a consulta con la National Crime Agency antes de presentarse al Parlamento. La sección 39, apartado 7, de la *Police Act* de 1996 requiere que las autoridades policiales tengan debidamente en cuenta los códigos emitidos en virtud de dicha Ley.

([84]) Manual del servicio de policía de Irlanda del Norte relativo al marco MoPI, capítulos 1 a 6.

(49) En Escocia, las fuerzas policiales se apoyan en el Record Retention Standard Operating Procedure (procedimiento operativo estándar de retención de registros) ([85]), que respalda la política de gestión de los registros del servicio de policía de Escocia ([86]). Dicho procedimiento operativo establece normas específicas de conservación para los registros en poder de la policía de Escocia.

(50) Además del requisito general de revisar los registros que aplica en todo el Reino Unido, puede encontrarse información específica en normas localizadas. Algunos ejemplos de ello son, en relación con Inglaterra y Gales, la *Police and Criminal Evidence Act*, en su versión modificada por la *Protection of Freedom Act* (Ley de protección de la libertad) de 2012, que prevé la conservación de huellas dactilares y perfiles de ADN, así como un régimen específico para las personas no condenadas ([87]). La *Protection of Freedom Act* creó también el cargo de Commissioner for the Retention and Use of Biometric Material («Biometrics Commissioner») ([88]). Por su parte, en la revisión sobre imágenes protegidas de 2017 se establecen normas específicas sobre las imágenes protegidas ([89]). En lo que respecto a Escocia, la *Criminal Procedure (Scotland) Act* de 1995 establece las normas para la obtención y la conservación de huellas dactilares y muestras biológicas ([90]). Al igual que ocurre en Inglaterra y Gales, la legislación regula la conservación de datos biométricos en distintos casos ([91]).

2.4.5. *Seguridad de los datos*

(51) Los datos personales deben tratarse de modo que se garantice su seguridad, incluida la protección contra todo tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales. A tal fin, las autoridades públicas deben adoptar las medidas técnicas u organizativas apropiadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta los últimos avances y los costes conexos.

(52) Estos principios se reflejan en la sección 40 de la DPA de 2018, en virtud de la cual, de manera similar al artículo 4, apartado 1, letra f), de la Directiva (UE) 2016/680, los datos personales tratados para cualquiera de los fines de aplicación de la ley deben tratarse de tal manera que se garantice una seguridad adecuada de los mismos mediante la

([85]) Procedimiento operativo estándar de retención de registros de la policía de Escocia, disponible en el siguiente enlace: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Para más detalles sobre la gestión de los registros, véase la información relacionada con los registros nacionales de Escocia, disponible en el siguiente enlace: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Los períodos de conservación varían en función de si una persona ha sido condenada por la ley o no (secciones 63I a 63KI de la PACE de 1984). Por ejemplo, en el caso de un adulto condenado por un delito que pueda quedar registrado como antecedente penal, sus huellas dactilares y su perfil de ADN pueden conservarse de forma indefinida (sección 63I, apartado 2, de la PACE de 1984), mientras que la conservación está limitada en el tiempo si la persona condenada es menor de dieciocho años, si el delito es un delito «leve» que puede quedar registrado como antecedente penal y la persona no ha sido condenada con anterioridad (sección 63K de la PACE de 1984). La conservación en el caso de una persona arrestada o acusada de un delito, pero no condenada, está limitada en el tiempo a tres años (sección 63F de la PACE de 1984). Para que pueda haber una extensión del período de conservación, esta debe aprobarla una autoridad judicial (sección 63F, apartado 7, de la PACE de 1984). En el caso de personas arrestadas o acusadas de un delito leve, pero no condenadas, no está permitida la conservación de los datos (secciones 63D y 63H de la PACE de 1984).

([88]) La sección 20 de la *Protection of Freedom Act* de 2012 crea el cargo de comisionado para la retención y el uso de material biométrico (Biometrics Commissioner). 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 designa con arreglo al *Code for Public Appointments* (Código de nombramientos públicos), disponible en el siguiente enlace: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) 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.

([89]) *Review of the Use and Retention of Custody Images* («Revisión del uso y la conservación de imágenes protegidas», documento en inglés), disponible en el siguiente enlace: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Secciones 18 y ss. de la *Criminal Procedure (Scotland) Act* de 1995.

([91]) Los períodos de conservación varían en función de si la persona ha estado condenada por un delito [sección 18, apartado 3, de la *Criminal Procedure (Scotland) Act* de 1995] o de si es menor de edad. En el último caso, el período de conservación es de tres años a partir de la condena en la audiencia del menor [sección 18E, apartado 8, de la *Criminal Procedure (Scotland) Act* de 1995]. Los datos de personas arrestadas, pero no condenadas, no pueden conservarse [sección 18, apartado 3, de la *Criminal Procedure (Scotland) Act* de 1995], salvo en casos específicos y en función de la gravedad del delito [sección 18A de la *Criminal Procedure (Scotland) Act* de 1995]. La *Scottish Biometrics Commissioner Act* (Ley del comisionado de biometría de Escocia) de 2020 (véase https://www.legislation.gov.uk/asp/2020/8/contents) crea el cargo de Scottish Biometrics Commissioner, que debe preparar y revisar los códigos de práctica (aprobados por el Parlamento escocés) en relación con la adquisición, conservación, uso y destrucción de datos biométricos en el ámbito penal (sección 7 de la *Scottish Biometrics Commissioner Act* de 2020).

aplicación de medidas técnicas u organizativas adecuadas. Esto incluye proteger los datos contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales ([92]). La sección 66 de la DPA de 2018 especifica, además, que todo responsable y todo encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado frente a los riesgos que derivan del tratamiento de los datos personales. De acuerdo con las notas explicativas, el responsable del tratamiento debe valorar los riesgos y aplicar medidas de seguridad adecuadas sobre la base de su evaluación; por ejemplo, cifrado o niveles específicos de habilitación de seguridad para el personal que trata los datos ([93]). La evaluación también debe tener en cuenta, por ejemplo, la naturaleza de los datos tratados y otros factores o circunstancias pertinentes que puedan afectar a la seguridad del tratamiento.

(53) El régimen que rige el cumplimiento de los principios de seguridad de los datos es muy similar al que establecen los artículos 29 a 31 de la Directiva (UE) 2016/680. En particular, en caso de violación de la seguridad los datos personales en relación con los datos personales que son competencia del responsable del tratamiento, de acuerdo con la sección 67, apartado 1, de la DPA de 2018, el responsable debe, sin dilación indebida y siempre que sea posible, en el plazo de las setenta y dos horas posteriores al conocimiento de la violación, notificar la violación de la seguridad de los datos personales a la ICO ([94]). La obligación de notificación no se aplica cuando no es probable que la violación de la seguridad de los datos personales dé lugar a un riesgo para los derechos y libertades de las personas ([95]). El responsable del tratamiento debe documentar los hechos relacionados con cualquier violación de la seguridad de los datos personales, sus efectos y las medidas correctivas emprendidas de manera que permita a la ICO verificar el cumplimiento de la DPA ([96]). Si un encargado del tratamiento tiene conocimiento de una violación de la seguridad de los datos personales, debe notificarlo al responsable del tratamiento sin dilación indebida ([97]).

(54) En virtud de la sección 68, apartado 1, de la DPA de 2018, si es probable que una violación de la seguridad de los datos personales represente un riesgo alto para los derechos y libertades de las personas, entonces el responsable del tratamiento debe informar al interesado de la violación de la seguridad sin dilación indebida ([98]). La notificación debe incluir la misma información que la notificación destinada a la ICO descrita en el considerando 53. Esta obligación no aplica si el responsable del tratamiento ha aplicado las medidas de protección técnicas y organizativas adecuadas que se aplicaron a los datos personales afectados por la violación de la seguridad. Tampoco aplica si el responsable del tratamiento ha adoptado medidas ulteriores que garanticen que ya no existe la probabilidad de que se confirme el alto riesgo para los derechos y libertades del interesado. Por último, el responsable del tratamiento no está obligado a notificar al interesado si hacerlo implica un esfuerzo desproporcionado ([99]). En este caso, debe ponerse la información a disposición del interesado de otra forma igualmente efectiva, por ejemplo, por medio de una comunicación pública ([100]). Si el responsable del tratamiento no ha informado al interesado de la violación de la seguridad, la ICO, tras haber recibido la notificación pertinente con arreglo a la sección 67 de la DPA, y tras valorar la probabilidad de que la violación de la seguridad resulte en un riesgo alto, puede solicitar que el responsable del tratamiento informe al interesado acerca de la violación de la seguridad ([101]).

([92]) De acuerdo con las notas explicativas a la DPA de 2018 (véase la nota a pie de página 45), el responsable del tratamiento debe, en particular: diseñar y organizar su seguridad para adaptarla a la naturaleza de los datos personales que posee y el daño que puede resultar de una violación de la seguridad de los datos; tener claro qué persona dentro de su organización es responsable de garantizar la seguridad de la información; garantizar que cuentan con la seguridad física y técnica adecuada, respaldada por políticas y procedimientos sólidos y personal confiable y bien capacitado; estar preparado para responder a cualquier violación de la seguridad de los datos de forma rápida y eficaz.

([93]) Apartado 221 de las notas explicativas a la DPA de 2018 (véase la nota a pie de página 45).

([94]) La sección 67, apartado 4, de la DPA de 2018 establece que la notificación debe incluir una descripción de la naturaleza de la violación de la seguridad de los datos personales (incluidos, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales afectados), el nombre y la información de contacto de un punto de contacto, la descripción de las consecuencias probables de la violación de la seguridad de los datos personales y una descripción de las medidas adoptadas por el responsable del tratamiento, o propuestas para su adopción, a fin de abordar la violación de la seguridad de los datos personales (en particular, cuando proceda, medidas para mitigar sus posibles efectos adversos).

([95]) Sección 67, apartado 2, de la DPA de 2018.

([96]) Sección 67, apartado 6, de la DPA de 2018.

([97]) Sección 67, apartado 9, de la DPA de 2018.

([98]) En virtud de la sección 68, apartado 7, de la DPA de 2018, el responsable del tratamiento debe restringir, total o parcialmente, la provisión de información al interesado en la medida en que, y durante tanto tiempo como, la restricción sea, teniendo en cuenta los derechos fundamentales y los intereses legítimos del interesado, una medida necesaria y proporcionada para a) evitar obstruir una consulta, investigación o procedimiento oficial o judicial; b) no comprometer la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas.

([99]) Sección 68, apartado 3, de la DPA de 2018.

([100]) Sección 68, apartado 5, de la DPA de 2018.

([101]) Sección 68, apartado 6, de la DPA de 2018, sujeto a la limitación prevista en la sección 68, apartado 8, de la DPA.

2.4.6. *Transparencia*

(55) Debe informarse a los interesados de las principales características del tratamiento de sus datos personales. Este principio de protección de datos se refleja en la sección 44 de la DPA de 2018 que, de manera similar al artículo 13 de la Directiva (UE) 2016/680, dispone que el responsable del tratamiento tiene la obligación general de poner a disposición del interesado información sobre el tratamiento de sus datos personales (ya sea poniendo la información a disposición del público de forma general o de cualquier otra forma) ([102]). La información que debe ponerse a disposición incluye a) la identidad y los datos de contacto del responsable del tratamiento; b) cuando corresponda, los datos de contacto del delegado de protección de datos; c) los fines para los cuales el responsable del tratamiento trata los datos personales; d) la existencia de los derechos del interesado para solicitar del responsable del tratamiento el acceso a sus datos personales, así como su rectificación o supresión de los mismos y la limitación de su tratamiento; y e) la existencia del derecho a presentar una reclamación ante la ICO y los detalles de contacto de la oficina ([103]).

(56) El responsable del tratamiento debe también, en casos específicos a efectos de permitir el ejercicio de los derechos del interesado con arreglo a la DPA de 2018 (por ejemplo, cuando los datos personales que se están tratando se recogieron sin el conocimiento del interesado), proporcionar al interesado información sobre a) el fundamento jurídico para el tratamiento; b) el plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, sobre los criterios utilizados para determinar ese plazo; c) cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales; d) la información que sea necesaria para permitir el ejercicio de los derechos del interesado con arreglo a la parte 3 de la DPA de 2018 ([104]).

2.4.7. *Derechos individuales*

(57) Deben otorgarse al interesado una serie de derechos protegidos jurídicamente. La parte 3, capítulo 3, de la DPA de 2018 concede a las personas los derechos de acceso, rectificación, supresión y restricción ([105]), que son equiparables a los previstos en el capítulo 3 de la Directiva (UE) 2016/680.

(58) En la sección 45 de la DPA de 2018 se establece el derecho de acceso. En primer lugar, una persona tiene derecho a obtener una confirmación por parte del responsable del tratamiento de si sus datos personales están siendo tratados o no ([106]). En segundo lugar, en caso de que los datos personales estén siendo tratados, el interesado tiene derecho a acceder a los mismos y a recibir la siguiente información sobre el tratamiento: a) los fines y las bases jurídicas del tratamiento; b) las categorías de datos de que se trate; c) el destinatario al que se han comunicado los datos; d) el plazo durante el cual se van a conservar los datos personales; e) la existencia del derecho del interesado a la rectificación y la supresión de los datos personales; f) el derecho a presentar una reclamación; y g) toda información sobre el origen de los datos personales de que se trate ([107]).

(59) De conformidad con la sección 46 de la DPA de 2018, el interesado tiene derecho a solicitar al responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. El responsable del tratamiento debe rectificar (o, cuando los datos sean inexactos porque resulten incompletos, completar) los datos sin dilación indebida. Si los datos personales deben conservarse a efectos probatorios, el responsable del tratamiento debe (en lugar de rectificarlos) limitar su tratamiento ([108]).

([102]) La Guía para el tratamiento con fines de aplicación de la ley proporciona el siguiente ejemplo: «Tiene un aviso de privacidad genérico en su sitio web que cubre información básica sobre la organización, el fin para el que trata los datos personales, los derechos del interesado y su derecho a presentar una reclamación ante la ICO. Ha recibido información de que una persona estaba presente cuando se cometió un delito. Al entrevistar a esta persona por primera vez, debe proporcionarle la información genérica, así como información adicional de apoyo, para permitir que ejerza sus derechos. Solo puede restringir el tratamiento leal de la información que está proporcionando si este afectara negativamente a la investigación que está llevando a cabo» [*Guide to Law Enforcement Processing, «What information should we supply to an individual?»* («Guía para el tratamiento con fines de aplicación de la ley. ¿Qué información debe facilitarse al interesado?», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3].

([103]) La Guía para el tratamiento con fines de aplicación de la ley establece que la información suministrada sobre el tratamiento de datos personales debe ser concisa, inteligible y de fácil acceso; escrita en un lenguaje claro y sencillo, adaptada a las necesidades de las personas vulnerables, entre las que se incluyen los menores de edad; y de forma gratuita [*Guide to Law Enforcement Processing, «How should we provide this information?»* («Guía para el tratamiento con fines de aplicación de la ley. ¿Cómo debe proporcionarse la información?», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1].

([104]) Sección 44, apartado 2, de la DPA de 2018.

([105]) Para un análisis en detalle de los derechos del interesado, véase la Guía para el tratamiento con fines de aplicación de la ley, disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Sección 45, apartado 1, de la DPA de 2018.

([107]) Sección 45, apartado 2, de la DPA de 2018.

([108]) Sección 46, apartado 4, de la DPA de 2018.

(60) La sección 47 de la DPA de 2018 otorga a las personas el derecho a la supresión y restricción del tratamiento. El responsable del tratamiento debe ([109]) suprimir los datos personales sin dilación indebida cuando el tratamiento de los mismos infrinja cualquiera de los principios de protección de datos, los fundamentos jurídicos del tratamiento o las garantías relacionadas con el archivo y el tratamiento sensible. Asimismo, el responsable del tratamiento debe suprimir los datos si tiene la obligación jurídica de hacerlo. No obstante, si los datos personales deben mantenerse a efectos probatorios, el responsable del tratamiento debe (en lugar de eliminarlos) limitar su tratamiento ([110]). El responsable del tratamiento debe restringir el tratamiento de los datos personales si el interesado cuestiona la exactitud de los mismos, pero no es posible determinar si son exactos o no ([111]).

(61) Cuando un interesado solicite la rectificación o supresión de datos personales o la restricción de su tratamiento, el responsable del tratamiento debe informar al interesado por escrito de si se ha cursado la solicitud y, en caso de haberse denegado, debe informar al interesado de los motivos de la denegación, así como de las vías de reparación disponibles (el derecho del interesado a presentar una solicitud ante la ICO para investigar si la restricción se ha aplicado de forma lícita, el derecho a presentar una reclamación ante la ICO y el derecho a solicitar una orden de cumplimiento ante un tribunal) ([112]).

(62) Cuando el responsable del tratamiento rectifique los datos personales recibidos de otra autoridad competente, debe notificarlo a dicha autoridad ([113]). Cuando el responsable del tratamiento rectifique, suprima o restrinja el tratamiento de datos personales que haya comunicado, debe notificarlo a los destinatarios y estos, de igual manera, deben rectificar, suprimir o restringir el tratamiento de los datos personales (en la medida en que tengan la responsabilidad de hacerlo) ([114]).

(63) Además, el interesado tiene derecho a que el responsable del tratamiento le informe sin dilación indebida sobre una violación de la seguridad de los datos, cuando haya probabilidades de que entrañe un riesgo alto para los derechos y las libertades de las personas ([115]).

(64) En relación con los citados derechos del interesado, y de manera similar a lo que dispone el artículo 12 de la Directiva (UE) 2016/680, el responsable del tratamiento tiene la obligación de garantizar que toda información proporcionada al interesado se entregue de una forma concisa, inteligible y de fácil acceso ([116]) y, en la medida de lo posible, debe proporcionarse en el mismo formato que la solicitud ([117]). El responsable del tratamiento debe cumplir con la solicitud del interesado sin dilación indebida o, en cualquier caso, antes, en principio, del final del plazo de un mes a partir del momento de la solicitud ([118]). Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de una persona, puede solicitar información adicional y retrasar la tramitación de la solicitud hasta que se determine la identidad de la persona en cuestión. El responsable del tratamiento puede solicitar una tasa razonable o negarse a actuar cuando considere que la solicitud es manifiestamente infundada ([119]). La ICO ha proporcionado orientación sobre cuándo se considera que una solicitud es manifiestamente infundada o excesiva y cuándo se puede solicitar una tarifa ([120]).

(65) Además, con arreglo a la sección 53, apartado 4, de la DPA de 2018, el secretario de Estado puede especificar, mediante regulaciones, la cuantía máxima de una tasa.

([109]) Un interesado puede solicitar al responsable del tratamiento la supresión de los datos personales o la restricción de su tratamiento (en todo caso, los deberes del responsable del tratamiento de suprimir los datos o restringir su tratamiento aplican independientemente de que se solicite o no).

([110]) Sección 46, apartado 4, y sección 47, apartado 2, de la DPA de 2018.

([111]) Sección 47, apartado 3, de la DPA de 2018.

([112]) Sección 48, apartado 1, de la DPA de 2018.

([113]) Sección 48, apartado 7, de la DPA de 2018.

([114]) Sección 48, apartado 9, de la DPA de 2018.

([115]) Sección 68 de la DPA de 2018.

([116]) Sección 52, apartado 1, de la DPA de 2018.

([117]) Sección 52, apartado 3, de la DPA de 2018.

([118]) La sección 54 de la DPA de 2018 define el significado de «plazo de tiempo aplicable», que significa el período de un mes, o un período más largo que pueda especificarse en las regulaciones, comenzando a partir del momento pertinente (cuando el responsable del tratamiento recibe la solicitud en cuestión; cuando el responsable del tratamiento recibe la información, si la hubiera, solicitada en relación con una solicitud en virtud de la sección 52, apartado 4, de la DPA de 2018; o cuando se paga la tasa, si la hubiera, aplicada en relación con la solicitud en virtud de la sección 53 de la DPA de 2018).

([119]) Sección 53, apartado 1, de la DPA de 2018.

([120]) De acuerdo con la orientación de la ICO, un responsable del tratamiento puede decidir cobrar a un sujeto si su solicitud es manifiestamente infundada o excesiva, pero aun así elige responder a ella. En este caso, la tasa debe ser razonable y debe poder justificarse el coste. Véase *Guide to Law Enforcement Processing, «Manifestly unfounded and excessive requests"* («Guía para el tratamiento con fines de aplicación de la ley. Solicitudes manifiestamente infundadas y excesivas», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1. Restricciones de los derechos del interesado y obligaciones de transparencia

(66) Una autoridad competente puede, en determinadas circunstancias, restringir ciertos derechos del interesado: el derecho de acceso ([121]), el derecho a ser informado ([122]), a ser notificado acerca de una violación de la seguridad de los datos personales ([123]) y a ser informado del motivo de la denegación de una solicitud de rectificación o supresión ([124]). De forma similar a lo que estipula el capítulo III de la Directiva (UE) 2016/680, la autoridad competente solo puede aplicar la restricción cuando sea, teniendo en cuenta los derechos fundamentales y los intereses legítimos del interesado, necesaria y proporcionada para: a) evitar la obstrucción de indagaciones, investigaciones o procedimientos oficiales o judiciales; b) no comprometer la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas.

(67) La ICO ha proporcionado orientación sobre la aplicación de esas restricciones. De acuerdo con esta orientación, los responsables del tratamiento deben realizar un análisis caso por caso para compensar los derechos del individuo con el daño que la comunicación causaría. En concreto, deben justificar cualquier restricción que se haya aplicado como necesaria y proporcionada, y solo pueden limitar lo que se proporciona si esto pudiera perjudicar los fines antes mencionados ([125]).

(68) Hay también otra serie de orientaciones emitidas por las autoridades competentes que brindan información detallada sobre todos los aspectos de la legislación de protección de datos, incluida la aplicación de las restricciones de los derechos de los interesados ([126]). Por ejemplo, por lo que respecta a la sección 45, apartado 4, el manual de protección de datos del National Police Chiefs Council (Consejo de Jefes de Policía Nacional) afirma: «Es importante señalar que las restricciones solo pueden señalarse en la medida en que sea necesario y tan solo durante el tiempo necesario. En consecuencia, no está permitida una aplicación general de la restricción a todos los datos personales de un solicitante o la aplicación permanente de la restricción. En relación con este último punto, a menudo se da el caso de que, en un primer momento, es necesario proteger de su comunicación los datos personales recogidos sin el conocimiento de un interesado que es sospechoso en una investigación, a fin de evitar perjudicar la investigación mientras está en curso, pero, posteriormente, la comunicación no encerraría ningún daño si los datos personales se hubieran comunicado a la persona durante una entrevista. Las fuerzas policiales pueden adoptar procesos que garanticen que la aplicación de estas restricciones sea solo en la medida requerida y solo durante el tiempo necesario» ([127]). Esta guía ofrece también ejemplos de cuándo es probable que se aplique cada una de las restricciones ([128]).

(69) Además, en relación con la posibilidad de restringir cualquiera de los derechos mencionados más arriba en aras de la protección de la «seguridad nacional», un responsable del tratamiento puede solicitar un certificado firmado por un ministro del Gabinete o por el fiscal general (o el abogado general de Escocia) que certifique que una restricción de tales derechos constituye una medida necesaria y proporcionada para la protección de la seguridad nacional ([129]). El Gobierno del Reino Unido ha emitido una guía sobre los certificados de seguridad nacional, con arreglo a la DPA de 2018, que señala en especial que cualquier limitación de los derechos de los interesados para salvaguardar la seguridad nacional debe ser proporcionada y necesaria ([130]) (para más información sobre los certificados de seguridad nacional, consulte los considerandos 131 a 134).

([121]) Sección 45, apartado 4, de la DPA de 2018.
([122]) Sección 44, apartado 4, de la DPA de 2018.
([123]) Sección 68, apartado 7, de la DPA de 2018.
([124]) Sección 48, apartado 3, de la DPA de 2018.
([125]) Véase, por ejemplo, la información relativa al derecho de acceso en la Guía para el tratamiento con fines de aplicación de la ley, disponible en el siguiente enlace:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Véase, por ejemplo, el *Data Protection Manual for Police Data Protection Professional* («Manual de protección de datos para los profesionales de la protección de datos de las fuerzas policiales», documento en inglés) emitido por el National Police Chiefs Council (véase la nota a pie de página 27) o la guía proporcionada por la Serious Fraud Office, disponible en el siguiente enlace: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Manual de protección de datos del National Police Chiefs Council, página 140 (véase la nota a pie de página 27).
([128]) El Manual de protección de datos del National Police Chiefs Council establece que «evitar obstruir una indagación, investigación o procedimiento oficial o jurídico» es probable que sea pertinente para los datos personales tratados para pesquisas, procedimientos de juzgados de familia, investigaciones disciplinarias internas no penales e investigaciones como la Independent Inquiry into Child Sexual Abuse (investigación independiente sobre el abuso sexual infantil); Mientras que «proteger los derechos y libertades de otras personas» es pertinente para los datos personales que también se relacionarían con otras personas, así como con el solicitante (Data protection Manual of the National Police Chiefs Council, página 140, véase la nota a pie de página 27).
([129]) Sección 79 de la DPA de 2018.
([130]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, 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.

(70) Además, cuando se aplique una restricción a los derechos de un interesado, la autoridad competente debe informar al interesado sin dilación indebida de que sus derechos se han restringido, de los motivos de la restricción y de las vías de reparación disponibles, salvo que proporcionar dicha información socave el motivo de la aplicación de la restricción ([131]). Como garantía adicional contra el uso indebido de las restricciones, el responsable del tratamiento debe registrar los motivos de la restricción de la información y poner el registro a disposición de la ICO, si lo solicita ([132]).

(71) Si el responsable del tratamiento se niega a proporcionar información adicional en aras de la transparencia, o el acceso a la misma, o rechaza una solicitud de rectificación, supresión o limitación del tratamiento, el individuo en cuestión puede solicitar a la ICO que investigue si el responsable del tratamiento ha empleado la restricción de manera lícita ([133]). El individuo en cuestión puede también presentar una reclamación ante la ICO o solicitar a un tribunal que ordene al responsable del tratamiento que atienda la solicitud ([134]).

2.4.7.2. Decisiones automatizadas

(72) Las secciones 49 y 50 de la DPA de 2018 cubren, respectivamente, los derechos relacionados con las decisiones automatizadas y las garantías que deben aplicarse ([135]). De manera similar al artículo 11 de la Directiva (UE) 2016/680, el responsable del tratamiento solo puede tomar una decisión significativa basada únicamente en el tratamiento automatizado de datos personales si así lo requiere o autoriza la ley ([136]). Una decisión se considera significativa si es probable que tenga un efecto jurídico adverso sobre el interesado o afecte significativamente al interesado ([137]).

(73) Cuando el responsable del tratamiento esté obligado o autorizado por ley a tomar una decisión significativa, la sección 50 de la DPA de 2018 establece las garantías que se aplicarán a dicha decisión (que se define como «decisión significativa admisible»). Tan pronto como sea posible, el responsable del tratamiento debe informar al interesado de la toma de la decisión. El interesado tiene derecho entonces a solicitar, en el plazo de un mes, que el responsable del tratamiento reconsidere la decisión o tome una nueva decisión que no se esté basada únicamente en el tratamiento automatizado. El responsable del tratamiento deberá valorar la solicitud e informar al interesado del resultado de su valoración. La DPA de 2018 otorga al secretario de Estado el poder de adoptar regulaciones para garantías adicionales ([138]). Hasta la fecha no se ha adoptado ninguna regulación de este tipo.

2.4.8. *Transferencias ulteriores*

(74) El nivel de protección de los datos personales transferidos desde una autoridad encargada de garantizar el cumplimiento de la ley de un Estado miembro a una autoridad encargada de garantizar el cumplimiento de la ley del 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 de la autoridad encargada de garantizar el cumplimiento de la ley 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.

([131]) Sección 44, apartados 5 y 6; sección 45, apartados 5 y 6; sección 48, apartado 4, de la DPA de 2018.
([132]) Sección 44, apartado 7; sección 45, apartado 7; y sección 48, apartado 6, de la DPA de 2018.
([133]) Sección 51 de la DPA de 2018.
([134]) Sección 167 de la DPA de 2018.
([135]) En relación con el ámbito del tratamiento automatizado, las notas explicativas a la DPA de 2018 especifican que: «estas disposiciones hacen referencia a las decisiones totalmente automatizadas y no al tratamiento automatizado. El tratamiento automatizado (incluida la elaboración de perfiles) se produce cuando se lleva a cabo una operación con los datos sin necesidad de intervención humana. En el ámbito de aplicación de la ley se emplea de manera regular para filtrar grandes conjuntos de datos en cantidades manejables para que un operador humano los use. Las decisiones automatizadas son una forma de tratamiento automatizado y requieren que la decisión final se tome sin intervención humana» (apartado 204 de las notas explicativas a la DPA de 2018; véase la nota a pie de página 45).
([136]) Además de las protecciones previstas en la DPA, existen otras restricciones legislativas en el marco jurídico del Reino Unido, que se aplican a los organismos encargados de hacer cumplir la ley y evitarían el tratamiento automatizado (incluida la elaboración de perfiles) que dan lugar a discriminación contraria a Derecho. La *Human Rights Act* de 1998 incorpora los derechos del CEDH en la legislación del Reino Unido, incluido el derecho del artículo 14 del Convenio: la prohibición de discriminación. De manera similar, la *Equality Act* de 2010 prohíbe la discriminación hacia personas con características protegidas (que incluyen sexo, raza, discapacidad, etc.).
([137]) Sección 49, apartado 2, de la DPA de 2018.
([138]) Sección 50, apartado 4, de la DPA de 2018.

(75) La parte 3, capítulo 5, de la DPA de 2018 ([139]) regula el régimen del Reino Unido relativo a las transferencias internacionales y refleja el enfoque adoptado en el capítulo V de la Directiva (UE) 2016/680. En particular, para que una autoridad competente pueda transferir datos personales a un tercer país debe cumplir tres condiciones: a) la transferencia debe ser necesaria para un fin de aplicación de la ley; b) la transferencia debe basarse en: i) una norma en materia de adecuación en relación con un tercer país, ii) si no se basa en una norma en materia de adecuación, debe hacerlo entonces en la existencia de garantías adecuadas, o iii) si no se basa en una norma en materia de adecuación ni en garantías adecuadas, debe basarse en circunstancias especiales; y c) el destinatario de la transferencia debe ser: i) una autoridad pertinente (es decir, el equivalente a una autoridad competente) en un tercer país; ii) una «organización internacional pertinente», por ejemplo un organismo internacional que lleve a cabo funciones correspondientes a cualquiera de los fines de aplicación de la ley; o iii) una persona que no sea una autoridad pertinente, pero solo en el caso de que la transferencia sea estrictamente necesaria para la consecución de uno de los fines de aplicación de la ley; no hay derechos y libertades fundamentales del interesado en cuestión que primen sobre el interés público que exige la transferencia; una transferencia de datos personales a una autoridad pertinente de un tercer país sería ineficaz o inapropiada; el destinatario está informado de los fines para los que pueden tratarse los datos ([140]).

(76) Las normas en materia de adecuación con respecto a un tercer país, un territorio o un sector dentro de un tercer país, una organización internacional, o una descripción ([141]) de dicho país, territorio, sector u organización las adopta el secretario de Estado. En cuanto al estándar que debe cumplirse, el secretario de Estado debe evaluar si dicho territorio/sector/organización garantiza un nivel adecuado de protección de los datos personales. La sección 74A, apartado 4, de la DPA de 2018 especifica que, para ello, el secretario de Estado debe tener en consideración una serie de elementos que reflejen los enumerados en el artículo 36 de la Directiva (UE) 2016/680 ([142]). En este sentido, la parte 3 de la DPA de 2018 constituye, desde el final del período transitorio, «legislación nacional derivada de la UE» que, como se explicó, debían interpretar los tribunales del Reino Unido de acuerdo con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea que data de antes de la salida del Reino Unido de la Unión y los principios generales del Derecho de la Unión, de modo que tuviera efecto de manera inmediata antes del final del período transitorio. Esto incluye la norma del nivel de protección «esencialmente equivalente» que, por lo tanto, se aplicará a las evaluaciones de adecuación realizadas por las autoridades del Reino Unido.

(77) Por lo que respecta al procedimiento, las normas 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

([139]) Este nuevo marco entró en vigor al final del período transitorio, en especial la facultad del secretario de Estado para emitir normas en materia de adecuación. Sin embargo, la normativa *DPPEC Regulations* (en particular, los apartados 10 a 12, del anexo 21, que dicha normativa introduce en la DPA de 2018) dispone que determinadas transferencias de datos personales durante el período transitorio y una vez finalizado el mismo se traten como si estuvieran basadas en normas en materia de adecuación. Estas transferencias incluyen transferencias a terceros países que son objeto de una decisión de adecuación de la UE al final del período transitorio y a Estados miembros de la UE, los estados de la Asociación Europea de Libre Comercio (AELC) y el territorio de Gibraltar en virtud de su aplicación de la Directiva sobre protección de datos en el ámbito penal al tratamiento de datos con fines de aplicación de la ley [los estados de la AELC aplican la Directiva (UE) 2016/680 como resultado de sus obligaciones en virtud del acervo de Schengen]. Esto significa que, una vez finalizado el período transitorio, las transferencias a estos países pueden seguir realizándose de la misma forma que antes de la retirada de la UE. Una vez finalizado el período transitorio, el secretario de Estado deberá realizar una revisión de las conclusiones de adecuación en el plazo de cuatro años.

([140]) Secciones 73 y 77 de la DPA de 2018.

([141]) Las autoridades del Reino Unido aclararon que la descripción de un país o una 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, una norma en materia de adecuación en relación con tan solo ciertos tipos de transferencias de datos).

([142]) Véase la sección 74A, apartado 4, de la DPA de 2018, que establece que cuando se evalúa la adecuación del nivel de protección «el secretario de Estado debe, en concreto, tener en cuenta a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluidas la seguridad pública, la defensa, la seguridad nacional, el Derecho penal y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de los datos, las normas profesionales y las medidas de seguridad, incluidas las normas para las transferencias ulteriores de datos personales a otro tercer país u organización internacional que se apliquen en el tercer país o en la organización internacional en cuestión, la jurisprudencia, así como los derechos del interesado efectivos y exigibles y un derecho de recurso administrativo y judicial efectivo de los interesados cuyos datos personales son transferidos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y ejecutar el cumplimiento de las normas en materia de protección de datos, incluidos los poderes ejecutivos adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros; y c) los compromisos internacionales asumidos por el tercer país o la organización internacional correspondiente, u otras obligaciones que deriven de convenios o instrumentos jurídicamente vinculantes o de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales».

al proponer la elaboración de futuras normas en materia de adecuación del Reino Unido ([143]). 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 ([144]).

(78) De conformidad con la sección 74B, 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 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.

(79) De forma similar a lo que establece el artículo 37 de la Directiva (UE) 2016/680, en ausencia de una norma de adecuación, es posible realizar una transferencia de datos personales en el contexto de la aplicación de la ley cuando se han establecido las garantías adecuadas. Dichas garantías se aseguran mediante a) un instrumento jurídicamente vinculante que contenga las garantías adecuadas para la protección de los datos personales; o b) una evaluación por parte del responsable del tratamiento que, una vez valoradas todas las circunstancias que concurren en la transferencia, concluya que existen garantías apropiadas con respecto a la protección de los datos ([145]). Además, cuando las transferencias se basan en garantías adecuadas, la DPA de 2018 establece que, además de la función normal de supervisión de la ICO, las autoridades competentes deben ofrecer información específica acerca de las transferencias a la ICO ([146]).

(80) 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» ([147]). 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 inminente y grave para la seguridad pública 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) ([148]). Cabe señalar que los puntos d) y e) no se aplican si los derechos y libertades del interesado prevalecen sobre el interés público en la transferencia ([149]). 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.

(81) En estas circunstancias, debe documentarse la fecha, la hora y la justificación de la transferencia, así como el nombre y cualquier otro tipo de información pertinente sobre el destinatario y una descripción de los datos personales transferidos, y esta documentación se pondrá a disposición, previa solicitud, de la ICO ([150]).

(82) La sección 78 de la DPA de 2018 regula el escenario de las «transferencias ulteriores», es decir, cuando los datos personales que se han transferido del Reino Unido a un tercer país se transfieren posteriormente a otro tercer país o una organización internacional. De conformidad con la sección 78 apartado 1, el responsable del tratamiento del Reino Unido que realiza la transferencia debe establecer como condición de la misma que los datos no se transfieran a un tercer país sin la autorización del responsable del tratamiento que transfiere los datos. Además, de acuerdo con el artículo 78, apartado 3, y de forma similar a lo dispuesto en el artículo 35, apartado 1, letra e), de la Directiva (UE) 2016/680, en caso de que se requiera dicha autorización, se aplican una serie de requisitos sustantivos. En concreto,

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

([144]) Durante este período de cuarenta días, ambas cámaras del Parlamento tienen la oportunidad, si lo desean, de votar en contra de las normas; si se aprueba dicha votación, la norma dejará en última instancia de tener efecto jurídico.

([145]) Sección 75 de la DPA de 2018.

([146]) De acuerdo con la sección 75, apartado 3, de la DPA de 2018, cuando una transferencia de datos se realice sobre la base de garantías adecuadas: a) la transferencia debe documentarse, b) la documentación se pondrá a disposición, previa solicitud, de la ICO y c) la documentación debe incluir, en específico, i) la fecha y la hora de la transferencia, ii) el nombre y cualquier información pertinente sobre el destinatario, iii) la justificación de la transferencia, y iv) una descripción de los datos personales transferidos.

([147]) *Guide to Law Enforcement Processing, «Are there any special circumstances?»* («Guía para el tratamiento con fines de aplicación de la ley. ¿Existen circunstancias especiales?», documento en inglés), disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Sección 76 de la DPA de 2018.

([149]) Sección 76 de la DPA de 2018.

([150]) Sección 76, apartado 3, de la DPA de 2018.

a la hora de decidir si autoriza o no una transferencia, una autoridad competente debe asegurarse de que la transferencia ulterior sea necesaria a efectos de aplicación de la ley y debe considerar, entre otros factores, a) la gravedad de las circunstancias que dieron lugar a la solicitud de autorización, b) el fin para el que se transfirieron originalmente los datos personales, y c) las normas para la protección de datos personales que se aplican en el tercer país u organización internacional al que se transferirían los datos personales.

(83) Además, cuando los datos objeto de una transferencia ulteriormente desde el Reino Unido se transfirieron originalmente desde la Unión Europea, se aplican garantías adicionales.

(84) En primer lugar, la sección 73, apartado 1, letra b), de la DPA de 2018 establece, de manera similar a lo previsto en el artículo 35, apartado 1, letra c), de la Directiva (UE) 2016/680, que en el caso de que los datos personales hayan sido transmitidos originalmente o puestos a disposición del responsable del tratamiento u otra autoridad competente por parte de un Estado miembro, se entiende que dicho Estado miembro, o cualquier persona con sede en el mismo que sea una autoridad competente a efectos de la Directiva (UE) 2016/680, ha autorizado la transferencia de acuerdo con la ley del Estado miembro.

(85) Sin embargo, de manera similar a lo que establece el artículo 35, apartado 2, de la Directiva (UE) 2016/680, dicha autorización no es necesaria cuando a) la transferencia es necesaria para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o un tercer país o para los intereses fundamentales de un Estado miembro, y b) la autorización previa no puede conseguirse a su debido tiempo. En este caso, debe informarse sin dilación a la autoridad del Estado miembro en cuestión que habría sido responsable de decidir si se autoriza la transferencia ([151]).

(86) En segundo lugar, en el caso de que datos transferidos originalmente desde la Unión Europea al Reino Unido, sean transferidos por parte del Reino Unido a un tercer país que posteriormente los transferirá a otro tercer país, se aplica el mismo planteamiento. En este caso, de conformidad con la sección 78, apartado 4, de la DPA de 2018, la autoridad competente del Reino Unido no puede autorizar la última transferencia en virtud de la sección 78, apartado 1, de dicha Ley salvo que el «Estado miembro [que haya transferido originalmente los datos en cuestión], o cualquier persona con sede en el mismo que sea una autoridad competente a efectos de la Directiva sobre protección de datos en el ámbito penal haya autorizado la transferencia de conformidad con la legislación de dicho Estado miembro». Estas garantías son importantes ya que permiten a las autoridades de los Estados miembros asegurar la continuidad de la protección, de conformidad con la legislación de la UE en materia de protección de datos, a lo largo de toda la «cadena de transferencia».

(87) Este nuevo marco para las transferencias internacionales entró en vigor al final del período transitorio ([152]). Sin embargo, los párrafos décimo a decimosegundo, del anexo 21, de la DPA de 2018 (introducidos por la normativa *DPPEC Regulations*) establecen 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. Estas transferencias incluyen transferencias a un Estado miembro, los países de la AELC y terceros países que fueron objeto de una decisión de adecuación de la UE al final del período transitorio, así como al territorio de Gibraltar. En consecuencia, las transferencias a estos países pueden seguir realizándose como antes de la retirada del Reino Unido de la Unión. 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 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.

2.4.9. *Rendición de cuentas*

(88) De conformidad con el principio de responsabilidad, las autoridades públicas que tratan datos están obligadas a adoptar las medidas técnicas y organizativas apropiadas para cumplir efectivamente con sus obligaciones en materia de protección de datos y deben poder demostrar el respeto de estas obligaciones, en particular ante la autoridad de control competente.

(89) Este principio se refleja en la sección 56 de la DPA de 2018, que introduce una obligación general de rendición de cuentas para el responsable del tratamiento, es decir, la obligación de aplicar medidas técnicas y organizativas adecuadas para garantizar, y poder demostrar, que el tratamiento de datos personales cumple con los requisitos de la parte 3 de la DPA de 2018. Las medidas aplicadas deben revisarse y actualizarse cuando sea necesario y, cuando sean proporcionadas en relación con el tratamiento, deben incluir políticas de protección de datos adecuadas.

([151]) Sección 73, apartado 5, de la DPA de 2018.

([152]) 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.

(90) De conformidad con el capítulo V de la Directiva (UE) 2016/680, las secciones 55 a 71 de la DPA de 2018 prevén distintos mecanismos para garantizar la rendición de cuentas y permitir que los responsables y encargados del tratamiento demuestren su cumplimiento. En concreto, los responsables del tratamiento deben aplicar medidas de protección de datos desde el diseño y por defecto, esto es, para garantizar que la aplicación de los principios de protección de datos se realiza de manera efectiva, y deben mantener registros de todas las categorías de actividades de tratamiento que son competencia del responsable del tratamiento (incluida información sobre la identidad del responsable, los datos de contacto del delegado de protección de datos, los fines del tratamiento, las categorías de destinatarios de las comunicaciones y una descripción de las categorías de interesados y datos personales) y mantener estos registros a disposición de la ICO cuando los solicite. El responsable y el encargado del tratamiento también deben mantener registros de ciertas operaciones de tratamiento y ponerlas a disposición de la ICO ([153]). Los responsables del tratamiento, en concreto, también están obligados a colaborar con la ICO en el desempeño de sus tareas.

(91) La DPA de 2018 establece también requisitos adicionales para el tratamiento que suponga un alto riesgo para los derechos y libertades de las personas. Estos incluyen la obligación de realizar evaluaciones de impacto relativas a la protección de datos y de consultar a la ICO antes del tratamiento si la evaluación indica que dicho tratamiento podría suponer un alto riesgo para los derechos y libertades de las personas (en ausencia de medidas para mitigar el riesgo).

(92) Además, los responsables del tratamiento deben designar un delegado de protección de datos, salvo que el responsable del tratamiento sea un tribunal u otra autoridad judicial que actúe en el ejercicio de su función judicial ([154]). El responsable del tratamiento debe garantizar que el delegado de protección de datos está involucrado en todos los asuntos relacionados con la protección de los datos personales, que dispone de los recursos necesarios y del acceso a los datos personales y a las operaciones de tratamiento, y puede realizar sus tareas de forma independiente. En la sección 71 de la DPA de 2018 se establecen las funciones del delegado de protección de datos, en particular la provisión de información y asesoramiento, supervisar el cumplimiento, así como colaborar y actuar como punto de contacto para la ICO. Al llevar a cabo sus tareas, el delegado de protección de datos debe prestar la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.

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

2.5.1. *Supervisión independiente*

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

(94) 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 ([155]). El/la Information Commissioner supervisa también el tratamiento de datos personales por parte de las autoridades competentes cuando entra dentro del ámbito de la parte 3 de la DPA de 2018 ([156]). 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 ([157]). El departamento que ampara al/a la Information Commissioner es el Departamento de Cultura, Medios de Comunicación y Deporte ([158]) del Reino Unido.

([153]) Sección 62 de la DPA de 2018.
([154]) Sección 69 de la DPA de 2018.
([155]) Artículo 36, apartado 2, letra b), de la Directiva (UE) 2016/680.
([156]) Sección 116 de la DPA de 2018.
([157]) *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.
([158]) 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).

(95) La independencia del/de la Information Commissioner se establece explícitamente en el artículo 52 del RGPD del Reino Unido, que refleja los requisitos establecidos en el artículo 52, apartados 1 a 3, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([159]). 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 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.

(96) 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* ([160]), 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 ([161]).

(97) El/la Information Commissioner ocupa el cargo por un período de hasta siete años 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 ([162]). 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 ante la Cámara de que se trate en el que se 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 ([163]).

(98) 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 ([164]) [*Data Protection (Charges and Information) Regulations*] y ascienden al 85-90 % del presupuesto anual de la oficina ([165]); ii) subvención que puede conceder el Gobierno a la ICO y que se emplea principalmente para financiar los costes operativos de la oficina en lo que respecta a las funciones no relacionadas con la protección de datos ([166]); iii) tasas por servicios ofrecidos ([167]). Actualmente no se cobra ninguna de estas tasas.

(99) 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 que entran en el ámbito de aplicación de la parte 3 de dicha Ley. Estas funciones incluyen el control de la aplicación de la parte 3 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

([159]) 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) (DO L 119 de 4.5.2016, p. 1).

([160]) *Governance Code on Public Appointments* («Código de gobernanza sobre nombramientos públicos», documento en inglés), disponible en el siguiente enlace: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) *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.

([162]) 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.

([163]) Párrafo tercero, del anexo 12, de la DPA de 2018.

([164]) Sección 137 de la DPA de 2018.

([165]) 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, de la DPA de 2018 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. 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.

([166]) 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 158).

([167]) Sección 134 de la DPA de 2018.

información a un interesado en relación con el ejercicio de sus derechos como interesado; y llevar a cabo investigaciones. 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. Sin embargo, la supervisión del poder judicial está a cargo de organismos especializados, que se examinan a continuación.

2.5.1.1 Ejecución, incluidas sanciones

(100) 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 aplicación de la parte 3 de la DPA de 2018. La ICO tiene poderes para notificar al responsable o al encargado del tratamiento de una supuesta infracción de la parte 3, para emitir avisos a un responsable o encargado del tratamiento de la probabilidad de que las operaciones de tratamiento previstas infrinjan las disposiciones de la parte 3 y para emitir sanciones a un responsable o encargado del tratamiento cuando las operaciones de tratamiento hayan infringido las disposiciones de la parte 3. Además, la ICO puede emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento del Reino Unido, al Gobierno o a otras instituciones y organismos, así como al público, sobre cualquier cuestión relacionada con la protección de los datos personales ([168]).

(101) Asimismo, la ICO dispone de poderes para:

— 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») ([169]);

— 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, («aviso de evaluación») ([170]);

— obtener el acceso a documentos 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»);

— ejercer poderes correctivos, en especial mediante avisos y sanciones o emitiendo órdenes mediante avisos de ejecución, que requieren que los responsables/encargados del tratamiento adopten o se abstengan de adoptar medidas específicas («aviso de ejecución») ([171]); y

— emitir multas administrativas en forma de aviso de sanción («aviso de sanción») ([172]).

(102) 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 ([173]). Un aviso de ejecución puede imponer requisitos que la ICO considere apropiados con el fin de remediar la infracción. Un aviso de sanción requiere que la persona pague a la ICO la cuantía especificada en el aviso. Puede emitirse un aviso de sanción cuando se ha producido un incumplimiento de ciertas disposiciones de la DPA de 2018 ([174]) o puede darse a un responsable o encargado del tratamiento que no ha cumplido con un aviso de información, un aviso de evaluación o un aviso de ejecución.

(103) En específico, para determinar si debe entregarse un aviso de sanción a un responsable o encargado del tratamiento y determinar la cuantía de la sanción, la ICO debe tener en cuenta las cuestiones enumeradas en la sección 155, apartado 3, de la DPA de 2018, incluida la naturaleza y gravedad de la infracción, la intencionalidad o negligencia de la infracción, cualquier medida adoptado por el responsable o encargado del tratamiento para mitigar el daño sufrido por los interesados, el grado de responsabilidad del responsable o encargado del tratamiento (teniendo en

([168]) Párrafo segundo, del anexo 13, de la DPA de 2018.
([169]) Sección 142 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 143 de la DPA de 2018).
([170]) Sección 146 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 147 de la DPA de 2018).
([171]) Secciones 149 a 151 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 152 de la DPA de 2018).
([172]) Sección 155 de la DPA de 2018 (sujeto a las limitaciones previstas en la sección 156 de la DPA de 2018).
([173]) 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.
([174]) En concreto, la ICO puede emitir un aviso de sanción por el incumplimiento de una disposición con arreglo a la sección 149, apartados 2, 3, 4 o 5, de la DPA de 2018.

cuenta las medidas técnicas y organizativas aplicadas por este último), cualquier violación previa pertinente por parte del responsable o encargado del tratamiento; y, por otro lado, las categorías de datos personales afectadas por la infracción y si la sanción sería efectiva, proporcionada y disuasoria.

(104) La cuantía máxima de la sanción que puede imponerse mediante un aviso de sanción es a) 17,5 millones de libras esterlinas cuando se trata de un incumplimiento de los principios de protección de datos (secciones 35 a 37, sección 38, apartado 1, sección 39, apartado 1, y sección 40 de la DPA de 2018), obligaciones de transparencia y derechos individuales (secciones 44, 45, 46, 47, 48, 49, 52 y 53 de la DPA de 2018), y principios para las transferencias internacionales de datos personales (secciones 73, 75, 76, 77 o 78 de la DPA de 2018); y b) 8,7 millones de libras esterlinas en los demás casos ([175]). En caso de 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.

(105) Según los últimos informes anuales (2018-2019 ([176]) y 2019-2020 ([177])), la ICO ha llevado a cabo una serie de investigaciones relacionadas con el tratamiento de datos personales por parte de las autoridades de control de la aplicación del Derecho penal. Por ejemplo, la ICO realizó una investigación y publicó un dictamen en octubre de 2019 sobre el uso de la tecnología de reconocimiento facial en lugares públicos con fines de aplicación de la ley. La investigación se centró en especial en el uso de capacidades de reconocimiento facial en vivo por parte de la policía de Gales del Sur y la Policía Metropolitana de Londres. Además, la ICO investigó la «Gangs Matrix» ([178]) 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 el uso de los datos.

(106) 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.

(107) Otro ejemplo de una acción de ejecución reciente es la multa de 325 000 libras esterlinas emitida por la ICO en mayo de 2018 contra el Crown Prosecution Service por la pérdida de múltiples DVD sin cifrar que contenían grabaciones de entrevistas policiales. Además, la ICO llevó 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.

(108) Además de los poderes de ejecución de la ICO mencionados más arriba, 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 los 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 ([179]); 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 ([180]); 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 ([181]), realizar declaraciones falsas en respuesta a un aviso de información o destruir información en relación con avisos de información y evaluación ([182]).

(109) La ICO tiene también el deber, con arreglo a la sección 139 de la DPA de 2018, de presentar ante cada cámara del Parlamento un informe general sobre el ejercicio de sus funciones en virtud de la DPA de 2018 ([183]).

([175]) Sección 157 de la DPA de 2018.

([176]) *Annual Report and Financial Statements 2018-2019* («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/2615262/annual-report-201819.pdf.

([177]) *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 157).

([178]) Una base de datos que registraba inteligencia relacionada con presuntos miembros de bandas y víctimas de delitos relacionados con bandas.

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

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

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

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

([183]) Como se estipula en el contrato de gestión, el informe anual debe: i) contemplar cualquier empresa, filial o empresa en participación bajo el control de la ICO; ii) cumplir con el *Treasury's Financial Reporting Manual* (Manual de información financiera del Tesoro); iii) contener una declaración de gobierno que establezca las formas en las que el contable ha gestionado y controlado los recursos empleados en el organismo durante el transcurso del año, demostrando el nivel de éxito de la gestión de los riesgos en aras de la consecución de sus metas y objetivos; y iv) describir las actividades principales y el desempeño durante el año financiero anterior y exponer de forma resumida los planes futuros (Contrato de gestión 2018-2021, apartado 3.26; véase la nota a pie de página 158).

2.5.2. *Supervisión del poder judicial*

(110) 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 realiza la supervisión. Cuando el responsable del tratamiento actúa en el ejercicio de su función judicial, la ICO no puede ejercer sus funciones de supervisión ([184]) y, en consecuencia, organismos especiales realizan la supervisión. Esto refleja el enfoque adoptado en el artículo 32 de la Directiva (UE) 2016/680.

(111) 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) ([185]). Además, el Lord Chief Justice y el Senior President of Tribunals emitieron un aviso de privacidad ([186]) que establece cómo los tribunales de Inglaterra y Gales tratan los datos personales para las funciones jurisdiccionales. Los poderes judiciales de Irlanda del Norte ([187]) y Escocia ([188]) emitieron una notificación similar.

(112) 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) ([189]). 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 ([190]).

(113) 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 ([191]).

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

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

([185]) 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 formal, advertencia 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.

([186]) 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.

([187]) 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.

([188]) 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.

([189]) 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.

([190]) Cuando la reclamación o la infracción se consideren graves, se remitirá al Judicial Complaints Officer (oficial de quejas judiciales) para una investigación en exhaustiva 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.

([191]) 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).

2.5.3. *Acciones administrativas y judiciales*

(115) 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.

(116) 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 pertinente de la parte 3 de la DPA de 2018 ([192]). Tal como se describe en los considerandos 100 a 109, la ICO tiene el poder de evaluar la conformidad del responsable y el encargado del tratamiento con la DPA de 2018, de exigirles que adopten o se abstengan de adoptar las medidas necesarias en caso de incumplimiento, así como de imponer multas.

(117) En segundo lugar, la DPA de 2018 otorga el derecho a la tutela judicial contra la ICO. Si la ICO no «procesa» ([193]) una reclamación presentada por el interesado, el reclamante tiene acceso a la tutela judicial, ya que puede apelar ante un Tribunal de Primera Instancia ([194]) para que ordene a la ICO que adopte las medidas adecuadas para responder a la reclamación o para informar al reclamante acerca del progreso de la misma ([195]). 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 ([196]).

(118) 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 sección la 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. Además, con arreglo a la sección 169 de la DPA de 2018, toda persona que sufra un daño 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.

(119) En cuarto lugar, en la medida en que una persona 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. En virtud de la parte 3 de la DPA de 2018, los responsables del tratamiento, es decir, las autoridades competentes, son siempre autoridades públicas en el sentido de la *Human Rights Act* de 1998. 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 ([197]).

([192]) Sección 165 de la DPA de 2018.

([193]) 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.

([194]) 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.

([195]) Sección 166 de la DPA de 2018.

([196]) Secciones 161 y 162 de la DPA de 2018.

([197]) Véase el asunto *Brown v Commissioner* de 2016 de la Policía Metropolitana de Londres, en el que el tribunal resolvió a favor de una reparación para la demandante en el contexto de la protección de datos en una acción interpuesta contra la policía. El tribunal falló a favor de la demandante, confirmando sus reclamaciones de incumplimiento de las obligaciones de la DPA de 1998, de incumplimiento de la *Human Rights Act* de 1998 (y el derecho relacionado en el artículo 8 del Convenio Europeo de Derechos Humanos) y el agravio por uso indebido de información privada (la parte demandada finalmente admitió el incumplimiento de la DPA y el Convenio Europeo de Derechos Humanos, por lo que la sentencia se centró en qué medida correctiva era apropiada). Como resultado de estos incumplimientos, el tribunal dispuso una indemnización monetaria para la demandante.

(120) 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 ([198]). El tribunal también puede declarar que una disposición de la legislación primaria es incompatible con uno derecho garantizado en virtud del Convenio Europeo de Derechos Humanos.

(121) 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.

2.6. **Intercambio posterior**

(122) El Derecho del Reino Unido autoriza 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»), sujeto a ciertas condiciones.

(123) 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 ([199]). En este caso, todas las garantías que establece la parte 3 de la DPA de 2018, y que se analizan más arriba, se aplican al tratamiento que realiza la autoridad receptora.

(124) En el ordenamiento jurídico del Reino Unido, distintas leyes permiten explícitamente intercambio posterior. 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 una autoridad pública ([200]), o en caso de una deuda debitada a una autoridad pública o a la Corona ([201]); ii) la *Crime and Courts Act* de 2013 permite el intercambio de información con la National Crime Agency (NCA) ([202]) 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 ([203]).

(125) Estas leyes establecen explícitamente que el intercambio de información debe respetar las normas establecidos en la DPA de 2018. Además, el College of Policing ha emitido una práctica profesional autorizada sobre intercambio de información ([204]) para ayudar a la policía a cumplir con sus 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 ([205]).

(126) 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 ([206]). Este tipo de intercambio 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 o una oficina de servicio social para

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

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

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

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

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

([203]) Sección 68 de la *Crime and Courts Act* de 2013, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) 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.

([205]) Véase, por ejemplo, el asunto *M 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.

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

menores); 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. Como se especifica en la Decisión adoptada en virtud del Reglamento (UE) 2016/679, las garantías que establecen el RGPD del Reino Unido y la parte 2 de la DPA de 2018 proporcionan un nivel de protección esencialmente equivalente al que se garantiza en el contexto de la Unión ([207]).

(127) En el segundo escenario, en relación con el intercambio con fines de seguridad nacional de datos recogidos 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 *Counter Terrorism Act* (Ley contra el terrorismo) de 2008 (CTA 2008) ([208]). 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».

(128) Por lo que respecta a las condiciones en virtud de las cuales pueden compartirse datos con fines de seguridad nacional, la *Intelligence Services Act* (Ley de servicios de inteligencia) y la *Security Service Act* (Ley del servicio de seguridad) limitan la capacidad de los servicios de inteligencia para obtener datos a lo que se considera necesario para el desempeño de sus funciones estatutarias. Con arreglo a la parte 3 de la DPA de 2018, las autoridades competentes 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* ([209]). La sección 20 de la CTA 2008 deja claro que cualquier intercambio de datos con arreglo a la sección 19 de esta Ley 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 DPA de 2018. Además, las autoridades encargadas de garantizar el cumplimiento de la ley y los servicios de inteligencia son autoridades públicas a efectos de la Human Rights Act de 1998 y, por tanto, deben garantizar que actúan de conformidad con los derechos garantizados por el Convenio Europeo de Derechos Humanos, incluido su artículo 8. Es decir, estos requisitos implican que todo intercambio de datos entre los organismos encargados de garantizar el cumplimiento de ley y los servicios inteligencia debe cumplir con la legislación en materia de protección de datos y con el Convenio Europeo de Derechos Humanos.

(129) El tratamiento por parte de los servicios de inteligencia de datos personales recibidos u obtenidos de autoridades encargadas de garantizar el cumplimiento de la ley con fines de seguridad nacionales está sujeto a una serie de condiciones y garantías ([210]). La parte 4 de la DPA de 2018 se aplica a todo tratamiento de datos personales por

([207]) Decisión de Ejecución de la Comisión de conformidad con la Directiva (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido C(2021) 4800.

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

([209]) La sección 2, apartado 2, de la *Intelligence Services Act* de 1994 (véase https://www.legislation.gov.uk/ukpga/1994/13/contents) 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 proceso 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 (véase https://www.legislation.gov.uk/ukpga/1989/5/contents) 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 proceso 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».

([210]) La *Investigatory Powers Act* de 2016 también regula las garantías y las limitaciones que aplican a los poderes de los servicios de inteligencia y, junto con el *Regulation of Investigatory Powers Act* (Ley de regulación de los poderes de investigación) de 2000 para Inglaterra, Gales e Irlanda del Norte y la *Regulation of Investigatory Powers (Scotland) Act* de 2000 para Escocia, establecen el fundamento jurídico para el uso de tales poderes. No obstante, estos poderes no son pertinentes en el contexto del «intercambio posterior», ya que solo contemplan la recogida directa de datos personales por parte de los servicios de inteligencia. Para una evaluación de los poderes otorgados a los servicios de inteligencia en virtud de la *Investigatory Powers Act*, véase la Decisión de Ejecución de la Comisión de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección adecuada de los datos personales por el Reino Unido C(2021) 4800.

parte de los servicios de inteligencia o realizado en su nombre. Esta parte establece los principios fundamentales de la protección de datos (licitud, lealtad y transparencia ([211]); limitación de la finalidad ([212]); minimización de los datos ([213]); exactitud ([214]); limitación del plazo de conservación ([215]) y seguridad ([216]); asimismo, impone condiciones sobre el tratamiento de categorías especiales de datos ([217]), establece los derechos de los interesados ([218]), requiere la protección de datos desde el diseño ([219]) y regula las transferencias internacionales de datos personales ([220]).

(130) 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, cuando dicha exención sea necesaria para salvaguardar la seguridad nacional. 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. Es posible acogerse a esta exención sobre la base de un análisis caso por caso ([221]). Tal como aclararon las autoridades del Reino Unido y como confirma la jurisprudencia de los tribunales del Reino Unido, «a) 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» ([222]). La ICO es la encargada de supervisar si la exención se ha utilizado adecuadamente o no ([223]).

([211]) 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.

([212]) 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).

([213]) Los datos personales deben ser adecuados, pertinentes y no excesivos (sección 88 de la DPA de 2018).

([214]) Los datos personales deben ser exactos y, si fuera necesario, actualizados (sección 89 de la DPA de 2018).

([215]) Los datos personales no deben conservarse más tiempo del necesario (sección 90 de la DPA de 2018).

([216]) 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.

([217]) Sección 86, apartado 2, letra b), y anexo 10, de la DPA de 2018.

([218]) 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.

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

([220]) 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.

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

([222]) Sección H del *UK Explanatory Framework for Adequacy Discussions* del Reino Unido: *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), pp. 15 y 16, disponible en el siguiente enlace: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Véase también el asunto *Baker v Secretary of State* (véase la nota a pie de página 220), 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.

([223]) 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, disponible en el siguiente enlace: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Además, en relación con la posibilidad de restringir cualquiera de los derechos mencionados más arriba en aras de la protección de la «seguridad nacional», la sección 79 de la DPA de 2018 contempla la posibilidad de que un responsable del tratamiento solicite 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 ([224]). El Gobierno del Reino Unido ha publicado una guía sobre certificados 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 ([225]). Todos los certificados de seguridad nacional deben publicarse en el sitio web de la ICO ([226]).

(132) El certificado debe tener una duración determinada de no más de cinco años, de modo que el poder ejecutivo pueda revisarlo periódicamente ([227]). 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 ([228]).

(133) 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. Es decir, 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 debe aplicarse caso por caso. 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 ([229]).

(134) Cualquier persona directamente afectada por la emisión de un certificado puede apelar ante el Tribunal Superior ([230]) contra el certificado ([231]) o, cuando el certificado identifique datos mediante una descripción general, impugnar la aplicación del certificado a datos específicos ([232]).

(135) El tribunal revisará la decisión de emisión del certificado y decidirá si existían motivos razonables para su emisión ([233]). 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 ([234]).

([224]) 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 párrafo decimoséptimo, 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. De momento no se ha emitido ningún certificado de seguridad nacional en virtud de la DPA de 1998.

([225]) 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.

([226]) 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.

([227]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 15, véase la nota a pie de página 225.

([228]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 5; véase la nota a pie de página 224.

([229]) 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/.

([230]) 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.

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

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

([233]) En el asunto *Baker v Secretary of State* (véase la nota a pie de página 221), 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.

([234]) Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional, apartado 25; véase la nota a pie de página 224.

(136) 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 ([235]) 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. 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») ([236]). Solo es posible apelar a las exenciones basadas en el perjuicio en la medida en que la aplicación de 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.

(137) De lo anterior se desprende que la limitación 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.

(138) 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 ([237]).

(139) 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, en particular, 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; y llevar a cabo investigaciones.

(140) 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 ([238]). 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 ([239]).

(141) 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 llevar a cabo

([235]) 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.

([236]) 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 222.

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

([238]) De conformidad con la lectura combinada de la secciones 149, apartado 2, y 155 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. (Para más información sobre los avisos de ejecución y sanción, véanse los considerandos 102 y 103).

([239]) 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.

inspecciones de conformidad con las obligaciones internacionales, los poderes de entrada e inspección y las normas sobre infracciones ([240]). Como se explica en el considerando 136, estas excepciones se aplican solo si resulta necesario y proporcionado, y siempre caso por caso. La aplicación de dichas exenciones pueda ser objeto de un recurso judicial ([241]).

(142) La ICO y los servicios de inteligencia del Reino Unido han firmado un memorando de entendimiento ([242]) 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 reciba una reclamación, la ICO evaluará si se ha apelado de forma correcta a cualquiera de las exenciones relacionadas con la seguridad nacional. En virtud de la Guía del Gobierno del Reino Unido sobre certificados de seguridad nacional con arreglo a la *Data Protection Act*, debe darse respuesta 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 ([243]).

(143) Por su parte, el Intelligence and Security Committee (Comité de Inteligencia y Seguridad) realiza una supervisión parlamentaria del tratamiento de datos por parte de las agencias de inteligencia. El Comité tiene su fundamente jurídico en la *Justice and Security Act* 2013 (JSA de 2013) ([244]). Esta Ley establece al Intelligence and Security Committee como un comité del Parlamento del Reino Unido. 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 ([245]). El Intelligence and Security Committee debe presentar un informe anual al Parlamento sobre el desempeño de sus funciones y otros informes que considere oportunos ([246]).

(144) 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 los servicios de seguridad nacional. La JSA de 2013 también especifica que el Intelligence and

([240]) 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).

([241]) Véase, por ejemplo, el asunto *Baker v Secretary of State for the Home Department* (véase la nota a pie de página 221).

([242]) Memorando de entendimiento entre la ICO y la United Kingdom Intelligence Community; véase la nota a pie de página 231.

([243]) 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).

([244]) 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.

([245]) 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.

([246]) En el siguiente enlace pueden encontrarse los informes y declaraciones en línea del Intelligence and Security Committee: http://isc.independent.gov.uk/committee-reports. 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://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.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.

Security Committee puede realizar investigaciones sobre cuestiones operativas cuando estas no estén relacionadas con operaciones en curso ([247]). El memorando de entendimiento entre el primer ministro y el Intelligence and Security Committee ([248]) especifica en detalle los elementos que deben tenerse en cuenta al valorar si una actividad no forma parte de ninguna operación en curso ([249]). El primer ministro puede también solicitar al Intelligence and Security Committee que investigue operaciones en curso y puede revisar la información proporcionada voluntariamente por los servicios de seguridad nacional.

(145) 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 ([250]). Las autoridades del Reino Unido explicaron que, en la práctica, se oculta muy poca información al Intelligence and Security Committee ([251]).

(146) Por lo que respecta a la reparación, en primer lugar, en virtud de la sección 165, apartado 2, de la DPA de 2018, un interesado puede presentar una reclamación ante la ICO si cree que, en relación con los datos personales que le conciernen, se ha producido una violación de la parte 4 de la DPA de 2018, incluido cualquier uso abusivo de las derogaciones y restricciones en materia de seguridad nacional.

(147) 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 ([252]), a oponerse al tratamiento ([253]) y a la rectificación o supresión de los datos.

(148) 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 ([254]). Los daños incluyen tanto las pérdidas económicas como los daños que no implican pérdidas económicas, como puede ser la ansiedad ([255]).

(149) Por último, una persona puede presentar una reclamación ante el Investigatory Powers Tribunal (Tribunal de Poderes de Investigación) por cualquier conducta por parte de los servicios de inteligencia del Reino Unido, o efectuada en su nombre ([256]). El Investigatory Powers Tribunal (IPT) se estableció en virtud de la *Regulation of Investigatory Powers Act* de 2000 para Inglaterra, Gales e Irlanda del Norte y en virtud de la *Regulation of Investigatory Powers (Scotland) Act* 2000 para Escocia (RIPA de 2000), y es independiente del poder ejecutivo ([257]). En virtud de la sección 65 de la RIPA de 2000, Su Majestad nombra a los miembros del IPT por un período de cinco años.

(150) Los miembros del Tribunal pueden ser destituidos de su cargo por decisión de Su Majestad en respuesta a un discurso ([258]) de ambas cámaras del Parlamento ([259]).

(151) De conformidad con la sección 65 de la RIPA de 2000, para que una persona pueda presentar un recurso ante el IPT («requisito de legitimación») debe creer i) 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 ([260]), y ii) que la

([247]) Sección 2 de la JSA de 2013.
([248]) 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.
([249]) Apartado 14 del memorando de entendimiento entre el primer ministro y el Intelligence and Security Committee, véase la nota a pie de página 248.
([250]) 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).
([251]) Sección H del *UK Explanatory Framework for Adequacy Discussions* del Reino Unido: *National Security*, p. 43.
([252]) Sección 94, apartado 11, de la DPA de 2018.
([253]) Sección 99, apartado 4, de la DPA de 2018.
([254]) 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».
([255]) Sección 169, apartado 5, de la DPA de 2018.
([256]) Véase la sección 65, apartado 2, letra b), de la RIPA de 2000.
([257]) En virtud del anexo 3 de la RIPA de 2000, los miembros deben tener experiencia judicial concreta y pueden ser reelegidos para el cargo.
([258]) En relación con el concepto de «discurso», véase la nota a pie de página 183.
([259]) Párrafo primero, punto 5, del anexo 3, de la RIPA de 2000.
([260]) Sección 65, apartado 4, de la RIPA de 2000.

conducta se ha producido en «circunstancias impugnables» ([261]) o que «la han llevado a cabo los servicios de inteligencia o se ha llevado a cabo en su nombre» ([262]). Dado que, en particular, este estándar de «creencia» se ha interpretado de manera bastante difusa ([263]), llevar un caso ante el IPT está sujeto a requisitos de relativa baja legitimación.

(152) Cuando el IPT 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 ([264]). 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 ([265]).

(153) El IPT debe notificar al reclamante si ha habido una resolución a su favor o no ([266]). 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 o emitir otra medida que considere adecuada ([267]). 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.

(154) En concreto, una persona puede presentar una reclamación, y obtener reparación, ante el IPT si considera que una autoridad pública ha actuado (o se propone actuar) de forma incompatible con los derechos garantizados por el Convenio Europeo de Derechos Humanos, incluido el derecho a la privacidad y la protección de los datos y que es, en consecuencia, ilícita en virtud de la sección 6, apartado 1, de la *Human Rights Act* de 1998. El IPT tiene jurisdicción exclusiva para todas las reclamaciones relacionadas con la *Human Rights Act* que incumben a los servicios de inteligencia. 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 IPT 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 IPT es, en principio, susceptible de control jurisdiccional: véase *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ([268]). Si el IPT 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 ([269]).

([261]) 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).

([262]) 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 IPT 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 o 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.

([263]) 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*).

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

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

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

([267]) Esto puede incluir una orden que requiera la destrucción de cualquier registro de información en poder de una autoridad pública en relación con cualquier persona.

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

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

(155) Tras agotar los recursos nacionales, una persona puede obtener reparación ante el Tribunal Europeo de Derechos Humanos por violaciones de los derechos garantizados por el Convenio Europeo de Derechos Humanos, incluido el derecho a la privacidad y la protección de los datos.

(156) De lo anterior se deduce que el intercambio por parte de las autoridades encargadas de garantizar el cumplimiento del Derecho penal del Reino Unido de datos transferidos en virtud de la presente Decisión con otras autoridades públicas, incluidos los servicios de inteligencia, está enmarcado por limitaciones y condiciones que garantizan que dicho intercambio posterior será necesario y proporcionado y estará sujeto a garantías específicas de protección de datos con arreglo a la DPA de 2018. Además de lo anterior, organismos independientes supervisan el tratamiento de datos por parte de las autoridades públicas interesadas y las personas afectadas tienen acceso a recursos judiciales efectivos.

3. **CONCLUSIÓN**

(157) La Comisión considera que la parte 3 de la DPA de 2018 garantiza un nivel de protección de los datos personales transferidos a efectos de control de la aplicación del Derecho penal desde las autoridades competentes de la Unión a las autoridades competentes del Reino Unido que es esencialmente equivalente al que garantiza la Directiva (UE) 2016/680.

(158) 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.

(159) 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 especial en el contexto del intercambio de datos personales entre las autoridades encargadas de garantizar el cumplimiento de la ley y otras autoridades públicas, como los organismos 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.

(160) Por lo tanto, debe concluirse que el Reino Unido garantiza un nivel adecuado de protección a tenor del artículo 36, apartado 2, de la Directiva (UE) 2016/680, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

(161) 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.

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

(162) 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.

(163) Por lo tanto, toda decisión de adecuación adoptada por la Comisión en virtud del artículo 36, apartado 3, de la Directiva (UE) 2016/680 vincula a todos los órganos de los Estados miembros destinatarios, incluidas las 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 a responsables o encargados del tratamiento en el Reino Unido sin necesidad de obtener ninguna autorización adicional.

(164) Al mismo tiempo, cabe recordar que, de conformidad con el artículo 47, apartado 5, de la Directiva (UE) 2016/680 y como explicó el Tribunal de Justicia en la sentencia Maximillian Schrems, 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 ([270]).

([270]) *Schrems*, apartado 65.

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

(165) De conformidad con el artículo 36, apartado 4, de la Directiva (UE) 2016/680, 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 las transferencias de datos personales a terceros países, en particular mediante la celebración de acuerdos internacionales, y al impacto que pueda tener en el nivel de protección que se garantiza a los datos transferidos en virtud de la presente Decisión, así como a la eficacia del ejercicio de los derechos individuales en los ámbitos cubiertos por la presente Decisión. 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.

(166) Con el fin de facilitar esta supervisión, las autoridades del Reino Unido deben informar regular y 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, en particular en lo que respecta a los elementos señalados en el considerando 165.

(167) 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 Unión en relación con la transferencia de datos personales desde la UE a las autoridades competentes del 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, incluidos los órganos de supervisión, no garantizan el nivel de protección necesario.

(168) 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.

(169) 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 58, apartado 2, de la Directiva (UE) 2016/680 con el fin de suspender o derogar, total o parcialmente, esta Decisión.

(170) 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.

(171) 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 58, apartado 3, de la Directiva (UE) 2016/680, actos de ejecución inmediatamente aplicables que suspendan, deroguen o modifiquen la Decisión.

6. DURACIÓN Y RENOVACIÓN DE LA PRESENTE DECISIÓN

(172) Debe tenerse 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.

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

(174) 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 deberá adoptarse de conformidad con el procedimiento contemplado en el artículo 58, apartado 2, de la Directiva (UE) 2016/680.

7. **CONSIDERACIONES FINALES**

(175) El Comité Europeo de Protección de Datos publicó su dictamen ([271]), que se ha tomado en consideración en la elaboración de la presente Decisión.

(176) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité establecido en virtud del artículo 58 de la Directiva (UE) 2016/680.

(177) De conformidad con el artículo 6 *bis* del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea (TUE) y al Tratado de Funcionamiento de la Unión Europea (TFUE), no son vinculantes para Irlanda las normas establecidas en la Directiva (UE) 2016/680 y, por tanto, tampoco las establecidas en esta Decisión de Ejecución, relativas a tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, del TFUE en la medida en que no sean vinculantes para Irlanda las normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas sobre la base del artículo 16 del TFUE. Además, en virtud de la Decisión de Ejecución (UE) 2020/1745 del Consejo ([272]), la Directiva (UE) 2016/680 entrará en vigor y se aplicará con carácter provisional en Irlanda a partir del 1 de enero de 2021. Irlanda, por tanto, está vinculada por la presente Decisión de Ejecución, en las mismas condiciones que se aplican a la ejecución de la Directiva (UE) 2016/680 en el país, tal como se establece en la Decisión de Ejecución (UE) 2020/1745 en lo que respecta al acervo de Schengen, en el cual participa.

(178) De conformidad con lo dispuesto en los artículos 2 y 2 *bis* del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no está sujeta por las normas establecidas en la Directiva (UE) 2016/680 y, por tanto, tampoco por las establecidas en esta Decisión de Ejecución, que se relacionan con el tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, del TFUE, ni está sujeta a su aplicación. Sin embargo, dado que la Directiva (UE) 2016/680 se basa en el acervo de Schengen, Dinamarca, de conformidad con el artículo 4 de dicho Protocolo, notificó el 26 de octubre de 2016 su decisión de aplicar la Directiva (UE) 2016/680. Por lo tanto, Dinamarca está obligada por el Derecho internacional a aplicar la presente Decisión de Ejecución.

(179) Por lo que respecta a Islandia y Noruega, la presente Decisión de Ejecución constituye un desarrollo de las disposiciones del acervo de Schengen establecidas en el Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen ([273]).

(180) Por lo que respecta a Suiza, la presente Decisión de Ejecución constituye un desarrollo de las disposiciones del acervo de Schengen establecidas en el Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([274]).

(181) Por lo que respecta a Liechtenstein, la presente Decisión de Ejecución constituye un desarrollo de las disposiciones del acervo de Schengen establecidas en el Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([275]).

([271]) Dictamen 15/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con el Reglamento (UE) 2016/680 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-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Decisión de Ejecución (UE) 2020/1745 del Consejo, de 18 de noviembre de 2020, sobre la puesta en aplicación de las disposiciones del acervo de Schengen relativas a la protección de datos y sobre la puesta en aplicación provisional de determinadas disposiciones del acervo de Schengen en Irlanda (DO L 393 de 23.11.2020, p. 3).

([273]) DO L 176 de 10.7.1999, p. 36.

([274]) DO L 53 de 27.2.2008, p. 52.

([275]) DO L 160 de 18.6.2011, p. 21.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

A los efectos del artículo 36 de la Directiva (UE) 2016/680, el Reino Unido garantiza un nivel adecuado de protección para los datos personales transferidos de la Unión Europea a las autoridades públicas Reino Unido responsables de la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de su ejecución.

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 47 de la Directiva (UE) 2016/680 en relación con las transferencias de datos a autoridades públicas del Reino Unido dentro del 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 y se ejercen los derechos individuales, 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.

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 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 58, apartado 2, de la Directiva (UE) 2016/680.

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