IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

Garantías legales de la privacidad en el Reino Unido: la (des)protección de datos después del *brexit*

Marina Sancho López
Universidad Internacional de Valencia

Fecha de presentación: julio de 2018
Fecha de aceptación: febrero de 2019
Fecha de publicación: abril de 2019

Resumen

En el derecho británico, las referencias jurídicas de lo que en la actualidad identificamos como «derecho a privacidad» están íntimamente relacionadas con la protección de la información personal de los ciudadanos. La *Data Protection Act 1984* fue una legislación precursora en materia de protección de datos, que llegó a inspirar a la propia Directiva 95/46/CE (ahora derogada por el Reglamento General de Protección de Datos 2016/679).

Una segunda etapa para la protección de la privacidad en el Reino Unido se consolidó con la aprobación de la *Human Rights Act 1998* (a imagen y semejanza del Convenio Europeo de Derechos Humanos), que supuso un punto de inflexión para el sistema legal anglosajón (e hizo las funciones de una *Bill of Rights* en el ordenamiento constitucional británico) y que, a partir de entonces, reconoció el derecho a la privacidad en su artículo 8.

En la actualidad, esta cuestión se encuentra en una tercera etapa, integrada por distintos acontecimientos y cuyo futuro está aún por determinar. Por una parte, se ha producido una disminución del alto estándar de protección del que gozaba la privacidad en el Reino Unido a través de la legislación especial dictada en los últimos quince años. En segundo lugar, el *brexit* obliga a reconsiderar el modelo de protección de la privacidad, así como la protección de datos, pues, cuando se efectúe la desconexión, el Reino Unido será considerado un «tercer Estado» y el flujo de datos entre este y la UE serán «transferencias internacionales».

Mientras tanto, ha entrado en vigor el Reglamento de Protección de Datos, directamente aplicable también en el Reino Unido y que, hasta el momento de su salida de la Unión Europea, obliga a la legislación británica a adaptarse al nuevo articulado europeo, como se ha hecho mediante la *Data Protection Act 2018*.

Palabras clave
privacidad, *brexit*, datos personales, GDPR, Binding Corporate Rules, Standard Form Contracts

Tema
derecho constitucional, derecho comunitario, derecho comparado

Legal guarantees of privacy in the United Kingdom: (lack of) data protection after Brexit

Abstract
In British law, the legal references for what we currently identify as privacy law are closely related to the protection of citizens' personal information. The 1984 Data Protection Act was pioneering data protection legislation, and even inspired Directive 95/46/EC, now repealed by General Data Protection Regulation 2016/679.

A second stage of privacy protection in the United Kingdom was consolidated with the approval of the 1998 Human Rights Act — in the image and likeness of the European Convention on Human Rights —, which represented a turning point for the United Kingdom legal system, acting as a Bill of Rights in the British constitutional order and which, from then on, recognized the right to privacy in its Article 8.

This issue is currently immersed in a third stage, made up of various events, and its future is still to be determined. On the one hand, there has been a reduction in the high standard of protection that privacy enjoyed in the United Kingdom thanks to the special legislation enacted over the last 15 years. On the other hand, Brexit makes it necessary to reconsider the privacy protection model, in addition to data protection, since when the "disconnection" takes place, the United Kingdom will be considered a "third country" and the data flow between it and the EU will be "international transfers".

Meanwhile, the Data Protection Regulation has come into force. It is also directly applicable in the United Kingdom and, until the latter leaves the European Union, it obliges British legislation to adapt to the new European legislation, as it has done through the 2018 Data Protection Act.

Keywords
privacy, brexit, personal data, GDPR, binding corporate rules, standard form contracts

Topic
Constitutional law, Community law, Comparative law

1. Consideraciones preliminares acerca del sistema jurídico anglosajón

En el estudio de esta cuestión debe tenerse en cuenta que el ordenamiento jurídico británico reviste ciertas peculiaridades. En primer lugar, por la dicotomía de su sistema legal, que aúna dos corrientes aparentemente contrapuestas, esto es, de un lado su tradición jurídica del *common law*, íntimamente ligado al precedente judicial. Por otro lado, un positivismo jurídico creciente a raíz de la integración europea, adoptando el principio de soberanía nacional mediante el cual se legitima al Parlamento para legislar en cualquier ámbito del derecho.

En segundo lugar, este particular fenómeno se une al hecho de que el Reino Unido no cuenta con una constitución escrita, sino con lo que ha sido llamado «*unwritten constitution*», que otorga fuerza vinculante al *common law y al precedente legal* (*case law*), a las disposiciones normativas de origen parlamentario (*statutory law*), así como a los tratados internacionales. Todo ello siguiendo el criterio orientador del concepto *rule of law*,[1] clave de bóveda del ordenamiento constitucional británico, porque a partir de este terminan desarrollándose una serie de principios político-constitucionales específicos, que proveen a la ciudadanía de derecho y libertades exigibles.[2]

Las concretas particularidades del sistema constitucional anglosajón permiten la mutabilidad de su contenido, adaptando sus reglas y principios a las circunstancias concretas de cada momento histórico. La volatilidad de su sistema de valores queda patente también en la configuración de los derechos y libertades ciudadanas, así como en sus garantías, lo cual también se plasma en la evolución del modelo británico de protección de la privacidad.

2. La evolución del sistema británico de protección de la privacidad

Se ha convenido en situar la creación del derecho a la privacidad en el *common law* en el artículo que en 1890 escribieron Warren y Brandeis en la *Harvard Law Review* titulado «The right to privacy».[3] Sin embargo, la evolución de este nuevo derecho evolucionó de forma distinta en la vertiente norteamericana y anglosajona de dicho sistema jurídico.

Históricamente, el *common law* anglosajón no reconocía ningún derecho a la privacidad ni tampoco contemplaba un derecho a la responsabilidad civil; sin embargo, sí que ofrecía remedios parciales, principalmente, a través de las figuras de la *breach of confidence* (revelación de secretos), el *trespass* (allanamiento), la *nuisance* (perjuicio, molestias) o la *defamation and malicious falsehood* (difamación).[4]

En el derecho anglosajón, las referencias jurídicas de lo que en la actualidad identificamos como derecho a privacidad están íntimamente relacionadas con la protección de la información personal de los ciudadanos. Vivieron sus comienzos en los años setenta, a raíz de la incipiente introducción de los ordenadores en la sociedad británica.[5]

Hubo que esperar hasta el Convenio del Consejo de Europa de 1981 para la protección de datos personales, para que el Reino Unido estableciese los pilares de lo que sería el derecho a la protección de datos moderno, a través de la *Data Protection Act 1984*. Esta norma integra el primer paso para la protección de ciertas esferas privadas de los británicos; de hecho, fue una de las primeras leyes en materia sustancial de protección de datos en todo el mundo, cuyo primer objetivo era establecer el régimen jurídico sobre la tenencia y el procesamiento automatizado de información.

1. El concepto *rule of law* reviste una gran complejidad, pues, si bien conceptualmente puede resultar un tanto vago, a su vez se emplea como criterio de principio legal para el respeto de los derechos y de las libertades públicas. Para un examen pormenorizado del complejo concepto *rule of law* resulta referente obligado, entre otros, Raz (1979).
2. Cfr. Dicey (2013).
3. Warren y Brandeis (1890).
4. De hecho, ya en el siglo XVIII se encuentra jurisprudencia anglosajona reconociendo ciertos espacios de privacidad, como es el caso de la inviolabilidad del domicilio. *Entick v. Carrington* [1765] EWHC KB J98 95 ER 807, King's Bench, 2 de noviembre de 1765
5. Cfr. Dworkin (1973).

Uno de los aspectos clave de esta ley fue el establecimiento de los principios fundamentales en los que se debía cimentar toda actuación relacionada con los datos personales, conformado por ocho puntos de contenido muy general. En cuanto a las garantías, consagró por vez primera derechos de información, acceso, rectificación y borrado de datos personales; obligó a aquellos que almacenaban datos personales a inscribirse en un registro específico; creó una autoridad de control independiente para su supervisión (The Office of the Data Protection Registrar); e implantó unos órganos jurisdiccionales especiales para tratar asuntos en materia de protección de datos (el Information Rights Tribunal, entre otras).[6]

Si bien la *Data Protection Act 1984* fue una legislación precursora en materia de protección de datos[7] y su aplicación estaba produciendo efectos satisfactorios, su derogación por la *Data Protection Act 1998* respondió a exigencias europeas, por la implementación de la Directiva 95/46/CE, así como debido a la evolución de la tecnología en ese lapso de tiempo. Por tal razón, ambas normas comparten el mismo esquema normativo, así como tienen terminología común.[8]

Una segunda etapa para la protección de la privacidad se consolidó con la aprobación de la Human Rights Act 1998 (HRA, en adelante), que supuso un punto de inflexión para el proceder del sistema legal anglosajón,[9] pues de alguna manera vino a paliar la ausencia de una *Bill of Rights* en el ordenamiento constitucional británico, que, hasta entonces, dejaba en manos del *case law* la protección de los derechos y libertades de la ciudadanía.

A través de los derechos recogidos en la HRA, se produce una equivalencia, tanto conceptual como normativa, con los derechos y libertades reconocidos por el Convenio Europeo de Derechos Humanos (CEDH); se reformulan las relaciones entre el Parlamento y los órganos jurisdiccionales en la interpretación y aplicación de las leyes,[10] así como para la protección de la privacidad, reconocida en su artículo 8, que pasa a tutelarse como mecanismo adicional al derecho de protección de datos.[11]

Además de convertir en vinculante el contenido del CEDH, la HRA impone a todos los poderes públicos la obligatoriedad de actuar, en el ejercicio de sus funciones, de forma compatible con los derechos del convenio,[12] lo que incluye también a la judicatura.[13] A partir de entonces, los tribunales del Reino Unido tienen la obligación de interpretar la legislación conforme a los derechos del CEDH[14] y de acatar en todo lo posible la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos.[15]

Del mismo modo, supuso un paso decisivo en la protección de la privacidad, mediante el reconocimiento del derecho a la vida privada en su artículo 8, derecho que, hasta entonces, no gozaba de soporte legal específico en la legislación británica y que, a partir de este momento, se instituyó como un bien jurídico a proteger,[16] bajo una fórmula legal que resulta directamente aplicable tanto para los indivi-

6. Bainbridge (2005).
7. Encontramos un *statutory instrument* precedente en materia de datos: *The Medecines (Data Sheet) Regulations 1972*, de 30 de diciembre de 1972. No obstante, esta regulación jurídica era muy escasa y sectorial; se constreñía a la ordenación de las recetas médicas y de los prospectos de los medicamentos.
8. Cfr. Carey (1998).
9. Harvers (2000).
10. Correcher Mira (2018).
11. A partir de la entrada en vigor de la HRA, bajo el amparo de su artículo 8, el derecho a la privacidad comienza a ser directamente invocable en la jurisdicción inglesa, lo que supuso campo de cultivo para las disputas jurisprudenciales. Sin duda, dicho precepto del CEDH es el que más impacto ha ocasionado en la jurisdicción inglesa, aunque solo sea por el número de veces que ha sido invocado. Cfr. Tugendhat y Christie (2002).
12. Cfr. Ashworth, Emmerson, MacDonald (2012).
13. Lo que no fue bien recibido por parte de la doctrina, que recriminó el peso y el poder que la HRA ha concedido a la judicatura. Cfr. Gearty (2002).
14. Cfr. Grosz (2000).
15. Hickman (2011).
16. Si bien la protección de la privacidad no gozaba de antecedentes significativos en la legislación británica, a partir de la entrada en vigor de la HRA pasa a formar parte de los derechos e intereses que el Reino Unido debe proteger como valor fundamental para garantizar la autonomía y la dignidad personal que le son intrínsecas. Cfr. Endicott (2001).

duales como para las autoridades públicas.[17] Destaca la jurisprudencia del TEDH en relación con el artículo 8, pues ha sido esencial en la formación y la aplicación jurídica del derecho a la privacidad por los tribunales británicos, cosa que ha contribuido a perfilar y ampliar su significado.[18]

La tercera y última de las fases que ha incidido en dicha cuestión viene integrada por múltiples acontecimientos; de hecho, su futuro está aún por determinar. Puede destacarse aquí, por un lado, como, con el paso de los años, se ha producido una disminución del alto estándar de protección del que gozaba la privacidad en el Reino Unido que se ha proyectado en leyes como la *Anti-Terrorism Crime and Security Act 2001* o la *Data Retention Regulation and Investigatory Powers Act 2014*, que, bajo la excusa de la amenaza terrorista o el control de los mercados financieros, permiten de facto la vigilancia masiva de los ciudadanos y que, claramente, abogan por la limitación del espacio privado de las personas, lo que le ha supuesto al Reino Unido más de una reprimenda por parte del Tribunal de Estrasburgo.[19]

3. El *brexit*: un punto de inflexión para la privacidad y la protección de los datos personales

Sin embargo, todo el sistema anteriormente descrito está a punto de prescribir debido al convulso rumbo político que azota el Reino Unido, consecuencia del creciente euroescepticismo británico, que se consagró el 23 de junio de 2016 con los resultados del referéndum que dieron la victoria al *brexit* y que conllevará la salida de Gran Bretaña de las instituciones comunitarias en un futuro próximo.[20]

En el momento de redacción de estas líneas, el Gobierno británico parece inclinarse por una salida total de las instituciones europeas, lo que supondría renunciar a ser parte del Convenio Europeo de Derechos Humanos, bajo el pretexto de que los mismos derechos les serán aplicables mediante la *Human Rights Act 1998*.[21]

Entre tanto, y dentro de este contexto, ha entrado en vigor el Reglamento General de Protección de Datos 2016/679 (GDPR, por sus siglas en inglés, publicado dos meses antes de dicho referéndum), directamente aplicable en el Reino Unido y que, hasta el momento en que se produzca la desconexión total con la Unión Europea, supone la obligación de adaptar la legislación británica al nuevo articulado europeo (como finalmente se ha hecho a través de la *Data Protection Act 2018*, en vigor), lo que determina, en un futuro inmediato, la naturaleza de las relaciones que tendrán lugar entre la Unión Europea y el Reino Unido.[22]

Sin entrar a valorar la idoneidad de los mecanismos empleados para garantizar la seguridad jurídica de los ciudadanos británicos, lo cierto es que hay numerosas normas que dejarán de tener vigencia en un horizonte próximo si no se buscan fórmulas jurídicas que remedien la situación. El futuro inmediato pasa por negociar los términos de cada uno de las normas aplicables en la actualidad como consecuencia de la pertenencia a la UE y mitigar así sus efectos ante la desconexión.

En función de lo que tarde en demorarse la escisión y de la solución por la que se opte, la aplicación del GDPR tendrá una mayor o menor brevedad en su vigencia, pues, cuando el Reino Unido abandone definitivamente la Unión Europea, dejará de ser un Estado miembro y el flujo de datos desde un país miembro hacia el Reino Unido (y viceversa) tendrá la consideración de «transferencias internacionales».

17. Sirva como ejemplo, la sentencia *Campbell v. Mirror Group Newspapers Ldt* [2004] UKHL 22 o la *Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt* [2003] EWHC 2629 (Ch).
18. Wadham (2015).
19. Entre otras, *Gillan v. UK* [2010] ECHR 28.
20. Aproximadamente el 52 % de quienes ejercieron su derecho a voto escogieron abandonar la Unión Europea. El resultado de dicho referéndum fue inesperado. Sin embargo, el contexto político de los años precedentes en el Reino Unido hacía bastante verosímil tal posibilidad, al haber ido arraigando un sentimiento antieuropeo, como se manifestó en su momento en las elecciones al Parlamento Europeo celebradas en mayo de 2014 y en las que la primera fuerza política fue el UKIP, que obtuvo el 26,77 % de los votos.
21. Si bien no en los mismos términos, pues es con el afán de ganar en soberanía, dejarán de someterse a una autoridad europea superior (TEDH) en cuanto a su interpretación.
22. Cfr. Gee y Young (2016).

Hay quien defiende la adopción de una opción mixta, esto es, que el Reino Unido, como país independiente, forme parte del Espacio Económico Europeo,[23] en cuyo caso debería adoptar igualmente las disposiciones del reglamento, por comprender este una de las materias relevantes en los acuerdos del EEE. Así, mientras el Reino Unido podría continuar beneficiándose del mercado único, no tendría la obligación de cumplir con ciertas políticas europeas a las que estaba adscrito hasta ahora y con las que siempre se ha mostrado en desacuerdo, como, por ejemplo, la política pesquera[24] común.

Sin embargo, ello no parece demasiado creíble, principalmente si tenemos en cuenta que uno de los motivos que han precipitado al Reino Unido al *brexit* es el anhelo de una mayor soberanía, así como su disconformidad con ciertas decisiones europeas, por lo que cuesta imaginarse al Reino Unido como socio de un Espacio Económico Europeo en el que no va a tener ningún papel decisivo para la adopción de acuerdos, pero donde, sin embargo, se le va a exigir el cumplimiento de ciertos estándares. Otra cosa sería que, en su inclusión en el EEE, se negociase un trato privilegiado por tratarse de un antiguo socio europeo.

Lo más probable es que el Reino Unido tome la consideración de «tercer Estado», por lo que, entre otras muchas cosas, se pondría fin al libre flujo de datos entre el país británico y la UE en los términos actuales. Esto, sin embargo, no significaría el fin de la transferencia de datos entre ambas partes, pues podría iniciarse un proceso mediante el que se evalúe el nivel de protección de los datos en dicho territorio que, en caso de ser favorable (y considerarse un país "seguro" por parte de la Comisión Europea) permitiría el flujo de datos entre ambos territorios (como también se produce con los Estados Unidos, a través del acuerdo *Privacy Shield*).

Este procedimiento está expresamente previsto en el artículo 45 del GDPR[25] que dispone los diferentes parámetros que la Comisión debe tener en cuenta para evaluar la adecuación del nivel de protección, entre otros: la legislación pertinente, el acceso de las autoridades públicas a los datos personales o los recursos administrativos y demás acciones judiciales previstas para el reconocimiento de los derechos y libertades de los interesados, objeto del tratamiento.

Asimismo, otro de los factores que tener en cuenta en dicho examen está relacionado con la existencia de autoridades independientes de control encargadas de supervisar el cumplimiento en materia de protección de datos, con poderes de ejecución suficiente, y que dichos órganos estén en contacto directo con los organismos europeos de control, así como con los dispuestos en los distintos Estados miembros. Habrá que ver, pues, el papel que desempeñará la ICO (*Information Comisissioner's Officer*, el equivalente británico a la AEPD) una vez consumado el *brexit*.[26]

Esta protección será revisada periódicamente, al menos cada cuatro años, que es el periodo de vigencia máximo que se le otorga a esta certificación de seguridad. No obstante, mientras dicha evaluación se lleva a cabo y teniendo en cuenta, sobre todo, las circunstancias especiales que rodean al Reino Unido, el artículo 46 prevé el flujo de datos entre terceros países, a falta de decisión por parte de la Comisión, cuando el tercer país en cuestión hubiera ofrecido garantías adecuadas, y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas que quedan detalladas a continuación en el mismo precepto, y que es de suponer que están implementadas en el Reino Unido, dado que, hasta ahora, ha contado con el paraguas de la legislación europea en dicha materia.

De todas formas, conviene hacer hincapié en que, mientras se redactan estas líneas, el proceso de negociación entre la Unión Europea y el Reino Unido sigue su camino (no con demasiado éxito, debe reconocerse) y las noticias que se obtienen de esta y otras materias se suceden con cuentagotas. Sin embargo, atendiendo a los hechos hasta ahora acaecidos, el Gobierno británico ha presentado varios

23. Jay (2017).
24. Heinig (2016).
25. Artículo 45.1: «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».
26. Cfr. Carey (2008).

documentos sobre los que fija su posición sobre asuntos claves; uno de estos es la transferencia de datos personales entre los Estados miembros y el Reino Unido. En ellos, el Gobierno afirma su deseo de mantener la cooperación con la UE en materia de protección de datos para que el flujo de información entre ambos no se vea interrumpido, esgrimiendo principalmente, razones comerciales y de seguridad.[27]

3.1. Opción primera: declararse país seguro

El objetivo del Gobierno británico, según ha explicado el Ministerio de Industrias Digitales y Creativas, es adoptar una legislación propia que incorpore las novedades introducidas por el GDPR para, una vez consumado el *brexit*, disponer de unas disposiciones legales equiparables[28] con la Unión Europea, de modo que no se limite el tráfico de datos personales entre ambos.[29]

Para eso han aprobado un texto normativo, la *Data Protection Act 2018* (que deroga la *Data Protection Act 1998*), en el que han incorporado derechos reconocidos en el reglamento, como el de acceso a los datos, a su traslado y a su borrado, incluido el derecho al olvido. También han incorporado prerrogativas nuevas como la facultad de solicitar el borrado automático de todo lo publicado en las redes sociales con una edad menor a los dieciocho años.

En la nueva *Data Protection Act 2018* se amplía la noción de «datos personales» al integrar en este concepto el ADN de las personas, la dirección IP de los usuarios, así como las *cookies* de Internet. La vocación continuista del texto se observa en la adopción del criterio de *accountability* impuesto en el GDPR, y que tiene como premisa exigir a las empresas que traten con información personal una responsabilidad activa en su gestión, anticipándose a los hechos y demostrando permanentemente que están cumpliendo la ley.

Se incorporan también al texto medidas proteccionistas con los consumidores y usuarios. Se dota a la Information Comissioner's Office[30] de mayores poderes para defenderlos, así como se regula la existencia de la figura del delegado de Protección de Datos (*Data Protection Officer*). Con el objetivo de disuadir a las grandes empresas del mal uso de la información personal de sus clientes, se ha previsto un incremento notable de las multas que pueden acarrear sus acciones.

La opción de incorporar a la legislación doméstica del Reino Unido las previsiones dispuestas en el GDPR, para conseguir una equivalencia legislativa y esquivar la catalogación como país no seguro una vez que se consolide el *brexit* y el Reino Unido pase a considerarse un tercer país es una opción válida, aunque hace aguas de cara al futuro. Con el tiempo, esto obligaría a la legislación británica a incorporar incondicionalmente aquellas modificaciones que vayan surgiendo en materia de protección de datos en la UE, aún sin participar de las discusiones ni las negociaciones, lo que, dada la naturaleza de las relaciones institucionales y la beligerancia con la que los británicos han defendido hasta ahora sus divergencias en esta materia, resulta francamente poco creíble.

Sin embargo, otro de los escenarios posibles es que el Reino Unido modifique el sentido de su nueva *Data Protection Act 2018*, una vez que se despoje de las exigencias europeas, inclinándose por escoger fórmulas más acordes con su tradición jurídica del *common law*, menos proteccionista para la privacidad de los ciudadanos y más acorde con el neoliberalismo. No hay que olvidar que el libre mercado y la mejora de la competencia han sido dos de los argumentos principales esgrimidos por los partidos políticos que se posicionaron a favor del *brexit*, así como que el organismo británico regulador en materia de protección de datos (el ICO) ha criticado con dureza las disposiciones del GDPR al considerarlo un obstáculo para las operaciones comerciales del siglo XXI.

27. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf> [Fecha de consulta: 23 de junio de 2018].
28. Hay que tener en cuenta que, bajo las últimas interpretaciones de la normativa europea, ya no es suficiente una legislación «adecuada», sino que esta debe ser «equivalente», cosa difícil de lograr, a menos que se adopte íntegramente el contenido del GDPR.
29. Hay que tener en cuenta, sin embargo, el alto estándar que se viene exigiendo por la Unión Europea en relación con la transferencia de datos personales a terceros países, como se vio en el famoso caso *Maximillian Schrems v. Data Protection Commissioner*, Asunto C-362/14, de 6 de octubre de 2015.
30. Homólogo británico de la Agencia Española de Protección de Datos.

Así las cosas, no parece descabellado pensar que, más allá de los esfuerzos iniciales por evitar toda disparidad con las directrices europeas en materia de protección de datos, el Reino Unido adopte en el futuro políticas y normativas dirigidas a obtener rédito económico de los datos personales. Si bien esta vía le comportaría no poder ser considerado como «país seguro» a los efectos del GDPR, lo cierto es que, en la práctica, nada obstaría a los británicos a obtener, a fuerza de negociación, un acuerdo internacional con la Unión Europea para la transferencia internacional de datos, como el que esta tiene en vigor con los Estados Unidos (el llamado *Privacy Shield*[31]).

3.1.1. La legislación doméstica como obstáculo

Otra de las cuestiones determinantes a la hora de examinar la adecuación del Reino Unido a los estándares de privacidad europeos es su legislación doméstica en materia de protección de datos. Precisamente, este punto es el que compromete más a los británicos, sobre todo por la *Investigatory Powers Act 2016* (popularmente conocida como *Snooper's Charter*), ley que implanta prerrogativas desorbitadas y de dudosa legalidad hacia el Gobierno Inglés y que, de facto, permite la vigilancia masiva de sus ciudadanos.[32]

Habrá que comprobar si la permanencia de esta legislación después del *brexit* es compatible con el estándar de protección exigido, cosa que parece muy alejada de las actuales propuestas políticas y jurídicas de la Unión Europea.[33] De hecho, conviene señalar cómo el TJUE dispuso hace escasos meses que el almacenamiento indiscriminado de datos es incompatible con las normas europeas,[34] y lo hizo, precisamente, declarando que la ley británica *Data Retention and Investigatory Powers Act 2014* (DRIPA), antecesora de la actual *Investigatory Powers Act 2016* que la derogó, carecía de las salvaguardas mínimas y, en consecuencia, resultaba incompatible con la UE.[35]

De este modo, nada parece seguro para el futuro del Reino Unido en materia de protección de datos, pues esta ley, junto con otros extremos comentados, podrían suponer hechos determinantes para declararlo territorio no seguro, cosa que no parece tan descabellada si tenemos en cuenta que con el mismo argumento, en el famoso caso *Schrems*,[36] el TJUE invalidó en 2015 el acuerdo *Safe Harbor* para la transferencia internacional de datos entre Estados Unidos y la UE.[37]

3.1.2. La deriva rupturista como segundo obstáculo

Por otra parte, tampoco ayuda que el Parlamento británico haya decidido, mediante votación mayoritaria, dejar de aplicar la Carta de Derechos Fundamentales de la UE[38] (incluida en el Tratado de Lisboa de 2007), que, a grandes rasgos, es el instrumento jurídico que reafirma el contenido dispuesto en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Públicas, así como las cartas sociales adoptadas por la UE y por el Consejo de Europa, y que, además, ratifica a los países firmantes en su

31. En este escenario, el Reino Unido debería adoptar sus propios acuerdos con aquellos territorios con los que quiera mantener un flujo de datos, como la Unión Europea o como Estados Unidos, con su propia versión del *Privacy Shield*, como, por ejemplo, ha hecho Suiza.
32. Entre otras previsiones, obliga a los proveedores de servicios de Internet y a los operadores de telefonía móvil a almacenar los datos de la actividad en línea de sus clientes durante un periodo de doce meses, permite a las autoridades acceder a los ICR sin orden judicial y por parte de un gran espectro de organismos públicos que poco o nada tienen que ver con la investigación de delitos trascendentes, y prescinde, en la mayoría de los casos, de la obligatoriedad de una orden judicial.
33. Cfr. Jay (2017).
34. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 21 de diciembre de 2016, en los Asuntos acumulados C-203/15 y C-698/15.
35. Ya hay jurisprudencia en contra de esta legislación – Por ejemplo, *Secretary of State for the Home Department v. Watson & Others*, C1/2015/2612 & 2613, [2018] EWCA Civ 70, Court of Appeal (Civil Division) — que, además, resulta incompatible con la Directiva 2016/680 para el tratamiento de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
36. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) en el Asunto C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, de 6 de octubre de 2015.
37. Mediante ésta, se anula la Decisión de la Comisión 2000/520/CE, de 26 de julio, que, con arreglo a la Directiva 95/46/UE, establecía el nivel adecuado de protección de las garantías internacionales entre ambos territorios.
38. El Parlamento británico votó a favor de abandonar algunas normas europeas, entre ellas la Carta Europea de Derechos Fundamentales de la UE, como parte de la batería de propuestas que adoptar con el *brexit* (*The EU Withdrawall Bill*). Pese a que una iniciativa del partido laboralista pretendía mantener la permanencia de la carta pese al *brexit*, esta enmienda fue rechazada por 317 votos a 299.

compromiso de cumplimentar la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos, ofreciendo una mayor seguridad jurídica dentro de la UE.[39]

Esta decisión es una de las pocas excepciones a la presunta voluntad continuista de los británicos, aunque parece que el contenido de esta carta va a incorporarse a la legislación británica post-*brexit* mediante la adopción como propios de los derechos y principios reconocidos hasta el momento por la jurisprudencia de los tribunales europeos en referencia a la carta, claramente esta solución no ofrece garantías suficientes en términos de seguridad jurídica.

De hecho, en cuanto a la protección de datos personales, este nuevo escenario añade dificultades a la intención del Gobierno británico de crear un entorno jurídico equivalente a la protección que proporciona la Unión Europea a través del GDPR, que, además, hace constantes referencias a la carta a lo largo de su articulado.

La Carta, cuyo artículo 8 contiene una previsión específica relativa al derecho de protección de datos, es un texto fundamental en tanto que ha supuesto un paso más en la regulación de esta materia, mucho más allá del artículo 16 del TFUE, el artículo 8 del Convenio Europeo de Derechos Humanos o la propia Directiva 95/46/CE (ahora derogada), todos ellos dedicados a la protección de este mismo extremo. Conviene recordar que, desde que la carta obtuvo el estatus de Tratado Internacional en 2009, muchas decisiones del Tribunal de Justicia de la Unión Europea (así como de los propios tribunales británicos) se han basado en sus disposiciones, asimismo su criterio interpretativo se ha convertido en indispensable a la hora de evaluar solicitudes de transferencias internacionales de datos con terceros países.[40] El cumplimiento de la carta, pues, podría haber sido un elemento más que determinante para que la Unión Europea considerase al Reino Unido como un «país seguro» en materia de protección de datos.

3.2. Opción segunda: adoptar *Binding Corporate Rules*

La segunda de las opciones que podría emplearse tras la salida del Reino Unido de la Unión Europea sería adoptar las llamadas *Binding Corporate Rules* (BCR), que han sido traducidas al castellano como «normas corporativas vinculantes».

Las normas corporativas vinculantes son, a grandes rasgos, un conjunto de reglas (una especie de código de conducta, pero con carácter vinculante) específicas sobre el tratamiento de los datos personales que lleva a cabo un grupo empresarial, normalmente multinacional, mediante el cual dicha corporación garantiza ante los organismos reguladores que la transferencia internacional de datos entre miembros del mismo grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta cumple con la normativa europea con independencia de que el país de destino garantice o no un nivel adecuado de protección de esos datos de acuerdo con los parámetros de la legislación del país de su origen.

Esta opción, que en la práctica ya estaba en funcionamiento,[41] se recoge ahora y expresamente en el

39. Tomás Mallén (2017) destaca como este desenlace es consecuente con las reticencias históricas del Reino Unido hacia la Carta de Derechos Fundamentales de la Unión Europea, a la que reiteradamente han acusado de obstaculizar la lucha contra el terrorismo y el crimen organizado, y cuyo exponente máximo resultó el *opt-out* británico respecto de esta, mediante el cual «se abrió paso a una perversa dinámica de la Europa a varias velocidades», al constituir dicha excepción una «reserva contraria al objeto y al fin del propio Tratado de Lisboa».
40. Como ejemplo, el Dictamen 1/15 del Tribunal de Justicia (Gran Sala) de 26 de julio de 2017 acerca de la idoneidad sobre la transferencia de los datos del registro de nombres de pasajeros entre la UE y Canadá, en el que el TJUE dispuso que para juzgar los hechos solo iba a tener en cuenta el artículo 8 de la Carta de Derechos Fundamentales de la UE porque esta establecía las condiciones de tratamiento de datos de una manera más específica que el propio artículo 16 del TFUE: «En efecto, si bien es cierto que ambas disposiciones declaran que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, únicamente el artículo 8 de la carta prescribe de manera más específica, en su apartado 2, las condiciones en que tales datos pueden ser objeto de tratamiento», par. 120.
41. En la práctica, se ha convertido en una vía de escape para ciertas empresas multinacionales cuyas transferencias no cumplen las exigencias europeas. Esto ha ocasionado que tanto la doctrina como los gobiernos exijan la adopción de medidas efectivas para asegurar un estándar aceptable en materia de protección de datos. Así, se están empezando a exigir vincular estos mecanismos a conceptos como *accountability* o la responsabilidad social corporativa, entre otros. Moerel (2012).

GDPR,[42] para el caso de que la Comisión disponga que un tercer país, parte de su territorio o una organización internacional, ya no garantiza un nivel de protección adecuado, lo que, consecuentemente, llevaría a la prohibición de transferir datos entre este y la Unión Europea, «salvo que se cumplan los requisitos del presente reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes».[43]

El artículo 47 del reglamento dispone que la autoridad de control competente aprobará normas corporativas vinculantes siempre que se cumplan los requisitos que a continuación enumera. Van desde garantizar el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, hasta tener previsto un procedimiento de reclamación ante la autoridad competente, pasando por la obligación de realizar auditorías periódicas.

Sin embargo, se evidencian problemas prácticos a la hora de adoptar BCR, pues, para su implementación, se requiere la autorización previa de todas las agencias nacionales de protección de datos, lo que plantea el problema de qué estatus tendrá la ICO británica después del *brexit*. En principio, no parece lógico que continúe gozando de la misma posición jurídica que hasta ahora, pues, quizá no desde un principio, con el paso del tiempo y la evolución jurídica puede no ofrecer las mismas garantías que sus homólogos europeos. No obstante, para salvar este obstáculo, podrían adoptarse acuerdos de reconocimiento mutuo de procedimientos entre las agencias estatales de protección de datos de los Estados miembros y la ICO, aunque para ello debería existir inevitablemente cierta equivalencia entre los estándares de protección de la normativa británica y la europea.

3.3. Opción tercera: emplear *Standard Form Contracts*

Una última solución, aunque más antigua[44] y parcialmente efectiva, sería la autorización de las transferencias internacionales de datos en función de cláusulas contractuales tipo, estandarizadas por distintas decisiones de la Comisión Europea, y que se prevén en el artículo 46 del GDPR, junto con las normas corporativas vinculantes, para el caso de ausencia de una decisión por la que se constate la adecuación de la protección de los datos en un tercer país, con el objeto de tomar medidas que traten de compensar dicha situación.

Para este supuesto se prevé la adopción de cláusulas tipo de protección de datos adoptadas por la Comisión[45] o por una autoridad de control capaz de asegurar la observancia de los requisitos de protección de datos y derechos de los interesados, así como que sean adecuados a los estándares de protección dentro de la Unión, incluida la exigibilidad por parte del interesado de sus derechos, así como de las acciones legales efectivas, lo que le permitiría obtener la reparación o una indemnización tanto en la Unión Europea como en un tercer país. Dice el GDPR que «en particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto».[46]

Es decir, se trata de un acto jurídico creado al amparo del Derecho de la Unión o de los Estados miembros, por el cual se vincula al encargado del tratamiento de datos respecto del responsable y se establecen el objeto, la duración, la naturaleza y la finalidad del tratamiento de determinados datos personales, así como las obligaciones y los derechos del responsable.

42. Sin embargo, este sistema no es nuevo, ya se encontraba previsto en la Directiva 95/46/CE que ahora el GDPR deroga, así como, por ejemplo, en nuestra LOPD de 1999.
43. Consideración preliminar 107.
44. Este mecanismo era el que empleaba la Agencia Española de Protección de Datos antes de 2009, cuando empezó a autorizar transferencias internacionales de datos en función de las *Binding Corporate Rules*.
45. Hasta la fecha, la Comisión Europea ha publicado dos tipos de contratos con cláusulas tipo: en primer lugar, de protección para las transferencias de datos realizadas desde organismos de control en la Unión Europea, hacia otros establecidos fuera de esta o del Espacio Económico Europeo; en segundo lugar, cuando el destino de los datos sea una entidad de procesamiento de datos no europea. Ambos tipos de contratos se encuentran disponibles en: <https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en> [Fecha de consulta: 25 de junio de 2018].
46. Consideración preliminar 108.

La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos no debe obstar a que los responsables o encargados incluyan estas en un contrato más amplio (como un acuerdo entre dos encargados) o a que añadan otras cláusulas o garantías adicionales, siempre que mantengan los niveles de protección de los interesados. El reglamento hace hincapié en la conveniencia de complementar los contratos tipo con otras garantías de protección, pues es consciente de la limitada seguridad jurídica que estas ofrecen como mecanismo efectivo de control, motivo por el cual la Comisión se reserva, en todo caso, las competencias de ejecución.

En este punto, conviene comentar que el GDPR ha introducido grandes cambios respecto del régimen de transferencias internacionales anterior; por ejemplo, en relación con los exportadores de datos, pues, por primera vez, se permite que este sea tanto un responsable como un encargado del tratamiento, acabando con la disparidad de criterios de las legislaciones nacionales de los Estados miembros que, en muchos casos, limitaba las exportaciones a aquellos que eran responsables del tratamiento. A partir de ahora, se dinamizan las transferencias internacionales mediante la subcontratación de terceros países de prestadores de servicios establecidos en la UE, lo que, en términos de seguridad, no parece lo más propicio.

Esta vocación del GDPR de estimular las transferencias se observa también en la reducción de los supuestos en los que es necesaria autorización y notificación previa de las transferencias internacionales.[47] Mientras que la normativa anterior obligaba a los exportadores de datos a solicitar a la autoridad nacional de control una autorización previa (que era concedida solo si conseguían acreditar las garantías suficientes) para poder transferir datos a importadores establecidos en terceros países que no gozaban de un nivel adecuado de protección, el GDPR permite que las transferencias se realicen sin necesidad de autorización ni notificación previa, excepto para casos contados como, por ejemplo, cuando las garantías se aporten mediante un contrato *ad hoc* o se trate de una situación en la que prime el interés legítimo del responsable del tratamiento.

No obstante todo lo anteriormente expuesto, desde un punto de vista eurocentrista y en cuanto a la protección de los derechos y libertades, no hay que perder de vista que, en algunos casos, el GDPR será de aplicación a ciertas compañías británicas con independencia de la determinación que tome finalmente el Reino Unido, dado que el objeto del nuevo reglamento es preservar los derechos y las mismas garantías a los ciudadanos europeos frente a todas las compañías que se dediquen al tratamiento de datos personales en la UE, aun cuando estas no se encuentren domiciliadas en suelo europeo. Así pues, lo único cierto después del *brexit* es que el GDPR será de aplicación a las empresas británicas que procesen datos personales de los europeos o que monitoricen su comportamiento en suelo europeo, por extensión del principio de territorialidad instaurado en el artículo 3 del GDPR.

4. Conclusiones

La evolución del sistema de protección de la privacidad por parte del Reino Unido ha sufrido grandes fluctuaciones en cuanto al estado de la cuestión y su protección, hasta el punto de que, habiéndose situado a la cabeza de la protección de datos personales, hoy parece adoptar posturas diametralmente opuestas. De hecho, el Reino Unido es actualmente uno de los países del mundo que más vigilada tiene a su sociedad,[48] más aún con la aprobación de algunas normas de urgencia en materia de terrorismo altamente controvertidas, como la derogada DRIPA.

Mientras que se encuentran vestigios de la protección del derecho a la privacidad en jurisprudencia inglesa que data del siglo XVIII,[49] desde los últimos quince años, estamos asistiendo a una degradación de dicho sistema de protección por parte de las políticas del Reino Unido, agravada

47. Por esta y otras cuestiones, cuesta creer que el fin último del GDPR sea ampliar el margen de derechos y garantías de los ciudadanos europeos frente a sus datos, pues, salvo excepciones, el propósito general parece ser armonizar las legislaciones con el fin de no obstaculizar el mercado interior ni la libre competencia.
48. Así lo advirtió ya en 2004, Richard Thomas, el responsable de la ICO, cuando dijo que el Reino Unido se estaba convirtiendo en una sociedad vigilada, en sus propias palabras: «*sleepwalking into a surveillance society*».
49. *Entick v. Carrington* [1765].

aún más por la coyuntura actual derivada del *brexit*, así como su posible salida de instrumentos como el CEDH.

Lo acontecido en el Reino Unido es una muestra de la susceptibilidad de los sistemas jurídicos a sufrir variaciones en función de las necesidades sociales, culturales y económicas, pero también en función de las prioridades políticas del momento. Partiendo de dicha premisa, resulta paradójico como, ahora más que nunca, en el entorno global y digital en el que nos insertamos y que proporciona constantemente nuevas amenazas para la privacidad (a la par que otorga innumerables ventajas para la sociedad, de lo contrario sería negar la mayor), el Reino Unido ha resuelto (o bien por razones ideológicas aparejadas a lograr un mayor control social, o bien plegándose a la lógica del beneficio), desincentivar el estándar de protección que había conseguido instaurar para la privacidad de sus ciudadanos.[50]

A raíz de las últimas innovaciones tecnológicas, los acontecimientos terroristas de los últimos tiempos y el rumbo neoliberal de las recientes políticas públicas puede decirse que el Reino Unido ha sufrido un cambio sustancial en cuanto a la privacidad se refiere (perceptible incluso antes de ratificarse en su decisión de abandonar la Unión Europea), alejándose cada vez más de los estándares europeos y su proteccionismo, e inclinándose hacia el modelo norteamericano y su principio de no intervención.[51]

De hecho, en la actualidad, el Gobierno británico posee unos poderes de vigilancia y recopilación de información mucho mayores que en cualquier momento de su historia; en muchos aspectos, más amplios que los disponibles para las autoridades en países democráticos comparables.[52] Sin embargo, más allá del exceso de vigilancia o de la intromisión en la privacidad a manos de los poderes públicos,[53] lo verdaderamente preocupante es que, en connivencia con estos, cada vez son más las compañías privadas que están almacenando datos personales para hacer negocios o con propósitos que hoy por hoy se desconocen.[54]

Pese a que el ejercicio de acciones que pueden resultar invasivas de la privacidad en el Reino Unido[55] son de conformidad con la legislación vigente en materia de protección de datos, siempre hay excepciones en función de conceptos jurídicos indeterminados que, además, se ven afectados por normas especiales con gran incidencia en la materia, como la polémica *Investigatory Powers Act 2016*. De hecho, como ya se ha visto, son muchas las veces en las que los tribunales europeos han recriminado al Reino Unido la ineficacia práctica del derecho a la privacidad.

Los argumentos británicos para justificar dicha realidad se basan tradicionalmente en la inexistencia en su legislación de un reconocimiento expreso del derecho a la privacidad,[56] cuestión que, si bien se ha tratado de suplir con figuras jurídicas que solo otorgan una protección parcial e inefectiva de este derecho, con la entrada en vigor del GDPR deberían verse prácticamente superadas.

De este modo, el nuevo escenario político que se presenta para el Reino Unido es incierto, pues, una vez que deje de estar sometido a los criterios europeos en materia de protección de datos, mucho más conservadores que los estándares anglosajones y del *common law*, puede que sus ciudadanos vean revertidas las protecciones que les brindaba la legislación europea de acuerdo con la nueva tendencia británica, encaminada hacia una liberalización de la privacidad. Pronto saldremos de dudas.

50. Resulta interesante poner en relación las decisiones políticas y legislativas que se derivan del estándar existente de privacidad con el nivel de democracia efectiva. Cfr. Schwartz (1999).
51. «In the United Kingdom, our interviews with privacy leaders revealed a privacy field that straddles the Atlantic in a deeply liminal state: one foot standing on American soil and one foot firmly planted on the Continent», Bamberguer *et al.* (2015).
52. Mathieson (2010).
53. Solove (2006).
54. O'Neil (2018).
55. Cfr. Harcourt (2014).
56. Colvin (2002).

5. Referencias bibliográficas

ASHWORTH, A.; EMMERSON, B.; MACDONALD, A. (2012). *Human Rights and Criminal Justice*. Londres: Sweet and Maxwell.

BAINBRIDGE, D. (2005). *Data Protection Law* (2ª. ed.). Gran Bretaña: XPL publishing.

BAMBERGUER K. A. [*et al.*] (coords.) (2015). *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*. Cambridge: Massachusetts Institute of Technology Press.

CAREY, P. (2008). *Data Protection Handbook*. Londres: The Law Society.

CAREY, P. (1998). *Data Protection Act 1998*. Londres: Blackstone Press Limited.

COLVIN, M. (2002). *Developing Key Privacy Rights*, Portland: Hart publishing.

CORRECHER MIRA, J. (2018). *Principio de legalidad penal: ley formal vs. law in action*. Valencia: Tirant lo Blanch.

DICEY, A. V. (2013). *Introductory to the study of the law of the constitution*. Oxford: Oxford University Press.

DWORKIN, C. K. (1973). «The Younger Committee Report on Privacy». *The Modern Law Review,* vol. 36, n.º 4, págs. 399-406.

ENDICOTT, T. (2001). «International Meaning: Comity in Fundamental Rights Adjudication». *International Journal of Refugee Law,* vol. 13, págs. 280-292. <https://doi.org/10.1093/ijrl/13.3.280>

GEARTY, C. (2002). «Reconciling Parliamentary democracy and human rights». *Law Quaterly Review,* n.º 118, pág. 269 y ss.

GEE, G.; YOUNG, A. L. (2016). «Regaining Sovereignty? Brexit, the UK Parliament and the Common Law». *European Public Law*, vol. 22, págs. 131-148.

GROSZ, S. [*et al.*] (coords.) (2000). *Human Rights. The 1998 Act and the European Convention*. Londres: Sweet and Maxwell.

HARCOURT, B. E. (2014). «Governing, Exchanging, Securing: Big Data and the production of a digital knowledge». *Public Law and Legal Theory Working Paper Group*.

HARVERS, P. [*et al.*] (coords.) (2015). «The Convention and the Human Rights Act: A New Way of Thinking». *An Introduction to Human Rights and the Common Law*. Oxford: Hart Publishing, págs. 5-29.

HEINIG, H. M. (2016). «Is Europe in a Crisis of Faith?», *German Journal Law*, vol. 17, págs. 29-32.

HICKMAN, T. (2011). *Public Law after the Human Rights Act*, Hart Publishing, Oxford.

JAY, R. (2017). *Guide to the General data Protection Regulation*. Londres: Sweet & Maxwell.

MATHIESON, K. (2010). *Privacy Law Handbook*. Londres: The Law Society.

MOEREL, L. (2012). *Binding Corporate Rules. Corporate Self-regulation of Global Data Transfers*. Oxford: Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199662913.001.0001>

O'NEIL, K. (2018). *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing.

RAZ, J. (1979). *The authority of law. Essays on law and morality*. Oxford: Oxford Clarendon Press.

SCHWARTZ, P. M. (1999). «Privacy and Democracy in Cyberspace». *Vanderbilt Law Review*, vol. 52, págs. 1610-1672.

SOLOVE, D. J. (2006). «A taxonomy of Privacy». *University of Pennsylvania Law Review*, vol. 154, págs. 477-560. <https://doi.org/10.2307/40041279>

TOMÁS MALLÉN, B. S. (2017). «El *brexit* y su impacto en la Europa de los derechos: el desafío británico al derecho constitucional europeo». *UNED, Revista de Derecho Político*, n.º 100, págs. 1169-1208. <https://doi.org/10.5944/rdp.100.2017.20730>

TUGENDHAT, M; CHRISTIE, I. (2002). *The law of Privacy and The Media*. Nueva York: Oxford University Press.

WADHAM, J.; MOUNTFIELD, H.; PROCHASKA, E. (2015). *Blackstone's guide to The Human Rights Act*, 1998. Oxford: Oxford University Press.

WARREN, S. BRANDEIS, L. (1890). «The Right to Privacy». *Harvard Law Review*, vol. IV, n.º 5, págs. 193-220. <https://doi.org/10.2307/1321160>

Cita recomendada

SANCHO LÓPEZ, Marina (2019). «Garantías legales de la privacidad en el Reino Unido: la (des)protección de datos después del *brexit*». *IDP. Revista de Internet, Derecho y Política*. N.º 29, págs. 1-15. UOC [Fecha de consulta: dd/mm/aa].
<http://dx.doi.org/10.7238/idp.v0i29.3157>

Sobre la autora
Marina Sancho López
marina.sancho@uv.es

Doctora en Derecho
Directora del Máster Universitario en Abogacía y Práctica Jurídica
Universidad Internacional de Valencia

Tiene un máster de Derechos humanos, democracia y justicia internacional y ha desarrollado labores técnicas en la Conselleria de Gobernación y Justicia de la Generalitat Valenciana. Además, cuenta con una larga trayectoria en el acceso a la carrera judicial. Ha realizado diversas estancias de investigación y formación en diferentes instituciones y universidades europeas como el Max Planck Institute for Comparative and International Private Law de Hamburgo o la Universidad de Cambridge. Actualmente, colabora en el proyecto de investigación «Derecho civil valenciano y europeo» de la Universidad de Valencia y forma parte de varios proyectos de innovación educativa como el del grupo estable Manuales Jurídicos y Materiales Docentes 3.0. Asimismo, cuenta con numerosos artículos publicados en revistas jurídicas de reconocido prestigio y con aportaciones a diversas jornadas y congresos especializados.

Universidad Internacional de Valencia – VIU
C/ Pintor Sorolla, 21
46002 Valencia, España