LA REGULACIÓN DEL FLUJO DE DATOS PERSONALES ENTRE LA UNIÓN EUROPEA Y EL REINO UNIDO TRAS EL BREXIT

THE REGULATION OF THE FLOW OF PERSONAL DATA BETWEEN THE EUROPEAN UNION AND THE UNITED KINGDOM AFTER BREXIT

Ana Gascón Marcén
Profesora Contratada Doctora Interina
Universidad de Zaragoza

Recibido: 03.12.2019 / Aceptado: 13.12.2019
DOI: https://doi.org/10.20318/cdt.2020.5187

Resumen: El objetivo de este trabajo es considerar qué ocurrirá cuando Reino Unido se convierta en un país tercero para la Unión Europea y cómo afectará esto a la libre circulación de datos personales que existía antes de su salida del mercado único digital. Se prestará especial atención al análisis de los mecanismos que permitirían continuar transfiriendo datos desde el Espacio Económico Europeo al Reino Unido y, en particular, la posibilidad de una decisión de adecuación y los problemas que puede encontrar.
Palabras clave: protección de datos personales, Brexit, decisión de adecuación, Unión Europea, Reino Unido.

Abstract: The objective of this paper is to consider what will happen when the United Kingdom becomes a third State for the European Union and how this will affect the free movement of personal data that existed before its exit from the digital single market. Special attention will be paid to the analysis of the mechanisms that would allow the transfer of data from the European Economic Area to the United Kingdom and, in particular, the possibility of an adequacy decision and the problems it may encounter.
Keywords: personal data protection, Brexit, adequacy decision, European Union, United Kingdom

I. Introducción

1. Las noticias referentes al Brexit han hecho mucho énfasis en la posibilidad de grandes filas de camiones junto al Canal de la Mancha y desabastecimiento de comida o incluso medicamentos en el Reino Unido. Sin embargo, no sólo las mercancías cruzan las fronteras, sino que la economía europea fuertemente digitalizada, en especial la del Reino Unido, hace también imprescindible que los datos pa-

sen a través de las mismas.[1] Aunque esta transferencia sea invisible a los ojos, la salida del Reino Unido de la Unión Europea (UE) tendrá un fuerte impacto en la misma.

2. La economía del Reino Unido depende en gran medida de los servicios que suponen el 81% de su valor agregado bruto y el 83% de sus empleos,[2] y varios de los sectores con más peso dentro de la misma dependen de los flujos de datos transfronterizos como las finanzas, la banca o la hostelería.[3]

3. Por su parte, la Unión Europea se ha convertido en un líder mundial en la regulación de la protección de datos personales a través del Reglamento General de Protección de Datos (RGPD),[4] considerándolo como un derecho fundamental al consagrarlo como tal en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

4. Teniendo en cuenta el interés del Reino Unido en el libre flujo de datos y de la UE en la salvaguarda de los datos personales de los europeos, el objetivo de este trabajo es considerar qué ocurrirá cuando Reino Unido se convierta en un país tercero y cómo afectará esto a la libre circulación de datos personales que existía antes de su salida de la UE. Se prestará especial atención al análisis de los mecanismos que permitirían continuar transfiriendo datos personales desde el Espacio Económico Europeo[5] al Reino Unido y, en particular, la posibilidad de una decisión de adecuación y los problemas que puede encontrar.

II. El Reino Unido y el Reglamento General de Protección de Datos tras el Brexit

5. Uno de los mantras de la campaña de los partidarios del Brexit en el referéndum era retomar el control por parte del Reino Unido sobre las decisiones que le afectaban (*Let's take back control*). Este eslogan era engañoso porque una salida del Reino Unido de la UE no le granjeará sustraerse a cumplir ciertas normas de la UE sobre todo si se quiere tener acceso a sus mercados. Esto es obvio en ámbitos como el comercio o la competencia, pero también en lo relativo al flujo de datos personales.[6]

1. La aplicación extraterritorial del Reglamento General de Protección de Datos

6. Muchas empresas del Reino Unido tendrán que seguir aplicando el RGPD de la UE porque se trata de una norma que se aplica extraterritorialmente al tratamiento de datos personales de interesados que residan en la UE por parte de un responsable o encargado incluso si éste no está establecido en la

[1] Según D. Ciuriak, *Rethinking Industrial Policy for the Data-driven Economy*. CIGI Paper No. 192, Waterloo, 2018, p. 6, la circulación transfronteriza de datos es intrínseca a las transacciones comerciales. El autor considera que ésta es la nueva "quinta libertad" del comercio, después de la libre circulación de bienes, servicios, capitales y trabajadores.

[2] HOUSE OF COMMONS LIBRARY, *Services industries: Key Economic Indicators*, 2019. Disponible en: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN02786 (última consulta 14/11/2019).

[3] Además, la imposibilidad de transmitir datos afectará no sólo a la economía, sino a otros aspectos de la vida cotidiana, incluso puede imposibilitar que personas enfermas reciban el tratamiento médico apropiado. M. Scott, "Patients on both sides of Irish border face medical risks in no-deal Brexit", *Politico.eu* (8/22/19). Disponible en: https://www.politico.eu/article/ireland-northern-no-deal-brexit-patients-data-medical-records-privacy/ (última consulta 14/11/2019).

[4] 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), *DOUE* L 119, 4 de mayo de 2016, pp. 1–88.

[5] El RGPD se aplica en el Espacio Económico Europeo, que incluye, además de a los Estados miembros de la UE, a Islandia, Liechtenstein y Noruega. Si Reino Unido decidiera permanecer en este Espacio gozaría de la libre circulación de datos personales, pero parece poco probable porque esto supondría ir en contra del espíritu del Brexit, dado que tendría que seguir aplicando una gran parte de la normativa de la UE.

[6] Para K. Wimmer/ J. Jones, "Brexit and Implications for Privacy", *Fordham International Law Journal*, Vol. 40, nº 5, 2017, pp. 1553-1561, p. 1560, que comparan el Brexit con un divorcio, sería tentador concluir que, cuando recupere su soltería, el Reino Unido podrá jugar según sus propias reglas con respecto a la privacidad. Pero ésa es la teoría, la realidad es que el Reino Unido no ejercerá esta aparente libertad sin restricciones, sino que su futura actuación vendrá muy limitada y moldeada por los compromisos que establezca con la UE y otros terceros países.

UE, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la UE o el control de su comportamiento, en la medida en que este tenga lugar en la UE.[7]

7. Esto es muy significativo si se considera que el 75% de los flujos de datos internacionales del Reino Unido son con la UE,[8] y gran parte de la actividad económica del Reino Unido depende de estos flujos como se ha explicado *supra*.[9]

8. Multitud de empresas en el Reino Unido tendrán que cumplir el RGPD, y éste ni siquiera tendrá voz ni voto cuando se modifique la norma, algo que sí tenía con su pertenencia a la UE. Además, las compañías inglesas tendrán que cumplir con los estrictos estándares del RGPD sin contar con las ventajas que suponía estar en la UE.[10] Por ejemplo, tendrán que nombrar un representante en una Estado que sí pertenezca al Espacio Económico Europeo[11] y lidiar con las autoridades de protección de datos de ese país, además de con la inglesa. Esto puede influir en que si una multinacional debe decidir en qué Estado situar su sede europea decida no hacerlo en el Reino Unido sino en otro Estado que sí forme parte del Espacio Económico Europeo.

2. La limitación de los flujos transfronterizos de datos personales desde el Espacio Económico Europeo

9. El RGPD no permite transferir datos personales fuera del Espacio Económico Europeo si no existen las garantías adecuadas de protección de derechos. Es decir, las empresas tienen que recurrir para ello a una serie de mecanismos de diferente complejidad como las normas corporativas vinculantes, las cláusulas tipo de protección de datos, los códigos de conducta aprobados por la autoridad competente o los mecanismos de certificación.[12] Existen excepciones como contar con el consentimiento del interesado, pero éste debe acceder explícitamente a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él.[13] Además, las excepciones deben interpretarse de forma restrictiva y hacen referencia principalmente a actividades de tratamiento ocasionales y no repetitivas.[14]

---

[7] Art. 3 RGPD. Véase las *Guidelines 3/2018 on the territorial scope of the GDPR* del Comité Europeo de Protección de Datos; P. De Hert/ M. Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *International Data Privacy Law*, 2016, Vol. 6, nº. 3, pp. 230-243; y B. Greze, "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives", *International Data Privacy Law*, 2019, Vol. 9, nº. 2, pp. 109-128.

[8] TECHUK y FRONTIER ECONOMICS, *The UK Digital Sectors After Brexit*, 2017, p. 10. Disponible en: *https://www.techuk.org/insights/news/item/10086-the-uk-digital-sectors-after-brexit.* (última consulta 14/11/2019). Este informe también especifica que el 43% de las exportaciones totales del Reino Unido están relacionadas con los servicios, más de un tercio de estos flujos comerciales son con socios europeos, y la mayoría del comercio de servicios requiere el flujo de datos transfronterizos.

[9] Además, el RGPD establece considerables sanciones en caso de incumplimiento grave que pueden llegar a multas administrativas de 20 000 000 euro o, tratándose de una empresa, de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía (art. 83.5 y 6).

[10] D. Korff, *The Data Protection Implications of a 'No-Deal Brexit'* (23/08/2019). Disponible en: http://dx.doi.org/10.2139/ssrn.3441617 (última consulta 14/11/2019).

[11] Art. 27 RGPD.

[12] Art. 46 RGPD.

[13] Art. 49 RGPD. Los otros supuestos que considera este artículo son que la transferencia sea necesaria: para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; por razones importantes de interés público reconocido por el Derecho de la UE o de los Estados miembros (lo que dejaría fuera la legislación del Reino Unido); para la formulación, el ejercicio o la defensa de reclamaciones; o para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

Si no se cumple con ninguna de estas condiciones solo se podrá llevar a cabo la transferencia si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. Además, el responsable del tratamiento informará de la transferencia a la autoridad de control y al interesado al que también deberá hacerle saber los intereses legítimos imperiosos perseguidos.

[14] CEPD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, adoptadas el 25 de mayo de 2018.

A) La posible decisión de adecuación de la Comisión Europea respecto a Reino Unido

10. Lo más sencillo para las empresas y para el flujo de datos personales entre la UE y otro país es que la Comisión Europea emita una decisión de adecuación[15] al considerar que ese país garantiza un nivel de protección adecuado, es decir, esencialmente equivalente al de la UE. Esto ya se hizo con otros países como Uruguay, Andorra, Suiza o Israel. Así las transferencias no requerirán ninguna autorización específica, ni las empresas tendrán que recurrir a los otros mecanismos mencionados. Esto facilita mucho las cosas sobre todo para las pequeñas y medianas empresas.[16]

11. En el caso del Reino Unido, éste ha decidido que permitirá que los datos personales fluyan desde el mismo hacia la UE sin ningún tipo de exigencia adicional de su legislación.[17] Sin embargo, para que pase lo mismo en el caso de transferencias desde el Espacio Económico Europeo, se requiere la citada decisión de adecuación. Esta solución es la recogida en la Declaración política en la que se expone el marco de las relaciones futuras entre la Unión Europea y el Reino Unido,[18] y que acompaña al Acuerdo de Retirada.[19]

12. Los datos personales son uno de los primeros temas que trata la Declaración en la que se subraya la importancia de los flujos e intercambios de datos en todos los aspectos de las relaciones futuras. La Comisión Europea se compromete a iniciar lo antes posible, tras la retirada del Reino Unido, las evaluaciones respecto de dicho país, con ánimo de adoptar las decisiones correspondientes a más tardar a finales de 2020, si se cumplían las condiciones aplicables, consiguiendo así una transición sin obstáculos tras el período transitorio del Acuerdo de Retirada.[20]

13. El problema es que una decisión de adecuación puede tardar varios años como reconocía el propio informe *Operation Yellowhammer* de 2 de agosto de 2019 que el Gobierno del Reino Unido tuvo que hacer público en septiembre y que recogía los principales riesgos de un Brexit sin acuerdo. El propio Supervisor Europeo de Protección de Datos también predijo que podía llevar varios años.[21]

---

[15] Véase J. J. Gonzalo Domenech, "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros", *Cuadernos de Derecho Transnacional* (marzo 2019), Vol. 11, nº 1, pp. 350-371.

[16] En un discurso que dio el 19 septiembre de 2019 en Madrid Steve Barclay, Secretario de Estado del Reino Unido, en un desayuno organizado por Europa Press, el primer tema al que se refirió al hablar de la necesaria preparación por parte de la UE para el Brexit fue el de las transferencias de datos personales. En concreto, aseguró que, a pesar de que el Reino Unido había adoptado en su totalidad los requisitos de la UE sobre datos, la posición de la Comisión era que las empresas en España tendrán restricciones en los datos que podrán compartir con sus homólogas en el Reino Unido. Advirtió que esto afectaría no solo a la industria del turismo, con los 45 millones de vuelos desde el Reino Unido a España cada año, sino que tendría un impacto en las empresas mucho más amplio, y se preguntó si las pequeñas y medianas empresas españolas estaban completamente preparadas para ese tipo de cambio. Disponible en: https://www.gov.uk/government/speeches/secretary-of-state-speech-at-breakfast-event-hosted-by-europa-press-in-madrid (última consulta 14/11/2019).

[17] Department for Digital, Culture, Media & Sport, *Guidance: Amendments to UK data protection law in the event the UK leaves the EU without a deal*. Disponible en:

https://www.gov.uk/government/publications/data-protectionlaw-eu-exit/amendments-to-uk-data-protection-law-in-the-eventthe-uk-leaves-the-eu-without-a-deal-on-29-march-2019, (última consulta 14/11/2019).

[18] Declaración política en la que se expone el marco de las relaciones futuras entre la Unión Europea y el Reino Unido, 2019/C 384 I/02, XT/21050/2019/INIT, *DOUE* C 384I, 12.11.2019, pp. 178–193.

[19] 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, *DOUE* C 384I, 12.11.2019, pp. 1–177.

[20] Según el artículo 71.1 del Acuerdo de Retirada el Derecho de la UE sobre protección de datos personales se aplicará en el Reino Unido respecto del tratamiento de datos personales de interesados fuera del Reino Unido, siempre que los datos personales: se hayan tratado en virtud del Derecho de la UE en el Reino Unido antes del final del período transitorio; o sean tratados en el Reino Unido después del final del período transitorio con base en el presente Acuerdo. Esto tiene como resultado, según el artículo 73, que la UE no tratará los datos y la información obtenidos del Reino Unido antes del final del período transitorio, u obtenidos después del final del período transitorio sobre la base del presente Acuerdo, de forma diferente a los datos y la información obtenidos de un Estado miembro por el mero hecho de que el Reino Unido se haya retirado de la UE.

[21] Discurso de lanzamiento de su informe anual en Bruselas el 26 de febrero de 2019.

14. La mención a una posible decisión de adecuación en la Declaración para finales de 2020 se ha mantenido igual a pesar de las diferentes prórrogas del Brexit, porque es la única opción si entonces termina el período transitorio y se quiere evitar los problemas de una salida efectiva sin decisión de adecuación.

15. Si la salida de Reino Unido se hubiera producido el 30 de marzo de 2019, hubiera habido 21 meses para adoptar la decisión, pero con la última extensión a 31 de enero de 2020, la Comisión Europea contaría sólo con once meses.[22] La Comisión puede ser muy rápida pero sólo podrá comenzar la evaluación cuando efectivamente el Reino Unido haya salido de la UE y antes de adoptar la decisión debe solicitar un Dictamen del Comité Europeo de Protección de Datos (CEPD) y consultar a un comité compuesto por representantes de los Estados miembros (comitología) mediante el procedimiento de examen. Además, sin ser formalmente necesario, la Comisión Europea informa a la Comisión del Parlamento Europeo de Libertades Civiles, Justicia y Asuntos de Interior y el Parlamento Europeo puede decidir emitir una resolución al respecto. Resulta difícil imaginar que todo esto se pueda hacer bien en once meses, aunque está claro que la Comisión va a priorizarlo y no va a ponerlo en la cola esperando a terminar las negociaciones con otros países que también quieren una decisión de adecuación como Corea del Sur, México o India a pesar de lo que digan algunos expertos.[23]

16. En un principio, podría parecer que la decisión es sencilla porque el Reino Unido ha adecuado su legislación al RGPD a través de la *Data Protection Act* de 2018[24] y seguirá aplicándola tras la retirada de la UE.[25]

17. No obstante, el plan del Gobierno es realizar algunas modificaciones para adaptar las disposiciones del RGPD al Reino Unido tras el Brexit,[26] por lo que habría que ver cuáles serán esas modificaciones a medio plazo. De manera inminente no habrá cambios porque el Reino Unido no tiene tiempo para modificar las diferentes normas y ha recurrido a una solución de emergencia que básicamente, consiste en asumir el RGPD completo, con el *UK GDPR* o *United Kingdom General Data Protection Regulation*, a través de *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019* del 28 de febrero (2019, Nº419).

18. Este instrumento realiza los cambios necesarios y apropiados al texto del RGPD para convertirlo en una ley del Reino Unido de manera coherente, por ejemplo, reemplazando las referencias a los Estados miembros de la UE, instituciones, procedimientos y decisiones que ya no serán relevantes después del día de salida con referencias equivalentes del Reino Unido; o eliminando la obligación del *Information Commissioner's Office* (conocida por sus siglas en inglés como ICO) que es la autoridad de protección de datos del Reino Unido de cooperar con las autoridades de supervisión de otros Estados miembros de la UE.[27]

---

[22] Una extensión de este plazo es posible y sería razonable si se tiene en cuenta que en este periodo de tiempo deberán negociarse las condiciones de la futura relación de la UE con el Reino Unido, lo que entre otros elementos requerirá un acuerdo de libre comercio que parece poco probable que pueda negociarse y además cumplir con todos los requisitos formales para su celebración y entrada en vigor antes de esa fecha. Es por ello que el artículo 132 del Acuerdo de Retirada contempla que el Comité Mixto, antes del 1 de julio de 2020, podrá adoptar una decisión única por la que se prorrogue el período transitorio hasta un máximo de uno o dos años. Otra cuestión es el coste político de seguir alargando este proceso.

[23] D. Korff, *op. cit.,* p. 9.

[24] Esta ley además transpone 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, *DOUE* L 119 de 4 de mayo de 2016, pp. 89-131.

[25] *European Union Withdrawal Act.*

[26] INFORMATION COMMISSIONER'S OFFICE, *Data protection if there's no Brexit deal*, 2019, p. 4. Disponible en: https://ico.org.uk/media/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal-1-0.pdf (última consulta 14/11/2019).

[27] *Explanatory Memorandum to the Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit)*

19. Esta ley mantiene los estándares de protección de datos que existían con el RGPD y también tiene alcance extraterritorial, como se ha explicado que ocurre con el RGPD, porque se aplicará a las actividades de tratamiento relacionadas con la oferta de bienes o servicios a interesados en el Reino Unido o el control de su comportamiento.

20. Una vez pasado el Brexit, se podrá modificar esta ley y hay quien considera que será una buena oportunidad para que el Reino Unido relaje algunas de las reglas para facilitar el comercio (como propuso en las negociaciones sobre el RGPD),[28] siendo probable que los Estados Unidos le presionen en ese sentido.[29] Pero eso no será posible si quiere una decisión de adecuación porque la UE no va a aceptar rebajas en la exigencia a las empresas que les dé una ventaja sobre las de sus Estados miembros.[30]

21. Ni siquiera es seguro que la actual redacción de la *Data Protection Act* sea compatible con el RGPD porque contiene ciertas disposiciones controvertidas,[31] por ejemplo, crea ciertas excepciones a los derechos de los sujetos de datos para un efectivo control de la inmigración que no parecen tener ningún tipo de justificación en el RGPD.[32]

22. Además, para una decisión de adecuación no sólo se tiene en cuenta la ley general de protección de datos, sino también la 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.

23. En el ámbito de la conservación de datos personales, el TJUE ya dictó una sentencia que dictaminaba que la normativa del Reino Unido era incompatible con las normas europeas de protección de datos.[33] Aunque a raíz de esta sentencia se modificaron algunos elementos de la norma en octubre

---

Regulations 2019. Disponible en: https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsiem_9780111177594_en.pdf (última consulta 03/12/2019).

[28] D. J. B. Svantesson, F. H., Cate, O. Lynskey, Y. C. Millard, "The global data protection implications of 'Brexit'", *International Data Privacy Law,* Vol. 6, nº 3, 2016, pp. 167–169, p. 168, consideran que es plausible que, dado que la protección de datos no se trata como un derecho fundamental en el Reino Unido, el Brexit suponga que se acerque a aquellos Estados que desean regular el procesamiento de datos personales de manera diferente y lograr un equilibrio alternativo entre los derechos fundamentales y otros intereses, facilitando así un nuevo consenso internacional.

[29] L. Bannister/ R. Bergan, "Threat to our digital rights revealed in US-UK trade talks leak", *Open Democracy*, 2 de diciembre de 2019. Disponible en: https://www.opendemocracy.net/en/opendemocracyuk/threat-our-digital-rights-revealed-us-uk-trade-talks-leak/ (última consulta 03/12/2019).

[30] L. Moerel/ R. Tigner, "United Kingdom. Data Protection Implications of 'Brexit'", *European Data Protection Law Review*, Vol. 2, nº 3, 2016, pp. 381-383, p. 382.

[31] Véase K. Mc. Cullagh, "UK: GDPR adaptions and preparations for withdrawal from the EU", *National adaptations of the GDPR*, pp. 108-119. Disponible en: https://ueaeprints.uea.ac.uk/id/eprint/70040/ (última consulta 14/11/2019).

[32] Véase *Written evidence submitted by Liberty (DPB02) Data Protection Bill*, March 2018 o *Liberty's Abridged Briefing on the Data Protection Bill 2017: the Immigration Control Exemption.* Esta excepción de la Ley fue recurrida pero el tribunal inglés desestimó la demanda por considerar la excepción justificada por razones de interés público. Decisión del *High Court* de 3 de octubre de 2019 en el caso *Open Rights Group & the 3 million v. Secretary of State for the Home Department [2019] EWHC 2562 (Admin).* Los demandantes han recurrido esta decisión, véase Open Rights Group "Open Rights Group and the3million seek to appeal immigration exemption judgment", 3 de octubre de 2019. Disponible en: https://www.openrightsgroup.org/press/releases/2019/open-rights-group-and-the3million-seek-to-appeal-immigration-exemption-judgment¨(última consulta 14/11/2019).

Durante el juicio se demostró que la excepción está siendo utilizada por las autoridades británicas que se han valido de la misma para denegar el 60% de las solicitudes que han recibido en casos de inmigración desde principios de 2019 (L. O'Carroll, "UK decision to deny EU citizens access to data challenged in court", *The Guardian*, 23 de julio de 2019. Disponible en: https://www.theguardian.com/uk-news/2019/jul/23/uk-decision-deny-eu-citizens-access-personal-data-challenged-court (última consulta 14/11/2019).

La Plataforma de Cooperación Internacional para Migrantes Indocumentados (PICUM) presentó una queja formal ante la Comisión Europea contra el Reino Unido por incumplir el RGPD en relación a esta excepción. A la queja se sumaron varias organizaciones de migrantes y de derechos digitales. Véase PICUM, *Advocates bring first GDPR complaint to EU against UK data protection law for violating data rights of foreigners*, 1 de julio de 2019. Disponible en: https://picum.org/press-release-advocates-bring-first-gdpr-complaint-to-eu-against-uk-data-protection-law-for-violating-data-rights-of-foreigners/ (última consulta 14/11/2019).

[33] STJUE (Gran Sala) de 21 de diciembre de 2016, *Tele2 Sverige AB* c. *Post- och telestyrelsen y Secretary of State for the Home Department* c. *Tom Watson y otros*, asuntos acumulados C-203/15 y C-698/15, ECLI:EU:C:2016:970. EL TJUE consideró que el Derecho de la UE se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia,

de 2018, sigue habiendo serias dudas sobre su compatibilidad que han llevado al planteamiento de una nueva cuestión prejudicial sobre la materia pendiente ante el TJUE.[34]

24. Para evaluar si se adopta una decisión de adecuación, la Comisión también analiza las normas sobre transferencias ulteriores de datos personales a otro país y los compromisos internacionales asumidos por el país de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes. Aquí puede cobrar relevancia que el Reino Unido firmara el 3 de octubre de 2019 un acuerdo con Estados Unidos para facilitar el acceso a datos electrónicos para luchar contra delitos graves.[35] Éste es el primer acuerdo ejecutivo que celebra Estados Unidos con un Estado conforme a su *Clarifying Lawful Overseas Use of Data Act* conocida como *CLOUD Act* y permitirá que las autoridades de uno y otro país se puedan dirigir directamente a los intermediarios de servicios de Internet situados en el otro país y pedirles datos personales de sus usuarios sin tener que colaborar con las autoridades del Estado donde están situados los intermediarios y evitar así el largo procedimiento de los mecanismos de asistencia judicial mutua. La propia UE ha comenzado también las negociaciones para celebrar un acuerdo de esta naturaleza con Estados Unidos.[36]

25. El acuerdo entre Estados Unidos y Reino Unido tiene un fin legítimo y ventajas como regular algunas prácticas que ya se estaban llevando a cabo a través de canales informales. Sin embargo, la evaluación del mismo es ambivalente; ha sido considerado un claro avance por algunos[37] o un paso atrás por otros.[38] Sin entrar a valorarlo, lo cierto es que contiene menos salvaguardias respecto a la protección de los derechos fundamentales de los que se exigen al acuerdo que realizará la UE con Estados Unidos.[39]

---

la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Además, se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la UE.

[34] Cuestión prejudicial presentada por el *Investigatory Powers Tribunal*, en el caso *Privacy International* c. *Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service Srl, Secret Intelligence Service*, C-623/17. El Tribunal preguntó si tiene cabida en el Derecho de la UE un requisito por el cual un proveedor de redes de comunicación electrónica debe facilitar datos objeto de comunicaciones masivas a las Agencias de Seguridad e Inteligencia (ASI) de un Estado miembro de acuerdo con las instrucciones recibidas del Secretario de Estado. Además, el Tribunal preguntó si en caso de respuesta afirmativa a la primera cuestión, se aplicarían los requisitos de la anteriormente mencionada sentencia *Watson*, u otros requisitos además de los impuestos por el CEDH, a las referidas instrucciones del Secretario de Estado.

El Tribunal se mostraba especialmente preocupado porque parece obvio que el TJUE responderá que efectivamente su jurisprudencia debe aplicarse y entonces planteaba ¿cómo y en qué medida deben aplicarse dichos requisitos, habida cuenta de la necesidad esencial de las ASI de usar técnicas de adquisición y tratamiento masivo automatizado para proteger la seguridad nacional, y de la circunstancia de que tal capacidad, en caso de ser conforme con el CEDH, puede sufrir un menoscabo significativo como consecuencia de esos requisitos?

Si de la redacción de las cuestiones no se pudiera intuir el rechazo del *Investigatory Powers Tribunal* a la aplicación de la jurisprudencia del TJUE, éste dejó claro en su petición que estimaba que la imposición de los requisitos precisados en la sentencia *Tele2 Sverige* y *Watson*, en caso de ser aplicables, redundaría en perjuicio de la eficacia de las medidas adoptadas por las ASI para salvaguardar la seguridad nacional y supondría un riesgo para la seguridad nacional del Reino Unido.

[35] *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*. Disponible en: https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019 (última consulta 14/11/2019).

[36] Véase la Decisión del Consejo por la que se autoriza la apertura de negociaciones con miras a la celebración de un acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a pruebas electrónicas para la cooperación judicial en materia penal.

[37] J. Daskal/ P. Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards", *Lawfare*, 8 de octubre de 2019. Disponible en: https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards (última consulta 14/11/2019).

[38] K. Rodríguez / C. Fischer, "A Race to the Bottom of Privacy Protection: The US-UK Deal Would Trample Cross Border Privacy Safeguards", *Electronic Frontier Foundation,* 4 de octubre de 2019. Disponible en: https://www.eff.org/deeplinks/2019/10/race-bottom-privacy-protection-us-uk-deal-would-trample-cross-border-privacy (última consulta 14/11/2019).

[39] T. Christakis, "21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (and an Explanation of How it

Por tanto, puede ser un obstáculo para la decisión de adecuación porque nada impedirá que los datos que vayan a parar a los intermediarios situados en el Reino Unido sean suministrados a las autoridades americanas conforme a una petición estadounidense fundada en este acuerdo.[40]

26. Pero, sin duda, las cuestiones más delicadas se plantearán en torno al amplio acceso de los servicios de inteligencia del Reino Unido a los datos personales y las limitadas salvaguardas existentes a este respecto. Curiosamente, al ser una cuestión relacionada con la seguridad nacional está fuera del ámbito competencial de la UE y ésta no crea estándares para sus propios Estados,[41] pero sí tiene este ámbito en cuenta al analizar la situación en los países terceros, como se ha explicado.

27. Una futura decisión de adecuación respecto al Reino Unido tendrá que asumir la jurisprudencia del TJUE y, en particular, la sentencia del caso *Schrems*[42] que llevó a invalidar la decisión de adecuación respecto a Estados Unidos después de las revelaciones de Edward Snowden. El TJUE consideró que de los datos que le facilitó la Comisión había quedado probado que las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a ese país yendo más allá de lo que era estrictamente necesario y proporcionado para proteger la seguridad nacional, así como que las personas afectadas no disponían de vías jurídicas, administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión. Por ello la Comisión tuvo que negociar algunos cambios y exigir ciertos compromisos y garantías a Estados Unidos y elaboró otra decisión con nuevas salvaguardas (conocida como Escudo de seguridad o *Privacy Shield*) que también se encuentra en entredicho.[43]

28. Cabe recordar la condena al Reino Unido por el Tribunal Europeo de Derechos Humanos (TEDH) que consideró que el régimen de interceptación masiva de datos del Reino Unido infringía varios artículos del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) en su decisión de 2018 en el caso *Big Brother Watch*.[44] El caso se originó con los recursos acumulados presentados por periodistas, activistas y organizaciones de derechos humanos sobre

Works – With Charts)", *European Law Blog,* 13 de octubre de 2019. Disponible en: https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ (última consulta 14/11/2019).

[40] Los miembros del Parlamento Europeo Moritz Körner y Sophie in't Veld plantearon el 7 de octubre de 2019 una pregunta formal a la Comisión (E-003136/2019) sobre si considera que el Acuerdo es conforme al RGPD y a la Directiva sobre protección de los datos personales cuando son utilizados por autoridades policiales y de justicia penal y la jurisprudencia del Tribunal Europeo de Derechos Humanos, y si no es el caso si iba a iniciar un proceso de infracción. También han preguntado que, si el Reino Unido sale de la UE, cómo afectara este Acuerdo a la posible adopción de una decisión de adecuación.

En puridad, teniendo en cuenta que ésta es una materia compartida entre la UE y los Estados miembros y que la Unión Europea ha decidido ejercer ella esta competencia como denota la existencia de un mandato de negociación del Consejo a la Comisión para negociar un acuerdo ejecutivo con Estados Unidos, el Reino Unido debería haberse abstenido de firmar un acuerdo por su cuenta y éste sería nulo conforme al Derecho de la UE. No obstante, parece obvio que de cara a preparar su salida al Reino Unido le interesaba ir preparando el camino y la Comisión Europea no iba a poner obstáculos estando cercana la fecha de salida.

[41] El artículo 4 del Tratado de la UE establece que la Unión respetará las funciones esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro. Véase P. Vogiatzoglou/S. Fantin , "National and Public Security Within and Beyond the Police Directive", *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Vedder A, Schroers J, Ducuing C, Valcke P. (eds). Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 27-62.

[42] STJUE (Gran Sala) de 6 de octubre de 2015 *Maximillian Schrems* c. *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650. Véase M. I. Puerto/ P. Sferraza Taibi, "La sentencia *Schrems* del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional", *Revista Derecho del Estado*, Nº. 40, 2018, pp. 209-236; y E. Uría Gavilán, "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 *Schrem*s", *Revista de Derecho Comunitario Europeo*, Año nº 20, Nº 53, 2016, pp. 261-282.

[43] C. I. Cordero Álvarez, "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la *Cloud Act*", *Revista Española de Derecho Europeo*, nº. 70, 2019, pp. 49-107.

[44] STEDH de 13 de septiembre de 2018, *Big Brother Watch y otros* c. *Reino Unido*, asuntos acumulados nº. 58170/13, 62322/14 y 24960/15.

tres regímenes de vigilancia diferentes: la interceptación masiva de comunicaciones, el intercambio de inteligencia con gobiernos extranjeros, y la obtención de datos de comunicaciones de proveedores de servicios de comunicaciones.

29. El TEDH sostuvo que el régimen de interceptación masiva violó el artículo 8 del CEDH, ya que no había suficiente supervisión tanto de la selección de los intermediarios de Internet para la interceptación como del filtrado, búsqueda y selección de comunicaciones interceptadas para su examen, y las salvaguardas que rigen la selección de datos de comunicaciones relacionados para el examen fue inadecuada. El TEDH consideró que la operación de un régimen de interceptación masiva no violaba en sí misma el CEDH, pero señaló que dicho régimen tenía que respetar los criterios establecidos en su jurisprudencia. El TEDH sostuvo que el régimen para obtener datos de comunicaciones de proveedores de servicios de comunicaciones violó el artículo 8, ya que no se hizo conforme a la ley, y que tanto el régimen de interceptación masiva como el régimen para obtener datos de comunicaciones de proveedores de servicios de comunicaciones violaron el artículo 10 del CEDH, ya que no existían garantías suficientes con respecto al material periodístico confidencial.

30. El TEDH, además, consideró que el régimen para compartir información de inteligencia con gobiernos extranjeros no violaba el artículo 8 ni el 10, y rechazó por unanimidad las quejas formuladas por los recurrentes, en virtud del artículo 6, sobre el procedimiento interno para impugnar medidas de vigilancia secreta.

31. Los recurrentes ganaron puesto que se condenó al Reino Unido, sin embargo, la victoria fue agridulce porque varios de sus principales argumentos fueron ignorados. Según Vermeulen,[45] el TEDH no consideró problemáticos algunos de los aspectos más intrusivos de estas prácticas de vigilancia altamente controvertidas: la interceptación de comunicaciones en masa sigue siendo posible y el intercambio de información entre los *Five Eyes*[46] sale reforzado. Las anteriores sentencias ya citadas del TJUE creaban un estándar mucho más exigente que debería ser la norma en Europa[47] y el criterio principal para una decisión de adecuación, si bien se centraban en el acceso de autoridades policiales y no de agencias de inteligencia. Los recurrentes pidieron el reexamen de la sentencia que está pendiente de decisión por la Gran Sala del TEDH.

32. El Reino Unido ha modificado la legislación desde que se presentó el caso con la *Investigatory Powers Act* de 2016, pero ésta también fue considerada por el *High Court* del Reino Unido como parcialmente incompatible con los derechos fundamentales en el caso *Liberty*.[48] En concreto, el Tribunal concluyó que la parte 4 de la Ley era incompatible con los derechos fundamentales recogidos en la legislación de la UE en el ámbito de la justicia penal en lo referente al acceso a los datos conservados porque no se limitaba al propósito de combatir el "delito grave"; y el acceso a los datos no estaba sujeto a revisión previa por parte de un tribunal o un organismo administrativo independiente.

33. *Liberty* (apoyado por la *National Union of Journalists*) también intentó que los tribunales ingleses declararan la incompatibilidad de otras secciones de la *Investigatory Powers Act* de 2016 con la *Human Rights Act* de 1998 que integra los derechos del CEDH en el Derecho del Reino Unido. En concreto, argumentaron que las disposiciones de la Ley eran incompatibles con los artículos 8 y 10 del CEDH porque son demasiado ambiguas y carecen de las garantías mínimas establecidas por el TEDH,

[45] J. Vermeulen, "Big brother may continue watching you", *Strasbourg Observers*, 12 de octubre de 2018. Disponible en:https://strasbourgobservers.com/2018/10/12/big-brother-may-continue-watching-you/ (última consulta 14/11/2019).

[46] *Five Eyes* es una alianza que sirve como red de intercambio de inteligencia de la cual forman parte el Reino Unido, los Estados Unidos, Australia, Canadá y Nueva Zelanda.

[47] T. Christakis, "A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch judgment", *European Law Blog*, 20 de septiembre de 2018. Disponible en: https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/#more-4221 (última consulta 14/11/2019).

[48] Sentencia del *High Court* de 27 de abril de 2018, *The National Council for Civil Liberties (Liberty)* v. *Secretary of State for the Home Department, Secretary of State for Foreign and Commonwealth Affairs*, [2018] EWHC 975 (Admin).

además, de no ser necesarias en una sociedad democrática ni proporcionadas. También se arguyó que las garantías que fijaban no era suficientes, por ejemplo, no existían salvaguardas específicas para proteger las comunicaciones abogado-cliente o las fuentes confidenciales de los periodistas. Finalmente, se desestimó el recurso, pero durante el desarrollo de la fase probatoria de este caso se descubrió que el MI5 (Servicio de Inteligencia del Reino Unido) había gestionado datos personales de manera ilegal durante años, y, en concreto, había mantenido "un control inadecuado sobre dónde se almacenan los datos" y "los procesos de eliminación que se le aplicaban".[49]

34. Todavía hay además varios casos pendientes ante el TEDH como *Privacy International*[50] que cuestionan la compatibilidad de otras secciones de esta Ley con el CEDH. Los recurrentes consideraban probable que su equipo hubiera estado sujeto a una interferencia conocida como "explotación de la red informática" o "interferencia de equipo", coloquialmente conocida como "*hacking*" durante un período indefinido por el Servicio Secreto de Inteligencia del Reino Unido. Los recurrentes argumentaron que se habían vulnerado sus derechos protegidos en los artículos 8 y 10 del CEDH al considerar que esta injerencia en los mismos no era acorde a la ley en ausencia de un código de práctica que rija su uso; que no había ningún requisito de autorización judicial; que no había información en el dominio público sobre cómo se desarrollaban tales interferencias; y que no hay ningún requisito de filtrado para excluir material irrelevante. Los recurrentes también consideraron vulnerado su derecho a un recurso efectivo recogido en el artículo 13 del CEDH.

35. Todo esto supone que una decisión de adecuación sea un poco más compleja de lo que podría pensarse *a priori*. No obstante, es probable que el peso político y el interés económico de las transferencias de datos personales hagan que la Comisión acelere el proceso de elaboración de la decisión. Esto es lo que ha ocurrido en el caso japonés en el que la necesidad de que la decisión entrara en vigor coincidiendo aproximadamente con el Acuerdo de Asociación Económica[51] hizo que se superasen las reticencias de determinados sectores[52] sobre si efectivamente el sistema japonés presentaba una protección equivalente. La Comisión Europea terminó adoptando la decisión de adecuación respecto a Japón que ha sido la primera aprobada con el RGPD ya en aplicación[53] y que, por tanto, puede darnos algunas pistas sobre una futura decisión de adecuación respecto a Reino Unido.

36. Por ejemplo, en el caso japonés, también existían dudas sobre la compatibilidad con la protección de datos personales del amplio acceso por parte de las autoridades japonesas a los datos para salvaguardar la seguridad nacional. Este problema se salvó consiguiendo que el Gobierno japonés facilitara a la Comisión una serie de declaraciones, garantías y compromisos oficiales firmados al más alto nivel ministerial y de servicios[54] respecto a los límites y salvaguardas relativas a la recogida y utilización de información personal por parte de las autoridades públicas japonesas con fines coercitivos y de seguridad nacional. Algo muy similar ocurrió con el Escudo de Privacidad que cubre las transferencias con

[49] Sentencia del *Royal Court of Justice* de 29 de julio de 2019, *National Council for Civil Liberties (Liberty)) v. Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*, [2019] EWHC 2057 (Admin).

[50] Caso pendiente ante el TEDH, *Privacy International y otros* c. *Reino Unido*, nº. 46259/16.

[51] Acuerdo entre la Unión Europea y Japón relativo a una asociación económica, DOUE L 330, 27 de diciembre de 2018, pp. 3-899.

[52] Véase Dictamen 28/2018 sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales por parte de Japón, adoptado el 5 de diciembre de 2018; Resolución del Parlamento Europeo, de 13 de diciembre de 2018, sobre la adecuación de la protección de los datos personales que ofrece Japón (2018/2979(RSP)); G. Greenleaf, "Japan and Korea: Different Paths to EU Adequacy", *Privacy Laws & Business International Report*, 156, 2018, pp. 9-11; y G. Greenleaf, "Japan: EU Adequacy Discounted", *Privacy Laws & Business International Report*, 155, 2018, pp. 8-10.

[53] Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal, C/2019/304, *DOUE* L 76 de 19.3.2019, pp. 1-58.

[54] Firmaron la declaración: la Ministra de Justicia, el Consejero de la Secretaría del Gabinete, el Comisario General de la Agencia Nacional de Policía, la Secretaria General de la Comisión de Protección de la Información Personal, el Viceministro del Ministerio del Interior y de Comunicaciones, el representante de la Agencia de Inteligencia de la Seguridad Pública y el Viceministro administrativo de Defensa.

Estados Unidos cuya decisión se acompañó de una serie de cartas de altos funcionarios estadounidenses para recoger determinados compromisos.[55]

37. Mientras que algunos expertos alaban la flexibilidad de la UE para encontrar soluciones en casos como éstos,[56] puede dar lugar a una cierta inseguridad jurídica porque si la decisión de adecuación de Reino Unido no es lo suficientemente garantista corre el riesgo de ser anulada por el TJUE. Esto ya ocurrió con la citada decisión *Safe Harbour*[57] y es posible que ocurra con el Escudo de Seguridad sobre el que el Tribunal ha sido también llamado a pronunciarse.[58]

B. Otros posibles mecanismos para facilitar las transferencias de datos personales al Reino Unido

38. En realidad, desde el Reino Unido la opción preferida no era una decisión de adecuación, sino un acuerdo internacional específico sobre la protección de datos tras el Brexit.[59] La ventaja de un acuerdo de esta naturaleza es que se negociaría, no como la decisión de adecuación que es una decisión unilateral, y que, por tanto, la Comisión Europea no podría revisarlo o retirarse en cualquier momento.[60]

---

[55] El Gobierno estadounidense, a través de su Oficina del Director de Inteligencia Nacional, proporcionó a la Comisión una serie de declaraciones y compromisos detallados. El secretario de Estado firmó una carta en la que el Gobierno de los Estados Unidos se comprometió a crear un nuevo mecanismo de supervisión de las injerencias con fines de seguridad nacional, a saber, el Defensor del Pueblo en el ámbito del Escudo de Privacidad, independiente de los servicios de inteligencia. Por último, una declaración del Departamento de Justicia de los Estados Unidos describía las limitaciones y salvaguardias aplicables al acceso a los datos y a su utilización por parte de los poderes públicos a efectos de aplicación de la ley y otros fines de interés público. Todos estos documentos aparecen como anexos en la Decisión de ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU., *DOUE* L 207 de 1 de agosto de 2016, pp. 1-112.

[56] P. M. Schwartz, "Global Data Privacy: The EU Way", *New York University Law Review,* vol. 94, 2019, pp. 771-818.

[57] STJUE (Gran Sala) de 6 de octubre de 2015 *Maximillian Schrems* c. *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

[58] Casos pendientes ante el TJUE: recurso de anulación interpuesto el 25 de octubre de 2016 ante el Tribunal General, *La Quadrature du Net y otros* c. *Comisión*, T-738/16 y petición de decisión prejudicial planteada por la *High Court* (Irlanda) el 9 de mayo de 2018, *Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems,* C-311/18 (conocida como *Schrems II*). En relación con este último caso, cabe mencionar que en sus conclusiones de 19 de diciembre de 2019 el Abogado General, Saugmandsgaard Øe, consideró que la resolución del litigio principal no requería que el TJUE se pronunciara sobre la validez de la Decisión "Escudo de la privacidad". No obstante, el Abogado General expuso, con carácter subsidiario, las razones que le llevaban a tener dudas sobre la validez de la citada Decisión en lo que atañía a los derechos relativos a la vida privada y a la protección de datos personales, así como al derecho a la tutela judicial efectiva. En todo caso, es necesario esperar a la sentencia del TJUE dado que las conclusiones del Abogado General no son vinculantes.

La Comisión ha evaluado positivamente los avances en la aplicación del Escudo de Privacidad, si bien considera que deben tomarse algunas medidas adicionales para asegurar su efectividad. *Informe de la Comisión al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE-EE.UU*., COM(2019) 495 final. Sin embargo, el Parlamento Europeo opinó que el acuerdo del Escudo de Privacidad no proporcionaba el nivel adecuado de protección exigido por la legislación de protección de datos de la UE y la Carta, tal como los interpreta el TJUE; y planteó que la Comisión suspendiera el Escudo de Privacidad hasta que las autoridades de los Estados Unidos cumplieran con sus condiciones. *Resolución del Parlamento Europeo, de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.* (2018/2645(RSP)). El CEPD también se ha mostrado crítico y tiene una serie de preocupaciones importantes relativas a la compatibilidad del Escudo de Privacidad con el RGPD, siendo una de las principales la ausencia de controles sustanciales respecto al cumplimiento de este marco por parte de las empresas que no se puede olvidar que se autocertifican. Otros elementos que también le crean dudas son las transferencias posteriores, la aplicación de los principios cuando se trata de procesadores, así como el proceso de recertificación. Véase CEPD, *EU-U.S. Privacy Shield - Third Annual Joint Review*, adoptado el 12 de noviembre de 2019.

[59] Véase la audiencia del *Exiting the European Union Committee* de la Cámara de los Comunes sobre *The progress of the UK's negotiations on EU withdrawal*, celebrada el 9 de mayo de 2019.

El Gobierno del Reino Unido incluso publicó un documento en el que explicaba las ventajas de este mecanismo para la UE y explicaba por qué el Reino Unido debía ser tratado de manera diferente que cualquier otro Estado tercero. Véase HM GOVERNMENT, *Technical Note: Benefits of a new data protection agreement*, 2018, p. 1. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714677/Data_Protection_Technical_Note.pdf (última consulta 14/11/2019).

[60] Si bien la decisión de celebrar un acuerdo con el Reino Unido también podría ser declarada invalida por el TJUE, bien a través de un recurso de anulación, aunque existe un plazo muy corto para ello de sólo 2 meses (art. 263 TFUE), o bien en

39. Además, esto permitiría ir más allá de lo que posibilita una decisión de adecuación, por ejemplo, haciendo que no fuera necesario para las empresas del Reino Unido nombrar a un representante en el Espacio Económico Europeo o a la inversa a las de los Estados miembros del Espacio Económico Europeo no tener que hacerlo respecto al Reino Unido rebajando así costes. Además, podría negociarse que el ICO pudiera participar en el mecanismo de *one-stop-shop* o mecanismo de ventanilla única.[61]

40. Sin embargo, la UE no se ha mostrado partidaria de un acuerdo de esta naturaleza, sino que parece preferir seguir sus normas (el RGPD) sin hacer excepciones. Michel Barnier, jefe negociador por parte de la UE del Acuerdo de salida con el Reino Unido, dejó claro que una decisión de adecuación era la única posibilidad,[62] lo que además ha quedado constatado en la Declaración política.[63]

41. En ausencia de una decisión de adecuación (o de un hipotético acuerdo bilateral), existen otras posibilidades a disposición de las empresas para cumplir con los requisitos del RGPD en las transferencias transfronterizas de datos personales. La más utilizada son las cláusulas tipo de protección de datos adoptadas por la Comisión[64] o por una autoridad de control (y aprobadas por la Comisión).

42. Se trata de la opción más sencilla porque cualquiera puede utilizarlas y ya están redactadas. Además, pueden incluirse en un contrato más amplio y se pueden añadir otras cláusulas siempre que no contradigan, de forma directa o indirecta, las cláusulas tipo, ni mermen los derechos o las libertades fundamentales de los interesados.[65] Sin embargo, es necesario recalcar que estas cláusulas no se pueden modificar, por lo que no se puede negociar su contenido con la contraparte en un contrato, porque si esto ocurriera pasarían a considerarse cláusulas contractuales *ad hoc* y la autoridad nacional de supervisión competente debería aprobar estas cláusulas contractuales adaptadas, tras un dictamen del CEPD.

43. Estas cláusulas suelen incluir obligaciones del exportador e importador de datos, disposiciones relativas a la responsabilidad, la legislación aplicable, las posibles variaciones del contrato, la mediación y jurisdicción, la cooperación con las autoridades de control, el subtratamiento de datos, una cláusula de tercero beneficiario, e incluso las obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales.

44. Si una empresa decide optar por las clausulas tipo para legitimar sus transferencias transfronterizas de datos personales, éstas se incluirían en todo contrato que diera lugar a una transferencia de datos personales. Por ejemplo, una importante empresa inglesa cuando se anuló la decisión *Safe-Harbour* tuvo que incluirlas en más de dos millones de contratos en un mes para no realizar dichas transferencias hacia los Estados Unidos sin cobertura legal.[66] Incluso si estas cláusulas están pre-redactadas incluirlas en

el marco de la una cuestión prejudicial (art. 267 TFUE). Pero, en este caso, el Reino Unido estaría amparado por el Derecho Internacional dado que, en principio, una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado.

[61] Según el art. 56 RGPD, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado.

[62] *Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE),* Lisboa, 26 de mayo de 2018. Disponible en: https://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm (última consulta 14/11/2019).

[63] O. Patel/ N. Lea, *EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?,* UCL European Institute, 2019.

[64] Véase: Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, *DOUE* L 181 de 4 de julio de 2001, pp. 19-31; Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, *DOUE* L 385 de 29 de diciembre de 2004, pp. 74-84; y 2010/87/: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, *DOUE* L 39 de 12 de febrero de 2010, pp. 5-18.

[65] Considerando 109 RGPD.

[66] Ejemplo dado por Giles Derrington en una audiencia del *Exiting the European Union Committee* de la Cámara de los Comunes sobre *The progress of the UK's negotiations on EU withdrawal*, celebrada el 9 de mayo de 2019.

todos los contratos puede suponer un esfuerzo y coste económico elevado, y la contraparte puede no estar dispuesta a reabrir un determinado contrato e incluir cláusulas que no puede negociar. No obstante, ésta sigue siendo la opción más factible para las pequeñas y medianas empresas y es la que considera más conveniente la autoridad de protección de datos del Reino Unido para la mayoría de los casos tras el Brexit.[67]

45. No obstante, existe otro problema y es que la licitud de estas cláusulas está pendiente de un pronunciamiento del TJUE en el mencionado caso *Schrems* II.[68] En el que, entre otras muchas preguntas, el tribunal irlandés plantea si el hecho de que estas cláusulas sean aplicables al exportador de datos y al importador de datos, pero no resulten vinculantes para las autoridades nacionales de un tercer país, que pueden exigir al importador de datos que facilite a sus servicios de seguridad los datos personales transferidos con arreglo a esas cláusulas, impide que se apliquen las garantías de protección adecuadas previstas en el Derecho de la UE.[69]

46. Otra opción para las grandes empresas son las normas corporativas vinculantes. Éstas son las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.[70] Estas normas deben ser aprobadas por la autoridad nacional de supervisión competente tras un dictamen positivo del CEPD.[71] Crear unas normas de esta naturaleza sólo resulta rentable para grandes empresas multinacionales por su coste económico (en torno a las 250,000 libras)[72] y temporal.[73]

47. Cabe destacar que aproximadamente un tercio de las normas corporativas vinculantes han sido aprobadas por el ICO,[74] que ha sido, además, el primero en recibir un dictamen positivo del CEPD para unas normas de esta naturaleza tras el comienzo de la aplicación del RGPD.[75] Y esto en una fecha en la que en principio Reino Unido ya debería haber salido de la UE, lo que sirve como una prueba más

---

[67] INFORMATION COMMISSIONER'S OFFICE, *Data protection if there's no Brexit deal*, 2019, p. 8. Disponible en: https://ico.org.uk/media/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal-1-0.pdf (última consulta 14/11/2019).

[68] Caso pendiente ante el TJUE: petición de decisión prejudicial planteada por la *High Court* (Irlanda) el 9 de mayo de 2018, *Data Protection Commissioner* c. *Facebook Ireland Limited* y *Maximillian Schrems,* C-311/18 (conocida como *Schrems II*).

[69] En sus conclusiones de 19 de diciembre de 2019 sobre este caso, el Abogado General, Saugmandsgaard Øe, consideró que el hecho de que las cláusulas contractuales tipo no vinculen a las autoridades del país tercero de destino y no les impidan por tanto imponer al importador obligaciones incompatibles con el respeto de dichas cláusulas no conlleva por sí mismo que dicho mecanismo deba considerar inválido. Sino que la compatibilidad con la Carta de los Derechos Fundamentales de la UE depende de si existen mecanismos suficientemente sólidos que permitan garantizar que las transferencias basadas en las cláusulas contractuales tipo sean suspendidas o prohibidas en caso de incumplimiento de dichas cláusulas o de la imposibilidad de cumplirlas. En su opinión, éste será el caso cuando exista una obligación ―impuesta a los responsables del tratamiento y, en caso de inacción de estos últimos, a las autoridades de control― de suspender o prohibir una transferencia cuando, debido a un conflicto entre las obligaciones derivadas de las cláusulas tipo y las impuestas por la normativa del país tercero de destino, las mencionadas cláusulas no pueden ser respetadas.

En todo caso, es necesario esperar a la sentencia del TJUE dado que las conclusiones del Abogado General no son vinculantes, como ya se ha explicado anteriormente.

[70] Art. 4.20 RGPD.

[71] Art. 47 RGPD.

[72] HM GOVERNMENT, *The exchange and protection of personal data: a future partnership paper*, 2018, p. 12. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf (última consulta 14/11/2019).

[73] Además del tiempo que lleva elaborar las normas corporativas vinculantes, hay que añadir varios meses para que éstas consigan la autorización de la autoridad de protección de datos. A modo de ejemplo, en España el artículo 41.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que el procedimiento una vez haya sido instado por la entidad en cuestión tendrá una duración máxima de nueve meses, no obstante éste queda suspendido como consecuencia de la remisión del expediente al CEPD para que emita el dictamen pertinente.

[74] Dato facilitado por Stephen Hurley en una audiencia del *Exiting the European Union Committee* de la Cámara de los Comunes sobre *The progress of the UK's negotiations on EU withdrawal*, celebrada el 9 de mayo de 2019.

[75] *Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc*.

de la inseguridad jurídica creada por el Brexit, dado que las empresas no sabían si iniciar el proceso para la aprobación de sus normas corporativas vinculantes porque no sabían si la decisión que normalmente tarda varios meses llegaría antes o después de la salida del Reino Unido, y si es después el ICO ya no sería considerada una autoridad competente.

48. La salida del Reino Unido de la UE supondrá la consecuente salida del ICO del Comité Europeo de Protección de Datos y esto será una pérdida para la protección de datos en toda la UE dado que se trata de una de las autoridades más respetadas y cuyo trabajo aprovechan el resto de autoridades de otros Estados. El ICO es la mayor autoridad de control independiente de la UE, puesto que cuenta con más de 500 empleados[76] y es la autoridad que durante el primer año y medio desde la aplicación del RGPD propuso las sanciones más cuantiosas por su incumplimiento.[77] Desde el ICO se teme que su ausencia del Comité será muy negativa para el Reino Unido pues perderá su influencia en la materia. Sería interesante, teniendo en cuenta su relevancia, buscar algún encaje que le permitiera participar no sólo como observador en el Comité, ya que prescindir de su experiencia y liderazgo sería una perdida para el organismo que lidera la creación de muchos estándares en la materia.

49. Volviendo a la cuestión de otros instrumentos que permitan las transferencias transfronterizas, el RGPD ha creado dos que no existían en la Directiva anterior que son los códigos de conducta[78] y los mecanismos de certificación.[79] Sin embargo, su relativa novedad hace que haya mucha incertidumbre sobre los mismos. El propio ICO no consideraba probable que se adoptará ninguno antes de la salida del Reino Unido.[80]

50. También existen instrumentos exclusivamente disponibles para autoridades u organismos públicos. Una opción es utilizar un instrumento jurídicamente vinculante, como un acuerdo internacional bilateral o multilateral o un acuerdo administrativo, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Éstos últimos están sujetos a la autorización de la autoridad nacional de supervisión, tras un dictamen del CEPD.[81]

51. Por ejemplo, en el caso español, la Agencia Española de Protección de Datos colaborará con autoridades, instituciones, organismos y administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.[82]

III. El Reino Unido y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa

52. Más allá de los posibles mecanismos para facilitar las transferencias de datos personales desde el Espacio Económico Europeo al Reino Unido, es importante antes de cerrar este trabajo hacer

[76] Dato facilitado por Elizabeth Denham en una audiencia del *Exiting the European Union Committee* de la Cámara de los Comunes sobre *The progress of the UK's negotiations on EU withdrawal*, celebrada el 9 de mayo de 2019.

[77] El ICO propuso una sanción de 183 millones de libras a British Airways y otra de 99 millones de libras a la cadena hotelera Marriott.

[78] Art. 40 y 41 RGPD. Véase *EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation*.

[79] Art. 42 y 43 RGPD. Véase *EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation* y *EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*.

[80] INFORMATION COMMISSIONER'S OFFICE, *Data protection if there's no Brexit deal*, 2019, p. 21. Disponible en: https://ico.org.uk/media/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal-1-0.pdf (última consulta 14/11/2019). A pesar de ello, el ICO quería estar preparado y el CEPD adoptó el 2 de diciembre de 2019 su *Opinion 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR*.

[81] CEPD, *Nota informativa sobre transferencias de datos en virtud del RGPD en el caso de un Brexit sin acuerdo*, adoptada el 12 de febrero de 2019, pp. 4 y 5.

[82] Artículo 56.3.c de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *BOE* núm. 294, de 6 de diciembre de 2018, pp. 119788 a 119857.

una mención al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en 1981 por el Consejo de Europa, conocido como Convenio 108.

53. Este Convenio fue el primer instrumento internacional vinculante que se adoptó para proteger al individuo contra los abusos que pueden acompañar a la recopilación y el procesamiento de datos personales y buscaba regular al mismo tiempo el flujo transfronterizo de datos personales. La imposibilidad de negociar un tratado de esta naturaleza a nivel de las Naciones Unidas lo ha convertido en un estándar con vocación global más allá de las fronteras europeas, lo que hace que, además de por los 47 Estados miembros del Consejo de Europa,[83] haya sido ratificado por Estados como Argentina, Cabo Verde, Mauricio, México, Marruecos, Senegal, Túnez y Uruguay.

54. La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,[84] precedente legislativo del RGPD, básicamente precisaba y ampliaba los principios de este Convenio, algo que ha continuado el RGPD. Por eso, no es de extrañar que el considerando 105 del RGPD explique que, de cara a conseguir una decisión de adecuación, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país en sistemas multilaterales o regionales, en particular la adhesión al Convenio 108.[85]

55. Igual que la normativa de la UE se modernizó a través del RGPD, el Convenio lo hizo a través de un Protocolo que lo modificaba adoptado en 2018 (CETS 223).[86] El Protocolo buscaba responder a los nuevos retos, asegurar su implementación efectiva y proporcionar un marco legal multilateral robusto y flexible para facilitar el flujo de datos a través de las fronteras al tiempo que proporciona garantías efectivas cuando se utilizan datos personales.[87]

56. El Reino Unido estuvo entre los primeros en ratificar el Convenio en 1987, y fue también uno de los primeros en firmar su Protocolo de modernización el 10 de octubre de 2018.[88] Así que al final el país tendrá que seguir aplicando principios muy similares a los del RGPD, incluso si no aspirara a una decisión de adecuación, al tener que cumplir con sus obligaciones internacionales fijadas en este Convenio que, además, contiene un capítulo dedicado a los flujos transfronterizos de datos.

57. En su artículo 12, regula que una Parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo en la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la regla-

[83] Son miembros del Consejo de Europa, además de los Estados miembros de la UE: Albania, Andorra, Armenia, Azerbaiyán, Bosnia y Herzegovina, Rusia, Georgia, Islandia, Liechtenstein, Macedonia del Norte, Montenegro, Mónaco, Noruega, Moldavia, San Marino, Serbia, Suiza, Turquía y Ucrania.

[84] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *DOUE* L 281 de 23 de noviembre de 1995, pp. 31-50.

[85] G. Greenleaf, "'Modernised' Data Protection Convention 108 and the GDPR", *Privacy Laws & Business International Report* (2018) 154, pp. 22-23.

[86] G. Greenleaf, "Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives", *Privacy Laws & Business International Report*, (2016) 142, pp. 14-17.

[87] En su informe anual de 2018 a la Asamblea General de Naciones Unidas, el Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, alentó a los Estados miembros de la ONU a ratificar el Convenio 108 en su versión modernizada por el Protocolo.

[88] Según el artículo 37 del Protocolo, éste entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses después de la fecha en que todas las Partes del Convenio hayan expresado su consentimiento en obligarse por el Protocolo. En el caso de que este Protocolo no haya entrado en vigor después de la expiración de un período de cinco años desde la fecha en que se abrió a la firma, el Protocolo entrará en vigor con respecto a aquellos Estados que hayan expresado su consentimiento en obligarse por él, siempre que el Protocolo tenga al menos treinta y ocho Partes.

mentación de la otra Parte establezca una protección equivalente; o cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de protección de datos.

58. El Protocolo modifica considerablemente este artículo, convirtiéndolo en el 14 y poniéndolo en línea con el RGPD, dado que añade que una Parte puede limitar las transferencias si existe un riesgo real y grave de que la transferencia a otra Parte, o de esa otra Parte a un país que no sea Parte, conduzca a eludir las disposiciones del Convenio. Una Parte también puede limitar las transferencias si está obligada por normas armonizadas de protección compartidas por los Estados pertenecientes a una organización internacional regional, es decir, la UE, pero esto ya no se aplicaría al Reino Unido tras su salida.

IV. Conclusiones

59. Como se ha visto, en el ámbito de la protección de datos, la salida del Reino Unido de la UE va a ser sumamente problemática. El Acuerdo de Retirada sólo soluciona este problema hasta el 31 de diciembre de 2020, pero la cuestión permanece sobre cómo asegurar la libre transferencia transfronteriza de datos entre el Reino Unido y el Espacio Económico Europeo cuando el periodo de transición termine y se sientan plenamente los efectos de la salida del Reino Unido.

60. La incertidumbre a la que se ha sometido a las empresas tiene consecuencias económicas muy relevantes y es especialmente difícil de encarar por parte de las pequeñas y medianas empresas que no cuentan con mecanismos como las normas corporativas vinculantes. Lo más ventajoso para ellas sería una decisión de adecuación, pero en los pocos meses de período transitorio si éste efectivamente termina en 31 de diciembre de 2020, no parece posible que la Comisión Europea lleve a cabo un análisis profundo y que al Reino Unido le dé tiempo de hacer las necesarias reformas en su propia normativa y, además, realizar el resto de pasos necesarios del procedimiento de manera apropiada.

61. Una decisión de adecuación puede tardar años y si se hace en unos pocos meses eso será indicio de que la Comisión se ha visto forzada a poner por delante el interés económico de la protección de los derechos fundamentales.

62. Puesto que, como se ha visto, existen dudas sobre la compatibilidad de la actuación de las autoridades de inteligencia del Reino Unido para salvaguardar la seguridad nacional y el régimen de conservación de datos, y los estándares de protección europeos. Éstas serán probablemente las cuestiones en las que se ponga el foco de la evaluación de adecuación. Es necesario recordar además que, incluso si se llega a una decisión de este tipo, el TJUE la puede declarar inválida si no es lo suficientemente garantista.

63. En ese sentido, será relevante ver cómo se van resolviendo los múltiples casos pendientes citados tanto ante el TEDH como ante el TJUE, para aclarar los estándares de derechos humanos a los que se va a someter a las autoridades del Reino Unido.

64. La mejor manera de evitar contratiempos es que el Reino Unido empiece a trabajar en poner toda su normativa, también la relativa a la protección de la seguridad nacional, en línea con el Convenio Europeo de Derechos Humanos y con las normas de la UE para garantizar una auténtica protección de datos personales.

65. A la espera de una decisión de adecuación, tendría sentido desde un punto de vista de la gestión de riesgos y la precaución que cualquier empresa que quiera transferir datos personales desde el Espacio Económico Europeo al Reino Unido cumpla con las reglas del RGPD e incluya en sus nuevos contratos cláusulas tipo de protección de datos, pero sobre todo que revisen sus protocolos de funcionamiento para asegurarse de cumplir con los estándares que en éstas se prometen.