

Las transfencias de datos personales al Reino Unido en la era postbrexit (1)

Corral Sastre, Alejandro

Comentarios



Alejandro Corral Sastre

Profesor de Derecho Administrativo

Universidad CEU-San Pablo de Madrid

1. Introducción

El 23 de junio de 2016 los ciudadanos de la Unión Europea, al menos aquellos que nos consideramos europeos convencidos, sufrimos un duro golpe. El Reino Unido, uno de los Estados Miembros más antiguos de la Unión (2) , decidió, por medio de un referéndum no vinculante, separarse del proyecto europeo.

Desde entonces, todo el proceso ha estado rodeado de una incómoda incertidumbre: en cuanto a si el Gobierno iba a tener en cuenta el referéndum, dado que no era vinculante; sobre si se notificaría la decisión que daría comienzo al procedimiento del artículo 50 del Tratado de la Unión Europea (LA LEY 109/1994) (en adelante, TUE); acerca del papel que debe jugar el Parlamento Británico en todo el proceso; respecto a la posibilidad de que se celebre un segundo referéndum que anule en anterior; en qué posición quedarían los territorios del Reino Unido que, mayoritariamente, votaron a favor de la permanencia (3) ; entre otras muchas cuestiones que quedan en el aire. Todo ello aderezado, además, con unas elecciones anticipadas convocadas por la Primera Ministra, *Theresa May* (4) , en las que el partido conservador, lejos de consolidar una posición firme para la futura negociación con la Unión, perdió la mayoría absoluta en el Parlamento (5) , lo que generó aún más incertidumbre en todo este proceso. Sin dejar de mencionar la llegada a *Downing Street 10* de uno de los principales defensores del *Brexit*, incluso sin acuerdo: *Boris Johnson*, que ha intentado suspender el Parlamento británico en una decisión sin precedentes, revocada, por cierto, por el Tribunal Supremo.

La Unión Europea y el Gobierno de Reino Unido llegaron a un acuerdo sobre la retirada. Dicho Acuerdo es refrendado el 25 de noviembre de 2018 en la reunión extraordinaria del Consejo Europeo, en los términos exigidos por el artículo 50 del TUE (LA LEY 109/1994). Pero el Gobierno Británico se ha encontrado un importante obstáculo para la ratificación definitiva del acuerdo de retirada: la negativa del Parlamento manifestada hasta en dos ocasiones (6) . Esta circunstancia ha hecho que la situación se vuelva muy tensa a escasas semanas de la salida, inicialmente prevista para el 31 de octubre, aunque ha sido objeto de nueva prórroga hasta el 31 de enero del 2020 por parte de la UE.

Por su parte, el líder de la oposición laborista, *Jeremy Corbyn*, tras meses de ambigüedad, defiende, sin mucho entusiasmo, más bien con indiferencia, la posibilidad de celebrar un nuevo referéndum sobre la salida de la UE (7) . En cualquier caso, y con la fecha límite ya sobre nuestras cabezas, se vive una situación de falsa calma que nos acerca cada vez más a la temible salida sin acuerdo, es decir, a lo que se ha venido llamando *Brexit* duro.

En todo este proceso, para aportar todavía, si cabe, más incertidumbre, el Parlamento ha acordado su disolución convocando nuevas elecciones para el próximo 12 de diciembre, es decir, 50 días antes de la fecha prevista para la salida tras la nueva prórroga.

Cuando la salida de la Unión Europea sea definitiva, el Reino Unido será considerado como un tercer estado a efectos de la aplicación del RGPD

En este contexto, es necesario aclarar que este trabajo se basa en hipótesis que todavía no se han materializado, por lo que es posible que en el futuro no se hagan realidad. No obstante, lo considero un ejercicio necesario para situarnos en los diferentes escenarios que pueden darse respecto al derecho fundamental a la protección de datos personales, dado que cuando la salida sea definitiva, el Reino Unido será considerado como un tercer estado a efectos de la aplicación del Reglamento General de Protección de Datos (LA LEY 6637/2016) (8) (en adelante, RGPD), es decir, se habrá de tener en cuenta lo dispuesto en el Capítulo V (artículos 44 a 50), que regulan las

«transferencias internacionales de datos personales a terceros países u organizaciones internacionales», así como los correspondientes considerandos (del 101 al 116) que adquieren, como se verá, especial importancia.

Pero antes de referirnos a las consecuencias de *Brexit* sobre el derecho fundamental a la protección de datos, es necesario, según estimo, hacer referencia, siquiera breve, al contexto en que se produce la votación en el referéndum

2. Breve referencia al contexto económico, político y social en el Reino Unido del *Brexit*

Para realizar un esbozo aproximado de las consecuencias de la salida del Reino Unido de la Unión Europea, debemos acercarnos a las causas que lo provocaron. Es decir, por qué una muy reducida mayoría de ciudadanos británicos votaron a favor del *Brexit* (9) .

Parece que los ciudadanos del Reino Unido no votaron con toda la información sobre las posibles consecuencias económicas de la salida

En primer lugar, parece que los ciudadanos del Reino Unido no votaron con toda la información sobre las posibles consecuencias económicas de la salida. Así, algunos autores plantean que mucha información relevante fue deliberadamente escondida a los votantes (10) , lo que no puede ser considerado democrático, teniendo en cuenta la trascendencia de la votación, no solo para los ciudadanos británicos.

Pero si se analiza más en profundidad, hay un trasfondo social y político que no se puede desdeñar (11) . Así, parece que una de las principales razones que llevó a muchos ciudadanos a votar a favor de la salida fue la inmigración. Es decir, los ciudadanos británicos perciben que hay un exceso de inmigrantes y que ello se debe, fundamentalmente, a las políticas que se aprueban desde la «lejana» Bruselas, donde no se tienen en cuenta los problemas reales de los británicos (12) .

Por otro lado, no se puede negar que el *Brexit* es una consecuencia, casi inmediata, de la grave crisis económica mundial que se ha vivido en los últimos años. Los ciudadanos de clase media y trabajadores de todo el mundo han percibido que las políticas que se impulsan desde la Unión Europea, políticas en definitiva basadas en la globalización de la economía, lejos de beneficiarles, han contribuido a empeorar su situación y a mermar sus derechos sociales. Parece ser, por consiguiente, que el ciudadano medio del Reino Unido ha dado un voto de castigo a aquellos que, según su idea, realmente se benefician con la pertenencia del Reino Unido a la Unión: los trabajadores del sector financiero de la *City* (13) .

La situación económica y social del Reino Unido ha sido el caldo de cultivo idóneo para que surjan movimientos populistas de corte iliberal, es decir, partidos políticos que defienden un patriotismo excluyente y xenófobo (14) . Además, la crisis de los refugiados sirios y los atentados terroristas sufridos en los últimos años han alentado esta idea que, en definitiva, ha propiciado el resultado del referéndum.

Sirva esta lección para que no se vuelva a producir una situación semejante en otro Estado Miembro de la Unión Europea, pues como señala Daniel SARMIENTO, «Actuar como si la retirada del Reino Unido fuese únicamente una cuestión interna británica sería un planteamiento tan suicida como el de la orquesta del Titanic. La Unión debe realizar un proceso de reflexión no tanto para pensar el RU, sino en sí misma, so pena del que el *Brexit* sea el catalizador de un imparable efecto dominó que termine desbaratando el proyecto de integración europea en su totalidad» (15)

3. La regulación de las transferencias internacionales de datos

Si se tienen en cuenta que, tras el *Brexit*, antes o después, el Reino Unido será considerado un tercer país a efectos

del tratamiento de datos personales (16) , se ha de indicar aunque sea muy brevemente, como se regulan las transferencias internacionales de datos en el RGPD (LA LEY 6637/2016), pues existe alguna novedad respecto al régimen jurídico establecido en la Directiva 95/46 (LA LEY 5793/1995) (17) .

El concepto de transferencia internacional puede ampliarse a aquellos supuestos en los que no solo haya un envío de información, sino también una puesta a disposición de los datos para su consulta fuera del EEE

Sobre lo que deba ser considerado transferencia internacional, lo cierto es que el RGPD (LA LEY 6637/2016) no lo establece. Tampoco lo hacía la Directiva (18) . Una definición de transferencia internacional la encontramos en el artículo 12 del Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, donde se indica que son transmisiones de datos «a través de fronteras nacionales» (19) . Por otro lado, podemos acudir a la definición que nos ofrece nuestro ordenamiento interno en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LA LEY 13934/2007)

(en adelante, RLOPD (LA LEY 13934/2007)), en cuyo artículo 5.1.s), dedicado a definiciones, señala que una transferencia internacional de datos es un: «Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español» (20) . Es decir, transferencia internacional se producirá cuando haya un tratamiento de datos fuera del Espacio Económico Europeo (en adelante, EEE). (21) Se debe aclarar que el RLOPD (LA LEY 13934/2007) continua vigente en todo aquello que no se oponga o resulte incompatible con lo dispuesto en el RGPD (LA LEY 6637/2016) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) (en adelante LOPDGD (LA LEY 19303/2018)) que no deroga expresamente el Reglamento de desarrollo de la LOPD (LA LEY 13934/2007) de 1999 (22) .

Se trata, en cualquier caso, de una definición compleja y habrá que estar, en cada momento, a lo que establezca la jurisprudencia del Tribunal de Justicia de la Unión Europea. Parece, no obstante, que el concepto de transferencia internacional puede ampliarse a aquellos supuestos en los que no solo haya un envío de información, sino también una puesta a disposición de los datos para su consulta (23) .

3.1. Breve referencia a las transferencias internacionales de datos en la Directiva 95/46

La regulación de las transferencias internacionales de datos en la Directiva se encontraba en los artículos 25 y 26. Según estos preceptos, solo era posible realizar una transferencia internacional de datos cuando el país tercero correspondiente garantizara un nivel de protección adecuado (artículo 25). Esa era, por tanto, la regla general. Sin embargo, el artículo 26 reconocía un amplio elenco de excepciones, entre las que cabía destacar, en lo que ahora interesa, la reconocida en su apartado segundo, es decir, que el Estado Miembro podía autorizar una transferencia a un tercer país que no gozara de un nivel adecuado de protección, cuando el responsable de tratamiento ofreciera garantías suficientes de que los derechos de las personas fueran adecuada y suficientemente protegidos (24) .

Como veremos en los apartados siguientes, esa excepción a la que se acaba de hacer referencia, se ha convertido, con el RGPD (LA LEY 6637/2016), en regla general.

3.2. La regulación de las transferencias internacionales de datos según el RGPD

Lo primero que cabe destacar, respecto a la nueva regulación, es el sensible incremento de artículos referidos a las transferencias internacionales, lo que pone de manifiesto la importancia de la cuestión (25) . Así, de dos artículos que dedicaba la Directiva, se pasa a seis en el RGPD (LA LEY 6637/2016), muy extensos, además: del 44 al 49.

También es reseñable que mientras en la Directiva solo se preveía como transferencia internacional la cesión de datos a terceros países, el Reglamento amplía el sujeto destinatario a organizaciones internacionales, que son definidas en el artículo 4.26 de forma muy imprecisa (26) . Esta previsión puede llegar a ser problemática, ya que no se tiene en cuenta en la regulación el país donde esté ubicada la misma. En este sentido, no es lo mismo que la organización esté dentro del espacio EEE a que se sitúe fuera. No obstante, las características propias de estos sujetos de derecho internacional, con autonomía jurídica respecto de los países que la forman, hace necesario su referencia expresa en el Reglamento (27) .

Por otro lado, otra novedad importante en el RGPD (LA LEY 6637/2016) se refiere a que se permiten, como regla general, las transferencias internacionales no solo cuando el país tercero u organización internacional de que se trate ofrezca un nivel adecuado de protección (artículo 45), sino que se amplía a los supuestos en que el responsable y encargado de tratamiento ofrezcan garantías adecuadas (artículo 46). Es decir, este último supuesto pasa de ser una de las excepciones previstas en el artículo 26 de la Directiva, a ser considerado un supuesto normal, permitido sin autorización expresa, para que se realice una transferencia internacional de datos.

Siguiendo a PIÑAR MAÑAS, será posible una transferencia internacional de datos cuando: se base en una decisión de adecuación; en garantías adecuadas o en alguna de las excepciones previstas en el artículo 49 del RGPD

Por consiguiente, y siguiendo al profesor PIÑAR MAÑAS, será posible una transferencia internacional de datos a un tercer país u organización internacional cuando:

- Se base en una decisión de adecuación
- Se base en garantías adecuadas
- Se base en alguna de las excepciones previstas en el artículo 49 del RGPD (LA LEY 6637/2016) (28)

Teniendo en cuenta lo anterior, es importante, en primer lugar, señalar quien puede emitir una decisión de adecuación. En este sentido, el artículo 45.1 señala que será la Comisión quien decida qué «tercer país, territorio, sector específico u organización internacional» de que se trate, garantizan un nivel adecuado para que la transferencia no requiera ninguna autorización específica. Para dictar esa decisión, que se hace mediante un acto de ejecución, la Comisión debe evaluar una serie de elementos del tercer país, territorio, sector específico u organización internacional (artículo 45.2 del RGPD (LA LEY 6637/2016)) (29) . Llama la atención la posibilidad de que la decisión afecte no solo a un tercer país, sino también a un territorio (de un tercer país, se entiende) o sector específico. Ya se había admitido la posibilidad de que la decisión de adecuación afectase, exclusivamente, a un determinado número de empresas en un país determinado (30) , pero ahora se indica la posibilidad de que afecte a uno o varios territorios específicos, en el supuesto, según estimo, de que se trate de un estado compuesto o federal que reconozca cierta autonomía a los territorios que lo componen. En la misma línea, se puede reconocer un nivel de adecuación a uno o varios sectores económicos o de actividad específicos.

Como ya se ha indicado, otro supuesto normal de transferencia internacional de datos que no necesita autorización es que el responsable o encargado de tratamiento ofrezcan garantías adecuadas y «a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas (artículo 46.1, *in fine*). Estas garantías adecuadas pueden prestarse, según lo dispuesto en el artículo 46.2 del RGPD (LA LEY 6637/2016), mediante:

- a)** un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- b)** normas corporativas vinculantes;
- c)** cláusulas tipo de protección de datos adoptadas por la Comisión;
- d)** cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;
- e)** un código de conducta (31) ;
- f)** un mecanismo de certificación.

Mención especial merecen las normas corporativas vinculantes (32) , pues son una de las principales novedades del RGPD (LA LEY 6637/2016). Se definen en el artículo 4.20 como: «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». Estas normas corporativas vinculantes o *BCR's* por sus siglas en inglés, han planteado algún problema en el pasado, pues se trata, en definitiva, de supuestos de autorregulación. No obstante, hay que señalar que el RGPD (LA LEY 6637/2016) ha venido a aclarar, en gran medida, las dudas que planteaban, pues se realiza una regulación muy detallada y extensa en el artículo 47, donde se establecen los requisitos que tienen que cumplir y el contenido mínimo de las mismas (33) . Así, como requisitos, el artículo 47.1 señala que:

- a)** sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes

del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado, es decir, que tengan, como mínimo, esos elementos (34) .

Para terminar este epígrafe, debemos hacer una breve referencia a las excepciones para situaciones específicas recogidas en el artículo 49 del RGPD (LA LEY 6637/2016). Según este precepto: en ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia 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;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

En alguno de estos supuestos, por consiguiente, no será necesaria una autorización de las autoridades de control para realizar la correspondiente transferencia internacional. Este elenco de excepciones debe considerarse como *numerus clausus*, aunque algunas de ellas están enunciadas en términos muy amplios (35) .

3.3. Las transferencias internacionales de datos en la LOPDGDD

Por su parte, la norma española de adaptación al RGPD (LA LEY 6637/2016), esto es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) (LOPDGDD (LA LEY 19303/2018)), se refiere a las transferencias internacionales de datos personales en su Título VI, artículos 40 a 43.

La regulación contenida en estos preceptos se limita a completar y a adaptar la regulación prevista en el RGPD (LA LEY 6637/2016) a nuestro ordenamiento jurídico, como no podía ser de otra forma. En este sentido, concreta en la Agencia Española de Protección de Datos (AEPD), y en las agencias autonómicas (36) , la posibilidad de adoptar las cláusulas contractuales tipo para la realización de transferencias internacionales (artículo 41.1), previo sometimiento al dictamen del Comité Europeo de Protección de Datos. Asimismo, podrán aprobar las normas corporativas vinculantes a instancias de entidades que estén situadas en España. Es necesario también en este supuesto la solicitud de un dictamen al Comité.

Por otro lado, la AEPD y las autoridades autonómicas serán competentes para autorizar las transferencias de datos internacionales cuando países u organizaciones internacionales que no dispongan de decisión de adecuación o cuando no se amparen en ninguna de las garantías previstas más arriba, que podrá otorgarse en los siguientes supuestos (artículo 42.1):

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con

fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679 (LA LEY 6637/2016).

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

Además, los responsables de tratamiento deberán informar con carácter previo a la AEPD o, en su caso, las autoridades autonómicas, cuando pretendan realizar cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679 (LA LEY 6637/2016). Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

4. La aplicación del Reglamento General de Protección de Datos una vez se haya producido la salida efectiva

En este contexto al que me acabo de referir, y ya entrando de lleno en la materia a la que se refiere este trabajo, lo único que podemos saber con absoluta certeza, en el momento en que se escriben estas palabras, es el momento en el que se empezó a aplicar el RGPD (LA LEY 6637/2016). Como es sabido, el Reglamento se publicó en el Diario Oficial de la Unión Europea (en adelante, DOUE) el 4 de mayo de 2016. Su artículo 99 establece dos periodos distintos: entrada en vigor, por un lado, y aplicación, por otro. La razón de que se estableciera esta fase de adaptación (que no transposición) de dos años, más propia de las Directivas, parece estar en la necesidad de ofrecer a los Estados Miembros un amplio margen de adaptación a las importantes novedades que prevé la norma (37) .

Una vez que el RGPD (LA LEY 6637/2016) resulta plenamente aplicable en el Reino Unido, queda determinar que ocurrirá después del 31 de octubre del 2019. Los posibles escenarios son los siguientes:

- 1.** Que no se haya ratificado el Acuerdo de Retirada por el Parlamento británico y, por tanto, la separación se produzca sin Acuerdo de por medio entre ambas partes. Sería la materialización del denominado *Brexit* duro y, por tanto, en mi opinión, la menos deseada, aunque parece la más probable, a la vista de los últimos acontecimientos.
- 2.** Que finalmente el Parlamento británico apruebe Acuerdo de Retirada y, por tanto, el «divorcio» se rija por las reglas en el contenidas. En la fecha en la que se escriben estas páginas parece la opción menos probable, y sin embargo es la más deseable. Es importante señalar la importancia, en este supuesto, del período de transición al que luego me referiré.
- 3.** Por último, que la UE otorgue una nueva prórroga, de más o menos tiempo, para que Reino Unido ratifique finalmente el Acuerdo de Retirada, o se estudien otras posibilidades alternativas. Esta opción solo la veo viable si ocurre algo que justifique dicha nueva prórroga, es decir, un cambio de Gobierno, dimisión del Primer Ministro, o algo similar, ya que la UE no parece muy dispuesta a conceder otro plazo mayor

Teniendo en cuenta lo anterior, parece necesario analizar lo que ocurrirá en las hipótesis 1 y 2, es decir, como quedarán las transferencias tras un *Bréxit* duro y como serían con un *Brexit* con Acuerdo. La última de las hipótesis, la de la prórroga, supone simplemente alargar el fatídico momento, pero resulta interesante por la posibilidad de estudiar nuevas alternativas.

4.1. Influencia del Reino Unido en la configuración de la perspectiva europea del derecho fundamental a la protección de datos

No obstante, considero que antes de analizar más detenidamente los hipotéticos escenarios en los que quedaría el flujo de datos entre ambos lados del Canal de la Mancha después de la separación, es necesario, e incluso justo, hacer una breve referencia al compromiso del Reino Unido con la protección del derecho fundamental a la protección de datos.

Así, las aportaciones de los británicos es esta materia han sido muy

En materia de protección de datos los británicos han adoptado un enfoque innovador y flexible, buscando un equilibrio, nada fácil, entre las exigencias y requisitos legales, por un lado, y la realidad tecnológica por otro

relevantes. En general se puede manifestar que han adoptado un enfoque sobre la materia innovador y flexible, intentando buscar el equilibrio, nada fácil, entre las exigencias y requisitos legales, por un lado, y la realidad tecnológica por otro (38) .

Así, han sido pioneros en reconocer las dos caras de la misma moneda, al fusionar el derecho fundamental a la protección de datos con el derecho de acceso a la información pública (39) . Otra de las aportaciones al campo de la protección de datos viene de la mano de la creación del *Data Protection Tribunal*, un órgano independiente especializado en protección de datos y derecho de acceso a la información que tiene por misión resolver los recursos

que se interponen frente a la autoridad británica de protección de datos, es decir, el *Information Commissioner's Office*. Por último, y sin ánimo de ser exhaustivo, desde el Reino Unido se ha fomentado la utilización de códigos de conducta desde hace ya varias décadas, una política que se ha trasladado al RGPD (LA LEY 6637/2016) (artículo 40). La influencia del enfoque británico sobre la perspectiva europea derecho fundamental es, por consiguiente, patente.

En últimos tiempos, y pese a haber activado ya el artículo 50 del TFUE (LA LEY 6/1957) que implica la separación de la Unión Europea, los británicos no han cesado en su empeño de adaptarse el RGPD (LA LEY 6637/2016). De hecho, el pasado año han aprobado una nueva Ley de protección de datos, la *Data Protection Act 2018*, que deroga la anterior de 1998, y por la que el Reino Unido pretende adaptarse a los requerimientos del RGPD (LA LEY 6637/2016). Es importante observar que ha sido uno de los primeros países en adaptar formalmente su normativa. De hecho, aunque con escasos meses de diferencia, lo hicieron antes que España.

Por otro lado, *Information Commissioner's Office*, es una autoridad pública con competencias de inspección y sanción desde mucho antes de la entrada en vigor y aplicación del RGPD (LA LEY 6637/2016), algo que no pasaba en todos los países de la UE. Como es sabido, la Directiva 95/46 (LA LEY 5793/1995) /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 (en adelante, la Directiva o Directiva 95/46 (LA LEY 5793/1995)) (40) había sido interpretada de diferente forma por los Estados Miembros, algunos de los cuales no dotaban a sus autoridades de control internas de potestades sancionadoras directas, lo que ocasionaba importantes diferencias en la materia entre los diferentes países (41) .

Reino Unido mantiene un compromiso firme con el reconocimiento de este derecho fundamental, lo que podrían justificar, llegado el caso de ruptura sin acuerdo, un reconocimiento de nivel adecuado de protección

Todas estas consideraciones nos permiten afirmar que Reino Unido mantiene un compromiso firme con el reconocimiento de este derecho fundamental, lo que podrían justificar, llegado el caso de ruptura sin acuerdo, un reconocimiento de nivel adecuado de protección. E incluso, como plantean algunos autores, no considerarlo un «tercer país», sino analizar otras posibles vías que faciliten el flujo de datos sin acudir a los instrumentos previstos para las transferencias internacionales, aunque es cierto que esta propuesta tiene una difícil articulación jurídica (42) .

Vamos a ver, a continuación, los diferentes posibles escenarios:

4.2. El supuesto del Bréxit con Acuerdo o Brexit «blando». ¿Qué ocurre con la protección de datos?

Como es conocido, el 25 de noviembre del 2018, los 27 Estados Miembros de la UE refrendan el proyecto de Acuerdo de Retirada y aprueban el proyecto de Declaración Política sobre las relaciones futuras entre la UE y el Reino Unido. El 5 de diciembre del mismo año, la Comisión Europea inicia el procedimiento para la firma y celebración del Acuerdo de Retirada del Reino Unido de la UE. El 13 de diciembre, los dirigentes de la UE celebran una reunión extraordinaria del Consejo Europeo, en su composición del artículo 50, para debatir el *Brexit*. En ella, vuelven a confirmar sus Conclusiones de 25 de noviembre de 2018, en las que refrendaron el Acuerdo de Retirada y aprobaron la Declaración Política.

El 11 de enero de 2019, el Consejo (Art. 50) adopta una Decisión sobre la firma del Acuerdo de Retirada. También aprueba un proyecto de Decisión sobre la celebración del Acuerdo de Retirada y decide remitir dicho proyecto de Decisión al Parlamento Europeo para su aprobación. El 14 de enero de 2019, los presidentes *Tusk* y *Juncker*

intercambian correspondencia con la primera ministra *May*. En su carta, los presidentes responden a las cuestiones planteadas por la primera ministra del Reino Unido y aportan aclaraciones sobre el Acuerdo de Retirada del *Brexit* y la Declaración Política. Señalan lo siguiente: «Ambos estaremos listos para firmar el Acuerdo de Retirada tan pronto como se haya producido la votación significativa en el Parlamento del Reino Unido». Esta votación todavía no se ha producido y, según parece, con la suspensión del Parlamento británico no se producirá, por lo que nos vemos avocados a una salida sin acuerdo. No obstante, cabe mantener cierta esperanza habida cuenta de la resolución de la Corte Suprema de anular esta decisión de suspensión del parlamento. Los diferentes escenarios siguen abiertos.

En cualquier caso, al margen de lo que finalmente ocurra, es necesario analizar las previsiones que el Acuerdo de Retirada establece sobre el derecho fundamental a la protección de datos, ya que, de ratificarse finalmente el Acuerdo por el Parlamento británico, resultaría de aplicación.

De aplicarse el Acuerdo de retirada del Reino Unido, esta sería paulatina, por lo que durante un período de tiempo determinado la UE seguiría tratándole como un Estado miembro, salvo en lo que se refiere a la participación de este en las instituciones

En este sentido, debemos tener en cuenta que, de aplicarse el Acuerdo, la retirada sería paulatina, es decir, durante un período de tiempo determinado la UE seguiría tratado a Reino Unido como un Estado miembro, salvo en lo que se refiere a la participación de este en las instituciones. Así, según el artículo 2 del Acuerdo, que remite a su vez al artículo 126, establece un período transitorio hasta el 31 de diciembre de 2020 (43) .

Pero la regulación en materia de protección de datos viene recogida en el Título VII del Acuerdo, artículos 70 a 74. El artículo 70 establece que ha de entenderse por «Derecho de la Unión sobre protección de datos personales, incluyendo al RGPD (LA LEY 6637/2016), entre otras normas (44) . Es el artículo 71 el que regula, en concreto, que ocurre con el tratamiento de datos personales de interesados fuera del Reino Unido. En este sentido, el

precepto señala que se aplicará el Derecho de la Unión Europea en la materia siempre que:

- a) Los datos personales se hayan tratado en virtud del Derecho de la Unión en el Reino Unido antes del final del período transitorio, es decir, del 31 de diciembre de 2020; o
- b) Los datos personales sean tratados en el Reino Unido después del final del período transitorio con base en el presente Acuerdo

Pese a que la redacción o la traducción no resultan especialmente claras, la clave parece situarse, por consiguiente, en el período transitorio, de manera que se seguirá aplicando el Derecho de la Unión Europea (RGPD (LA LEY 6637/2016), entre otras normas) para todos los datos personales que se hayan tratado (obtenido) antes del 31 de diciembre de 2020, ya que es la legislación vigente sobre protección de datos en el Reino Unido. Después de este período, el tratamiento de datos personales de interesados de fuera del Reino Unido se ceñirá a lo dispuesto en el Acuerdo, que nada señala sobre la legislación aplicable más allá de lo que se indica en el artículo 134 sobre las disposiciones financieras. Es decir, después del período transitorio establecido en el Acuerdo, y salvo que este establezca otra cosa distinta, los datos personales tratados se regirán por la normativa británica, es decir, de momento, la *Data Protection Act 2018*, que es la adaptación del RGPD (LA LEY 6637/2016) en el ordenamiento británico.

El Acuerdo de retirada prevé la posibilidad de que la Comisión emita una decisión de adecuación del nivel de protección de datos sobre el Reino Unido, de modo que cualquier flujo de datos estaría amparado en la misma

Por su parte, el apartado 2 del artículo 71 prevé la posibilidad de la Comisión emita una decisión de adecuación del nivel de protección de datos sobre el Reino Unido, de modo que no sería aplicable lo establecido en el apartado 1 que más arriba se ha analizado, porque cualquier flujo de datos estaría amparado en esa decisión de adecuación.

Entiendo que esta sería la forma más adecuada de solventar el asunto ya que, como se ha señalado en otro lugar de este trabajo, no puede caber duda de que el Reino Unido tiene un nivel de protección del derecho fundamental a la protección de datos adecuado y conforme al RGPD (LA LEY 6637/2016) y restantes normas. De hecho, la *Data Protection Act 2018* es una adaptación a la normativa de la UE, en la que, como es lógico, se menciona al RGPD (LA LEY 6637/2016) como norma de referencia en esta materia, asumiendo, por consiguiente, su

aplicación.

4.3. Separación sin Acuerdo de Retirada: Brexit «duro»

En caso de un Brexit duro, el Reino Unido se convierte, de forma automática y sin transición, en un tercer estado a efectos del RGPD, por lo que habrá que acudir a los instrumentos previstos para las transferencias internacionales de datos

Teniendo en cuenta lo que ya se ha manifestado más arriba, es muy probable, por consiguiente, que el Reino Unido abandone la Unión después del 31 de octubre de 2019 sin que se haya ratificado el Acuerdo y, por tanto, materializándose el denominado *Brexit* duro, sin período de transición. En este supuesto, el Reino Unido se convierte, de forma automática, sin transición, repito, en un tercer estado a efectos del RGPD (LA LEY 6637/2016), por lo que habrá que acudir a los instrumentos previstos para las transferencias internacionales y que ya han sido analizados.

En este caso, hay que tener en cuenta que el RGPD (LA LEY 6637/2016) también habrá sido aplicado durante un plazo de tiempo determinado. Así, se habrá aplicado en Reino Unido durante más de un año y, posteriormente, es de esperar, seguirá ejerciendo influencia, por inercia, en las normas

posteriores que se puedan aprobar (sin mencionar, además, el artículo 3.2 del RGPD (LA LEY 6637/2016) que prevé un ámbito de aplicación territorial, en algunos supuestos, que supera el territorio de los 27 Estados miembros).

La idea latente en el Reino Unido es continuar con el espíritu de protección del derecho fundamental a la protección de datos que establece el RGPD y otras normas europeas

En cualquier caso, la idea latente en el Reino Unido es continuar con el espíritu de protección del derecho fundamental a la protección de datos que establece el RGPD (LA LEY 6637/2016) y otras normas europeas. No va a haber, por tanto, según parece, una ruptura total del Reino Unido respecto a la protección de este derecho fundamental. Tampoco puede haberlo, pues pese a la salida de la UE, seguiría estando vinculado por otros instrumentos internacionales, como el Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981 (45) . Así lo ha manifestado, expresamente, la autoridad de control británica (46) (*Information Commissioner's Office* o ICO, por sus siglas en inglés) en su estrategia internacional para los años 2017-2021 (47)

, aprobada en julio de 2017. De hecho, su intención es participar activamente en el Comité Europeo de Protección de Datos (48) mientras permanezca en la Unión y mantener relaciones con el resto de autoridades nacionales y europeas, en mayor beneficio de la protección del derecho fundamental.

Si esto es así, lo más probable es que una vez se produzca la salida del Reino Unido de la Unión, la Comisión, en un plazo más o menos breve (49) , dicte una decisión de adecuación del nivel de protección de datos para Reino Unido, de manera que se permitan las transferencias internacionales a su territorio en los términos establecidos en el artículo 45 del RGPD (LA LEY 6637/2016). No obstante, hasta que se dicte esa decisión de adecuación, los flujos de datos entre la Unión y Reino Unido deberán ampararse en alguna de las formulas previstas en el artículo 46 (garantías adecuadas), artículo 47 (BCR 's) o las excepciones del artículo 49, como ya se ha señalado en otro lugar.

Teniendo en cuenta el acercamiento entre Reino Unido y EEUU, es posible un cambio de perspectiva que se aproxime a la visión estadounidense en la materia

Hay que tener en cuenta, en cualquier caso, que el artículo 45.3 del RGPD (LA LEY 6637/2016) prevé que la decisión de adecuación establezca, además, un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes del país. No es probable que ese espíritu de respeto a los principios y bases del RGPD (LA LEY 6637/2016) cambien en los próximos años, pero teniendo en cuenta el acercamiento entre Reino Unido y Estados Unidos, es posible también que cambie la perspectiva en materia de protección de datos, aproximándose a la visión estadounidense en la materia, lo que podría implicar la pérdida del nivel

adecuado de protección. Esta posibilidad sería el peor escenario posible, el escenario del «*The «go it alone» model*».

4.4. Una nueva prórroga, demasiado corta, para estudiar otras alternativas

Como hemos manifestado más arriba la UE ha concedido una nueva prórroga hasta el 31 de enero del 2020 para que se llegue al ansiado acuerdo. La decisión de una nueva prórroga por parte de la UE podría facilitar que el Parlamento Británico finalmente aprobase el Acuerdo de Retirada y, por tanto, evitar enormes problemas en las relaciones futuras

entre ambas partes. No obstante, estamos ante una prórroga demasiado corta para explorar otras alternativas que faciliten las futuras relaciones entre el Reino Unido y el continente en esta materia

En cualquier caso, estimo que una prórroga más larga podría ser beneficiosa para explorar nuevas formas de regular las transferencias de datos entre ambas partes. Así, por ejemplo, se puede plantear que se ofrezca un estatus especial al Reino Unido en esta materia, considerando las transferencias no como internacionales sino como transfronterizas, con algún mecanismo adicional de protección, si se estima oportuno (un comité de observación o similar). En este supuesto, habría que analizar la posibilidad de que Reino Unido participase en los mecanismos de cooperación y coherencia, si fuera necesario, algo, entiendo, perfectamente viable.

Otra posibilidad que merecería un análisis meditado sería un acuerdo internacional específico sobre libre flujo de datos entre ambas partes, sin que sea considerado transferencia internacional, en una posición similar a la que tienen los países que forman parte del Espacio Económico Europeo (pero sin formar parte de él), con lo que no sería necesario acudir a las herramientas establecidas para una transferencia internacional, como es sabido.

En cualquier caso, la posición del Reino Unido en materia de protección de datos quedaría garantizada en las instituciones, permitiéndole intervenir en las reuniones del Comité Europeo de Protección de Datos, quizás como cualquier otro Estado miembro, o si no se considera oportuno, con otro estatus (observador o similar)

Estas alternativas implicarían, en cualquier caso, una modificación de las previsiones establecidas en el Acuerdo de Retirada, que no parece que las partes estén dispuestas a cambiar o a iniciar nuevas negociaciones sobre esta materia específica.

Muy improbable, también, pero no se puede desdeñar, sería la incorporación del Reino Unido al Espacio Económico Europeo. Esta solución es sencilla, pero tiene claros inconvenientes políticos para el Reino Unido, porque debería explicar a la ciudadanía que pese a haber abandonado la Unión se mantienen muchas de las políticas procedentes de la Unión Europea. Además, con una posición mucho menos relevante en las Instituciones

Sin embargo, en materia de protección de datos sería, quizás, lo más adecuado, teniendo en cuenta que el flujo de datos entre los miembros del EEE es libre y, por tanto, no se considera transferencia internacional según lo dispuesto en el RGPD (LA LEY 6637/2016).

4.5. Una posibilidad que no se ha materializado: Abandono unilateral antes de la fecha prevista para la salida. La ruptura total

Puestos a barajar escenarios, voy a referirme a continuación a uno ya altamente improbable, por la cercanía del 31 de octubre. No obstante, merece la pena analizarlo pues entiendo que puede ayudar a comprender mejor la situación actual del Reino Unido, con una importante crisis política interna y una sociedad civil dividida, precisamente, sobre el *Brexit*. Quizás sea un triste consuelo, pero, en mi opinión, hay que valorar el esfuerzo por llegar a un acuerdo con la UE, aunque este haya sido posteriormente rechazado, en varias ocasiones, por el Parlamento. El mismo Parlamento que, 24 horas después, rechaza mediante votación que la salida se haga efectiva sin ningún tipo de acuerdo (50) .

Este ha sido siempre el escenario más improbable, debido, fundamentalmente, a que desde el primer momento se planteó la necesidad de negociar con la UE. No obstante, siempre ha habido defensores de esta posibilidad de ruptura inmediata y sin previa negociación, que estaba prevista así en los tratados antes de Lisboa (51) , es decir, de la versión más dura del *hard Brexit*.

En relación con las consecuencias sobre la protección de datos, hay que tener en cuenta que, en este escenario, Reino Unido hubiera sido considerado a todos los efectos como un tercer país y, por consiguiente, las transferencias de datos a su territorio hubieran debido ser consideradas transferencias internacionales a todos los efectos desde el momento de la ruptura total.

Por otro lado, como ya se ha mencionado, y dado que su legislación interna ya se ha adaptado al RGPD (LA LEY 6637/2016) a través de la *Data Protection Act 1998*, de haberse producido la ruptura antes del 31 de octubre de 2019, su nivel de protección de datos debería considerarse adecuado a efectos de una posible decisión de la Comisión. Otra cuestión distinta, ya de índole político, es que la Comisión quisiera «castigar» esa separación unilateral no emitiendo la decisión de adecuación.

5. En cualquiera de los escenarios, el Reino Unido debe tener en cuenta las previsiones del RGPD

No obstante los escenarios a los que antes me he referido, se ha de tener en cuenta que el ámbito de aplicación territorial del RGPD (LA LEY 6637/2016), recogido en el artículo 3, hace que en el Reino Unido no se pueda desdeñar la aplicación del RGPD (LA LEY 6637/2016) en ningún caso (52) .

Así, se establece que el Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido (53) en la Unión cuando las actividades de tratamiento estén relacionadas con:

- a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
- b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Incluso en el peor de los escenarios, con una ruptura unilateral, el RGPD seguiría siendo aplicable en los supuestos señalados en el artículo 3.2 del RGPD.

Es decir, que independientemente del lugar de establecimiento (incluso en terceros países) del responsable o encargado de tratamiento, el RGPD (LA LEY 6637/2016) se aplica cuando se den algunos de estos supuestos. En definitiva, incluso en el peor de los escenarios, con una ruptura unilateral y un *The «go it alone» model*, el RGPD (LA LEY 6637/2016) seguiría siendo aplicable en los supuestos señalados en el artículo 3.2. Cuestión distinta es que las decisiones de aplicación del RGPD (LA LEY 6637/2016) puedan ser adecuadamente ejecutadas en territorio británico.

6. Conclusiones

El abandono de la Unión Europea por parte del Reino Unido va a tener importantes consecuencias en materia de protección de datos. Y es que, pasará a ser, salvo su improbable incorporación al EEE, un tercer país a efectos de aplicación del RGPD (LA LEY 6637/2016), por lo que habrán de tenerse en cuenta las herramientas previstas para las transferencias internacionales, con todas las dificultades y costes que ello genera para las empresas.

No obstante lo anterior, Reino Unido ha demostrado que pese a su salida de la UE hará todo lo posible por mantener un nivel de protección alto del derecho fundamental a la protección de datos, en los términos exigidos por la UE. Así lo acredita la aprobación de la *Data Protection Act 2018* y las manifestaciones efectuadas por la representante del ICO y del Gobierno.

Los diferentes escenarios que se han analizado pasan, en cualquier caso, por la aplicación del RGPD (LA LEY 6637/2016) durante el período transitorio previsto en el Acuerdo de Retirada, si es que este llega a aprobarse por el Parlamento.

Transcurrido ese plazo o en caso de separación sin Acuerdo, el Reino Unido pasará a ser un tercer estado a todos los efectos y los flujos de datos serán considerados transferencias internacionales, es decir, que habrán de utilizarse las diferentes herramientas previstas en el RGPD (LA LEY 6637/2016) para realizarlas, entre las que la decisión de adecuación parece la más idónea, sin desdeñar las demás, llegado el caso.

Al margen de otras alternativas más o menos creativas, que serían jurídicamente viables, pero políticamente improbables, como la de otorgar un estatus especial al Reino Unido en la materia, o acordar el libre flujo de datos entre ambas partes, lo que implicaría que el tráfico de datos no sería considerado como transferencias internacionales sino transfronterizas (activándose los mecanismos de cooperación y coherencia, si fuese necesario).

Todo ello si Reino Unido mantiene el espíritu de protección de datos europeo, del que ha sido, además, activo promotor. Pero pudiera darse el caso de que adoptase el que se ha venido en denominar *«The «go it alone» model»*, es decir, acercarse a otras posturas menos proteccionistas con este derecho fundamental, lo que implicaría importantes problemas en el flujo de datos entre ambas partes.

7. Bibliografía

CRAIG, P., *«Brexit: A Drama in Six Acts»*, *European law review*, núm. 4, 2016

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *«Information note on data transfers under the GDPR (LA LEY 6637/2016) in the event of a no-deal Brexit»*, 12 de febrero de 2019

COMISIÓN EUROPEA, «*Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*», 9 de enero de 2018.

DÍAZ-ROMERAL GÓMEZ, A., «Códigos de conducta en el Reglamento General de Protección de Datos (LA LEY 6637/2016)» en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M. (Coordinadores), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

DE HERT, P., y PAPAKONSTANTINO, V., «The rich contribution to the field of EU data protection: Let's not go for «third country» status after Brexit», *Computer Law & Security Review*, 33, 2017

GUASCH PORRAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014

JAMES, S., y QUAGLIA, L., «The political economy of finance in the UK and Brexit», en *The Political Economy of Brexit and the UK's National Business Model*, SPERI Paper No. 41, 2017

KORFF, D. «The data protection implications of a «No-Deal Brexit» (August 23, 2019), Disponible en SSRN: <https://ssrn.com/abstract=3441617> o <http://dx.doi.org/10.2139/ssrn.3441617>

MARTÍN DELGADO, I., «Brexit means Brexit... o no. Especulaciones, conjeturas y algunas consideraciones jurídicas al propósito de la decisión del Reino Unido de retirarse de la Unión Europea en el contexto del artículo 50 del TUE (LA LEY 109/1994)», *El Cronista del Estado Social y Democrático de Derecho*, núm. 64.

MULLOCK, J., y SHOOTER, S «*Brexit: Data protection and cybersecurity law implications*», <https://www.twobirds.com>

PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer, 2018

PIÑAR MAÑAS, J.L., «Transferencias de datos personales a terceros países u organizaciones internacionales» en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M. (Coordinadores), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

REMOLINA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014

RIPOL CARULLA, S., «Aplicación territorial del Reglamento» en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M. (Coordinadores), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

SARMIENTO, D., «Y después del Brexit... ¿Qué?», *El Cronista del Estado Social y Democrático de Derecho*, núm. 64

TATHAM, A. F., «Don't Mention Divorce at the Wedding, Darling!»: EU Accession and Withdrawal after Lisbon», en BIONDI, A., EECKHOUT, P., and RIPLEY, S., *EU Law after Lisbon*, Oxford Scholarship Online, 2012

TORREGROSA VÁZQUEZ, J., «Revisión de otros actos jurídicos de la Unión en materia de Protección de Datos, entrada en vigor y aplicación del Reglamento», en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M. (Coordinadores), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

WELFENS, P. J. J., «Cameron's information disaster in the referendum of 2016: an exit from Brexit?», *International Economics and Economic Policy*, octubre, 2016

(1) El presente trabajo se inscribe en el Proyecto de Investigación sobre *Protección de Datos, Seguridad e Innovación: Retos en un mundo global tras el Reglamento Europeo de Protección de Datos*, Ref. DER2016-79819-R, del programa I+D del Ministerio de Economía y Competitividad del que es investigador principal el Dr. D. José Luis Piñar Mañas: www.privacidadyacceso.com.

(2) Reino Unido se incorpora a la Unión Europea en 1973 junto con Irlanda y Dinamarca. No es por tanto uno de los Estados Miembros originarios, sino que se incorporó en la primera ampliación. No obstante, debemos señalar que la relación de Reino Unido con la Unión Europea ha sufrido, si se permite la expresión, muchos altibajos a lo largo de su historia.

(3) Según la página web de la BBC los resultados del referendun por territorios son los siguientes: *In England 53.4% of the votes were to leave the EU (15,188,406); in Northern Ireland 44.2% of the votes were to leave (349,442); in Scotland 38.0% of the votes were to leave (854,572)* consultado por última vez el 24 de julio de 2017 en http://www.bbc.com/news/politics/eu_referendum/results.

- (4) Theresa May llega al cargo tras la Dimisión de David Cameron, precisamente, por los resultados del referéndum.
- (5) El sistema electoral británico se basa en el *first-past-the-post*, es decir, «On polling day, the ballot paper is made up of candidates who are members of parties or independents. As only one MP will get elected, each party only stands one candidate to chose from. Voters put a cross next to their favourite candidate, or the candidate they like they most who they think has the best chance of winning», en este sentido, véase: www.electoral-reform.org.uk
- (6) La última votación sobre el Acuerdo del Brexit se ha producido el 12 de marzo de 2019 con un resultado de 391 votos negativos frente a 242 positivos.
- (7) Desde el primer momento se han albergado esperanzas de que la situación se revirtiera de alguna forma, así, véase, MARTÍN DELGADO, I., «Brexit means Brexit... o no. Especulaciones, conjeturas y algunas consideraciones jurídicas al propósito de la decisión del Reino Unido de retirarse de la Unión Europea en el contexto del artículo 50 del TUE (LA LEY 109/1994)», *El Cronista del Estado Social y Democrático de Derecho*, núm. 64. No obstante, y aun a riesgo de caer en un optimismo imprudente, se ven ciertos atisbos de esperanza en declaraciones como las del nuevo líder del partido liberaldemócrata, Vince Cable, quien abandera el movimiento *antibrexít*.
- (8) A estos efectos, Reino Unido no pertenecerá tampoco, al menos en principio, al Espacio Económico Europeo del que forman parte Islandia, Liechtenstein y Noruega.
- (9) Como es conocido, la votación al favor de la salida de la Unión Europea se impuso por muy poco: Votos a favor del *Brexit*: 17.410.742 (51,9%) Votos a favor de permanecer: 16.577.342 (48,1%) Total de votos: 33.577.342 Participación: 72%. <http://www.bbc.com>
- (10) WELFENS, P. J. J., «Cameron's information disaster in the referendum of 2016: an exit from Brexit?», *International Economics and Economic Policy*, octubre, 2016, pág., 540, «Prime Minister Cameron had not managed to include extremely important information on the economic effects of a BREXIT, from a study by the Treasury (HM Government 2016a) published on 18th April, 2016, in the 16-page info booklet (HM Government 2016b) which was sent out to all households: between 11th and 13th April to all households in England, and during the week from 8th May to all households in Scotland, Wales and Northern Ireland. The 6.2 % reduction in income as a long-term consequence of BREXIT, which Chancellor of the Exchequer George Osborne stressed in the press release on the 18th April, remained a fact hidden from the vast majority of households. If one takes into consideration the usual links between income trends and voting results in opinion polls/national elections and assumes a similar influencing factor in the case of a referendum, the BREXIT referendum would actually have resulted in a victory for the Remain camp had this information been more widely known. The Cameron government allowed the overwhelming majority of voters to cast their vote under a veil of ignorance regarding the economic consequences of a UK exit from the EU; a phenomenon which is historically unique. On the other hand, the Cameron government proved itself capable, when the situation of the referendum on Scottish independence arose in 2014, i.e. the preservation of the United Kingdom, of supplying all Scottish households with the relevant economic information, by providing two economically convincing info brochures to all households in Scotland, which contained meaningful insights on the expected consequences of a vote for Scottish independence according to experts, in a timely manner. Against this background, the 2016 referendum therefore appears as damaging to democratic quality standards and thus unfair to British voters and EU partner countries alike»
- (11) CRAIG, P., «Brexit: A Drama in Six Acts», *European law review*, núm. 4, 2016, págs. 447-468
- (12) SARMIENTO, D., «Y después del Brexit... ¿Qué?», *El Cronista del Estado Social y Democrático de Derecho*, núm. 64, pág. 42.
- (13) JAMES, S., y QUAGLIA, L., «The political economy of finance in the UK and Brexit», en *The Political Economy of Brexit and the UK's National Business Model*, SPERI Paper No. 41, 2017, págs. 7 a 10.
- (14) Me refiero fundamentalmente al Partido por la Independencia del Reino Unido, o *United Kingdom Independence Party* o *UKIP*, que realizaron una intensa campaña a favor de la salida de la Unión Europea.
- (15) SARMIENTO, D., «Y después del Brexit... ¿Qué?», *op. cit.*, pág. 44.
- (16) Así lo ha indicado la Comisión Europea en un aviso a los diferentes sectores interesados datado el 9 de enero de 2018, «*Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*». En el mismo sentido se ha pronunciado, el Comité Europeo de Protección de Datos en su informe «*Information note on data transfers under the GDPR (LA LEY 6637/2016) in the event of a no-deal Brexit*», adoptado el 12 de febrero de 2019.
- (17) Según el artículo 94 del RGPD (LA LEY 6637/2016) la Directiva queda derogada con efecto a partir del 25 de mayo de 2018, es decir, está derogada, pero sigue teniendo efectos. Es una consecuencia más del peculiar sistema de entrada en vigor del Reglamento.
- (18) Así lo pone de manifiesto PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales» en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, *op. cit.*, pág. 431.
- (19) REMOLINA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, págs. 170 a 172
- (20) GUASCH PORRAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, págs. 46 a 48.
- (21) Como es sabido, el Espacio Económico Europeo se instauró el 1 de enero de 1994 con motivo de un acuerdo entre países miembros de la Unión Europea y de la Asociación Europea de Libre Comercio (AELC), excepto Suiza. Su creación permitió a los países de la AELC participar en el mercado interior de la Unión Europea sin tener que adherirse a la UE. Los miembros son los 28 (27 tras el *Brexit*) países integrantes de la UE y los miembros de la AELC siguientes: Islandia, Liechtenstein y Noruega.

(22) La Disposición Derogatoria Única de la LOPDGDD (LA LEY 19303/2018) no deroga expresamente el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LA LEY 13934/2007). Su apartado tercero se limita a mencionar que «Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 (LA LEY 6637/2016) y en la presente ley orgánica»

(23) PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales» en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad, op. cit.*, pág. 433

(24) Artículo 26

Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

- a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
- b) 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 tomadas a petición del interesado, o
- c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
- d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
- e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
- f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

(25) Así lo pone de manifiesto PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales», *op. cit.*, pág. 428.

(26) «Organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

(27) PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales», *op. cit.*, pág. 439.

(28) *Ibidem*, pág. 434.

(29) 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

- a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, 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, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;
- b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
- c) 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.

(30) En este sentido, el sistema de Puerto Seguro, hoy sustituido por el *Privacy Shield*, permite que se realicen transferencias internacionales con determinadas empresas estadounidenses adheridas al mismo. Como es sabido, la Sentencia del Tribunal de Justicia de la Unión Europea en el asunto Sentencia en el asunto C-362/14 *Maximilian Schrems/Data Protection Commissioner*, de 6 de octubre de 2015, invalidó el sistema de Puerto Seguro, y tuvo que ser sustituido, después de unos meses de incertidumbre, por la Decisión de Ejecución (UE) 2016/1250 (LA LEY 12686/2016) de la Comisión, de 12 de junio de 2016 por el conocido como sistema de «Escudo de Seguridad». Un interesante análisis de esta sentencia puede encontrarse en PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer, 2018, págs. 201 a 205

(31) Sobre los códigos de conducta en el nuevo RGPD (LA LEY 6637/2016), véase DÍAZ-ROMERAL GÓMEZ, A., «Códigos de conducta en el Reglamento General de Protección de Datos (LA LEY 6637/2016)» en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad, op. cit.*, págs. 389 a 411.

(32) Sobre las normas corporativas vinculantes o BCR's, se deben tener en cuenta los documentos sobre la materia publicados por el Grupo de Trabajo del artículo 29, de entre los que cabe destacar, en mi opinión: WP212 *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*; y WP155 *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, entre los muchos trabajos publicados.*

(33) PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales», *op. cit.*, pág. 452, «Desde el punto de vista de las BCRs como fuente de obligaciones para los responsables y encargados el tema capital es el de su carácter vinculante en cuanto declaración unilateral de voluntad. Las posibles dudas que podrían plantearse entre nosotros teniendo en cuenta el sistema del Código Civil hoy deben entenderse

disipadas dado que las normas corporativas vinculantes, como tales, se recogen expresamente en una norma jurídica de directa aplicación como es un Reglamento de la Unión Europea. Una muestra más del alcance de la regulación de la protección de datos en nuestro ordenamiento.»

(34) El contenido mínimo de las normas corporativas vinculantes viene recogido en el artículo 47.2 del RGPD (LA LEY 6637/2016):

- a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
- b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;
- c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;
- d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;
- e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;
- f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
- g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;
- h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;
- i) los procedimientos de reclamación;
- j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;
- k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;
- l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);
- m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y
- n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

(35) PIÑAR MAÑAS, J. L., «Transferencias de datos personales a terceros países u organizaciones internacionales», *op. cit.*, pág. 455.

(36) En la actualidad, las únicas agencias autonómicas que tienen competencias efectivas en la materia son la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, siempre en relación a los tratamientos de datos que se hagan desde el sector público. Por su parte, con relación al Consejo de Transparencia y Protección de Datos de Andalucía, la Orden de 1 de agosto de 2019, de la Consejería de Turismo, Regeneración, Justicia y Administración Local, ha venido a fijar el 1 de octubre de 2019 como la fecha de inicio del ejercicio de las funciones en materia de protección de datos por parte del Consejo. A partir de entonces, corresponde al Consejo desempeñar tales funciones respecto de los tratamientos de los que sean responsables las instituciones autonómicas de Andalucía, la Administración de la Junta de Andalucía, la Administración Local en Andalucía y otras entidades dependientes de cualquiera de ellas, así como las universidades del sistema universitario andaluz, en los términos previstos en el artículo 57 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) (BOJA núm. 154, de 12 de agosto de 2019).

(37) En este sentido, véase TORREGROSA VÁZQUEZ, J., «Revisión de otros actos jurídicos de la Unión en materia de Protección de Datos, entrada en vigor y aplicación del Reglamento», en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M. (Coordinadores), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pág. 681, «Sin entrar en el nada desdeñable debate sobre la diferenciación entre la entrada en vigor y la aplicabilidad de las normas, es conveniente anotar que el legislador ha optado por implantar una comprensible etapa de transición de dos años hasta su aplicación»

(38) DE HERT, P., y PAPAKONSTANTINO, V., «The rich contribution to the field of EU data protection: Let's not go for «third country» status after Brexit», *Computer Law & Security Review*, 33, 2017, pág. 357.

(39) En España todavía nos queda un largo camino en este sentido pues, como es sabido, el derecho de acceso a la información no está a la altura del derecho a la protección de datos.

(40) Según el artículo 94 del RGPD (LA LEY 6637/2016) la Directiva queda derogada con efecto a partir del 25 de mayo de 2018, es decir, está derogada, pero sigue teniendo efectos. Es una consecuencia más del peculiar sistema de entrada en vigor del Reglamento.

(41) De hecho, esta es una de las razones por las que se aprueba un Reglamento para regular la protección de datos a nivel de la Unión Europea, para evitar la dispersión normativa y las diferencias entre los distintos Estados Miembros en la aplicación de las sanciones. Para una visión general del nuevo régimen sancionador véase mi trabajo CORRAL SASTRE, A., «El régimen sancionador en materia de protección de datos en el Reglamento General de la Unión Europea», en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, *op. cit.*, págs. 571 a 585.

(42) DE HERT, P., y PAPAKONSTANTINO, V., «The rich contribution to the field of EU data protection: Let's not go for «third country» status after Brexit», *op. cit.*

(43) Periodo que, de producirse una nueva prórroga, habría de ampliarse para ser realmente efectivo, según entiendo.

(44) Artículo 70. Definición

A efectos del presente título, se entenderá por «Derecho de la Unión sobre protección de datos personales»:

- a) el Reglamento (UE) 2016/679 (LA LEY 6637/2016), con excepción de su capítulo VII;
 - b) la Directiva (UE) 2016/680 (LA LEY 6638/2016) del Parlamento Europeo y del Consejo (90);
 - c) la Directiva 2002/58/CE (LA LEY 9590/2002) del Parlamento Europeo y del Consejo (91);
- cualesquiera otras disposiciones del Derecho de la Unión que regulen la protección de los datos personales.

(45) El Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Así lo han puesto de manifiesto MULLOCK, J., y SHOOTER, S «*Brexit: Data protection and cybersecurity law implications*», que se puede consultar en el siguiente enlace:
<https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security-law-implications>.

(46) Resulta necesario resaltar que la actual directora de la autoridad de control británica (ICO), Elizabeth Denham, es de nacionalidad canadiense y ha ocupado el cargo de *Privacy Commissioner for British Columbia* en Canadá. Este hecho puede llevar al optimismo en cuanto a la postura que adoptará Reino Unido durante y después del *Brexit*, por la dimensión internacional de la persona que está al mando de la autoridad de control independiente.

(47) Según este documento, el *Brexit* es uno de los principales retos a los que se enfrenta Reino Unido en materia de protección de datos, y expresamente se indica que: «*As the UK prepares to leave the EU, the formal relationship between the ICO and EU data protection authorities will change. Our relationship with our EU partners will remain highly important, including with the European Data Protection Board (EDPB) which will operate from May 2018 and on which the ICO will remain active and engaged until the UK's exit. In overseeing the enforcement of the General Data Protection Regulation (GDPR) (LA LEY 6637/2016) from 2018, and issuing guidance, the EDPB will be a highly influential global player in setting the direction for data protection and privacy standards.*

The strategy recognises that our direction on many of these challenges will often be driven by the outcome of the negotiations between the UK and the EU. Our priorities are designed to be compatible with a range of scenarios and enable the ICO to respond flexibly to different circumstances.

In 2017, the Secretary of State, Karen Bradley, and the UK Minister responsible for the digital economy, Matthew Hancock, made several statements to Parliament declaring the UK Government's commitment to comprehensively implementing GDPR (LA LEY 6637/2016), as planned, in 2018. The June 2017 Queen's Speech included a commitment to introduce a Data Protection Bill:

«To implement the General Data Protection Regulation and the new Directive which applies to law enforcement data processing, meeting our obligations while we remain an EU member state and helping to put the UK in the best position to maintain our ability to share data with other EU member states and internationally after we leave the EU.»

Our strategy presumes that GDPR (LA LEY 6637/2016) will also be assumed into UK law before exit to ensure there is continuity and certainty about UK law afterwards.

The ICO recognises the importance of the UK retaining a high estándar of data protection and data protection as a fundamental right. Our strategy recognises the possible role of EU laws and the Council of Europe in this after Brexit, directly or indirectly.

(48) El Comité Europeo de Protección de Datos es el órgano que viene a sustituir al Grupo de Trabajo del artículo 29 de la Directiva. Como es sabido, el Grupo de Trabajo del artículo 29 ha tenido un papel fundamental en la interpretación de la Directiva. Los documentos publicados han sido un referente en la materia y el representante del Reino Unido ha sido, tradicionalmente, muy activo. El RGPD (LA LEY 6637/2016) viene a reforzar esa posición al atribuir el Comité muy relevantes funciones según lo previsto en el artículo 70

(49) KORFF, D. estima que dicha decisión de adecuación no será tan fácil de conseguir y no será tan breve. Así lo manifiesta en su trabajo, disponible en SSRN: <https://ssrn.com/abstract=3441617> or <http://dx.doi.org/10.2139/ssrn.3441617>, «*The data protection implications of a «No-Deal Brexit»*. «After a «No-Deal Brexit» the UK will become, in data protection terms, an «inadequate» «third country», like (say) Russia or Nigeria.»:

In fact, the UK may find it more difficult than it seems to imagine to be recognised as affording «adequate» protection:18

Giovanni Buttarelli, Europe's data protection supervisor, warned negotiations could drag on for years as EU authorities would have to scrutinise how British spying agencies and the government handled the personal data of citizens and whether the UK met Europe's robust standards on surveillance.

«Adequacy could take years. We will have to assess law enforcement bodies,» said Mr Buttarelli. «Adequacy findings take a lot of work even if [the UK] is fully compliant with the GDPR (LA LEY 6637/2016)».

«A divorce is a divorce, so you need time before re-establishing certain relationships. Once you are out, it is all more complicated» he said. ...

The data protection supervisor said the UK would also have to get in a queue behind other third countries, such as Mexico, South Korea and India, who have all shown interest in striking data flows deal with the EU.

(50) Ciertamente es que por solo 4 votos de margen, es decir, 312 votos a favor de una retirada con acuerdo frente a 308 a favor de una retirada sin acuerdo.

(51) Se debe mencionar que esta era una de las posibilidades por la que optaban algunos autores antes de la incorporación del artículo 50 al Tratado de la Unión Europea (LA LEY 109/1994). Es decir, una salida drástica y sin autorización y apenas negociación con la Unión. Así lo describe, magníficamente, TATHAM, A. F., «Don't Mention Divorce at the Wedding, Darling!»: EU Accession and Withdrawal after Lisbon», en BIONDI, A., EECKHOUT, P., and RIPLEY, S., *EU Law after Lisbon*, Oxford Scholarship Online, 2012, «*Until the advent of the 2004 Constitutional Treaty, neither the original founding Treaties nor the succeeding treaties contained a provision allowing Member States to withdraw or secede—either in a negotiated or a unilateral manner— from the Union*»
«Nevertheless, those submissions generally reflected the three potential models for withdrawal mechanisms:140 (a) state primacy, where a Member State has an absolute, immediate and unilateral right to withdraw from a federation. This was essentially advocated by Dashwood and meant that the Member State had an unconditional right which did not require permission from EU institutions; (b) federal primacy, where a Member State is absolutely prohibited from withdrawing. Lamassoure did discuss the fact that in a federal141 restructuring (p.148) of the EU, the rule should be «once a member, always a member» but

regarded this and the confederal¹⁴² model as extremes. He therefore proposed a community option allowing withdrawal but «subject to strict and deterrent conditions»; and (c) federal control, where a Member State retains its sovereign right to withdraw, subject to negotiations with and the approval of the remaining states in the federation, thereby emphasizing the process as a mutually negotiated activity. Badinter's proposal, given in a more detailed manner, firmly followed this option and was closer to what was actually drafted for Article I-60 of the 2004 Constitutional Treaty. Although it never entered into force, its contents were later reproduced in the Lisbon Treaty with only minor technical changes»

(52) KORFF, D., op. cit., pág. 2, señala que «The GDPR (LA LEY 6637/2016) applies first and foremost to all processing by any controller or processor who is «established» in the EU, to the extent that the processing takes place «in the context of the activities of» the relevant establishment (Art. 3 (LA LEY 6637/2016)(1) GDPR (LA LEY 6637/2016)). From the date of a No-Deal Brexit, companies based in the UK will no longer be caught by this rule: their UK establishments will no longer be EU establishments.

But in case they think that this means they are now outside the scope of the GDPR (LA LEY 6637/2016), they should think again. This is because the GDPR also applies to controllers or processors who are not established in the EU, but who «offer goods or services» to individuals in the EU (in some «targeted» way), or who «monitor the behaviour» of such individuals (Article 3 (LA LEY 6637/2016)(2) GDPR)».

(53) Puede verse, en este sentido, RIPOL CARULLA, S., «Aplicación territorial del Reglamento», en en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos (LA LEY 6637/2016). Hacia un nuevo modelo europeo de privacidad*, op. cit., págs. 77 a 95.