Viernes 21 de mayo de 2021

P9_TA(2021)0262

Protección adecuada de los datos personales por parte del Reino Unido

Resolución del Parlamento Europeo, de 21 de mayo de 2021, sobre la protección adecuada de los datos personales por parte del Reino Unido (2021/2594(RSP))

(2022/C 15/23)

El Parlamento Europeo,

— Vista la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), en particular, sus artículos 7, 8, 16, 47 y 52,

— Vista la sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de 16 de julio de 2020, en el asunto C-311/18, Data Protection Commissioner / Facebook Ireland Limited y Maximillian Schrems (en lo sucesivo, «sentencia Schrems II») ([1]),

— Vista la sentencia del TJUE, de 6 de octubre de 2015, en el asunto C-362/14, Maximillian Schrems / Data Protection Commissioner (en lo sucesivo, «sentencia Schrems I») ([2]),

— Vista la sentencia del TJUE, de 6 de octubre de 2020, en el asunto C-623/17, Privacy International / Secretary of State for Foreign and Commonwealth Affairs ([3]),

— Vista su Resolución, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior ([4]),

— Vista su Resolución, de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU ([5]),

— Vista la Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos ([6]),

— Vista su Resolución, de 20 de mayo de 2021, sobre la sentencia del TJUE de 16 de julio de 2020, Data Protection Commissioner / Facebook Ireland Limited y Maximillian Schrems («Schrems II»), C-311/18 ([7]),

— Vista su Resolución, de 26 de noviembre de 2020, sobre la revisión de la política comercial de la UE ([8]),

— Visto el Acuerdo de Comercio y Cooperación, de 31 de diciembre de 2020, 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 ([9]),

— Vista su Resolución, de 28 de abril de 2021, sobre el resultado de las negociaciones entre la Unión Europea y el Reino Unido ([10]),

— Visto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ([11]) (Reglamento general de protección de datos — RGPD),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) DO C 378 de 9.11.2017, p. 104.
([5]) DO C 118 de 8.4.2020, p. 133.
([6]) DO C 345 de 16.10.2020, p. 58.
([7]) Textos Aprobados, P9_TA(2021)0256.
([8]) Textos Aprobados, P9_TA(2020)0337.
([9]) DO L 444 de 31.12.2020, p. 14.
([10]) Textos Aprobados, P9_TA(2021)0141.
([11]) DO L 119 de 4.5.2016, p. 1.

— 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 ([12]) (Directiva sobre protección de datos en el ámbito penal),

— Vista la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas ([13]),

— Vistas la propuesta de la Comisión, de 10 de enero de 2017, de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (COM(2017)0010) y la posición del Parlamento Europeo al respecto, adoptada el 20 de octubre de 2017 ([14]),

— Vistas las recomendaciones del Comité Europeo de Protección de Datos (CEPD), incluida su declaración de 9 de marzo de 2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas, y sus Recomendaciones 01/2020, de 10 de noviembre de 2020, sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE,

— Vistas las referencias sobre adecuación adoptadas por el Grupo de Trabajo del Artículo 29 el 6 de febrero de 2018 y respaldadas por el CEPD,

— Vistas las Recomendaciones 01/2021 del CEPD, de 2 de febrero de 2021, relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal,

— Vistas las propuestas de decisión de adecuación publicadas por la Comisión el 19 de febrero de 2021, una de conformidad con el RGPD ([15]) y la otra de conformidad con la Directiva sobre protección de datos en el ámbito penal ([16]),

— Vistos los dictámenes del CEPD 14/2021 y 15/2021, de 13 de abril de 2021, sobre el proyecto de Decisión de Ejecución de la Comisión de conformidad con la Directiva (UE) 2016/680 relativa a la protección adecuada de los datos personales por parte del Reino Unido,

— Vistos el Convenio Europeo de Derechos Humanos (CEDH) y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa, así como su protocolo de enmienda («Convenio 108+»), en el que el Reino Unido es parte,

— Visto el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por los Estados miembros del ejercicio de las competencias de ejecución por la Comisión,

— Visto el artículo 132, apartado 2, de su Reglamento interno,

— Vista la propuesta de Resolución de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior,

A. Considerando que la capacidad de transferir datos personales a través de las fronteras puede ser un motor fundamental de innovación, productividad y competitividad económica, y que reviste una importancia crucial de cara a una cooperación eficaz en la lucha contra la delincuencia organizada y grave transfronteriza y contra el terrorismo, que depende cada vez más del intercambio de datos personales;

B. Considerando que, en la sentencia Schrems I, el TJUE señaló que el acceso indiscriminado al contenido de las comunicaciones electrónicas por parte de las autoridades de inteligencia lesiona la esencia del derecho a la confidencialidad de las comunicaciones garantizado por el artículo 7 de la Carta y que los Estados Unidos no prevén vías de recurso suficientes contra la vigilancia masiva para los ciudadanos no estadounidenses, lo que vulnera el artículo 47 de la Carta;

([12]) DO L 119 de 4.5.2016, p. 89.
([13]) DO L 201 de 31.7.2002, p. 37.
([14]) A8-0324/2017.
([15]) Proyecto de Decisión de Ejecución de la Comisión de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativa a la protección adecuada de los datos personales por parte del Reino Unido.
([16]) Proyecto de Decisión de Ejecución de la Comisión de conformidad con 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.

C. Considerando que el Reino Unido ha sido tradicionalmente un importante socio comercial de muchos Estados miembros de la Unión, así como un estrecho aliado en el ámbito de la seguridad; que la Unión Europea y el Reino Unido deben mantener esta estrecha cooperación a pesar de la retirada del Reino Unido de la Unión, ya que será beneficiosa para ambas partes;

D. Considerando que las empresas europeas necesitan claridad y seguridad jurídicas, ya que la capacidad de transferir datos personales a través de las fronteras es cada vez más importante para todos los tipos de empresas que suministran bienes y servicios a escala internacional; que una decisión de adecuación relativa al Reino Unido en virtud del RGPD reviste una suma importancia, ya que muchas empresas europeas realizan intercambios comerciales a través del canal de la Mancha, en particular teniendo en cuenta que el Brexit sigue siendo muy reciente y que los flujos de datos dentro de la Unión no han estado sujetos a restricciones; que un fracaso en la adopción de un marco de adecuación sólido podría afectar a las transferencias comerciales transfronterizas de datos personales entre la Unión y el Reino Unido, así como generar unos elevados costes de conformidad;

E. Considerando que el Acuerdo de Comercio y Cooperación incluye una serie de salvaguardias y condiciones para el intercambio de datos personales pertinentes en el contexto de la exigencia del cumplimiento de la ley; que las negociaciones sobre los flujos de datos personales se llevaron a cabo en paralelo a las negociaciones sobre el Acuerdo de Comercio y Cooperación, pero no habían concluido al final del período de transición, el 31 de diciembre de 2020; que en el Acuerdo de Comercio y Cooperación se incluyó una «cláusula pasarela» como solución provisional, supeditada al compromiso del Reino Unido de no modificar su actual régimen de protección de datos, a fin de garantizar la continuidad de los flujos de datos personales entre el Reino Unido y la Unión hasta la adopción de una decisión de adecuación; que el período inicial de cuatro meses se ha prorrogado y expirará a finales de junio de 2021;

F. Considerando que la evaluación llevada a cabo por la Comisión antes de presentar su proyecto de decisión de ejecución es incompleta y no está en consonancia con los requisitos del TJUE para las evaluaciones de adecuación, como puso de relieve el CEPD en sus dictámenes sobre la adecuación, en los que recomienda a la Comisión que evalúe ulteriormente aspectos específicos de la legislación y la práctica del Reino Unido relativas a la recopilación masiva, la divulgación en el extranjero y los acuerdos internacionales en el ámbito del intercambio de información de inteligencia, el uso adicional de la información recopilada con fines de exigencia de cumplimiento de la ley y la independencia de los comisionados judiciales;

G. Considerando que la Comisión no ha tenido en cuenta determinados aspectos de la legislación o la práctica del Reino Unido, lo que ha dado lugar a proyectos de decisiones de ejecución que no son coherentes con el Derecho de la Unión; que el artículo 45 del RGPD establece que, al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular «[…] la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, […]» y «[…] los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales», lo que incluye los acuerdos internacionales en otros ámbitos que conlleven el acceso a datos o el intercambio de información y, por tanto, requiere una evaluación de esos acuerdos internacionales;

H. Considerando que el TJUE estableció con claridad en su sentencia Schrems I que «[…] al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de este, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de la Directiva 95/46/CE» (apartado 75);

I. Considerando que las actividades de los servicios de inteligencia y el intercambio con terceros países están excluidos del ámbito de aplicación del Derecho de la Unión con arreglo a los Tratados en lo que respecta a los Estados miembros, pues se incluyen en el ámbito de la necesaria evaluación de la adecuación del nivel de datos personales ofrecido por terceros países, como confirmó el TJUE en las sentencias Schrems I y II;

J. Considerando que las normas de protección de datos no solo se basan en la legislación vigente, sino también en su aplicación práctica, y que la Comisión solo evaluó la legislación, pero no su aplicación efectiva en la práctica, al preparar su decisión;

K. Considerando que la Comisión reconoce actualmente que doce terceros países proporcionan una protección suficiente en virtud del RGPD y ha concluido recientemente conversaciones con la República de Corea a este respecto; que el Reino Unido es el primer país al que la Comisión ha propuesto conceder la adecuación en virtud de la Directiva sobre protección de datos en el ámbito penal;

L. Considerando que el caso del Reino Unido difiere de todas las evaluaciones de adecuación anteriores, ya que afecta a un antiguo Estado miembro de la Unión que ha incorporado las disposiciones del RGPD a su legislación nacional y que, además, ha establecido que toda la legislación nacional derivada de la Unión, incluida la legislación de transposición de la Directiva sobre protección de datos en el ámbito penal, seguirá aplicándose una vez finalizado el período de transición;

I. **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS**

Observaciones generales

1. Señala que el Reino Unido es signatario del CEDH y del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; espera que el Reino Unido garantice el mismo marco mínimo en materia de protección de datos, a pesar de haber abandonado la Unión Europea;

2. Acoge con satisfacción el compromiso del Reino Unido de respetar la democracia y el Estado de Derecho y de proteger y dar efecto a nivel nacional a los derechos fundamentales, como los establecidos en el CEDH, incluidos los elevados niveles de protección de datos; recuerda que se trata de una condición previa necesaria para la cooperación de la Unión con el Reino Unido; recuerda que, a pesar de que el artículo 8 del CEDH sobre el derecho a la intimidad forme parte de la legislación nacional del Reino Unido a través de la Ley de derechos humanos de 1998 (Human Rights Act 1998), así como del *common law* a través del nuevo acto ilícito civil de uso indebido de la información personal (*tort of misuse of privacy information*), el Gobierno votó en contra de los esfuerzos por incluir un derecho fundamental a la protección de datos;

3. Señala que la Unión ha optado por un enfoque centrado en los derechos humanos en lo que se refiere a la gobernanza de los datos a la hora de desarrollar normas sólidas en materia de protección de datos en el marco del RGPD, y manifiesta, por tanto, su profunda preocupación por las declaraciones públicas del primer ministro del Reino Unido en las que declara que dicho país intentará desviarse de las normas de protección de datos de la Unión y establecer sus propios controles «soberanos» en este ámbito; considera que la estrategia nacional de datos del Reino Unido de 2020 representa un cambio que va de la protección de los datos personales a un uso y un intercambio más amplios de los datos incompatible con los principios de lealtad, minimización de datos y limitación de la finalidad propugnados en el RGPD; observa que, en sus dictámenes sobre la adecuación, el CEPD destacó que este hecho podría generar riesgos en la protección de los datos personales transferidos desde la Unión;

4. Señala que las decisiones de adecuación válidas contribuyen en gran medida a la protección de los derechos fundamentales de las personas y a la seguridad jurídica de las empresas; subraya, no obstante, que las decisiones de adecuación basadas en evaluaciones incompletas y sin una aplicación adecuada por parte de la Comisión pueden dar lugar al efecto contrario si se impugnan ante los tribunales;

5. Señala que la evaluación llevada a cabo por la Comisión antes de presentar su proyecto de decisión de ejecución era incompleta y no conforme con los requisitos del TJUE para las evaluaciones de adecuación, como puso de relieve el CEPD en sus dictámenes sobre la adecuación, en los que recomienda a la Comisión que evalúe ulteriormente aspectos específicos de la legislación y la práctica del Reino Unido relativas a la recopilación masiva, la divulgación en el extranjero y los acuerdos internacionales en el ámbito del intercambio de información de inteligencia, el uso adicional de la información recopilada con fines de exigencia de cumplimiento de la ley y la independencia de los comisionados judiciales;

Aplicación del RGPD

6. Expresa su preocupación por el cumplimiento deficiente y, a menudo, inexistente del RGPD por parte del Reino Unido cuando aún era miembro de la Unión; señala, en concreto, la falta de un cumplimiento adecuado por parte de la Oficina del Comisionado de Información del Reino Unido en el pasado; pone de relieve el ejemplo del archivo por parte de la Oficina del Comisionado de Información de una reclamación sobre tecnologías de la publicidad después de mantener dos encuentros con partes interesadas, redactar un informe [titulado «Update Report on Adtech» (Informe actualizado sobre las tecnologías de la publicidad)] y afirmar que la industria de las tecnologías de la publicidad parece mostrar inmadurez a la

hora de comprender los requisitos en materia de protección de datos, sin recurrir a ninguna de sus facultades para exigir el cumplimiento de la ley ([17]); manifiesta su preocupación por que este incumplimiento sea un problema estructural, recogido en el documento titulado «Regulatory Action Policy» (Política de acciones regulatorias) de la Oficina del Comisionado de Información, donde se afirma explícitamente que en la mayoría de los casos reserva sus facultades para los asuntos más graves, que representan los incumplimientos más graves de las obligaciones relativas a los derechos de información, y que estos asuntos comportan normalmente actos voluntarios, deliberados o por negligencia, o incumplimientos reiterados de obligaciones relativas a los derechos de información, que causan daños o perjuicios a las personas; subraya que, en la práctica, esta situación ha supuesto que no se hayan subsanado un gran número de infracciones de la legislación en materia de protección de datos en el Reino Unido;

7. Toma nota de la estrategia nacional de datos del Reino Unido, en su versión actualizada el 9 de diciembre de 2020, que sugiere que se producirá un cambio de la protección de los datos personales hacia un uso y un intercambio más amplios de los datos; señala que una posición descrita en la estrategia, según la cual «retener datos puede afectar negativamente a la sociedad», no es compatible con los principios de minimización de datos y limitación de la finalidad establecidos en el RGPD y el Derecho primario;

8. Toma nota de que la Comisión de Asuntos Constitucionales en 2004 ([18]) y la Comisión de Asuntos Públicos del Parlamento del Reino Unido en 2014 ([19]) recomendaron garantizar la independencia del Comisionado de Información convirtiéndolo en un funcionario del Parlamento que responda ante esta institución, en lugar de seguir siendo nombrado por el Departamento de Asuntos Digitales, Cultura, Medios de Comunicación y Deporte; lamenta que esta recomendación no haya sido objeto de seguimiento;

Tratamiento de datos para el control de la inmigración

9. Señala que la legislación del Reino Unido en materia de protección de datos contiene una excepción a determinados aspectos fundamentales de los derechos y principios de la protección de datos, como el derecho de acceso y el derecho del interesado a saber con quién se han intercambiado sus datos, en caso de que tal protección perjudique al control efectivo de la inmigración[20]; subraya que la supervisión y el cumplimiento del uso de la exención deben llevarse a cabo de conformidad con las normas exigidas en las referencias sobre adecuación, que exigen tener en cuenta tanto la práctica como el principio, al señalar que es necesario tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema establecido para garantizar la eficacia de dichas normas; reconoce que la aplicación de esta exención, que está al alcance de todos los responsables del tratamiento de datos en el Reino Unido, ha sido respaldada por la OCI y un tribunal y que solo puede invocarse caso por caso y aplicarse de manera necesaria y proporcionada; recuerda la información recientemente publicada según la cual entre el 1 de abril de 2018 y el 31 de marzo de 2019 se presentaron 17 780 solicitudes de acceso en relación con datos tratados relativos a 146,75 millones de interesados y de que esta exención relacionada con la inmigración se utilizó en más del 70 % de las solicitudes de interesados presentadas ante el Ministerio del Interior del Reino Unido en 2020 ([20]); destaca que, incluso en los casos en que el Ministerio del Interior del Reino Unido hizo uso de la excepción, no se denegó por completo el acceso a la información, sino que se limitó a los documentos censurados;

10. Señala que actualmente esta exención se aplica a los ciudadanos de la Unión que residan o tengan previsto residir en el Reino Unido; expresa su profunda preocupación por que la exención elimina oportunidades clave en lo que respecta a la rendición de cuentas y las vías de recurso, y subraya que este nivel de protección no es adecuado;

([17]) Lomas, N.: *UK's ICO faces legal action after closing adtech complaint with nothing to show for it* (La Oficina del Comisionado de Información se enfrenta a acciones legales tras archivar sin pruebas una denuncia sobre tecnología de la publicidad), TechCrunch, San Francisco, 2020.

([18]) Séptimo informe de la Comisión Especial de Asuntos Constitucionales, publicado por la Cámara de los Comunes el 13 de junio de 2006. En su apartado 108 puede leerse lo siguiente: «We see considerable merit in the Information Commissioner becoming directly responsible to, and funded by, Parliament, and recommend that such a change be considered when an opportunity arises to amend the legislation» (Observamos ventajas considerables en que el Comisionado de Información pase a ser directamente responsable ante el Parlamento y financiado por este, y recomendamos que se sopese este cambio cuando surja una oportunidad de modificar la legislación).

([19]) Informe de la Comisión de Administración Pública titulado «Who's accountable? Relationships between Government and arm's-length bodies» (¿Quién es responsable? Relaciones entre el Gobierno y los organismos independientes), publicado por la Cámara de los Comunes el 4 de noviembre de 2014. En su apartado 64 puede leerse lo siguiente: «The Information Commissioner and HM Inspectorate of Prisons should be more fully independent of Government and should report to Parliament. The Information Commissioner, Commissioner for Public Appointments and the Chair of the Committee on Standards in Public Life should become Officers of Parliament, as the Parliamentary and Health Service Ombudsman and the Comptroller and Auditor General already are» (El Comisionado de Información y la Inspección de Prisiones deben ser aún más independientes del Gobierno y depender del Parlamento. El Comisionado de Información, el Comisionado de Nombramientos Públicos y el presidente de la Comisión de Normas del Servicio Público deben pasar a ser funcionarios del Parlamento, como ya lo son el Defensor del Pueblo Parlamentario y del Sistema de Salud y el Interventor y Auditor General).

([20]) Comunicado de prensa de Open Rights Group, de 3 de marzo de 2021, titulado «Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office» (Los documentos revelan que una controvertida exención relacionada con la inmigración se ha aplicado en el 70 % de las solicitudes de acceso ante el Ministerio del Interior).

11. Reitera su profunda preocupación por una excepción a los derechos de los interesados en la política de inmigración del Reino Unido; reafirma su posición de que la exención en el tratamiento de datos personales a efectos de inmigración en virtud de la Ley de protección de datos del Reino Unido debe modificarse antes de que pueda pronunciarse una decisión de adecuación válida, como ya expresó en repetidas ocasiones, por ejemplo, en su Resolución, de 12 de febrero de 2020, sobre el mandato propuesto para las negociaciones de una nueva asociación con el Reino Unido de Gran Bretaña e Irlanda del Norte ([21]) y en la opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 5 de febrero de 2021 ([22]); pide a la Comisión que intente eliminar la exención para la inmigración, o que vele por que se reforme a fin de que la exención y su uso ofrezcan garantías suficientes a los interesados y no infrinjan las normas que se esperan de un tercer país;

Vigilancia masiva

12. Recuerda las revelaciones sobre una vigilancia masiva por parte de los Estados Unidos y el Reino Unido, hechas por el denunciante Edward Snowden; recuerda que el programa Tempora del Reino Unido, gestionado por su Centro Gubernamental de Comunicaciones (GCHQ, por sus siglas en inglés), intercepta las comunicaciones en tiempo real mediante cables de fibra óptica de la red principal de internet y registra los datos para que puedan tratarse y buscarse posteriormente; recuerda que esta vigilancia masiva del contenido y los metadatos de las comunicaciones se lleva a cabo independientemente de que existan sospechas concretas o datos objetivo;

13. Recuerda que, en las sentencias Schrems I (sistema de puerto seguro) y Schrems II (Escudo de la privacidad), el TJUE sostuvo que el acceso masivo al contenido de las comunicaciones privadas afecta a la esencia del derecho a la privacidad y que, en tales casos, deja de ser necesaria una prueba de necesidad y proporcionalidad; subraya que estos principios se aplican a las transferencias de datos a terceros países distintos de los EE. UU., incluido el Reino Unido;

14. Recuerda su Resolución, de 12 de marzo de 2014, que constató que los programas de vigilancia masiva llevados a cabo por la agencia de inteligencia británica GCHQ de una manera indiscriminada y no basada en sospechas son incompatibles con los principios de necesidad y proporcionalidad en una sociedad democrática y no son adecuados según el Derecho de la Unión en materia de protección de datos; reconoce que el Reino Unido ha reformado significativamente desde entonces sus leyes sobre vigilancia y ha introducido garantías que van más allá de las condiciones definidas por el Tribunal de Justicia de la Unión Europea (TJUE) en su sentencia Schrems II ([23]) y las garantías previstas en las leyes sobre vigilancia de la mayoría de los Estados miembros; acoge con satisfacción, en particular, la concesión de pleno acceso a un recurso judicial efectivo; recuerda que el Relator Especial de las Naciones Unidas sobre el derecho a la privacidad ha acogido con satisfacción las sólidas salvaguardas introducidas con la Ley sobre regulación de las facultades de investigación (Investigatory Powers Act o IPA) de 2016 en lo que atañe a la necesidad, la proporcionalidad y la autorización independiente por parte de un órgano judicial;

15. Recuerda que, en septiembre de 2018, el Tribunal Europeo de Derechos Humanos confirmó que los programas de interceptación y conservación masiva de datos del Reino Unido, incluido Tempora, eran ilegales e incompatibles con las condiciones necesarias para una sociedad democrática ([24]);

16. Considera inaceptable que las propuestas de decisión de adecuación no tengan en cuenta la falta de limitaciones en el uso de las competencias del Reino Unido en materia de datos en masa ni el uso que se hace realmente de las operaciones de vigilancia del Reino Unido y los EE. UU., tal como expuso Edward Snowden, especialmente los hechos siguientes:

a) no existe una supervisión sustantiva efectiva por parte de la Oficina del Comisionado de Información o de órganos jurisdiccionales sobre el uso de la exención de seguridad nacional en el Derecho del Reino Unido en materia de protección de datos;

b) las limitaciones al uso de «competencias en masa» del Reino Unido no están establecidas en la propia legislación, tal como exige el TJUE (sino que se dejan a la discreción del poder ejecutivo, con sujeción a un control judicial «respetuoso»);

([21]) Textos Aprobados, P9_TA(2020)0033.

([22]) Opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior sobre la celebración, en nombre de la Unión, del Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra, y del Acuerdo entre la Unión Europea y el Reino Unido de Gran Bretaña e Irlanda del Norte sobre procedimientos de seguridad para el intercambio y la protección de información clasificada, LIBE_AL (2021)680848.

([23]) Sentencia de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

([24]) Sentencia del Tribunal Europeo de Derechos Humanos, de 13 de septiembre de 2018, Big Brother Watch y otros / Reino Unido, solicitudes n.os 58170/13, 62322/14 y 24960/15.

c) la descripción de «datos secundarios» (metadatos) recogida en las propuestas de decisión es gravemente engañosa y no observa que estos datos pueden ser muy reveladores e intrusivos y están sujetos a sofisticados análisis automatizados (como consideró el TJUE en la sentencia Digital Rights Ireland ([25])), pero, con arreglo a la legislación del Reino Unido, los metadatos no están protegidos de manera significativa contra el acceso indebido, la recopilación masiva y el análisis basado en la inteligencia artificial por parte de las agencias de inteligencia del Reino Unido;

d) las agencias de la alianza «Five Eyes», en particular el GCHQ y la Agencia Nacional de Seguridad, comparten en la práctica todos los datos de inteligencia;

señala asimismo que, en relación con los Estados Unidos, los ciudadanos del Reino Unido están sujetos a algunas salvaguardias informales entre el GCHQ y la Agencia Nacional de Seguridad; expresa su profunda preocupación por el hecho de que estas salvaguardias no protejan a los ciudadanos o residentes de la Unión cuyos datos puedan ser objeto de transferencias ulteriores y de intercambio con la Agencia Nacional de Seguridad;

17. Pide a los Estados miembros que celebren acuerdos de «no espionaje» con el Reino Unido y pide a la Comisión que utilice sus intercambios con sus homólogos británicos para transmitir el mensaje de que, si el Reino Unido no modifica sus leyes y prácticas de vigilancia, la única opción viable para facilitar las decisiones de adecuación sería la celebración de acuerdos de «no espionaje» con los Estados miembros;

Transferencias ulteriores

18. Insiste enérgicamente en que la Ley sobre (la retirada de) la Unión Europea de 2018 [European Union (Withdrawal) Act 2018] establece que la jurisprudencia del TJUE generada antes del final del período de transición pasará a ser «Derecho de la Unión conservado» y, por tanto, jurídicamente vinculante para el Reino Unido; señala que el Reino Unido está vinculado por los principios y las condiciones definidos en las sentencias Schrems I y Schrems II del TJUE a la hora de evaluar la adecuación de otros terceros países; expresa su preocupación por que, pese a ello, los tribunales del Reino Unido dejarán de aplicar la Carta; señala que el Reino Unido ya no está bajo la jurisdicción del TJUE, que es la instancia suprema que puede interpretar la Carta;

19. Señala que las normas del Reino Unido sobre el intercambio de datos personales en virtud de la Ley de economía digital de 2017 (Digital Economy Act 2017) y sobre las transferencias ulteriores de datos de investigación, claramente, no son «esencialmente equivalentes» a las normas establecidas en el RGPD, según la interpretación del TJUE;

20. Expresa su preocupación por el hecho de que el Reino Unido se haya otorgado el derecho a declarar que otros terceros países o territorios ofrecen una protección de datos adecuada, independientemente de que la Unión haya considerado que el tercer país o territorio en cuestión ofrece tal protección; recuerda que el Reino Unido ya ha declarado que Gibraltar ofrece tal protección, a pesar de que la Unión no lo haya hecho; expresa su profunda preocupación por el hecho de que un estado de adecuación para el Reino Unido conduciría, por tanto, a la elusión de las normas de la Unión sobre transferencias a países o territorios que no se consideren adecuados con arreglo al Derecho de la Unión;

21. Toma nota de que, el 1 de febrero de 2021, el Reino Unido presentó una solicitud para adherirse a la asociación resultante del Tratado Integral y Progresista de Asociación Transpacífico (CPTPP, por sus siglas en inglés), en particular para beneficiarse de las normas modernas de comercio digital que permiten la libre circulación de datos entre los miembros, eliminan obstáculos innecesarios para las empresas, etc.; observa con preocupación que el CPTPP cuenta con once miembros, ocho de los cuales no tienen una decisión de adecuación de la Unión; expresa su profunda preocupación por las posibles transferencias ulteriores de datos personales de ciudadanos y residentes de la Unión a estos países en caso de concederse al Reino Unido una decisión de adecuación ([26]);

([25]) Sentencia del Tribunal de Justicia, de 8 de abril de 2014, Digital Rights Ireland Ltd / Ministro de Comunicaciones, Asuntos Marítimos y Recursos Naturales y otros y Kärntner Landesregierung y otros, asuntos C-293/12 y C-594/12, ECLI:EU:C:2014:238.

([26]) Comunicado de prensa del Departamento de Comercio Internacional del Reino Unido, de 30 de enero de 2021, titulado «UK applies to join huge Pacific free trade area CPTPP» (El Reino Unido solicita unirse al CPTPP, la gran zona de libre comercio del Pacífico).

22. Lamenta que la Comisión no haya evaluado el impacto y los posibles riesgos del Acuerdo de Asociación Económica Global entre el Reino Unido de Gran Bretaña e Irlanda del Norte y Japón, que incluye disposiciones sobre datos personales y sobre el nivel de protección de datos;

23. Expresa su preocupación por el hecho de que, si el Reino Unido incluyera disposiciones sobre transferencias de datos en cualquier futuro acuerdo comercial, entre otros, los acuerdos comerciales entre los Estados Unidos y el Reino Unido, el nivel de protección que ofrece el RGPD se vería socavado;

II. **DIRECTIVA SOBRE PROTECCIÓN DE DATOS EN EL ÁMBITO PENAL**

24. Destaca que el Reino Unido es el primer país para el que la Comisión ha sugerido la adopción de una decisión de adecuación en virtud de la Directiva (UE) 2016/680;

25. Toma nota del acuerdo, entre el Reino Unido y los Estados Unidos, relativo al acceso transfronterizo a los datos ([27]), en el marco de la Ley CLOUD estadounidense, que facilita las transferencias con fines policiales; expresa su profunda preocupación por que esto vaya a permitir a las autoridades estadounidenses acceder indebidamente a los datos personales de los ciudadanos y residentes de la Unión; comparte la preocupación del CEPD de que las salvaguardias previstas en el Acuerdo marco UE-EE. UU. ([28]), aplicado *mutatis mutandis*, pueden no cumplir los criterios de normas claras, precisas y accesibles en lo que respecta al acceso a los datos personales, o podrían no consagrar suficientemente dichas salvaguardas para que sean efectivas y aplicables con arreglo al Derecho del Reino Unido;

26. Recuerda que la sentencia del TJUE C-623/17 debe interpretarse en el sentido de que se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiscriminada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia estatales con el fin de proteger la seguridad nacional;

27. Observa que, en este asunto, el TJUE dictaminó que la recopilación masiva de datos llevada a cabo en el Reino Unido en virtud de la Ley sobre regulación de las facultades de investigación de 2000 (Regulation of Investigatory Powers Act 2000) era ilegal; señala que esta fue sustituida posteriormente por la Ley sobre facultades de investigación de 2016 (Investigatory Powers Act 2016; en lo sucesivo, «IPA 2016») con el fin de reforzar los principios de necesidad y proporcionalidad; subraya que la IPA 2016 somete la interceptación a supervisión judicial y faculta a las personas para acceder a sus datos y presentar reclamaciones ante el tribunal encargado de las facultades de investigación (investigatory powers tribunal); lamenta, no obstante, que la IPA 2016 siga permitiendo la práctica de la conservación masiva de datos;

28. Manifiesta su preocupación por las informaciones recientes según las cuales un sistema de recopilación y conservación masiva de datos forma parte de una serie de ensayos realizados por el Ministerio del Interior del Reino Unido en el marco de la IPA 2016;

29. Recuerda que, en su Resolución de 12 de febrero de 2020, el Parlamento Europeo destacó que «el Reino Unido no puede tener acceso directo a los datos de los sistemas de información de la Unión ni participar en las estructuras de gestión de las agencias de la Unión del espacio de libertad, seguridad y justicia, y que cualquier intercambio de información con el Reino Unido, incluidos los datos personales, debe estar sujeto a estrictas condiciones de salvaguardia, auditoría y supervisión, incluido un nivel de protección de los datos personales equivalente al previsto por el Derecho de la Unión»; toma nota de las deficiencias detectadas en la manera en que el Reino Unido aplicó la legislación en materia de protección de datos mientras seguía siendo miembro de la Unión; recuerda que el Reino Unido estaba copiando el Sistema de Información de Schengen (SIS) y manteniendo dicha copia; espera que los servicios encargados de la ejecución de las leyes del Reino Unido cumplan plenamente las normas aplicables al intercambiar datos personales en el futuro; recuerda que el Reino Unido conserva el acceso a algunas bases de datos de las autoridades policiales de la Unión únicamente con arreglo a un sistema de respuesta positiva o negativa, y que se encuentra legalmente excluido del acceso al SIS;

([27]) Acuerdo entre el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte y el Gobierno de los Estados Unidos de América, de 3 de octubre de 2019, sobre el acceso a los datos electrónicos con fines de lucha contra los delitos graves.

([28]) Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales (DO L 336 de 10.12.2016, p. 3).

30. Expresa su preocupación por las revelaciones de enero de 2021 de que se suprimieron accidentalmente 400 000 antecedentes penales de la aplicación informática nacional de la policía del Reino Unido; destaca que ello no inspira confianza en los esfuerzos del Reino Unido por proteger los datos con fines policiales;

31. Observa que la propuesta de decisión de adecuación evalúa exhaustivamente los derechos de cada autoridad del Reino Unido facultada por la legislación nacional para interceptar y conservar datos personales por motivos de seguridad nacional; acoge favorablemente, además, el hecho de que los informes de supervisión pormenorizados sobre las autoridades encargadas de los servicios de inteligencia proporcionen información relativa a las prácticas actuales de vigilancia del Reino Unido; pide a la Comisión que siga evaluando y supervisando los tipos de datos de comunicaciones que entran en el ámbito de las competencias de conservación de datos y de interceptación legal del Reino Unido;

32. Señala que el Acuerdo de Comercio y Cooperación entre la Unión Europea y el Reino Unido incluye títulos relativos al intercambio de datos de ADN, impresiones dactilares y matriculación de vehículos; la transferencia y el tratamiento de los datos del registro de nombres de los pasajeros (PNR, por sus siglas en inglés); la cooperación en materia de información operativa, y la cooperación con Europol y Eurojust, que serán aplicables independientemente de la decisión de adecuación; recuerda, no obstante, las preocupaciones expresadas en la opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de febrero de 2021, sobre el Acuerdo de Comercio y Cooperación, en relación con el uso especial y la conservación prolongada de los datos personales concedidos al Reino Unido en virtud de los títulos Prüm y PNR del Acuerdo de Comercio y Cooperación, que no están en consonancia con el uso y la conservación por parte de los diferentes Estados miembros; recuerda el derecho a interponer un recurso ante el TJUE con el fin de comprobar la legalidad del acuerdo internacional propuesto y, en particular, su compatibilidad con la protección de un derecho fundamental ([29]);

Conclusiones

33. Pide a la Comisión que garantice a las empresas de la Unión que la decisión de adecuación proporcionará una base jurídica sólida, suficiente y orientada al futuro para las transferencias de datos; subraya la importancia de garantizar que esta decisión de adecuación se considere aceptable si es revisada por el TJUE, y recalca que, por lo tanto, deben tenerse en cuenta todas las recomendaciones formuladas en el dictamen del CEPD;

34. Acoge con satisfacción el hecho de que las decisiones de adecuación solo se apliquen durante cuatro años, ya que el Reino Unido podría optar por modificar la legislación sujeta a la evaluación de adecuación de la Comisión ahora que ya no es un Estado miembro de la Unión; pide a la Comisión que, entretanto, siga supervisando el nivel de protección de datos en el Reino Unido tanto en lo que respecta a su legislación como en la práctica, y que realice una evaluación exhaustiva antes de renovar la decisión de adecuación en 2025;

35. Opina que, al adoptar las dos decisiones de ejecución, que no son coherentes con el Derecho de la Unión, sin haber resuelto todas las preocupaciones expresadas en la presente Resolución, la Comisión va más allá de las competencias de ejecución que le confieren el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680; se opone, por tanto, a los dos actos de ejecución porque los proyectos de decisiones de ejecución no son coherentes con el Derecho de la Unión;

36. Pide a la Comisión que modifique los dos proyectos de decisiones de ejecución con el fin de que sean plenamente coherentes con el Derecho y la jurisprudencia de la Unión;

37. Pide a las autoridades nacionales de protección de datos que suspendan la transferencia de datos personales a los que puedan acceder indiscriminadamente las autoridades de inteligencia británicas, en caso de que la Comisión adopte sus decisiones de adecuación en relación con el Reino Unido antes de que este país resuelva los problemas anteriormente mencionados;

38. Pide a la Comisión y a las autoridades competentes del Reino Unido que fijen un plan de acción para abordar cuanto antes las deficiencias detectadas en los dictámenes del CEPD y otras cuestiones pendientes en materia de protección de datos en el Reino Unido, que debe ser una condición previa para la decisión final sobre la adecuación;

39. Pide a la Comisión que siga supervisando de cerca el nivel de protección de datos, así como la legislación y las prácticas en materia de vigilancia masiva en el Reino Unido; señala que existen otras posibilidades jurídicas para la transferencia de datos personales al Reino Unido, contempladas en el capítulo V del RGPD; recuerda que, en consonancia con las directrices del CEPD, las transferencias amparadas en las excepciones para situaciones específicas previstas en el artículo 49 del RGPD han de tener carácter excepcional;

([29]) Resolución del Parlamento Europeo sobre el proyecto de Decisión de la Comisión por la que se determina el nivel de protección adecuado de los datos personales incluidos en los registros de nombres de pasajeros aéreos (PNR) transferidos a la Oficina de Aduanas y Protección de Fronteras de los Estados Unidos (DO C 103 E de 29.4.2004, p. 665).

40. Lamenta que la Comisión haya ignorado los llamamientos del Parlamento a suspender el Escudo de la privacidad hasta que las autoridades estadounidenses cumplan sus condiciones y haya preferido siempre «supervisar la situación» sin ningún resultado concreto en cuanto a protección de datos para las personas y seguridad jurídica para las empresas; insta a la Comisión a que aprenda de los errores del pasado, cuando desoyó los llamamientos del Parlamento y de expertos relativos a la conclusión y supervisión de anteriores decisiones de adecuación, y a que no deje al TJUE la correcta aplicación de la legislación de la Unión en materia de protección de datos a partir de reclamaciones de particulares;

41. Pide a la Comisión que supervise de cerca la legislación y las prácticas en materia de protección de datos en el Reino Unido e informe de inmediato y consulte al Parlamento acerca de cualquier modificación futura del régimen de protección de datos del Reino Unido, y que otorgue al Parlamento un papel de control en el nuevo marco institucional, también de organismos pertinentes como el Comité Especializado en Cooperación Policial y Judicial;

o

o o

42. Encarga a su presidente que transmita la presente Resolución a la Comisión, a los Estados miembros y al Gobierno del Reino Unido.