Recibido: 25 febrero 2020
Aceptado: 19 marzo 2020

Brexit, relaciones privadas internacionales y protección de datos de carácter personal: ¿y ahora qué?... ¿dejará de ser el Reino Unido un 'país seguro'?

Alfonso ORTEGA GIMÉNEZ*

SUMARIO: I. Planteamiento. II. Régimen jurídico de la protección de datos de carácter personal en el Reino Unido después del Brexit. 1. Marco normativo de protección de datos de carácter personal en el Reino Unido. 2. Régimen jurídico de la protección de datos de carácter personal, según el Acuerdo de Retirada entre el Reino Unido y la Unión Europea. 3. El principio general de transferencias y las decisiones de adecuación como instrumento principal para las transferencias internacionales de datos. III. Medidas que se deben adoptar en materia de protección de datos de carácter personal tras el Brexit. 1. Régimen de supervisión durante el periodo transitorio. 2. Incidencia del Brexit en los datos de carácter personal alojados en redes, sistemas de información y bases de datos del Reino Unido. 3. Instrumentos de transferencia de datos de carácter personal disponibles: A) Cláusulas Contractuales Tipo o *ad hoc*; B) Normas Corporativas Vinculantes; C) Transferencias internacionales de datos del Reino Unido a Estados miembros de la Unión Europea. IV. Aplicación extraterritorial RGPD y relaciones privadas internacionales. 1. Aplicación extraterritorial RGPD en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea. 2. Actividades de tratamiento relacionadas con la oferta de bienes o servicios a afectados en la Unión Europea, independientemente de si a estos se les requiere su pago. V. Reflexión final.

RESUMEN: El pasado 31 enero 2020 tuvo lugar, formalmente, la salida del Reino Unido de la Unión Europea. No obstante, en virtud del Acuerdo de Retirada firmado, el Reino Unido ha dejado de ser miembro de la Unión Europea, pero debe seguir aplicando, en materia de protección de datos de carácter personal el Reglamento General de Protección de Datos (RGPD), a todos los datos de interesados fuera del Reino Unido, que se hayan tratado con anterioridad al fin del periodo transitorio (que termina, *a priori*, el 31 diciembre 2020). Ello implica que, a efectos de exportación de datos, la situación del Reino Unido es equiparable a la de un Estado Miembro, por lo que durante el periodo de transición es de aplicación el RGPD; sin embargo la situación será completamente distinta una vez finalizado el periodo de transición que les obligará, tanto al Reino Unido como a la Unión Europea, a preparar un marco jurídico de nueva generación para afrontar los retos en materia de protección de datos de carácter personal que el actual entorno globalizado exige.

La salida de esta zona de "libre circulación de datos" implicará que el Reino Unido pase a ser considerado como "tercer país". No obstante, es presumible que la Comisión le otorgue el estatus de "país seguro", dado que heredaría la regulación vigente hasta el momento, desarrollada y

* Profesor Contratado Doctor de Derecho internacional privado de la Universidad Miguel Hernández de Elche (acreditado a Profesor Titular de Universidad) alfonso.ortega@umh.es. ORCID: 0000–0002–8313–2070

AEDIPr, t. XIX–XX, 2019–2020, pp. 43–65
ISSN 1578–3138
DOI: 10.19194/aedipr.19/20.02

aplicada al igual que el resto de los países de la Unión. Sin embargo, puede existir un lapso de tiempo entre que se produzca la separación definitiva de la Unión Europea y la Decisión de la Comisión de considerar a Reino Unido como país seguro, en cuyo caso, el movimiento de datos que se produjera en ese período sí que podría suponer una Transferencia Internacional de Datos, y por tanto, las empresas que contraten servicios de tratamiento o alojamiento de datos en Reino Unido podrían tener que regularizar estas transferencias para un periodo de tiempo indeterminado. También cabe la posibilidad de que la UE reaccione al Brexit con revanchismo, y que, entre las muchas trabas que le ponga a Reino Unido esté la de no reconocerle como "país seguro". Si fuese el caso, caería en un bloqueo de facto, similar al que llevamos sufriendo desde octubre de 2015, cuando se anuló el Acuerdo de Puerto Seguro con Estados Unidos.

PALABRAS CLAVE: BREXIT – REINO UNIDO – PROTECCIÓN DE DATOS – TRANSFERENCIA INTERNACIONAL DE DATOS.

Brexit, international private relations and personal data protection: what now? Will the UK cease to be a 'safe country'?"

ABSTRACT: On January 31, 2020, the United Kingdom left the European Union, formally. However, under the Withdrawal Agreement signed the United Kingdom has ceased to be a member of the European Union but must continue to apply, the Data Protection Regulation (GDPR) in matters of personal data protection, all data of interested parties outside the United Kingdom, that have been treated prior to the end of the transitional period (which ends, a priori, on December 31, 2020). This implies that, for the purpose of exporting data, the situation in the United Kingdom is comparable to that of a Member State, so that during the transition period the current GDPR is applicable; However, the situation will be completely different after the end of the transition period that will require both the United Kingdom and the European Union to prepare a new generation legal framework to meet the challenges in terms of personal data protection that the Current globalized environment demands.

Leaving this area of "free movement of data" will imply that the United Kingdom will be considered as "third country". However, it is presumable that the Commission will grant it the status of a "safe country", given that it would inherit the regulation in force so far, developed and applied, just like the rest of the countries of the Union. However, there may be a period of time between the final separation of the European Union and the Commission's decision to consider the United Kingdom as a safe country, in which case, the movement of data that occurred in that period itself This could mean an International Data Transfer, and therefore, companies that hire data processing or hosting services in the United Kingdom may have to regularize these transfers for an indeterminate period of time. There is also the possibility that the EU reacts to Brexit with revanchism, and that, among the many obstacles that it puts to the United Kingdom is that of not recognizing it as a "safe country". If this were the case, it would fall into a de facto blockade, similar to the one we have been suffering since October 2015, when the Safe Harbor Agreement with the United States was annulled.

KEYWORDS: BREXIT – UNITED KINGDOM – DATA PROTECTION – INTERNATIONAL DATA TRANSFER.

I. PLANTEAMIENTO

El Reino Unido, desde el pasado 31 enero 2020, ya no es un Estado miembro de la Unión Europea. Y, en "breve", el Reino Unido pasará a ser considerado un "tercer país" en materia de protección de datos de carácter personal. Conforme a lo previsto en 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, firmado en Bruselas y Londres el 24 enero 2020 (en adelante, el Acuerdo de Retirada).[1]

La salida de Reino Unido de la Unión Europea supone un cambio en todos los aspectos económicos y sociales, y en lo que a la protección de datos de carácter personal supone: las transferencias de datos personales desde la Unión Europea al Reino Unido pasarán a estar sometidas a mayores restricciones, lo que afectará tanto a prestadores de servicios, como a compañías que transfieran datos personales de clientes o trabajadores a sus sociedades matrices o filiales localizadas en el Reino Unido. De esta manera, salvo pacto específico, a partir de la fecha de retirada (= 1 enero 2021), será de aplicación las normas en materia de transferencias internacionales de datos personales a terceros países.

No obstante, es previsible que la Comisión otorgue al Reino Unido el estatus de "país seguro" dado que heredaría la regulación vigente hasta el momento, teniendo en cuenta que el Reino Unido fue uno de los primeros países de la Unión Europea en adaptar su normativa interna a las exigencias del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 abril 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 (en adelante, el RGPD) [2]. En este sentido, el Reino Unido ha dejado claro que el RGPD será "absorbido" por la ley del Reino Unido; sin embargo, las organizaciones que dependen de las transferencias internacionales de datos personales entre el Reino Unido y el Espacio Económico Europeo (en adelante, el EEE) pueden verse afectadas, puesto que la información personal ha podido fluir libremente entre organizaciones en el Reino Unido y la Unión Europea sin ninguna medida específica. Pese a que la Comisión le otorgue el estatus de "país seguro" puede existir un lapso de tiempo entre que se produzca la separación definitiva de la Unión Europea y la Decisión de la Comisión de considerar al Reino Unido como un "país seguro", en cuyo caso, el movimiento de datos que se produjera en ese período sí que podría suponer una "transferencia internacional de datos"; y, por tanto, p. ej., las empresas que contraten servicios de tratamiento o alojamiento de datos en Reino Unido podrían tener que regularizar estas transferencias para un periodo de tiempo indeterminado.

También cabe la posibilidad de que la Unión Europea reaccione al Brexit "con revanchismo", y que, entre las muchas trabas que le ponga a Reino Unido esté la de no reconocerle como "país seguro". Si fuese el caso, caería

[1] DO L 29 de 31.1. 2020.
[2] DO L 119 de 4.5. 2016.

en un bloqueo de facto, similar al que llevamos sufriendo desde octubre de 2015, cuando se anuló el Acuerdo de Puerto Seguro con Estados Unidos.[3]

II. RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL REINO UNIDO DESPUÉS DEL BREXIT.

Muchas son las consecuencias jurídicas que producirá la efectividad del Brexit. Respecto al ámbito de la protección de datos de carácter personal, la consolidación del Brexit establece que Reino Unido será considerado como "tercer país", obligando al Reino Unido a la "transformación" de un régimen jurídico de la protección de datos de carácter personal para afrontar el futuro "nuevo panorama".

1. Marco normativo de protección de datos de carácter personal en el Reino Unido

Actualmente, el Reino Unido cuenta con una normativa nacional en materia de protección de datos de carácter personal ya adaptada al RGPD; 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[4]. 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.

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*[5]. Por último, 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). Pese a haber activado ya el art. 50 del TUE, los británicos no han cesado en su empeño de adaptarse al RGPD: así, en 2018, aprobaron una nueva Ley de Protección de Datos: la *Data*

[3] A. Ortega Giménez y J.J. Gonzalo Domenech, "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro?", *Revista Aranzadi Unión Europea*, nº 11/2019, Editorial Aranzadi, S.A.U., 2019, pp. 1–23.

[4] D. Sarmiento, "Y después del Brexit… ¿Qué?", *El Cronista del Estado Social y Democrático de Derecho*, nº 64, p. 42.

[5] La *Information Commissioner's Office*, es una autoridad pública con competencias de inspección y sanción desde mucho antes de la entrada en vigor y aplicación RGPD.

Protection Act 2018, que derogó la anterior de 1998, y por la que el Reino Unido pretende adaptarse a los requerimientos actuales RGPD.

Posteriormente, se emitió la *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, la cual, haciendo uso de los poderes de la *European Union (Withdrawal) Act 2018*, con el fin de adecuar ciertas disposiciones europeas al derecho británico. En concreto, se ha decidido por adoptar el RGPD como ley propia: la *United Kingdom General Data Protection Regulation* (UK GDPR).

La *Data Protection* se asemeja al Derecho de la Unión Europea en protección de datos. El Reino Unido aspira a mantener una armonía de soluciones materiales en materia de datos personales entre la regulación europea y la interna británica; ¿la razón?: conseguir que más allá de la complejidad sobrevenida con el Brexit la equiparación de ambos bloques normativos (europeo *vs.* británico), evitando distorsiones de mercado y de derechos de la ciudadanía en un sector estratégico y de enorme repercusión[6].

Todas estas consideraciones nos permiten afirmar que el Reino Unido mantiene un compromiso firme con el reconocimiento de este derecho fundamental, lo que podrían justificar, llegado el momento del reconocimiento de nivel adecuado de protección; incluso, no ser considerado un "tercer país", sino analizar otras posibles vías que faciliten el flujo de datos sin acudir a los instrumentos previstos para las transferencias internacionales de datos de carácter personal[7].

2. Régimen jurídico de la protección de datos de carácter personal, según el Acuerdo de Retirada entre el Reino Unido y la Unión Europea

Como es conocido, el 25 noviembre 2018, los 27 Estados Miembros de la Unión Europea refrendaron el proyecto de Acuerdo de Retirada y aprobaron el proyecto de Declaración Política sobre las relaciones futuras entre la Unión Europea y el Reino Unido. El 5 de diciembre del mismo año, la Comisión Europea inició el procedimiento para la firma y celebración del mencionado Acuerdo de Retirada del Reino Unido de la Unión Europea. El 13 de diciembre, los dirigentes de la Unión Europea celebraron una reunión extraordinaria del Consejo Europeo, en su composición del art. 50, para

[6] *Vid.* "Brexit y la protección de datos personales: incógnitas e incertezas" [<http://www. legal today.com/blogs>].

[7] P. De Hert y V. Papakonstantinou, "The rich contribution to the field of EU data protection: Let's not go for third country *status* after Brexit", *Computer Law & Security Review*, nº 33, 2017, p. 357.

debatir el Brexit. En ella, vuelven a confirmar sus Conclusiones de 25 noviembre 2018, en las que refrendaron el Acuerdo de Retirada y aprobaron la Declaración Política. El 11 enero 2019, el Consejo adoptó una decisión sobre la firma del Acuerdo de Retirada, también se aprobó un proyecto de Decisión sobre la celebración del Acuerdo de Retirada; y se decidió remitir dicho proyecto de la Decisión al Parlamento Europeo para su aprobación[8].

Así, se hace necesario analizar las previsiones que el Acuerdo de Retirada establece sobre el derecho fundamental a la protección de datos (=Título VII del Acuerdo, concretamente en los arts. 70 a 74).

El art. 70 establece que debe entenderse por "Derecho de la Unión sobre protección de datos personales"; incluyendo al RGPD, entre otras normas[9].

Es el art. 71 el que regula, en concreto, qué 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 diciembre 2020; o, b) Los datos personales sean tratados en el Reino Unido después del final del período transitorio con base en el presente Acuerdo.[10]

---

[8] *Vid*. A. Corral Sastre, Las transferencias de datos personales al Reino Unido en la era postbrexit", *Diario la Ley*, nº 3, 2019, p. 14.

[9] Art. 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, con excepción de su capítulo VII;

b) la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo (90);

c) la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (91);

d) cualesquiera otras disposiciones del Derecho de la Unión que regulen la protección de los datos personales.

[10] Art. 71. *Protección de los datos personales*. 1. El Derecho de la Unión 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: a) se hayan tratado en virtud del Derecho de la Unión en el Reino Unido antes del final del período transitorio; o b) sean tratados en el Reino Unido después del final del período transitorio con base en el presente Acuerdo.

2. El ap. 1 no se aplicará en la medida en que el tratamiento de los datos personales en él contemplados esté sujeto a un nivel de protección adecuado a tenor de lo dispuesto en las decisiones que resulten de aplicación en virtud del art. 45, ap. 3, del Reglamento (UE) 2016/679 o del art. 36, ap. 3, de la Directiva (UE) 2016/680.

3. En la medida en que una decisión de las mencionadas en el ap. 2 haya dejado de ser aplicable, el Reino Unido garantizará un nivel de protección de los datos personales esencialmente equivalente al establecido en el Derecho de la Unión sobre protección de datos

Por lo tanto, podemos señalar en base al Acuerdo de Retirada que, durante el período transitorio, se seguirá aplicando el Derecho de la Unión Europea, en cuanto a la protección de datos para todos los datos personales que se hayan obtenido antes del 31 diciembre 2020, ya que el RGPD 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 art. 134 sobre las disposiciones financieras[11]. Es decir, después del período transitorio establecido en el Acuerdo de Retirada, y salvo que este establezca otra cosa, los datos personales tratados se regirán por la normativa británica, es decir, de momento, por la *Data Protection Act 2018*.

El ap. 2 del art. 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 ap. 1 del citado artículo, porque cualquier flujo de datos estaría amparado en esa decisión de adecuación. 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 como norma de referencia en esta materia, asumiendo, por consiguiente, su aplicación.

El Acuerdo de Retirada recoge en su art. 72, el tratamiento confidencial y uso restringido de los datos y la información en el Reino Unido[12]; el art. 73 se refiere al tratamiento de los datos e información obtenida del Reino

personales en lo que respecta al tratamiento de los datos personales de los interesados a que se refiere el ap. 1.

[11] Art. 134. *Facilidades ofrecidas a los auditores en relación con las disposiciones financieras*. El Reino Unido informará a la Unión de las entidades a las que haya encargado la realización de su auditoría de la aplicación de las disposiciones financieras contempladas en la presente parte. A petición del Reino Unido, la Unión proporcionará a dichas entidades encargadas cualquier información que razonablemente pueda solicitarse en relación con los derechos y las obligaciones del Reino Unido en virtud de la presente parte, y les proporcionará una asistencia adecuada que les permita cumplir su cometido. Al facilitar información y prestar asistencia en virtud del presente artículo, la Unión actuará de conformidad con el Derecho de la Unión aplicable, en particular con las normas de la Unión en materia de protección de datos. Las autoridades del Reino Unido y de la Unión podrán acordar las disposiciones administrativas adecuadas para facilitar la aplicación de los párrafos primero y segundo.

[12] Art. 72. *Tratamiento confidencial y uso restringido de los datos y la información en el Reino Unido.* Sin perjuicio de lo dispuesto en el art. 71, además del Derecho de la Unión sobre protección de datos personales, se aplicarán las disposiciones del Derecho de la Unión sobre tratamiento confidencial, restricción del uso, limitación del plazo de conservación y la obligación de supresión de los datos y la información respecto de los datos y la información obtenidos por autoridades u organismos oficiales del o en el Reino Unido o por entidades adjudicadoras, tal y como se definen en el art. 4 de la Directiva 2014/25/UE del Parlamento Europeo y del Consejo (92), del o en el Reino Unido: a) antes del final del período transitorio; o b) sobre la base del presente Acuerdo.

Unido[13]; y, por último, el art. 74, recoge lo relativo a la seguridad de la información[14].

3. El principio general de transferencias y las decisiones de adecuación como instrumento principal para las transferencias internacionales de datos

El principio contemplado en la normativa de aplicación determina que sólo se podrán efectuar transferencias internacionales de datos a un tercer país u organización internacional si: a) Cumple con todas las obligaciones relativas al tratamiento recogidas en la normativa aplicable; y b) Asegura las suficientes garantías a la hora de realizar la transferencia internacional, en especial, las consistentes en garantías en las ulteriores transferencias.

El primer instrumento que permite autorizar una transferencia internacional de datos es la existencia de una decisión de adecuación[15] en aquel país, Estado, u Organización Internacional, demostrando que garantice un nivel adecuado de protección, entendiéndolo como un nivel equivalente al otorgado por la Unión Europea, según la STJUE *Schrems*[16]. La

[13] Art. 73. *Tratamiento de los datos e información obtenidos del Reino Unido.* La Unión 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 Unión.

[14] Art. 74. *Seguridad de la información*. 1. Las disposiciones del Derecho de la Unión sobre protección de la información clasificada de la UE y la información clasificada de la Euratom se aplicarán respecto de la información clasificada obtenida por el Reino Unido, bien antes del final del período transitorio, bien sobre la base del presente Acuerdo, u obtenida del Reino Unido por la Unión o un Estado miembro, bien antes del final del período transitorio, bien sobre la base del presente Acuerdo.

2. Las obligaciones derivadas del Derecho de la Unión en materia de seguridad industrial se aplicarán al Reino Unido en aquellos casos en que el procedimiento de licitación, contratación o adjudicación de subvenciones relativo a un contrato clasificado, un subcontrato clasificado o un acuerdo de subvención clasificado se haya iniciado antes del final del período transitorio.

3. El Reino Unido garantizará que los productos criptográficos que utilicen algoritmos criptográficos clasificados desarrollados bajo el control de una autoridad de certificación criptográfica de un Estado miembro o del Reino Unido, y evaluados y certificados por una de dichas autoridades, y que hayan sido certificados por la Unión hasta el final del período transitorio y estén presentes en el Reino Unido no se transfieran a un tercer país.

4. Se aplicarán a dichos productos los requisitos, las limitaciones y las condiciones establecidos en la certificación para la Unión de los productos criptográficos.

[15] Una decisión de adecuación es una decisión adoptada por la Comisión Europea en base al art. 45 RGPD (por ejemplo, la decisión de adecuación sobre Japón adoptada por la Comisión el 23 enero 2019). La UE ya había adoptado otras decisiones de adecuación sobre terceros países como Argentina, Nueva Zelanda e Israel, entre otros). En la actualidad no existe una decisión de adecuación vigente para el Reino Unido.

[16] *Vid.* STJUE 6 octubre 2015, as. C–362/14 *Maximillian Schrems / Data Protection Commissioner*.

posición que ostenta la decisión de adecuación, a tenor de la redacción de los arts. 45 y 46 RGPD, supone el instrumento predilecto y el más garantista para las transferencias internacionales, puesto que la redacción del art. 46 RGPD demuestra que los otros instrumentos suponen una excepción a la existencia de una decisión de adecuación. El contenido mínimo que debe contener la legislación británica para obtener la decisión de adecuación se regula en el art. 45 RGPD[17].

[17] Art. 45. *Transferencias basadas en una decisión de adecuación*. 1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

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.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el ap. 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el ap. 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el art. 93, ap. 2.

Vid. Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 enero 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 (DO 19 marzo).

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones

En definitiva, se deben garantizar: 1) el contenido de las normas aplicables; y, 2) los medios para garantizar su aplicación efectiva. Este contenido debe ser completado con las disposiciones del WP254 del Comité Europeo de Protección de Datos "Referencias sobre adecuación", la cual se centra de manera más pormenorizada en los criterios del art. 45 RGPD. Pero observando la nueva legislación autónoma del Reino Unido, derivada del RGPD, el Reino Unido no debería tener apenas obstáculos a la hora de perseguir la decisión de adecuación, pero esa tarea llevará tiempo, mientras tanto se debe tomar las medidas necesarias para la circulación de datos personales.

III. MEDIDAS QUE SE DEBEN ADOPTAR EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL TRAS EL BREXIT.

Aunque el Reino Unido deje de ser miembro de la Unión Europea, según el mencionado Acuerdo de Retirada, debe seguir aplicando el derecho de la Unión Europea a todos los datos de interesados fuera del Reino Unido que se hayan tratado con anterioridad al fin del periodo transitorio. Ello implica que, a efectos de exportación de datos, la situación del Reino Unido es equiparable a la de un Estado Miembro. Para enviar datos al Reino Unido no

adoptadas con arreglo al ap. 3 del presente artículo y de las decisiones adoptadas sobre la base del art. 25, ap. 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el ap. 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del ap. 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el ap. 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el art. 93, ap. 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el art. 93, ap. 3.

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el ap. 5.

7. Toda decisión de conformidad con el ap. 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del art. 25, ap. 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

es preciso ampararse en ninguno de los instrumentos de transferencia internacional de datos previstos por el RGPD.

Las empresas que estén transfiriendo datos al Reino Unido pueden seguir haciéndolo del mismo modo que lo hacía hasta ahora; y es posible iniciar nuevas transferencias con los mismos criterios aplicados hasta la fecha mientras esté en vigor el Acuerdo de Retirada. Las futuras relaciones entre la Unión Europea y el Reino Unido en materia de protección de datos deberán establecerse en los acuerdos que comienzan a negociarse a partir de la entrada en vigor del Acuerdo de Retirada. En el ámbito de la protección de datos, la opción que, en principio, resulta más previsible es que la Comisión Europea pudiera adoptar una "decisión de adecuación" en la que se reconozca que el Reino Unido ofrece un nivel de protección esencialmente equivalente al que proporciona el marco normativo de la Unión Europea.

El propio Acuerdo de Retirada señala expresamente que "la Comisión Europea iniciará 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 cumplen las condiciones aplicables"[18]. Para poder adoptar estas decisiones la Comisión deberá evaluar el ordenamiento jurídico y la práctica en materia de protección de datos en los países candidatos a la adecuación, pudiendo negociar con ellos la introducción de cambios normativos o en la aplicación práctica de las normas que permitan asegurar la existencia de ese nivel adecuado de protección. Las decisiones se deben revisar regularmente, a fin de comprobar que se siguen dando las condiciones que permitieron su adopción. En el caso de que, finalmente, se produzca la declaración de adecuación mediante una decisión de la Comisión, el envío de datos al Reino Unido podría realizarse sin ningún tipo de requisito formal, de un modo similar en la práctica a como se haría para comunicaciones de datos entre los Estados Miembro.

1. Régimen de supervisión durante el periodo transitorio

El RGPD establece un sistema de supervisión relativamente complejo, basado en el sistema conocido como "ventanilla única". Este sistema consiste, en que cuando un responsable o encargado de tratamiento de datos tienen varios establecimientos en la Unión Europea, la supervisión de los tratamientos de datos que realicen se lleva a cabo de forma cooperativa

[18] [<https://www.lamoncloa.gob.es/brexit/preparacion2/Paginas/161019.aspx >] (fecha de consulta: 14/02/2020).

entre todas las autoridades de supervisión de los países donde existen establecimientos bajo la dirección y coordinación de una autoridad de supervisión "principal", que es la del Estado Miembro donde se sitúa el establecimiento principal del responsable o encargado. El mismo principio es aplicable cuando los tratamientos, tenga o no el responsable o encargado varios establecimientos en la Unión, afecta significativamente a personas en varios Estados Miembros.

Según los términos del Acuerdo de Retirada, la autoridad de supervisión del Reino Unido podrá seguir actuando como autoridad "principal" o autoridad afectada en los procedimientos en que estén involucrados responsables o encargados con establecimiento, principal o no, en el Reino Unido o personas en el Reino Unido que estén significativamente afectadas por estos tratamientos.

La autoridad de supervisión de Reino Unido deberá aplicar las disposiciones RGPD que regulan los procedimientos de supervisión y está sometida a las decisiones que puedan adoptar el Comité Europeo de Protección de Datos, la Comisión o el Tribunal de Justicia de la Unión Europea en los casos en que el RGPD prevé su intervención. Por lo que el "modelo de control" diseñado por el RGPD seguirá aplicándose como hasta ahora por lo que respecta a la autoridad de supervisión del Reino Unido mientras se mantenga la vigencia del Acuerdo de Retirada.

La única y sustancial diferencia es que la autoridad de supervisión del Reino Unido no podrá participar como miembro con derecho a voto en las reuniones del Comité Europeo de Protección de Datos (en adelante, el CEPA) dedicadas a dirimir conflictos entre autoridades en la aplicación de estas disposiciones relativas a la supervisión o control.

2. Incidencia del Brexit en los datos de carácter personal alojados en redes, sistemas de información y bases de datos del Reino Unido

Otra de las cuestiones preocupante es la relativa al alojamiento de datos en redes, sistemas de información y bases de datos británicos, y las incidencias jurídicas que ello puede acarrear (siendo una de las principales, el impacto que produciría sobre la cooperación judicial y policial existente en el Espacio Europeo, que se sustenta en la libre circulación de datos entre las autoridades de los Estados Miembros y la Unión Europea). Quiere ello decir que, ante la finalización del Acuerdo de retirada o que, finalmente, la Comisión no reconozca al Reino Unido como "país seguro", las autoridades de la Unión Europea y de sus Estados Miembros dejarán de tener acceso directo a las redes, sistemas de información y bases de datos del Reino

Unido, debiendo aplicar, en consecuencia, los marcos jurídicos y mecanismos de cooperación alternativos que ofrece el Derecho Internacional y cada uno de los ordenamientos jurídicos internos del Estado Miembro en cuestión.

Si bien lo anterior no implica un abandono de la cooperación judicial y policial con el Reino Unido, sí que se traduce en menores garantías en comparación con las políticas, protocolos y normas existentes en el ámbito territorial de la Unión Europea y los países que la integran. Por su parte, y como se desprende lógicamente de lo anterior, hay que tener en cuenta que, una vez se haya retirado el Reino Unido del Espacio Europeo, el acceso de las autoridades británicas a las redes, sistemas de información y bases de datos de la Unión Europea ya no será posible.

Con todo, ante el volumen de datos personales existente en los sistemas informáticos, ya sea de datos de la Unión Europea en el Reino Unido o de datos recibidos del Reino Unido antes de la fecha de retirada, no existe la obligación de suprimir de los sistemas nacionales o de la Unión Europea, tales datos obtenidos de forma legal por parte de organizaciones públicas y privadas, salvo en dos supuestos:

Cuando el Reino Unido solicite la supresión por ostentar un dominio sobre los datos en cuestión; o,

Cuando se determine por la autoridad competente una limitación del tratamiento de acuerdo con la normativa aplicable.[19]

3. Instrumentos de transferencia de datos de carácter personal disponibles

El Reino Unido dispondrá a falta de una decisión de adecuación tras el periodo transitorio, de los siguientes instrumentos de transferencia internacional de datos personales:

A) Cláusulas Contractuales Tipo o *ad hoc.*

La Unión Europea, en su misión de facilitar el movimiento internacional de datos personales, emitió una serie de Decisiones por las cuales se aprueban un clausulado a firmar entre el importador y exportador de datos personales, cuyo uso permite efectuar una transferencia internacional de datos personales sin necesidad de una autorización por parte de la

[19] *Vid.* Medidas de protección de datos y sistemas de información ante un eventual "Brexit" sin acuerdo en: [<https://www.lealtadis.es/medidas–proteccion–de–datos–y–sistemas–informacion–ante–un–brexit–sin acuerdo/>] (fecha de consulta: 14/02/2020).

autoridad de control competente. Actualmente, las Cláusulas Contractuales Tipo se dividen en dos grupos que son: a) Cuando se traten de transferencias entre responsables de tratamiento; o, b) Cuando se traten de transferencias entre encargados.

i) Cuando se traten de transferencias entre responsables de tratamiento. En este caso, podrán utilizarse las cláusulas recogidas en la Decisión 2001/497/CE, de 15 junio 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país entre responsables[20]; y la Decisión 2004/915/CE, de 27 diciembre 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 Estados (versión consolidada de 1 abril 2005)[21], modificada por la Decisión de ejecución 2016/2297/CE [22].

Las cláusulas contenidas en la Decisión 2001/497/CE prevén un régimen de responsabilidad solidaria entre ambos responsables en el caso de que el afectado haya sufrido algún tipo de perjuicio. En cambio, el conjunto de cláusulas de la Decisión 2004/915/CE regulan un régimen de responsabilidad basado en la debida diligencia[23] por la cual el importador y exportador de datos responderán ante los afectados por el incumplimiento de sus obligaciones respectivas. El exportador será responsable si no realiza esfuerzos razonables para determinar si el importador es capaz de cumplir sus obligaciones legales. Se prevé una mayor intervención del exportador a la hora de la resolución de las reclamaciones de los afectados. La autoridad de control podrá prohibir o suspender con más facilidad las transferencias si el exportador rechaza tomar medidas contra el importador para hacerle cumplir sus obligaciones.

Ambos conjuntos de cláusulas tienen una composición rígida. Solo se puede elegir uno de ellos, sin que quepa utilizar cláusulas de los dos modelos en un mismo contrato, ni modificar las existentes.

ii) Cuando se traten de transferencias entre encargados. En este supuesto, podrán utilizarse las cláusulas recogidas en la Decisión 2010/87/UE de la Comisión, de 5 febrero 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento

[20] DO L nº 181 de 4.6.2001.

[21] DO L nº 385 de 29.12.2004.

[22] DO L 344 de 17.12.2016.

[23] *Vid.* Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the *Maximilian Schrems v Data Protection Commissioner case* (C–362–14).

establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, modificada por la Decisión de ejecución 2016/2297/CE.[24]

Esta Decisión contiene cláusulas específicas para la subcontratación por un encargado del tratamiento establecido en un tercer país a otros subencargados establecidos en terceros países. También añaden las condiciones que debe cumplir el subtratamiento para garantizar que los datos personales sigan protegidos con independencia de una ulterior transferencia a un subencargado del tratamiento. Ese subtratamiento no podrá exceder de las operaciones estipuladas en el contrato; por lo que deberá adecuarse al principio de finalidad. Aun si el subencargado incumple sus obligaciones, el importador de datos continuará siendo responsable. Al igual que las anteriores cláusulas, no solo son exigibles entre los importadores y exportadores; también son exigibles por el afectado cuando sufra un perjuicio derivado de un incumplimiento contractual.

Es importante destacar que las Cláusulas tipo de protección de datos no pueden modificarse y deben firmarse tal como se entregan. No obstante, estos contratos pueden incluirse en un contrato más amplio y se pueden añadir cláusulas adicionales siempre y cuando no contradigan, de forma directa o indirecta, las Cláusulas tipo de protección de datos adoptadas por la Comisión Europea, en consonancia con el Considerando 109 RGPD.

Si se pretendiese modificar el contenido de las cláusulas, pasarán a considerarse contratos a*d hoc*. Estos contratos suponen cláusulas contractuales sin reconocimiento por parte de la Comisión sobre el contenido del clausulado, por lo que depende de la autoridad de control garantizar el contenido. Antes de efectuar cualquier transferencia, sobre la base de las cláusulas *ad hoc* la autoridad de control nacional competente debe autorizar estas cláusulas contractuales adaptadas, previo dictamen del CEPD[25].

B) Normas Corporativas Vinculantes

Cuando se traten de transferencias internacionales de datos entre empresas del mismo grupo, el RGPD ha previsto un régimen "a medida" para aquellas entidades, conocidas como Normas Corporativas Vinculantes (en lo sucesivo, NCV). El Considerando 110 RGPD otorga la posibilidad de que un grupo empresarial pueda invocar unas NCV autorizadas para efectuar

[24] DO L 344 de 17.12.2016.

[25] A. Ortega Giménez y J.J. Gonzalo Domenech, "Brexit y protección de datos de carácter personal…", *loc. cit.*, pp. 1–23.

transferencias internacionales de datos a otras entidades del grupo situadas en terceros países, siempre que tales normas incluyan las garantías necesarias, y que en ningún caso vendrán a sustituir la legislación imperativa sobre protección de datos[26].

Actualmente, el art. 4.20) RGPD los define 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". Son, en definitiva, normas internas adoptadas por un grupo multinacional de empresas que definen su política global con respecto a las transferencias internacionales de datos personales dentro de un mismo grupo empresarial a entidades situadas en países que no ofrecen un nivel adecuado de protección. Están destinadas únicamente a los grupos empresariales.

C) Transferencias internacionales de datos del Reino Unido a Estados miembros de la Unión Europea

Para los casos de transferencias internacionales desde el Reino Unido a la Unión Europea, dependerá del régimen jurídico que quede entre el Reino Unido y la Unión Europea.

Sí, al final, se aprueba el acuerdo, se seguirá aplicando el Derecho de la Unión Europea, por lo que nada cambiaría en este sentido, al menos, durante el periodo de transición.

En caso contrario, y puesto que el Reino Unido deja de obedecer a la normativa europea, será competencia de su Derecho interno determinar la legalidad de las transferencias internacionales de datos personales. En este caso, debemos acudir al régimen creado por el UK GDPR y la *Data Protection Act 2018*. En este sentido, al adoptar el RGPD como norma autónoma, asumen los mismos instrumentos de transferencias internacionales de datos personales; de forma que el Reino Unido:

- Reconocerá a los Estados del EEE como países seguros;
- Reconocerá a cómo países seguros aquellos que lo hayan sido declarados por la Unión Europea;

[26] *Vid.* H. Thomas y otros, *Legal Aspects of Digital Preservation*, Cheltenham, Edward Elgar Publishing, 2013, p. 86.

- Asumirá los modelos de Cláusulas Contractuales Tipo de la Comisión Europea; y
- Mantendrá las autorizaciones prestadas para las NCV.

Para facilitar esta transición, la *Information Commissioner's Officer* ha emitido una serie de plantillas para la realización de transferencias internacionales mediante las Cláusulas Contractuales Tipo.

VI. APLICACIÓN EXTRATERRITORIAL RGPD Y RELACIONES PRIVADAS INTERNACIONALES.

Una vez que el Brexit se materialice definitivamente y el periodo de transición finalice, a todos los responsables y encargados que traten datos personales de personas que estén en la Unión Europea les será de aplicación: a) las normas respecto a la aplicación extraterritorial RGPD, según el art. 3 RGPD, acorde con las Directrices 3/2018 sobre la aplicación territorial RGPD, del Comité Europeo de Protección de Datos; y, b) las normas de Derecho internacional privado, a la hora de atender a las reclamaciones tanto contractuales como extracontractuales en materia de protección de datos.

1. Aplicación extraterritorial RGPD en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea

A) Concepto de establecimiento en la Unión Europea

El art. 3.1º RGPD estipula que se aplicará la legislación europea cuando ese tratamiento de datos se lleve a cabo en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no. Así pues, cualquiera de esos actos realizados sobre los datos personales de cualquier individuo en el ámbito de la Unión se les aplicará la legislación europea. Es por este supuesto de sujeción que todas las empresas británicas que tengan *branchs* o entidades subsidiarias se encontrarán sujetas a esta legislación.

La cuestión más discutida por el TJUE ha sido la definición de "establecimiento". El RGPD en su Considerando 22 describe que "un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan

tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto".[27]

El concepto de "establecimiento" se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable. Se utiliza esta concepción flexible de establecimiento para garantizar el derecho a la protección de datos, como reza el Considerando 23 RGPD. Una vez descrita la del art. 4.16) RGPD ha considerado en su definición el concepto de "establecimiento principal". La inclusión de dicha definición aclara y delimita cuestiones altamente relevantes como la concreción de un establecimiento principal del responsable o de un encargado con varios establecimientos en la Unión mediante reglas marcadas por el principio de especialidad y jerarquía.

Así, en el supuesto de un responsable con varios establecimientos, como norma general se considerará principal el establecimiento desde se lleve a cabo la administración central en la Unión. Pero como norma especial, si las decisiones sobre los fines y los medios del tratamiento se toman en otro establecimiento, y tiene el poder para hacerlas efectivas, se considerará como principal este último.

En cuanto al supuesto de un encargado con varios establecimientos, se considerará principal el establecimiento en el que se lleve a cabo la administración central en la Unión. Si careciera de ella, como norma supletoria, será el establecimiento del encargado en la Unión Europea en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado.[28]

B) La relación entre el establecimiento y las actividades realizadas respecto al tratamiento de datos.

Tal y como se acaba de decir, y como se dicta en reiteradas SSTJUE[29], tal tratamiento debe llevarse a cabo "en el contexto de las actividades del establecimiento". Para explicar tal concepto, debemos acudir a las Directrices 3/2018 anteriormente mencionadas.

Para aclarar esta relación, el Comité Europeo de Protección de Datos nos recuerda la jurisprudencia la STJUE en el caso *Google Spain*, exige confirmar que las actividades de un establecimiento local y las actividades de

[27] STJUE *Weltimmo* (Asunto C–230/14) de 1 octubre 2015. ECLI:EU:C:2015:639.

[28] A. Ortega Giménez y J.J. Gonzalo Domenech, "Brexit y protección de datos de carácter personal…", *loc. cit.*, pp. 1–23.

[29] *Vid. Google Spain*, C–131/12, ECLI:EU:C:2013:424 (párr. 52); *Weltimmo*, C–230/14 ECLI: EU:C:2015:639 (párr. 35), y *Amazon EU Sàrl*, C–362/14 ECLI:EU:C:2015:650 (p. 78).

tratamiento de datos puedan estar inextricablemente vinculadas, Incluso si ese establecimiento no está asumiendo realmente ningún papel en el propio tratamiento de datos. Si el tratamiento de los datos se lleva a cabo por establecimientos no establecidos en la Unión, y el establecimiento en la Unión no interviene en dicho tratamiento, las actividades llevadas a cabo por ese establecimiento pueden, subsidiariamente, otorgar la protección que ofrece la legislación europea, siempre que exista esa "vinculación inextricable" entre las actividades del establecimiento en la Unión y el procesamiento de datos, independientemente de que el tratamiento se lleve a cabo en la Unión.

Teniendo claro el hecho de sujeción, ya no importa la localización geográfica, sino la relación de medio a fin entre el tratamiento de datos personales y la actividad realizada; ni siquiera se discrimina a los afectados los cuales se tratan los datos personales, siempre y cuando se encuentren en la Unión Europea. Atrás queda la interpretación otorgada por una defectuosa redacción del art. 3 RGPD, corregida por la Corrección de errores el 23 mayo 2018, la cual limitaba la aplicación a los datos personales de personas que residían en la Unión Europea.[30]

C) El criterio de localización en las relaciones responsables entre responsables y encargados.

Partiendo de la base de una primacía de la relación de la actividad con el tratamiento de datos sobre la localización geográfica del tratamiento, el criterio de localización se utiliza a la hora de determinar la aplicación de las obligaciones a los responsables y encargados de tratamiento. Debemos afirmar que, aunque ambos sujetos se caracterizan por tratar datos personales, no tienen el mismo régimen de obligaciones. El régimen de obligaciones del responsable del tratamiento está regido únicamente de manera legal; en cambio, el régimen del encargado de tratamiento variará si este está sito en la Unión Europea o en un tercer Estado. Si el encargado estuviese sito en la Unión Europea, no solo se le aplica las obligaciones RGPD, sino también las disposiciones contractuales del acuerdo del art. 28 RGPD, en particular, sobre el régimen de colaboración del encargado con el responsable en el cumplimiento de las obligaciones de este último. En cambio, si el encargado está sito fuera de la Unión Europea, no se le puede aplicar el RGPD, al no ser considerado un establecimiento del responsable, ni porque trate los datos de ciudadanos europeos, de forma que la aplicación RGPD se determina por las obligaciones contractuales que se determinen en el contrato. Añadido a esto, en el caso de que un responsable en la Unión

[30] A. Ortega Giménez y J.J. Gonzalo Domenech, "Brexit y protección de datos de carácter personal…", *loc. cit.*, pp. 1–23.

Europea recurra a un encargado británico, se deberá recurrir a las Cláusulas Contractuales Tipo, que con garantías adicionales para efectuar la transferencia internacional.

2. Actividades de tratamiento relacionadas con la oferta de bienes o servicios a afectados en la Unión Europea, independientemente de si a estos se les requiere su pago.

A) Concepto de interesado "que se encuentra en la Unión Europea"

El criterio del art. 3.2º facilita el sometimiento a la legislación europea de quienes no están establecidos en la Unión y tratan datos de individuos que se encuentran en ese territorio en circunstancias en las que se observa necesario aplicarlas[31]. El presente artículo fue modificado para esclarecer la redacción y el ámbito de aplicación como se comentó anteriormente, puesto que en la versión en otros idiomas, como en la española, exigía que los interesados "residan" en la Unión Europea, de forma que limitase el ámbito de aplicación a uno más adecuado, evitando una extralimitación abusiva del ámbito de aplicación[32].

B) Oferta de bienes y servicios a los interesados en la Unión Europea

El RGPD exige que se cumplan una serie de condiciones: a) El tratamiento efectivo de los datos personales; y b) La dirección de las actividades del responsable a interesados en la Unión Europea.

Debemos partir de la descripción que realiza el Considerando 23 RGPD, el cual determina que si el responsable o encargado ofrece bienes o servicios a afectados que se encuentren en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a afectados en uno o varios de los Estados miembros de la Unión (*targeting–based analysis*)[33]. El Considerando no contempla que la accesibilidad web, el uso de un tercer idioma común o datos de contacto como indicios de oferta de

[31] P.A. de Miguel Asensio, "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", *REDI*, 2015, nº 1º, vol. 69, 2017, p. 14.

[32] M. Brkan, "Data protection and conflict–of–laws: a challenging relationship", *European Data Protection Law Review*, vol. 2, nº 3, 2016, p. 337; D.J. Svantesson, *Extraterritoriality in Data Privacy Law*, Copenhague, Ex tuto Publishing, 2013, p. 107; J.J. Gonzalo Domenech, "Algunas cuestiones relevantes de Derecho internacional privado en el Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, nº 26, 2018, p. 413.

[33] M. Geist, "Is There a There? Toward Greater Certainty for Internet Jurisdiction", *Berkeley Technology Law Journal*, vol. 16, nº 3, 2001, pp. 1345–1406.

servicios y productos en la Unión, como dicta la STJUE *Wertimmo*. Sí considera, por el contrario, el uso de la lengua, la moneda, o la mención de clientes o usuarios que residen en la Unión indicios de que el encargado o responsable dirige su oferta al territorio de la Unión, en clara atención a la doctrina establecida en la STJUE *Pammer y Hotel Alpenhor*[34], consolidada en las SSTJUE *Mühlleitner*[35], y *Emrek*[36] [37], y avalada por el CEPD.

La jurisprudencia obliga a valorar la existencia de una actividad dirigida mediante determinados indicios, como la oferta de tales servicios o productos en Estados miembros de la Unión Europea, o la publicidad en distintos medios que facilitan su conocimiento por consumidores. El CEPD, en consonancia con la doctrina jurisprudencial ofrece un listado de indicios no exhaustivos, en los que se consideran como tal[38]:

- La UE o al menos un Estado miembro se designa por su nombre en relación con el bien o servicio ofrecido;
- El responsable del tratamiento o el encargado del tratamiento paga a un operador de motores de búsqueda por un servicio de referenciación en Internet con el fin de facilitar el acceso a su sitio por parte de los consumidores de la Unión; o bien el responsable del tratamiento o el encargado del tratamiento ha puesto en marcha campañas de comercialización y publicidad dirigidas al público de un país de la UE.
- El carácter internacional de la actividad de que se trata, como determinadas actividades turísticas;
- La mención de direcciones o números de teléfono específicos a los que se puede acceder desde un país de la UE;
- La utilización de un nombre de dominio de primer nivel distinto del tercer país en el que esté establecido el controlador o procesador, por ejemplo ".de", o la utilización de nombres de dominio de primer nivel neutrales, como ".eu";
- Descripción de las instrucciones de viaje desde uno o más Estados miembros de la UE hasta el lugar donde se presta el servicio;

[34] STJUE 7 diciembre 2010, *Pammer and Hotel Alpenhof*, C–585/08, ECLI:EU:C:2010:740.

[35] STJUE 6 septiembre 2012, *Daniela Mühlleitner,* C-190/11.

[36] STJUE 17 octubre 2013, *Emrek,* C-218/12, ECLI:EU:C:2013:494.

[37] *Vid.* El caso tratado en las SSTJUE citada no versa sobre protección de datos, sino de controversias en materia mercantil.

[38] La doctrina establecida por el TJUE deriva de la establecida por la *Supreme Court* estadounidense *Calder v. Jones* (465 U.S. 783 (1984)), en la que permite a los tribunales considerar si existe un mercado objetivo determinado mediante el uso de elementos como la lengua utilizada, la divisa, o la nacionalidad. Aunque algún sector entiende que a esta doctrina se le puede achacar su fuerte componente subjetivo. W.G. Jiménez–Benítez, "Rules for Offline and Online in Determining Internet Jurisdiction", *Revista Colombiana de Derecho Internacional*, nº 26, 2015, pp. 13–62, esp. 30.

- La mención de una clientela internacional compuesta por clientes domiciliados en varios Estados miembros de la UE, en particular mediante la presentación de cuentas elaboradas por dichos clientes;
- El uso de una lengua o moneda distinta de la utilizada generalmente en el país del comerciante, especialmente una lengua o moneda de uno o más Estados miembros de la UE; y/o
- El responsable del tratamiento ofrece la entrega de bienes en los Estados miembros de la UE.

Debe restringirse únicamente a la actividad de tratamiento por la cual determine la aplicación de la normativa, no al resto de sus actividades las cuales no tienen relación con la oferta de los bienes y servicios, puesto que una aplicación contraria sería extralimitada al objeto que persigue proteger.

V. Reflexión final

El abandono de la Unión Europea por parte del Reino Unido va a tener importantes consecuencias en materia de protección de datos de carácter personal. Y es que, como hemos analizado, pasará a ser, un "tercer país" a efectos de aplicación RGPD, por lo que habrán de tenerse en cuenta las herramientas previstas para las transferencias internacionales de datos, con todas las dificultades y costes que ello genera para las empresas.

Pese a la reciente materialización del Brexit no significa la total exención al cumplimiento RGPD, puesto en el caso de que una entidad británica trate datos personales de ciudadanos que se encuentren en la Unión Europea, ya sea en un marco de acuerdo o por la aplicación extraterritorial RGPD, deberá cumplir con las obligaciones RGPD.

Todo apunta a que el Reino Unido será considerado "país seguro", ya que ha demostrado que pese a su salida de la Unión Europea hará todo lo posible por mantener un "nivel de protección alto" respecto a la protección de datos, en los términos exigidos por el RGPD (así lo acredita la aprobación de la *Data Protection Act 2018* y, prueba de ello, es su adaptación al RGPD).

En definitiva, parece que el Reino Unido está comprometido con los altos estándares de protección de datos establecidos en el RGPD. Sin embargo, es posible que deban asegurarse de que existen garantías adecuadas para mantener cualquier flujo de datos desde la Unión Europea al Reino Unido. Respecto a las obligaciones de las entidades europeas, no variarán demasiado por la gran similitud de la legislación entre ambos bloques (*Reino Unido vs. Unión Europea)*.

BIBLIOGRAFÍA

Brkan, M.: "Data protection and conflict–of–laws: a challenging relationship", *European Data Protection Law Review*, nº 3, vol. 2, 2016, pp. 337 ss.

Corral Sastre, A.: Las transferencias de datos personales al Reino Unido en la era postbrexit", *Diario la Ley*, Especial Revista de Derecho Digital e Innovación, nº 3, 2019, p.p 14 ss.

De Hert, P. y Papakonstantinou, 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*, nº 33, 2017, pp. 357 ss.

De Miguel Asensio, P.A.: "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", *REDI*, 2015, nº 1º, vol. 69, 2017, pp. 14 ss.

Geist, M.: "Is There a There? Toward Greater Certainty for Internet Jurisdiction", *Berkeley Technology Law Journal*, *nº* 3º, vol. 16, 2001, pp. 1345–1406.

Gonzalo Domenech, J.J.: "Algunas cuestiones relevantes de Derecho internacional privado en el Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, nº 26, 2018, pp. 404–437.

Jiménez-Benítez, W.G.: "Rules for Offline and Online in Determining Internet Jurisdiction", *Revista Colombiana de Derecho Internacional*, nº 26, 2015, pp. 13–62.

Ortega Giménez, A. y Gonzalo Domenech, J.J.: "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro" ?, *Revista Aranzadi Unión Europea*, nº 11/2019, 2019, pp. 1–23.

Sarmiento, D.: "Y después del Brexit… ¿Qué?", *El Cronista del Estado Social y Democrático de Derecho*, nº 64, pp. 42 ss.

Svantesson, D. J.: *Extraterritoriality in Data Privacy Law*, Ex tuto Publishing, Copenhague, 2013, pp. 107 ss.

Thomas, H. y otros: *Legal Aspects of Digital Preservation*, Cheltenham, Edward Elgar Publishing, 2013.