

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: ALCANCE, CONFLICTOS Y DESAFÍOS



Marina Tuñas Carballo
(miembro de la
Asociación de Derecho
de la Universidad
Carlos III de Madrid)

1. Introducción

La globalización de los flujos de información y la expansión exponencial de los servicios digitales han desdibujado las fronteras tradicionales del Derecho Internacional, exigiendo la reconfiguración de los principios jurisdiccionales. En este nuevo panorama, el Reglamento General de Protección de Datos (“RGPD”) se erige como pieza normativa central del modelo europeo de gobernanza digital, al establecer un sistema de garantías robusto que trasciende los límites territoriales de la Unión.

El denominado *Brussels Effect* encuentra en la aplicación extraterritorial del RGPD su expresión paradigmática: la capacidad de la Unión para proyectar sus estándares normativos más allá de sus fronteras.

No obstante, el despliegue práctico de este régimen normativo plantea desafíos jurídicos, institucionales y operativos, como, por ejemplo, la necesidad de conciliar la ambición normativa de las instituciones europeas con los recursos disponibles de los Estados Miembros.

El presente artículo se ha propuesto examinar los elementos fundamentales de la aplicación extraterritorial del Reglamento, a partir de un enfoque metodológico que combina el análisis del articulado con el estudio de la jurisprudencia europea.

El modelo de protección de datos personales ha evolucionado hacia una forma de jurisdicción funcional, en la que la aplicabilidad del régimen normativo no depende ya del lugar de establecimiento del responsable del tratamiento, sino de la localización del interesado y de la voluntad activa de la Unión para proteger sus valores fundamentales allí donde estos puedan verse comprometidos.

2. Marco teórico y normativo

a. Análisis del artículo 3 del Reglamento de Protección

La Carta de los Derechos Fundamentales de la Unión Europea (“CDUE”) ha consagrado el derecho a la protección de los datos personales como manifestación autónoma del derecho al respeto de la vida privada¹¹⁷. En desarrollo de este mandato constitucional, el Reglamento (UE) 2016/679¹¹⁸ (“RGPD” o “Reglamento”) ha sido diseñado para garantizar que los mecanismos de protección no se vean menoscabados por la nacionalidad o el lugar de establecimiento de la entidad responsable del tratamiento.

Frente a un modelo de jurisdicción clásico, anclado en el principio de territorialidad, la introducción del Reglamento Europeo no hizo sino confirmar una tendencia que ya había sido delineada por el Tribunal de Justicia de la Unión Europea (“TJUE”), al exigir el cumplimiento de los estándares normativos europeos a aquellos responsables que, con independencia de su ubicación, hayan desarrollado su actividad en la Unión¹¹⁹.

Siguiendo lo dispuesto en el Artículo 3(2) RGPD, la normativa europea será aplicable cuando se ofrezcan bienes o servicios que se dirijan a interesados ubicados en uno o varios de los Estados Miembros o cuando se controle su comportamiento. Ambos supuestos requieren una interpretación sistemática del Reglamento, en línea con la jurisprudencia del TJUE, así como con las Directrices y Protocolos del Comité Europeo de Protección de Datos (“EDPB”) y de las autoridades nacionales de supervisión.

i. Datos personales

Se entiende por *dato personal* toda información sobre una persona física identificado o identificable¹²⁰. Dicha definición abarca no sólo datos evidentes como el nombre o la dirección postal, sino también cualquier información que, por sí sola o en combinación con otros elementos, permita identificar directa (o *indirectamente*) al titular.

En sentencias clave como el asunto *Bayer* (C-582/14), el TJUE ha contribuido a perfilar esta interpretación al determinar que una dirección IP puede ser considerada un dato

¹¹⁷ Carta Europea de Derechos Fundamentales. Artículo 8(1). «Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan»

¹¹⁸ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

¹¹⁹ STJUE de 13 de mayo de 2014. *Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (ECLI:EU:C:2014:317)

¹²⁰ Reglamento (UE) 2016/679. Artículo 4(1)

personal si el responsable del tratamiento dispone de medios legales razonables para identificar al usuario¹²¹.

ii. Interesados en la Unión

El interesado –la persona física cuyos datos personales son objeto del tratamiento– ocupa el eje central del sistema europeo de protección de datos. Así lo establece el Considerando 14 del Reglamento al señalar que la protección conferida debe aplicarse a las personas físicas con independencia de su nacionalidad o lugar de residencia¹²².

Desde esta perspectiva, las instituciones europeas han adoptado un modelo de protección que prioriza la presencia efectiva del interesado en la Unión como criterio objetivo para determinar la aplicabilidad del Reglamento.

En efecto, tal y como ha precisado el Comité Europeo de Protección de Datos, lo determinante es el lugar donde el interesado se encuentre en el momento en que se ofrece el servicio o se monitoriza el comportamiento del interesado, sin que resulte relevante ni la duración de su estancia en la Unión ni su estatus legal.

No obstante, esta amplitud objetiva se ve matizada por un segundo requisito: la intencionalidad del responsable del tratamiento. La mera presencia física en territorio europeo no basta, por sí sola, para activar la aplicación del Reglamento. Es imprescindible que la actividad se dirija de forma deliberada al mercado o territorio europeo, ya sea mediante la oferta de bienes o servicios (*art. 3(2)(a)*), o bien, a través de la monitorización del comportamiento de los interesados (*art. 3(2)(b)*).

Con la incorporación de este segundo requisito se excluiría del ámbito de aplicación aquellos supuestos en los que el acceso desde la Unión se produce de manera incidental o fortuita, sin intención por parte del responsable de alcanzar el mercado europeo. De este modo, si un servicio digital ha sido diseñado para ser comercializado en un tercer Estado, el eventual acceso por parte de uno de sus usuarios desde la Unión no activaría la aplicación del Reglamento¹²³.

¹²¹ STJUE Patrick Breyer v Bundesrepublik Deutschland (C-582/14). «(...) una dirección IP dinámica, en combinación con la fecha de la sesión de consulta a la que se refiere, constituye (...) un dato personal»

¹²² RGPD. Considerando 14. La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales

¹²³ Comité Europeo de Protección de Datos. Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3) – p.17

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Artículo 3(2) RGPD no consolida una aplicación extraterritorial basada en el estatus personal del interesado, sino una aplicación basada en dos elementos concatenados: (i) la presencia del interesado en el territorio de la Unión y (ii) la intención del responsable de tratar los datos personales de dichos interesados. Solo la concurrencia de ambos elementos justificaría la aplicación del Reglamento.

iii. Oferta de bienes y servicios

El mero acceso a un sitio web desde un Estado Miembro no constituye, por sí solo, indicio suficiente para deducir la voluntad del responsable de dirigirse al territorio europeo. De igual modo, tampoco resultan concluyentes –cuando se analizan aisladamente- la incorporación de una dirección de correo electrónico o el uso de una lengua que coincide con la del país de establecimiento del responsable¹²⁴.

Si bien, el asunto C-585/08 *Pammer y Hotel Alpenhoff*¹²⁵ se enmarca en el contexto del Reglamento Bruselas I, los criterios adoptados por el Tribunal han sido utilizados tras la entrada en vigor del RGPD para identificar aquellas actividades que se dirigen deliberadamente al mercado europeo¹²⁶.

Entre ellos, cabe destacar a título ejemplificativo los siguientes elementos: (a) la mención expresa de la Unión Europea o de uno o varios Estados miembros en relación con los bienes o servicios ofrecidos; (b) la contratación de servicios de publicidad o posicionamiento orientados específicamente al mercado europeo; (c) el uso de lenguas o monedas propias de la Unión Europea; o (d) la oferta expresa de entrega o envío de los productos a los Estados Miembros¹²⁷.

¹²⁴ RGPD. Considerando 23. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

¹²⁵ Tribunal de Justicia de la Unión Europea (TJUE). (2010). *Heinz-Leo Pammer v. Reederei Karl Schlüter GmbH & Co. KG y Hotel Alpenhof GesmbH v. Oliver Heller*, Asuntos acumulados C-585/08 y C-144/09, (ECLI:EU:C:2010:740)

¹²⁶ EPDB. Directrices 3/2018 (nº 7) – p.19

¹²⁷ EPDB. Directrices 3/2018 (nº 7) – p.21

iv. Control de comportamiento

Además del supuesto relativo a la oferta de bienes o servicios, el Reglamento General de Protección de Datos también contempla las actividades relacionadas con el control del comportamiento. Esta vía, prevista en el Artículo 3(2)(b) RGPD, permite activar las garantías del texto normativo incluso cuando no exista una relación comercial o contractual directa entre el responsable y el interesado.

Precisamente, es necesario realizar una valoración más detallada, que atienda a la finalidad subyacente del tratamiento, en especial cuando se empleen técnicas orientadas a observar, analizar o predecir comportamientos, preferencias o actitudes del interesado.

Aunque el Considerando 24 se refiere específicamente al seguimiento a través de Internet, el Comité Europeo de Protección de Datos ha interpretado que el concepto del control del comportamiento debe entenderse en un sentido amplio, abarcando también otros métodos y tecnologías que persigan fines equivalentes, aunque no estén basados exclusivamente en entornos digitales¹²⁸.

A título ilustrativo —y sin carácter exhaustivo— se consideran prácticas típicas de control del comportamiento: (i) la geolocalización de los interesados mediante dispositivos móviles o sensores inteligentes; (ii) la utilización de técnicas de publicidad comportamental¹²⁹; (iii) la monitorización del estado de salud y, (iv) en general cualquier procedimiento que permita elaborar perfiles individualizados con fines predictivos o analíticos¹³⁰.

¹²⁸ RGPD. Considerando 24. *Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes*

¹²⁹ Grupo de Trabajo de Protección de Datos del Artículo 29. Dictamen 2/2010 sobre publicidad comportamental en línea. *La publicidad comportamental es publicidad basada en la observación continuada del comportamiento de los individuos. La publicidad comportamental busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento*

¹³⁰ EPDB. Directrices 3/2018 (nº 7) – p.22

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

b. Transferencias internacionales de datos

Delimitado el ámbito de aplicación extraterritorial del Reglamento, procede analizar los mecanismos jurídicos que permiten la transferencia de datos a un tercer país u organización internacional¹³¹.

i. Decisiones de Adecuación

El Artículo 45 del RGPD permite a la Comisión Europea reconocer que el país o entidad destinataria ofrece un nivel de protección adecuado, esencialmente equivalente al vigente en la Unión. La Comisión tiene la facultad de adoptar dicha decisión tras haber evaluado el ordenamiento jurídico del país receptor, incluyendo la legislación en materia de protección de datos, prácticas institucionales, los mecanismos de supervisión disponibles y demás recursos de que disponen los interesados cuyos datos han sido transferidos.

La adopción de una decisión de adecuación eximiría al responsable del tratamiento de la obligación de establecer garantías adicionales para la transferencia, permitiendo que ésta se lleve a cabo en condiciones similares a las existentes dentro del Espacio Económico Europeo (“EEE”), simplificando significativamente el proceso desde el punto de vista administrativo¹³².

ii. Herramientas de salvaguarda

En ausencia de una decisión de adecuación, debe recurrirse a una de las herramientas previstas en el Artículo 46 del RGPD a fin de garantizar que la transmisión se ajusta a los estándares de protección exigidos por el Derecho de la Unión.

Entre los mecanismos más comunes deben destacarse las cláusulas contractuales tipo (*Standard Contractual Clauses* o SCCs)¹³³ y las normas corporativas vinculantes (*Binding Corporate Rules* o BCRs).

¹³¹ Directrices 05/2021 sobre la interacción entre la aplicación del artículo 3 y las disposiciones sobre transferencias internacionales conforme al Capítulo V del RGPD

¹³² Comisión Europea. (s. f.). *Adecuación de la protección de datos para países no pertenecientes a la UE*. <<https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=es&etrans=es>>

¹³³ Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

iii. Excepciones

Siguiendo lo dispuesto en el Artículo 49 del RGPD, el legislador europeo ha permitido que, bajo determinadas condiciones, puedan realizarse transferencias internacionales de datos aún en ausencia de las medidas de salvaguarda anteriores.

Reguladas con mayor precisión en las Directrices 2/2018 del Comité Europeo de Protección de Datos¹³⁴, las excepciones previstas cumplirían una función residual. Su finalidad es permitir la transferencia de datos en circunstancias excepcionales, cuando no es posible recurrir a ninguno de los mecanismos delineados en los artículos anteriores.

Entre los supuestos contemplados, debe destacarse la provisión que permite la transferencia de datos cuando ésta sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento¹³⁵.

A modo de ejemplo práctico, en el contexto de una solicitud de movilidad internacional, se requerirá el envío de las calificaciones académicas del estudiante europeo a una institución situada fuera del Espacio Económico Europeo. Si bien esta transferencia ocasional podría justificarse a amparo de la excepción mencionada, si este tipo de transferencias se convierten en práctica habitual, la Universidad deberá implementar las garantías estructurales necesarias.

A la luz de lo anterior, las excepciones del Artículo 49 no han sido concebidas para sustituir a las herramientas principales de protección, sino que actúan como mecanismos de último recurso en contextos excepcionales. Su aplicación debe realizarse con extrema cautela, atendiendo a los principios de necesidad, proporcionalidad y transparencia.

c. Cambio de paradigma: Schrems

La resolución del TJUE, en el asunto C-311/19 ("*Sentencia Schrems II*")¹³⁶, ha marcado un hito trascendental en el desarrollo europeo de protección de datos. No sólo se han redefinido las exigencias jurídicas que condicionan la circulación de datos personales

¹³⁴ Comité Europeo de Protección de Datos. (2018). *Directrices 2/2018 sobre las derogaciones del artículo 49 del Reglamento 2016/679*

¹³⁵ RGPD. Artículo 49(1)(b): En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes: b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado

¹³⁶ Asunto C-311/18. Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020. *Data Protection Commissioner contra Facebook Ireland Ltd y Maximillian Schrems (Schrems II)* (ECLI:EU:C:2020:559)

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

fuera del EEE, sino que se ha intensificado el principio de responsabilidad proactiva de los actores implicados, reforzando la proyección extraterritorial de la normativa europea.

El Tribunal invalidó la Decisión de Ejecución (UE) 2016/1250¹³⁷ (*comúnmente conocida como Privacy Shield*¹³⁸) al considerar que el ordenamiento jurídico de los Estados Unidos no ofrecía nivel de protección equivalente al exigido por el Derecho de la Unión.

En particular, el TJUE cuestionó el acceso indiscriminado por parte de las autoridades públicas a los datos transferidos desde Europa, así como la ausencia de mecanismos efectivos de control jurisdiccional y de reparación accesibles para los ciudadanos europeos cuyos derechos pudieran verse afectados por dicho tratamiento¹³⁹.

Tras la invalidez del *Privacy Shield*, todas las transferencias de datos que se amparaban en dicho marco quedaron desprovistas de base jurídica, situando a los Estados Unidos en la misma posición que cualquier otro tercer país que carece de una decisión de adecuación conforme al Reglamento.

Esta nueva situación obligó a los responsables del tratamiento a revisar los mecanismos empleados para legitimar dichas transferencias, prestando especial atención al uso de las cláusulas contractuales tipo.

Si tras la implementación de garantías adicionales, no consigue alcanzarse el nivel de protección exigido por el RGPD; el responsable del tratamiento deberá suspender la transferencia o abstenerse de realizarla. En caso contrario, serán las autoridades nacionales de protección de datos quienes deberán intervenir en ejercicio de sus competencias, ordenando el cese de la transferencia conforme a lo previsto en el Artículo 58(2)¹⁴⁰.

En este sentido, el Tribunal ha delineado un sistema de gobernanza en tres niveles: (i) la Comisión Europea mantiene la competencia para adoptar decisiones de adecuación, (ii) los responsables del tratamiento asumen la tarea de evaluar la legalidad y eficiencia de las garantías aplicables, y, (iii) finalmente, las autoridades nacionales de control son las

¹³⁷ Comisión Europea. (2016). *Decisión de Ejecución (UE) 2016/1250 de la Comisión, relativa a la adecuación de la protección proporcionada por el régimen “EU-US Privacy Shield”* (DO L 207, p. 1–112). Diario Oficial de la Unión Europea.

¹³⁸ Marco jurídico adoptado por la Comisión Europea, el 12 de julio de 2016, mediante la Decisión de Ejecución (UE) 2016/1250, que legitimaba las transferencias internacionales de datos personales desde la Unión Europea a empresas establecidas en Estados Unidos que se hubieran adherido voluntariamente, bajo el aura de protección de una serie de principios en la transmisión de datos

¹³⁹ García-Perrote Martínez, I., & García Micó, T. G. (2020). *Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II*. *InDret* Vol. 3, 2020 (551-559)

¹⁴⁰ ECLI:EU:C:2020:559 - §118

encargadas de supervisar el cumplimiento del Reglamento y de imponer las medidas correctoras pertinentes en caso de detectarse infracciones¹⁴¹.

El impacto de la Sentencia *Schrems II* trasciende el marco específico de las relaciones entre la Unión y los Estados Unidos, al determinar los principios de alcance general que resultan de aplicación a cualquier transferencia internacional de datos, institucionalizando una cultura de responsabilidad reforzada y evaluación continua¹⁴².

d. Recomendaciones 01/2020: metodología estructurada para la garantía del nivel de protección exigido

En respuesta a las incertidumbres operativas suscitadas por el fallo del TJUE, el Comité Europeo de Protección de Datos adoptó las Recomendaciones 01/2020¹⁴³ (las “Recomendaciones”). Estas recomendaciones no sólo responden a las exigencias impuestas por el Tribunal, sino que configuran una guía metodológica para la operación efectiva de los principios rectores del Reglamento.

Las Recomendaciones se articulan en una secuencia de seis pasos que han de ser observados por los responsables o encargados del tratamiento que pretendan transferir datos personales a un tercer país. Este enfoque estructurado se alinea con el principio de responsabilidad proactiva, núcleo operativo del RGPD, y refuerza la arquitectura multinivel delineada por el TJUE en *Schrems II*, al exigir una implicación constante, individualizada y documentada por parte de los sujetos exportadores¹⁴⁴.

Se exige a los exportadores conocer, en todo momento y con precisión, el destino geográfico de los datos que se transfieren, así como asegurarse de que su utilización se limita a un fin legítimo, concreto y estrictamente necesario, en consonancia con el Artículo 5 del RGPD¹⁴⁵.

Localizado el país destinatario, las entidades responsables deberán seleccionar el instrumento jurídico que legitima la transferencia. En ausencia de una decisión de

¹⁴¹ Fuentes Máiquez, A. (2021). *Comentario de la STJUE de 16 de julio de 2020, C-311/18 (Schrems II)*. *ICADE. Revista de la Facultad de Derecho*, (110), 1–10.

¹⁴² Miguel, P. A. de (2020). Implicaciones de la declaración de invalidez del Escudo de Privacidad. *La Ley Unión Europea*, 84

¹⁴³ Comité Europeo de Protección de Datos. (2021). *Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales en la UE*

¹⁴⁴ Miguel, P. A. de (2020). Implicaciones de la declaración de invalidez del Escudo de Privacidad. *La Ley Unión Europea*, 84.

¹⁴⁵ RGPD. Artículo 5(1)(c). *Los datos personales serán: c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

adecuación, deberán utilizarse los mecanismos contemplados en el Artículo 46, como las cláusulas contractuales tipo o as normas corporativas vinculantes. De forma excepcional, la transferencia podría acogerse a uno de los escenarios previstos en el Artículo 49 del RGPD, aunque el EDPB ha reiterado que tales excepciones deben ser interpretadas restrictivamente, en tanto que derogan el régimen general de garantías.

El tercer punto exige una evaluación rigurosa de la legislación y de las prácticas administrativas del Estado receptor, conocido también como el *análisis riesgo-país*. En concreto, deben analizarse factores como el acceso que las autoridades pueden tener a los datos personales, la eficacia de los mecanismos de supervisión, así como la disponibilidad de las vías de recurso accesibles para los interesados.

Cuando, como resultado de dicha evaluación, se constate que el instrumento utilizado no basta por sí solo para garantizar un nivel de protección equivalente al exigido por la Unión, será necesario adoptar garantías adicionales. El Anexo II de las Recomendaciones ofrece ejemplos orientativos de las herramientas que pueden ser utilizadas para compensar dicho déficit; si bien, el EDPB ha insistido que recae sobre el ámbito de competencias de la entidad exportadora, determinar, caso por caso, cuáles son las medidas más adecuadas a la naturaleza de los datos transferidos, al contexto específico de la operación y al régimen jurídico aplicable.

La aplicación de las herramientas de salvaguarda puede requerir la obtención previa de autorización por parte de las autoridades nacionales, conforme a lo previsto en el Artículo 46 del RGPD¹⁴⁶, u otro requisito formal que debe observarse al implementar las garantías de salvaguarda delineadas en el paso anterior.

Finalmente, como elemento diferenciador respecto de directrices anteriores, es obligación de las entidades exportadores revisar periódicamente las circunstancias legales y fácticas en las que se ha ejecutado la transferencia internacional. Tan es así que el proceso de evaluación no debe considerarse cerrado tras la ejecución de la transferencia, sino que debe mantenerse como una práctica continua de vigilancia y actualización, en línea con la lógica dinámica y evolutiva del principio de responsabilidad proactiva.

¹⁴⁶ RGPD. Artículo 46(3) Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. (4) La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo

Este enfoque estructurado se enmarca en el principio de responsabilidad proactiva, eje funcional del RGPD, consolidando la arquitectura multinivel delineada por el TJUE en la comentada Sentencia *Schrems II*.

3. Efecto Bruselas: desafíos jurídicos

a. Efectividad en la aplicación del Reglamento

Desde su concepción, el Reglamento General de Protección de Datos ha sido ideado como un instrumento normativo de alcance extraterritorial. Este enfoque expansivo ha contribuido a consolidar el denominado *Brussels Effect*, entendido este último como la capacidad de la Unión Europea de imponer sus estándares regulatorios más allá de las fronteras de los Estados Miembros¹⁴⁷.

Organismos gubernamentales y corporaciones multinacionales han adaptado su productos y servicios a las exigencias normativas europeas, particularmente a las derivadas de la aplicación del RGPD. Ejemplo paradigmático es el de Google, que, tras la invalidez del *Privacy Shield*, revisó y adaptó su política de privacidad con el objetivo de garantizar una mayor transparencia en el tratamiento de datos personales¹⁴⁸.

b. Insuficiencia de recursos

Si bien, el Artículo 57 del RGPD ha delimitado las funciones que las autoridades nacionales de protección de datos deben acometer, la falta de recursos financieros, humanos y técnicos ha podido obstaculizar la implementación efectiva del Reglamento¹⁴⁹.

El crecimiento exponencial del número de reclamaciones individuales, unido a la asunción de nuevas competencias, ha ampliado la carga de trabajo de los supervisores nacionales, sin que ello haya venido acompañado de un incremento proporcional de los recursos disponibles. Véase como ejemplo de esta dinámica legislativa el Artículo 5(6) del Reglamento de Inteligencia Artificial¹⁵⁰, que obliga a las autoridades de control nacionales a remitir informes anuales a la Comisión Europea sobre el uso de sistemas de identificación biométrica en espacios públicos. Esta ampliación competencial, sin un

¹⁴⁷ Bradford, A. (2020) *The Brussels Effect: How the European Union Rules the World*. OUP USA

¹⁴⁸ Diego Estévez (2019) *Google cambia su política de privacidad para adaptarse al RGPD*. Adenda

¹⁴⁹ Agencia Europea de los Derechos Fundamentales. (2024) *RGPD en práctica. Experiencias de las autoridades nacionales*

¹⁵⁰ Unión Europea. (2024). *Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión*.

fortalecimiento estructural paralelo, amenazaría con comprometer la eficacia del sistema de garantías previsto en el marco europeo.

c. Disparidad en la aplicación

La normativa europea se articula mediante un sistema multinivel que combina la competencia nacional de las autoridades de control con mecanismos de cooperación y coherencia coordinados por el EDPB. No obstante, en la práctica, la aplicación uniforme del RGPD se ve dificultada por las diferencias jurídicas y culturales entre los Estados Miembros. Existen divergencias respecto a la interpretación del articulado, así como en los niveles de sanción, procedimientos de investigación y prioridades regulatorias. Ejemplo de estas asimetrías se encuentra en el contraste entre la carga de trabajo de la Autoridad de Protección de Datos de Irlanda (DPC), sede de las grandes tecnológicas como Meta, Google o Microsoft, y otras autoridades nacionales como la Agencia Española de Protección de Datos, cuyas sanciones han tenido un menor impacto económico¹⁵¹.

Por apariencia, estas diferencias podrían contribuir a generar un clima de tensión, debilitando el establecimiento de un estándar europeo homogéneo. A ello se suma la dificultad estructural para coordinar actuaciones entre autoridades con capacidades dispares y prioridades distintas.

d. Estrategias corporativas para eludir la aplicación del RGPD

Otro de los desafíos a la efectividad del RGPD en clave global reside en las estrategias empresariales orientadas a eludir la aplicación extraterritorial.

En respuesta a la entrada en vigor del Reglamento, las grandes plataformas digitales modificaron su arquitectura organizativa con el objetivo de minimizar la aplicación directa del Reglamento a su actividad internacional. En el caso de Meta, más de 1.500 millones de cuentas de usuarios situados en África, Asia y Oceanía fueron trasladados desde la filial irlandesa a servidores en Estados Unidos, a fin de eludir la aplicación directa de la normativa europea¹⁵². Posteriormente, en 2021, repitió esta estrategia trasladando a los usuarios del Reino Unido a su filial en California tras el Brexit, anticipando una posible divergencia regulatoria con respecto al derecho de la Unión¹⁵³.

¹⁵¹ Santilari, M. (2022) Spanish Data Protection Agency Imposes 10 Million Euro Fine on Google: Highest Fine to Date. Clifford Chance

¹⁵² Ingram, D. (2019) Facebook to Put 1.5 Billion Users Out of Reach of New EU Privacy Law. Reuters

¹⁵³ TechCrunch. (2020). *Facebook to move UK users out of EU's privacy jurisdiction next year, post-Brexit*

Estas decisiones empresariales revelan la existencia de un patrón de conducta orientado a reducir la exposición jurídica a la normativa europea, y ponen de manifiesto las limitaciones materiales de un sistema que, pese a su diseño ambicioso, carece de herramientas efectivas para impedir la deslocalización estratégica de la responsabilidad legal.

Paralelamente, las empresas más poderosas han explotado la asimetría entre los recursos materiales de los que disponen y los de las autoridades nacionales de control, utilizando sofisticadas estrategias procesales para ralentizar o mitigar las sanciones impuestas. En Alemania, por ejemplo, los Tribunales redujeron de 9,55 millones a 900.000 euros la sanción impuesta a una empresa de telecomunicaciones por considerar que se había sobreestimado el volumen de negocio local¹⁵⁴.

4. Conclusiones

La aplicación extraterritorial del Reglamento General de Protección de Datos se erige como la máxima expresión del denominado *Brussels Effect*, mediante el cual la Unión Europea habría proyectado sus estándares regulatorios más allá del territorio jurisdiccional clásico. Al adoptar este enfoque funcional, el Reglamento habría roto con la lógica tradicional del derecho internacional privado para centrarse en la protección efectiva del derecho a la privacidad.

El legislador europeo ha decidido condicionar la aplicabilidad de la normativa europea a la ubicación de los interesados y a la intencionalidad que subyace a la actividad del responsable del tratamiento. Esta doble exigencia garantizaría una aplicación legítima y proporcionada del régimen europeo, evitando tanto una expansión normativa arbitraria como conflictos jurisdiccionales innecesarios.

La simplicidad que parece caracterizar esta extraterritorialidad resulta ser meramente aparente en la práctica. La sentencia *Schrems II* reconfigura sustancialmente el régimen de transferencias internacionales, al invalidar el *Privacy Shield* y exigir, de forma incondicionada, que el nivel de protección garantizado en el país de destino sea sustancialmente equivalente al europeo. Esta exigencia ha desbordado el plano estrictamente jurídico para introducir una dimensión geopolítica en el análisis, vinculada al escrutinio del ordenamiento jurídico y de las prácticas institucionales de los Estados terceros. La metodología propuesta por las Recomendaciones 01/2020 articula una respuesta estructurada, pero que exige capacidades técnicas y recursos que no todos los

¹⁵⁴ Lintvedt, M. N. (2022). *Putting a price on data protection infringement*. *International Data Privacy Law*, 12(1), 1–15

EXTRATERRITORIALIDAD DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

operadores están en condiciones de asumir, especialmente aquellos situados fuera del núcleo corporativo europeo.

La responsabilidad proactiva depende, en gran medida, de la posibilidad real de fiscalización por parte de las autoridades competentes, pero también de la existencia de mecanismos de cooperación transfronteriza y de los recursos de los que dispongan las autoridades nacionales de control. La experiencia demuestra que ni el mecanismo de coherencia ni el liderazgo del EDPB han sido suficientes para eliminar las diferencias entre Estados Miembros, especialmente en contexto donde confluyen intereses económicos políticos y tecnológicos.

Por último, las sanciones administrativas previstas, si bien significativas, han visto limitado su efecto disuasorio, en parte por su aplicación desigual y por la utilización estratégica de los procedimientos judiciales para dilatar o mitigar sus efectos por parte de las grandes corporaciones.

En suma, el RGPD ha definido un marco normativo ambicioso que aspira a consolidar una soberanía digital europea mediante la protección efectiva de los datos personales más allá de sus fronteras territoriales. Sin embargo, dicha ambición sólo podrá materializarse si se acompaña de una consolidación institucional que dote a las autoridades de control de los recursos necesarios, de la armonización interpretativa entre los Estados Miembros y de un compromiso político sostenido para asegurar la coherencia y legitimidad del modelo europeo.