DOCUMENTOS DE TRABAJO · GLOBAL POLITICS AND LAW

Nº 2/2026 · DERECHO ADMINISTRATIVO

DERECHO ADMINISTRATIVO

Transferencias internacionales de datos personales

De la relación bilateral del RGPD a la regulación triangular en la práctica

Julio V. González García

Catedrático de Derecho Administrativo · Universidad Complutense de Madrid

globalpoliticsandlaw.com/papeles-de-fondo/[slug-del-paper]/

Versión [1.0] · junio 2026

DATOS DE LA PUBLICACIÓN

Título	Transferencia Internacional de datos
Autor	Julio V. González García
Filiación	Catedrático de Derecho Administrativo · UCM
Serie	Documentos de trabajo · Working Papers de Global Politics and Law
Número	Nº 2/206
Versión	[1.0] — [Junio 2026]
DOI / URL	DOI: 10.5281/zenodo.20798756 transferencia-internacional-datos-personales
Área temática	Derecho administrativo · Digitalización
Palabras clave	datos personales, transferencia internacional de datos, decisiones de adaptación
Contacto	julio.gonzalez@gplaw.es

CITA RECOMENDADA

González García, J. V. (2026). Transferencia internacional de datos». *Documentos de Trabajo. Working Papers de Global Politics and Law*, nº 2/2026 globalpoliticsandlaw.com/papeles-de-fondo/[slug]/

LICENCIA

HISTORIAL DE VERSIONES

Versión	Fecha	Descripción
v1.0	Junio 2026	*Primera publicación.*

Resumen

Escriba aquí el resumen en español (150-250 palabras). El resumen debe recoger: el objeto del trabajo, la metodología o aproximación empleada, los argumentos principales y la conclusión central. Evite el uso de abreviaturas no explicadas.

Palabras clave: [kw1] · [kw2] · [kw3] · [kw4] · [kw5]

Abstract

Write here the English abstract (150-250 words). The abstract should cover: the object of the paper, the methodology or approach used, the main arguments, and the central conclusion.

Keywords: [kw1] · [kw2] · [kw3] · [kw4] · [kw5]

Sumario

I. Planteamiento: la transferencia internacional de datos en la economía digital globalizada

La economía del siglo XXI es la de los datos personales. Parafraseando lo que Karl Marx señala en *El Capital*[1], se podría decir que, en el mundo del siglo XXI, el ciudadano no es un agente libre y su vampiro es hoy una variante del capital —los captadores de datos— que no cesan en su empeño mientras quede una gota de sangre, un dato, que extraer. Es el capitalismo de la vigilancia al que se refiere Zuboff.[2]

Este capitalismo de la captura de datos se traduce en dos factores íntimamente vinculados. Por un lado, la obtención de los rendimientos derivados de esos datos, en un fenómeno en el que el ciudadano no obtiene nada. Por otro, es el capitalismo que anticipa y moldea comportamientos, lo que se traduce en una uniformidad social impulsada por las grandes tecnológicas. Y, desde un punto de vista metodológico, la obsesión por los datos —y, con ella, el impulso a su transferencia— se traduce en una suerte de solucionismo: la creencia, errónea, de que con un número indefinido de datos y algoritmos podremos resolver todos los problemas. Con ello se elimina la capacidad de análisis del ser humano.[3] Desde esta perspectiva, la problemática de la transferencia de datos es esencial en la economía digital, y lo será más con el desarrollo de la inteligencia artificial, que se nutre especialmente de datos personales y cuya respuesta, desde la óptica de la protección, no ha sido aún regulada, ni siquiera en la reciente reglamentación europea de la IA.

Todo ello se sostiene desde Europa, que es una *isla* en materia de protección de datos personales dentro de un mundo en el que la vigilancia y la captación están mucho más flexibilizadas y en el que no existen las garantías propias de nuestro ordenamiento. Posiblemente por ello, la Administración del presidente Trump ha situado como objetivo la derogación de la legislación europea —tanto el RGPD como el resto de la normativa de servicios de la sociedad de la información—, que ha obligado a los grandes operadores estadounidenses a modificar sus formas de comercialización.

Conviene recordar, no obstante, que las notas básicas del Reglamento General de Protección de Datos (RGPD, en adelante) están recogidas en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de modo que su erosión no es un mero ajuste regulatorio, sino la afectación de un derecho fundamental de configuración constitucional europea. En este sentido, además del derecho a la protección de los datos de carácter personal, el párrafo segundo reconoce el derecho de la ciudadanía a que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del

---

[1] Concretamente, Marx señala que "El capital es trabajo muerto que sólo se reanima, a la manera de un vampiro, al chupar trabajo vivo, y que vive tanto más cuanto más trabajo vivo chupa".

[2] Zuboff, S., *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, 2020.

[3] Morozov, E., "The Real Privacy Problem", *MIT Technology Review*, 2013. La crítica al "solucionismo tecnológico" se desarrolla con amplitud en *To Save Everything, Click Here*, PublicAffairs, 2013.

consentimiento dela persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación".

Este capitalismo de los datos se desarrolla, además, en un mundo globalizado, lo que eleva el grado de complejidad de la protección real. Una globalización que ha hecho del intercambio de bienes, servicios —y datos— su razón de ser. La diferencia decisiva es que, a diferencia de la mercancía, el dato es un bien no rival, ubicuo y reproducible sin coste apreciable: puede estar en muchos lugares a la vez, copiarse de forma instantánea y permanecer accesible mucho después de que su titular crea haberlo extinguido. Esa naturaleza singular es la que, como veremos, hace insuficiente trasladar al dato el modelo jurídico pensado para el comercio de cosas.

En la actualidad transferimos datos personales fuera de nuestras fronteras a diario, sin que la ciudadanía se dé cuenta de que está ocurriendo. Un correo electrónico que cualquiera de nosotros envíe a sus estudiantes pasa por servidores de Google, que pueden ubicarse en cualquier país del mundo y que está sometido a una norma estadounidense, aunque haya pocos metros de distancia entre profesor y estudiante. La localización de los usuarios de teléfonos con sistema operativo Android se remite automáticamente a los servidores de la misma empresa y sirve para saber si el bar al que vamos está concurrido -y para construir sesgos de comportamiento-. Cuando se recurre a un centro de atención telefónica deslocalizado y este accede a nuestros datos para resolver un problema, se está realizando una transferencia internacional. El espacio que hemos adquirido a cualquier operador de nube estará previsiblemente gestionado por una entidad domiciliada en los Estados Unidos, Israel, China o la India, y los datos, por nimios que sean, circulan a diario entre servidores que hacen pantalla para mejorar la latencia. Otro tanto sucede cuando operamos en la aplicación del banco que llevamos en el dispositivo, que se apoya en servidores de algún operador estadounidense; e incluso cuando la Administración remite una notificación electrónica a través de servidores a los que resulta aplicable la CLOUD Act, sobre la que volveremos.

Incluso al referirnos a la ciberdelincuencia aludimos a un problema normalmente internacional a través del cual se produce una transferencia de datos, con consecuencias desde la perspectiva del Derecho interno a tenor del Reglamento DORA.[4]

Más allá de la realidad práctica, el problema que genera la transferencia internacional es doble. Por un lado, constituye probablemente el factor de mayor riesgo para el derecho fundamental, ese derecho cuyo "contenido … consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles

[4]Reglamento (UE) 2022/2554, sobre la resiliencia operativa digital del sector financiero (DORA).

puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".[5]

Por otro lado, uno de los factores que impulsan esa desprotección deriva de que no existe un estándar común en todo el mundo, lo que genera disfunciones que la normativa europea pretende corregir, aunque, como veremos, con dificultad, pues el estándar global es mucho más laxo que el europeo. A ello se suma la insuficiente percepción por parte de la opinión pública.

Desde la perspectiva de los proveedores de servicios vinculados a los datos, la percepción de los estándares legales sirve sobre todo para hacer de la competencia entre ordenamientos un elemento esencial de su devenir empresarial, buscando aquel que resulte más laxo. Y este es un factor que el ciudadano, por regla general, desconoce o sobre el que tiene impresiones equivocadas: por tomar un dato simple, no importa que el servidor de Google esté domiciliado en Zaragoza, sino que, desde una perspectiva regulatoria, ese servidor pertenece a una empresa sometida a la legislación de los Estados Unidos. Nos encontramos, así, ante una asimetría de conocimiento que repercute negativamente en los derechos de los titulares de los datos.

Los titulares de los datos -la ciudadanía, pero también las empresas y las Administraciones públicas- suelen vivir en un mundo de placebo hasta el momento en que reciben alguna comunicación indeseable y se preguntan quién y cómo ha tenido conocimiento de sus datos. No se es consciente, por ejemplo, de cuáles son las cláusulas de remisión de archivos a través de WhatsApp o de Gmail, ni de cómo quedan desguarnecidos al publicarlos en redes sociales. Y, tomando en cuenta el elemento netamente tecnológico, cabe plantearse si los órganos jurisdiccionales están en condiciones técnicas de resolver estos problemas cotidianos.

Hay, en consecuencia, una gran distancia entre el Derecho formal -el del RGPD y las normas complementarias- y el Derecho practicado, por recoger la afortunada expresión de Alejandro Nieto. Vivimos, además, en un contexto en el que la legislación de máxima protección no va de la mano de la mayor innovación en las industrias y tecnologías de gestión de los datos: no hay más que recordar que el mercado de la nube está copado por tres empresas, las tres estadounidenses. Esa disociación entre quien fija el estándar y quien controla la infraestructura es, en el fondo, el hilo conductor de cuanto sigue.

II. El ámbito de aplicación del Reglamento y el problema de la norma aplicable

La cuestión más relevante en materia de protección de datos es la de la norma aplicable. Aunque desde Europa pensemos que estamos suficientemente protegidos con el RGPD, esta norma no cubre todas las situaciones, ni siquiera aquellas en las que

[5]Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, fundamento jurídico 6.º; ponente, Excmo. Sr. D. Julio Diego González Campos.

parece hacerlo, como cuando los datos están almacenados en un servidor situado en Zaragoza, por tomar el lugar donde se está construyendo un gran nodo.

Conviene, por ello, comenzar por el ámbito de aplicación del propio Reglamento. El artículo 3 lo determina con arreglo a dos criterios. El primer criterio es el del establecimiento del responsable o del encargado del tratamiento: el RGPD se aplica al tratamiento efectuado en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, con independencia de que el tratamiento tenga lugar dentro de ella.

El segundo critero es el del ofrecimiento de bienes y servicios a interesados que se encuentren en la Unión o del seguimiento de su comportamiento, aunque el responsable esté establecido fuera; en tal caso, el responsable extracomunitario queda directamente sujeto al Reglamento y obligado, incluso, a designar un representante en la Unión.[6]

De esta doble regla conviene retener una consecuencia que suele generar confusión. Que una empresa de fuera de la Unión quede sometida al Reglamento -por ofrecer servicios a personas que están en Europa o por seguir su comportamiento- no significa que pase a estar "dentro" de Europa a efectos de la circulación de datos. Son dos cuestiones diferentes: una cosa es *si* el Reglamento se aplica a esa empresa, y otra distinta es *qué requisitos* deben cumplirse para enviarle datos desde la Unión. Pensemos en una empresa estadounidense que ofrece una aplicación a usuarios españoles: el Reglamento es derecho aplicable, sí, pero cuando una empresa europea le remite datos personales sigue habiendo una transferencia internacional que exige sus propias garantías.

Dicho de otro modo, el artículo 3 decide si el Reglamento entra en juego; y solo después, el capítulo V impone las cautelas para enviar los datos al exterior, cautelas que pueden ser exigibles incluso cuando quien los recibe está, él mismo, sujeto al Reglamento. Por eso el Comité Europeo de Protección de Datos insiste en no mezclar ambos planos.

El RGPD no ha sido especialmente minucioso al configurar las normas de conflicto que delimitan el alcance de su contenido. Se trata de una cuestión relevante en la medida en que ningún Estado está dispuesto a dejar de aplicar su propia normativa, lo que genera solapamientos y, en ocasiones, conflictos abiertos de leyes -señaladamente con las legislaciones de seguridad nacional de terceros países, a las que más adelante volveremos-. El resultado es un espacio de fricción en el que un mismo dato puede quedar simultáneamente reclamado por dos ordenamientos con exigencias incompatibles.

A este marco hay que añadir los Tratados comerciales de nueva generación, que incluyen cláusulas de protección de datos concebidas para que no constituyan un factor de limitación del comercio. Tampoco en ellos está concretado el régimen de protección aplicable; o, para ser más exactos, no se ha producido una concreción de la normativa

[6] El artículo 27 del RGPD obliga al responsable o encargado no establecido en la Unión, pero sujeto al Reglamento por la vía del artículo 3, apartado 2, a designar por escrito un representante en la Unión.

aplicable, que en ocasiones se remite a acuerdos ulteriores, como sucede en el Tratado con México.[7] Por último, no puede olvidarse el régimen que pudiera derivarse de los acuerdos alcanzados en el marco de la Organización Mundial del Comercio, que pueden añadir aspectos concretos a la regulación.

Como puede verse, un problema de derechos fundamentales como este plantea, ya de entrada, serias dificultades de conocimiento para la ciudadanía; dificultades que alcanzan incluso a la identificación de los órganos ante los que cabe recabar protección.

III. El concepto de transferencia internacional de datos

Partiendo de lo anterior, y dada la relevancia de la transferencia internacional -especialmente en el comercio electrónico-, conviene iniciar el análisis de la normativa europea por el propio concepto, algo que, paradójicamente, no figura definido en el RGPD.

La definición hoy de referencia procede de las Directrices 05/2021 del Comité Europeo de Protección de Datos, asumidas después por la Comisión en sus informes de aplicación. Conforme a esas directrices, para que exista una transferencia internacional en sentido propio tienen que darse, a la vez, tres condiciones:

i) La primera es que quien maneja los datos -ya sea quien decide sobre ellos (el responsable) o quien los trata por cuenta de aquel (el encargado)- esté sujeto al Reglamento por ese tratamiento concreto; dicho de otro modo, el punto de partida es siempre un tratamiento que el Derecho europeo ya protege.

ii) La segunda es que ese sujeto, al que llamamos *exportador*, comunique los datos o simplemente los ponga a disposición de otro responsable o encargado distinto, el *importador*: basta, por tanto, con permitir el acceso, sin necesidad de que los datos «viajen» físicamente de un sitio a otro.

iii) Y la tercera es que ese importador se encuentre en un país ajeno a la Unión -o sea una organización internacional, de acuerdo con lo que señala el artículo 44 del RGPD-, sin que importe que él mismo esté o no sujeto al Reglamento en virtud del artículo 3. Conviene insistir en este último matiz, porque es el que más confusión genera: lo decisivo no es si el destinatario tiene obligaciones bajo el Reglamento, sino que esté situado fuera del territorio de la Unión.

[7] Sobre la conexión entre protección de datos y comercio internacional, véase Otero García-Castrillón, C., "Protección de datos en la economía digital. Una aproximación desde la regulación del comercio internacional", en Rodríguez Pineau, E. y Torralba Mendiola, E. (dirs.), *La protección de las transferencias transnacionales de datos*, Thomson Reuters Aranzadi, 2021, páginas 33 y siguientes.

Solo cuando concurren las tres condiciones (un dato protegido por el Derecho europeo, que pasa de un sujeto a otro, y cuyo receptor está fuera de la Unión) estamos ante una transferencia internacional y se activan las cautelas del capítulo V..[8]

Esta delimitación tiene tres consecuencias prácticas que conviene subrayar:

i) La primera es que la internacionalidad no se define aquí por comparación con el territorio de los Estados, sino con el de la Unión: las transferencias intracomunitarias están cubiertas por el propio Reglamento y son, desde este punto de vista, "situaciones puramente internas".

ii) Conviene precisar, además, una distinción que suele pasar inadvertida: no todo dato que pasa físicamente por el extranjero es una transferencia internacional. Las comunicaciones electrónicas se fragmentan y se encaminan por la ruta disponible en cada momento, que puede atravesar servidores de terceros países aun cuando el origen y el destino estén en la Unión. Ese mero tránsito (en el que los servidores intermedios solo reencaminan la información, sin que nadie reciba ni consulte su contenido) no constituye una transferencia, porque falta el importador que la define. Otra cosa es que sea inocuo: la información en tránsito puede ser interceptada, de manera que el riesgo no se desvanece, sino que se reconduce hacia el deber de seguridad del tratamiento, que el Reglamento impone por una vía propia, señaladamente a través del cifrado de las comunicaciones del artículo 32[9].

iii) La tercera idea es complementaria de la anterior y, en cierto modo, su reverso. Si el dato que solo transita por el extranjero no es una transferencia, sí lo es, en cambio, el simple acceso a un dato desde fuera de la Unión, aunque ese dato no se mueva de donde está. Lo decisivo no es dónde se encuentra físicamente la información, sino quién puede verla. Pensemos en una empresa europea cuya base de datos está alojada en un servidor situado en España, pero que contrata el soporte técnico a un proveedor con técnicos en la India: cada vez que uno de esos técnicos se conecta para resolver una incidencia y visualiza los datos de los clientes, hay una puesta a disposición y, por tanto, una transferencia internacional (pese a que el archivo no haya salido nunca de España). Basta con que alguien situado en un tercer país pueda consultarlos. Y la distinción no es un tecnicismo: de ella depende qué garantías hay que adoptar. Si calificamos la operación como transferencia, el responsable tendrá que apoyarla en uno de los instrumentos del capítulo V (una decisión de adecuación, las cláusulas contractuales tipo u otra de las garantías que veremos con posterioridad); si la pasara por alto creyendo que

[8] Comité Europeo de Protección de Datos, Directrices 05/2021 sobre la interacción entre la aplicación del artículo 3 y las disposiciones relativas a las transferencias internacionales del capítulo V del RGPD, donde se fija la noción de transferencia a partir de tres criterios acumulativos.

[9] El deber de seguridad arranca del principio de integridad y confidencialidad del artículo 5, apartado 1, letra f), del RGPD, y se concreta en las medidas técnicas y organizativas del artículo 32, apropiadas al riesgo. A ello se añade, si la interceptación llega a materializarse en una brecha, el régimen de notificación de violaciones de seguridad de los artículos 33 y 34.

«el dato no viaja», quedaría sin la cobertura que el Reglamento exige y expuesto a sanción.

IV. Un océano normativo: el régimen básico y sus complementos

La indefensión del titular de los datos no es consecuencia de la falta de normativa. Más bien al contrario: la normativa es abundante, ya sea a la hora de reconocer derechos, de prever protocolos o de remediar ataques.

La transferencia internacional surge en buena parte de los negocios jurídicos; sin duda en todas las operaciones de comercio electrónico internacional, que son las más frecuentes. Hay datos personales que se transfieren entre operadores económicos cuando pedimos una camiseta a un operador chino que la trae, en un azaroso viaje en barco, hasta el puerto de Algeciras: allí la recoge un operador de paquetería, que la cede a un repartidor autónomo encargado de la última milla, que la lleva a nuestro domicilio (acaso para dejarla de mala manera en la puerta de algún vecino que accede así a nuestros datos). A toda esa actividad principal, con sus complementos, se aplican el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Y lo mismo sucede cuando adquirimos criptoactivos en una máquina parecida a las de venta automática de refrescos, situada en un centro comercial.

Al mismo tiempo, cuando hacemos una llamada a través de WhatsApp —o incluso una llamada telefónica ordinaria— también generamos datos. En tal caso encontramos la tenue protección que dispensa la legislación de telecomunicaciones, que cuenta con un capítulo dedicado a los derechos de los usuarios finales. A todos nos han vulnerado ese derecho a no ser molestados, en una llamada para vendernos un nuevo paquete de telecomunicaciones que, por el castellano de quien la realiza, intuimos producida en otro lugar del mundo. Y el Reglamento DORA, en fin, contiene también una regulación que afecta a nuestros datos personales, complementaria de la anterior, en los casos de ataques dirigidos a captarlos.

En este océano normativo, por tanto, hay que concretar el régimen básico, que es el que proporciona la legislación general de protección de datos.

V. Del esquema bilateral formal a la relación triangular

La tesis central de este trabajo puede enunciarse de este modo: cuando nos encontramos ante una transferencia internacional, ¿cabe afirmar realmente que la relación afecta solo a dos países, el del domicilio del emisor y el del receptor? O, dicho de otro modo, ¿es válido un esquema de transferencia sencilla, propio del intercambio de bienes, o hay que dar un paso más a la vista de las peculiaridades del dato?

La solución no es única, porque tampoco lo son los medios a través de los cuales se realiza la transferencia. El esquema previsto en los artículos 44 y siguientes del RGPD puede bastar en aquellos casos en los que la transferencia se realiza mediante un

soporte físico (un disco duro con los datos), siempre que estos se almacenen en servidores domiciliados en el país de destino y no queden sometidos a una legislación distinta. En esos supuestos, el dato pasa de un ordenador a otro y el marco del Reglamento parece adecuado. Pero no es lo usual.

Las cosas cambian en cuanto entran en juego las redes de telecomunicaciones y el almacenamiento en la nube. Entonces ya no basta con mirar a quien envía los datos y a quien los recibe: hay que analizar también al titular de la infraestructura por la que circulan y se guardan, y al país en que esa empresa está domiciliada, porque con ella viaja el régimen jurídico al que está sometida. Dicho de otro modo, en una transferencia corriente hay que analizar tres posiciones, no dos: el emisor, el receptor y el vehículo. Y, a veces, aparece una cuarta, cuando el operador de la nube subcontrata a su vez parte del servicio en otro proveedor. La relación, que sobre el papel parecía cosa de dos, se vuelve así triangular y, a menudo, cuadrangular.

Un ejemplo lo aclara. Una clínica española contrata a una empresa española para gestionar las historias clínicas de sus pacientes; aparentemente, los datos no salen de España. Pero esa empresa aloja la información en los servidores de un gran proveedor de nube estadounidense, que a su vez replica los datos en centros de distintos países para garantizar el servicio. Aunque el emisor y el receptor formal sean ambos españoles, el dato ha quedado bajo el alcance del operador de la nube y, con él, de la legislación de su país de origen. Esa es la clave: la posición jurídica del vehículo no es neutral. Arrastra consigo el ordenamiento del Estado en que está domiciliado, de manera que la ley aplicable al receptor formal puede verse desplazada, en la práctica, por la ley aplicable a quien controla la infraestructura. El dato puede estar físicamente en Madrid y, sin embargo, ser alcanzable por una autoridad extranjera en virtud de la ley que rige a su custodio.

Esta realidad práctica, que desborda el marco jurídico-formal del RGPD, es tanto más relevante cuanto que las legislaciones de los países prestadores de servicios de nube suelen ser expansivas en su aplicabilidad, vinculada, aparentemente, a problemas de seguridad nacional. Es este el escenario en el que ha de comprobarse el cumplimiento de la regla de la protección equivalente. Piénsese en los supuestos en que siempre habrá transferencia: almacenamiento de datos en servidores ubicados en el exterior o bajo el dominio de una empresa extranjera; contratación de servicios de procesamiento con proveedores externos; o acceso a bases de datos corporativas desde sedes internacionales.

Por ello, aunque el mecanismo aparentemente más razonable de los previstos en el RGPD sea el de las decisiones de adecuación, en la práctica resultará con frecuencia insuficiente, y deberá verse reforzado por los instrumentos contractuales (singularmente, las cláusulas contractuales tipo aprobadas por la Comisión el 4 de junio de 2021), complementados a su vez con las medidas suplementarias que exige la jurisprudencia tras *Schrems II*.

Como se verá, esos tres niveles (la decisión de adecuación, las garantías adecuadas y las medidas suplementarias) funcionan como una escalera que el responsable va subiendo solo cuando el peldaño anterior no basta: si no hay país declarado seguro, se acude a las garantías del contrato; y si estas no neutralizan el riesgo que plantea la ley

del país de destino, se añaden medidas adicionales. Ese orden no es casual, sino que constituye la traducción jurídica de la estructura triangular que aquí se defiende, porque cada peldaño responde a uno de los vértices del problema: se ha de analizar el receptor pero también el vehículo de transmisión y el ordenamiento que lo gobierna.

VI. La regla general: el principio de protección equivalente

El artículo 44 del RGPD y la jurisprudencia comunitaria han establecido que la transferencia internacional fuera del marco comunitario exige el cumplimiento del principio de equivalencia de la protección. Es una regla sencilla de formular, pero que obliga a articular una investigación previa sobre el marco jurídico del Estado de destino, así como a examinar los medios a través de los cuales puede llegarse a esa conclusión. En esa delimitación, las dos sentencias del Tribunal de Justicia sobre los sucesivos acuerdos con los Estados Unidos resultan capitales.

Conviene precisar la terminología, a menudo confundida. La primera de ellas, *Schrems I*, de 6 de octubre de 2015, declaró inválido el régimen de "puerto seguro" (*Safe Harbor*).[10] La segunda, *Schrems II*, de 16 de julio de 2020, anuló el *Privacy Shield* y, al tiempo, confirmó con matices la validez de las cláusulas contractuales tipo, imponiendo sobre el exportador la carga de evaluar el nivel de protección del país de destino[11].

Como precisó el Tribunal de Justicia en *Schrems II*, "la evaluación del nivel de protección … debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos …, los elementos pertinentes del sistema jurídico de dicho país". La evaluación tiene, por tanto, dos planos: el contractual, entre las partes, y el del propio ordenamiento del tercer país, singularmente en cuanto al acceso de sus autoridades. Más allá del análisis de cada relación contractual, el dato relevante es el del país destinatario —lo que confirma que el vehículo a través del cual circula el dato es, también, jurídicamente relevante.

El estándar exigible se asienta sobre los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales: respeto de la vida privada, protección de datos y tutela judicial efectiva. De ellos extrae el Tribunal dos exigencias materiales. La primera es que cualquier injerencia de los poderes públicos del tercer país respete el contenido esencial del derecho y se ajuste a los principios de necesidad y proporcionalidad, de modo que no caben programas de acceso masivo e indiscriminado a los datos. La segunda es que el interesado disponga de vías de recurso efectivas ante un órgano

[10]Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, asunto C-362/14, *Schrems* ("Schrems I"), que declaró inválida la Decisión 2000/520/CE sobre el acuerdo de "puerto seguro" (*Safe Harbor*).

[11]Sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems* ("Schrems II"), que declaró inválida la Decisión 2016/1250 sobre el *Privacy Shield* y confirmó, con matices, la validez de las cláusulas contractuales tipo. Véanse en particular sus apartados 132 y 133.

independiente. Sobre esta segunda exigencia —y sobre cuándo un órgano administrativo puede satisfacerla— gira buena parte del contencioso reciente.

Importa subrayar, por último, un matiz que la jurisprudencia ha consolidado: la equivalencia exigida no es identidad. No se requiere que el tercer país garantice un nivel *idéntico* al europeo, sino *sustancialmente equivalente*; esto es, garantías que, en su conjunto, resulten comparables en eficacia, aunque sus mecanismos difieran. Es un estándar de resultado, no de calco en el diseño institucional. La frontera entre la flexibilidad razonable y la complacencia es, sin embargo, tenue, y sobre ella se proyecta la crítica que más adelante se formula a propósito de los Estados Unidos y cuál es la actitud de las autoridades comunitarias. Conviene retener, en fin, que la evaluación no es un acto único, sino un juicio dinámico: lo que hoy es equivalente puede dejar de serlo si cambia la legislación del tercer país, y de ahí la obligación de seguimiento continuo que pesa sobre el exportador y sobre la Comisión.

Este carácter dinámico de la evaluación es muy relevante y, sin embargo, no suele tenerse debidamente presente en la práctica de la Unión. Basta con observar cómo se mantiene la validez de ciertas decisiones de adecuación aun después de que el ordenamiento jurídico y la práctica del país de destino hayan cambiado de manera sustancial. El caso de Israel ilustra bien hasta qué punto ese carácter dinámico se proclama más que se ejerce. No es que su decisión de adecuación (de 2011, adoptada bajo la antigua Directiva 95/46) haya quedado sin revisar: la Comisión la reexaminó, junto con las otras diez decisiones preexistentes, en su primer informe de revisión de enero de 2024, y la reconfirmó.

El problema está en la intensidad de ese examen. La revisión se apoyó casi por entero en el plano comercial y privado, hasta el punto de que la propia Comisión recomendó elevar a rango legal protecciones que hasta entonces descansaban en instrumentos sub-legales y en la práctica de los tribunales. En cambio, apenas entró a valorar lo decisivo desde la óptica de las sentencias Schrems: los amplios poderes de interceptación y vigilancia de las agencias de seguridad e inteligencia, ejercidos sin un control judicial independiente o suficiente; el deterioro del Estado de Derecho que las propias instituciones europeas habían advertido (y que llevó a la Comisión a suspender temporalmente el proceso en 2023; la calificación de las transferencias a los territorios ocupados; o el impacto de la legislación restrictiva sobre asociaciones y organizaciones no gubernamentales[12]. El resultado es una reconfirmación que conserva la apariencia de un juicio renovado, pero que esquiva precisamente aquellos elementos del ordenamiento y de la práctica que, de haberse examinado con el rigor que el estándar exige, comprometerían la conclusión de equivalencia.

[12] Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión del funcionamiento de las decisiones de adecuación adoptadas con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE, COM(2024) 7 final, de 15 de enero de 2024. Las objeciones a la reconfirmación relativa a Israel fueron sistematizadas por una coalición de organizaciones de la sociedad civil (European Digital Rights (EDRi), Access Now, Statewatch y otras) en su carta abierta a la Comisión de 22 de abril de 2024, que reclamaba aclaración sobre el Estado de Derecho, el papel de las entidades de seguridad nacional, las transferencias ulteriores más allá de las fronteras internacionalmente reconocidas, el procedimiento de revisión y el contexto del conflicto de Gaza a la luz del Derecho internacional.

VII. Las decisiones de adecuación

El mecanismo más sencillo para permitir la transferencia es el de las decisiones de adecuación. Conforme al artículo 45 del RGPD, supone que "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", en cuyo caso la transferencia "no requerirá ninguna autorización específica". Es, por así decirlo, un presupuesto habilitante general: una vez adoptada la decisión, los datos fluyen hacia el país de destino en las mismas condiciones que dentro de la Unión, sin trámite adicional alguno.

En la actualidad existe en torno a una quincena de países y territorios con decisión de adecuación en vigor (entre otros, Andorra, Argentina, Canadá (entidades comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, Reino Unido, República de Corea, Suiza, Uruguay y los Estados Unidos), a los que se ha sumado, como decisión más reciente, Brasil, mediante la Decisión de Ejecución (UE) 2026/179, de 26 de enero de 2026, primera de carácter mutuo.[13] Junto a las decisiones que abarcan un país en su conjunto, el artículo 45 admite también adecuaciones parciales o sectoriales, referidas a un territorio o a determinados sectores —lo que explica que, en el caso de los Estados Unidos, la adecuación se circunscriba a las entidades adheridas al marco de privacidad, y no al ordenamiento en bloque.

El procedimiento para adoptarlas no es trivial. La Comisión examina con detalle la legislación y la práctica del tercer país (incluidas las normas sobre acceso de las autoridades públicas), recaba el dictamen del Comité Europeo de Protección de Datos y somete el proyecto a la aprobación del comité de representantes de los Estados miembros, antes de adoptar la decisión definitiva. Se trata, pues, de un acto de ejecución dotado de garantías procedimentales reforzadas, precisamente por el alcance general de sus efectos.

Esas decisiones no son, además, definitivas. El artículo 45 impone su revisión periódica, al menos cada cuatro años, y habilita a la Comisión a suspenderlas, modificarlas o derogarlas si el tercer país deja de garantizar un nivel adecuado.[14] Esta revocabilidad no es un detalle técnico: las sentencias Schrems han mostrado que una decisión de adecuación puede caer de un día para otro, dejando a miles de operadores que confiaban en ella obligados a reconducir sus transferencias, de manera súbita, a los instrumentos del artículo 46. La estabilidad jurídica que la adecuación promete convive, así, con una fragilidad estructural que conviene no perder de vista.

De acuerdo con el artículo 45, son tres los elementos primordiales que la Comisión analiza antes de adoptar una decisión de esta naturaleza.

---

[13] Decisión de Ejecución (UE) 2026/179 de la Comisión, de 26 de enero de 2026, relativa a la adecuación del nivel de protección conferido por Brasil; primera decisión de adecuación de carácter mutuo.

[14] El artículo 45, apartado 3, prevé la revisión periódica de las decisiones de adecuación, al menos cada cuatro años; sus apartados 4 y 5 habilitan a la Comisión a suspenderlas, modificarlas o derogarlas. El artículo 97 impone, además, una evaluación periódica de la aplicación del Reglamento.

i) El primer criterio es el más amplio y el de mayor peso, porque atiende al entorno jurídico e institucional del país de destino en su conjunto. No se trata solo de comprobar que exista una ley de protección de datos que contenga un marco similar de protección, sino que ha de procederse, además, al análisis del entorno jurídico en el que opera la norma, en particular, la vigencia real del Estado de Derecho y el respeto de los derechos fundamentales; la legislación en materia de seguridad pública, defensa, seguridad nacional y proceso penal, y, muy especialmente, las condiciones en que las autoridades del Estado pueden acceder a los datos personales.

Lo decisivo no es el texto regulado sino el Derecho practicado, para lo que hay que hacer un análisis de la jurisprudencia y en la práctica administrativa. Dentro de este criterio, el elemento verdaderamente esencial es doble: que los interesados dispongan de derechos efectivos y exigibles (y no meramente proclamados) y que existan vías reales de reparación, tanto administrativas como judiciales, a las que puedan acudir quienes vean comprometidos sus datos. Es precisamente aquí donde se concentró el examen de las sentencias Schrems: de poco sirve un buen catálogo de derechos si los servicios de inteligencia pueden acceder a los datos sin límites proporcionados y sin que el afectado disponga de un recurso ante un órgano independiente.

ii) El segundo criterio se centra en la pieza institucional que da vida a todo el sistema: la existencia de una o varias autoridades de control independientes y, sobre todo, su funcionamiento efectivo. No basta con que el país de destino haya creado un organismo de supervisión; ese organismo debe ser realmente independiente del poder político y de los sujetos a los que vigila, estar dotado de poderes efectivos para investigar y sancionar, asistir y asesorar a los ciudadanos en el ejercicio de sus derechos y cooperar con las autoridades de control de la Unión. La independencia y la eficacia van aquí de la mano: una autoridad nominal, sin medios ni capacidad sancionadora real, no satisface la exigencia, porque deja a los derechos sin un garante que los haga valer. Esta cooperación con las autoridades europeas es, además, la que permite que el sistema funcione de forma coordinada y no como compartimentos estancos.

iii) El tercer criterio recoge, en sentido estricto, los compromisos internacionales asumidos por el país de destino: su adhesión a instrumentos y a sistemas multilaterales o regionales de protección de datos; dentro de los cuales el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su versión actualizada ocupan un puesto prevalente. Esa pertenencia ofrece una garantía añadida, porque acredita que el país comparte un estándar reconocido y se somete a mecanismos de control externos a su propio ordenamiento. A este criterio conviene asociar (aunque el Reglamento lo ubique técnicamente dentro del primero) la valoración de cómo regula ese Estado las transferencias ulteriores: de nada serviría exigir un alto nivel de protección al primer destinatario si este pudiera, acto seguido, reenviar los datos a un cuarto país sin garantías, haciendo que la cobertura se evapore en el siguiente eslabón. Uno y otro aspecto cierran el círculo, asegurando que la protección no se diluya más allá del país que ha sido objeto de la decisión.

Conviene reseñar, junto a este mecanismo, la existencia de otros instrumentos derivados de los Tratados comerciales de nueva generación. El Tratado CETA, por ejemplo, dispone de cláusulas específicas de protección de datos en relación con los servicios financieros, las telecomunicaciones y el comercio electrónico; y existen

previsiones que vinculan comercio electrónico y protección de datos en los acuerdos con Japón, Singapur o México, que fijan un marco propio sobre la premisa de que las cláusulas de protección de datos no perjudiquen el comercio. La coexistencia de estos dos planos —el del capítulo V y el del Derecho del comercio internacional— añade un grado adicional de complejidad, pues no siempre es evidente cuál prevalece cuando sus exigencias divergen.

VIII. Un cauce paralelo: las "decisiones de adecuación indirectas" y los Tratados comerciales de nueva generación

Junto al cauce típico del artículo 45 existe un segundo plano, menos visible, pero de creciente importancia a la hora de señalar la adecuación de terceros países al marco comunitario: el de los Tratados comerciales de nueva generación, que incorporan capítulos sobre comercio electrónico y flujos transfronterizos de datos.

La relación entre ese plano y el capítulo V del Reglamento no es sencilla, y conviene tratarla por separado, porque de su correcta comprensión depende evitar un equívoco extendido: el de creer que un acuerdo comercial puede, por sí mismo, habilitar la transferencia de datos personales como si fuera una decisión de adecuación. No es así -o no exactamente-, y de ahí que quepa hablar, con cautela, de «decisiones de adecuación indirectas».

Durante años, la política comercial y la política de protección de datos discurrieron en la Unión en tensión: la primera empujaba hacia la liberalización de los flujos; la segunda, hacia su control. El compromiso interno se alcanzó en enero de 2018, cuando la Comisión adoptó las llamadas cláusulas horizontales sobre flujos transfronterizos de datos y protección de datos personales en los acuerdos comerciales y de inversión[15].

Su arquitectura es doble. De un lado, comprometen a las partes a permitir la circulación transfronteriza de datos y a no imponer determinadas exigencias de localización. De otro lado, lo que constituye el factor decisivo es que blindan el régimen europeo mediante una excepción amplia y autoaplicativa: la protección de datos personales se reconoce como derecho fundamental, las normas sobre transferencias se consideran a priori medidas apropiadas y quedan sustraídas a la impugnación por la vía del acuerdo comercial.

De esta construcción se sigue una consecuencia de gran importancia. El Tratado comercial no crea un título autónomo de transferencia ni desplaza al capítulo V, sino que lo presupone y lo protege. Dicho de otro modo, la Unión mantiene la protección de datos y el comercio como dos vías separadas que pueden complementarse, pero no confundirse, como ha insistido el Supervisor Europeo de Protección de Datos al recordar que un derecho fundamental no puede ser objeto de negociación comercial[16].

---

[15] Cláusulas horizontales sobre los flujos transfronterizos de datos y la protección de los datos personales y la privacidad en los acuerdos comerciales y de inversión de la Unión, refrendadas por la Comisión el 31 de enero de 2018 y publicadas en julio de 2018.

[16] Dictamen del Supervisor Europeo de Protección de Datos sobre las recomendaciones de apertura de negociaciones de comercio digital con la República de Corea y con Singapur (2023), que recuerda que

Un acuerdo de comercio digital con un tercer país no exime, por tanto, de fundar la transferencia en una decisión de adecuación o en alguna de las garantías del artículo 46.

Y, sin embargo, la separación es más nítida en la teoría que en la práctica. La realidad muestra que la adecuación y el comercio caminan entrelazados, hasta el punto de que la decisión de adecuación opera con frecuencia como el verdadero «capítulo de datos» de una relación comercial. El caso de Japón lo ejemplifica perfectamente: la adecuación mutua de 2019 acompañó la entrada en vigor del Acuerdo de Asociación Económica, y solo después se incorporaron al propio Acuerdo, mediante una negociación específica, las cláusulas sobre flujos de datos, configurando el mayor espacio mundial de transferencias seguras[17]. Algo análogo sucedió con el Reino Unido, cuyo Acuerdo de Comercio y Cooperación previó un mecanismo puente para los flujos a la espera de la decisión de adecuación que llegó en 2021; con Corea del Sur, cuya adecuación de 2021 enmarca la apertura de negociaciones de comercio digital; y, más recientemente, con Brasil, cuya adecuación mutua de enero de 2026 se inscribe en el horizonte de la relación con Mercosur. En otros casos, como el de México, el acuerdo se limita a una cláusula de remisión en blanco, que aplaza la cuestión a una negociación ulterior.

En todos esos supuestos, el tratado no concede la equivalencia, pero tiene un impacto de impulso, en ocasiones de condicionamiento y sobre todo de acompañamiento. Es en este sentido en el que cabe hablar de «decisiones de adecuación indirectas»: no porque el Tratado sustituya al acto del artículo 45, sino porque la decisión de adecuación deja de ser un juicio aislado de derechos fundamentales para convertirse, en la práctica, en una pieza de la arquitectura comercial, negociada en paralelo y al servicio de un objetivo de liberalización de los flujos. La etiqueta es, por ello, menos una categoría jurídica que una advertencia.

A este cuadro bilateral se superpone el plano multilateral. En el marco de la Organización Mundial del Comercio, el artículo XIV del Acuerdo General sobre el Comercio de Servicios contempla una excepción que permite a los Estados adoptar medidas necesarias para proteger la intimidad de las personas en relación con el tratamiento de sus datos, y la iniciativa conjunta sobre comercio electrónico ha venido negociando reglas sobre flujos en las que la Unión ha tratado de incorporar sus cláusulas horizontales[18]. La protección de datos se juega, así, también en un tablero global en el que la presión liberalizadora es mayor.

Frente a esa presión, el límite es el mismo que rige para las decisiones de adecuación: ningún cauce puede rebajar el estándar de la Carta. El Tribunal de Justicia lo dejó claro en su Dictamen 1/15, al examinar el proyecto de acuerdo entre la Unión y Canadá sobre el tratamiento y la transferencia de los datos de los registros de pasajeros y declararlo

---

los diálogos sobre comercio y sobre protección de datos pueden complementarse, pero han de seguir vías separadas

[17] La adecuación de Japón se declaró mediante la Decisión de Ejecución (UE) 2019/419, de 23 de enero de 2019; las disposiciones sobre flujos de datos se incorporaron con posterioridad al Acuerdo de Asociación Económica UE-Japón mediante una negociación específica.

[18] Artículo XIV, letra c), inciso ii), del Acuerdo General sobre el Comercio de Servicios (AGCS).

parcialmente incompatible con los artículos 7, 8 y 52 de la Carta[19]. O dicho de otro modo, los acuerdos internacionales que articulan transferencias de datos quedan sometidos al control de los derechos fundamentales, de modo que la diplomacia comercial no puede operar como una puerta trasera para sortear las exigencias de la doctrina Schrems.

El riesgo que encierra este cauce paralelo es, en definitiva, el de la subordinación: que el juicio de equivalencia —que es, recordémoslo, una valoración de derechos fundamentales— acabe plegándose a la lógica del intercambio comercial, en la que la fluidez de los datos es un activo y su protección, un coste. Es la misma competencia de ordenamientos a la baja que recorre todo este trabajo, ahora vista desde el ángulo del comercio internacional. Y es una razón más para sostener que la frontera entre la equivalencia y la concesión debe trazarse con firmeza: el día en que la adecuación se conceda para cerrar un acuerdo, y no porque el tercer país proteja de verdad, la protección habrá dejado de ser un derecho para convertirse en moneda.

Esta imbricación produce, además, un efecto de cierre que conviene no pasar por alto. Una vez que los flujos de datos quedan anclados en un tratado, una decisión negativa de adecuación, o la revocación de una ya existente, se convierte en la práctica en una quimera. No porque el tratado lo impida jurídicamente: las cláusulas horizontales, por su carácter autoaplicativo, preservan intacta la facultad de la Unión de proteger los datos, y la propia jurisprudencia Schrems (junto con el artículo 45) no solo permite, sino que obliga a suspender o derogar la decisión cuando la equivalencia decae. El obstáculo no es de Derecho, sino de economía política: retirar la adecuación a un socio comercial es un acto hostil desde un punto diplomático, que dejaría además a miles de operadores sin cobertura, con lo que el Tratado, en la práctica dejaría de tener sentido. De manera que la obligación jurídica de revocar coexiste con la imposibilidad práctica de hacerlo, y esa contradicción es, quizá, la expresión más nítida de la competencia de ordenamientos a la baja.

Recordemos un dato que confirma esa dificultado. No consta que la Comisión hay revocado nunca, por iniciativa propia y por razones de equivalencia, una decisión de adecuación: las únicas que fueron anuladas lo han hecho por obra del Tribunal de Justicia, en Schrems I y Schrems II. Las revisiones periódicas, que sobre el papel son el mecanismo de control, han operado hasta ahora como un ritual de reconfirmación: en la revisión de 2024 se mantuvieron las once decisiones anteriores al Reglamento (incluida la israelí, con los problemas que se vieron con anterioridad), y la decisión británica se renovó en diciembre de 2025, hasta 2031, pese a las objeciones sobre la rebaja introducida por la Data (Use and Access) Act[20].[1]

l único correctivo que abarata esa reversión es la cláusula de extinción o *sunset*, presente, de forma singular, en las decisiones relativas al Reino Unido, que caducan si

[19] Dictamen 1/15 del Tribunal de Justicia, de 26 de julio de 2017, relativo al proyecto de acuerdo entre Canadá y la Unión Europea sobre la transferencia y el tratamiento de datos del registro de nombres de los pasajeros (PNR)

[20] Las decisiones de adecuación británicas, adoptadas en 2021 con una cláusula de extinción, fueron prorrogadas técnicamente en junio de 2025 y renovadas el 19 de diciembre de 2025, hasta el 27 de diciembre de 2031, previa opinión del Comité Europeo de Protección de Datos y aprobación en comitología, tras la entrada en vigor de la Data (Use and Access) Act de 2025

no se renuevan de forma expresa. Pero la práctica ha mostrado sus límites: lejos de dejar expirar la decisión a la vista de las dudas suscitadas por la reforma británica, la Comisión la renovó, y fue el propio Reino Unido el que recortó el alcance de su reforma para no comprometer la adecuación. El cierre, una vez más, operó en un solo sentido. La lección es que el sistema confía la garantía última no a la revisión administrativa, sino al control judicial; y que, cuando ese control también se relaja (como late en la sentencia Latombe, a la que luego me referiré), la protección queda inerme.

IX. El problema en la práctica de las decisiones de adecuación

Las decisiones de adecuación pueden constituir un mecanismo idóneo para la protección de los derechos. Ahora bien, el papel lo aguanta casi todo, y la práctica ofrece más de un motivo de cautela. Ya vimos cómo la decisión relativa a Israel se mantuvo tras una revisión que esquivó precisamente las cuestiones de seguridad nacional y de Estado de Derecho que comprometían la equivalencia. Israel no constituye, lamentablemente, un caso aislado y, por ello conviene ordenar los demás en orden creciente a su importancia. La clave de la crítica radica en la distancia que marcan entre la decisión y la realidad.

El primer problema es el de la **actualización** de las decisiones de adecuación. Once de las decisiones de adecuación en vigor son anteriores al propio Reglamento General de Protección de Datos (más allá de que algunas hayan podido adaptarse después), de modo que buena parte del sistema descansa sobre juicios de equivalencia formulados bajo un estándar que la jurisprudencia posterior, señaladamente las sentencias Schrems, ha elevado de forma considerable.

Que la primera revisión de conjunto no se completara hasta 2024 da idea de la inercia con que opera un mecanismo que, en teoría, debería ser un instrumento vivo. Y, cuando por fin se procedió a la revisión de las decisiones de adecuación, su impacto fue limitado. Las 11 decisiones fueron reconfirmadas por la decisión sin excepción, lo que se puede interpretar de modo que la revisión funcionó más como un trámite de continuidad que como un verdadero contraste del nivel de protección a la luz del estándar reforzado por las sentencias Schrems.

El segundo problema es de **cobertura**, y se aprecia mejor por las omisiones que hay en la Unión Europea en contextos económicos extraordinariamente importantes en el contexto de globalización económica. No existe ninguna decisión referida a la República Popular China, pese a que una parte muy relevante del comercio electrónico se realiza con empresas radicadas allí.

Es una manifestación de realismo: difícilmente podría afirmarse la equivalencia de un ordenamiento que subordina el tratamiento de datos a amplias facultades de acceso estatal y que impone, además, sus propias exigencias de localización y de seguridad. La consecuencia tiene un impacto en los derechos de la ciudadanía europea: un volumen ingente de transferencias cotidianas hacia China discurre, en el mejor de los casos, por la vía más exigente de las garantías adecuadas y, en el peor, sin cobertura real, en una suerte de zona gris que el sistema de adecuación no ilumina porque, sencillamente, no entra en ella.

El tercero, y más grave, es de **diseño**. Las decisiones de adecuación no abordan el problema que más erosiona el estándar europeo: el de la subcontratación de infraestructuras o servicios (desde lo más simple, los centros de atención al cliente) deslocalizadas en terceros países. Valga un ejemplo: la India, sobre la que no existe decisión de adecuación y sobre la que, sin embargo, recae buena parte de la actividad mundial de tratamiento de datos. La raíz del desajuste es conceptual. El sistema de adecuación razona país por país, con una lógica binaria (se es adecuado o no se es) y una mirada estática; pero la cadena real de tratamiento es transversal, se fragmenta entre múltiples jurisdicciones y se recompone a diario al hilo de cada subcontratación. La foto fija de la adecuación capta mal una realidad que es, por naturaleza, dinámica y distribuida. Este dato vuelve a confirmar la tesis central de este artículo: el factor decisivo no es el país del receptor formal, sino el conjunto de eslabones por los que el dato circula.

Conviene recordar, en todo caso, que la existencia de una decisión de adecuación no exime de las obligaciones contractuales propias de la relación entre responsable y encargado —artículo 28 del Reglamento— ni del correspondiente contrato que garantice la legitimidad del origen de los datos. La adecuación habilita la transferencia; no dispensa del resto del Reglamento

X. El problema permanente de los Estados Unidos

Sin duda, los Estados Unidos constituyen el punto más conflictivo de la transferencia internacional. La conflictividad deriva de dos factores que se refuerzan entre sí: la mayor parte de los datos circulan a través de infraestructuras de empresas de aquel país, y su legislación no deja de provocar sobresaltos en relación con los estándares europeos. En un contexto político como el actual, la dificultad resulta especialmente significativa, ya que la presión estadounidense para modificar el marco europeo es estable, sobre todo cuando se sanciona a las empresas de aquel país por incumplir el marco regulatorio europeo.

Como es conocido, las relaciones en esta materia han estado marcadas por las decisiones que negaron a los Estados Unidos la condición de territorio seguro. Schrems I y Schrems II han venido considerando que no garantiza un nivel de protección equivalente. El problema, sin discusión, reside en qué se ha hecho desde Europa en ejecución de esas sentencias cuando los datos siguen pasando por las infraestructuras de Amazon Web Services, Azure y Google. Francia, eso sí, ha restringido el uso de soluciones de Microsoft para el alojamiento de datos sensibles del sector público, en aplicación de su doctrina de «nube de confianza», precisamente a raíz de este problema.

Durante el mandato del presidente Biden se produjeron dos hechos significativos. Por un lado, la Executive Order 14086, de 7 de octubre de 2022, *Enhancing Safeguards for United States Signals Intelligence Activities*, que constituyó un prerrequisito para

aprobar el nuevo marco de referencia[21]. En ella los Estados Unidos se comprometieron a que sus actividades de inteligencia respetaran los principios de necesidad y proporcionalidad (aspectos que el TJUE echaba en falta) y a articular un mecanismo de reparación en dos niveles para los europeos afectados. Por otro, la promulgación de la Reforming Intelligence and Securing America Act (RISAA), que reautorizó y modificó la sección 702 de la FISA y que, en lo que aquí interesa, mantiene la posibilidad de imponer a los operadores de nube (los que todos usamos: Amazon, Google o Microsoft) la comunicación de ciertas comunicaciones que discurren por sus servidores[22]. Coexisten, así, una norma pensada para tranquilizar a Europa y otra que ensancha las facultades de acceso de la inteligencia estadounidense: la tensión entre ambas está en el origen de las dudas que el marco sigue suscitando.

Todo ello permitió alcanzar un nuevo marco de referencia, validado por la Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023, relativa al Marco de Privacidad de Datos UE-EE. UU.[23] Resultan, sin embargo, paradójicos varios elementos que conviene desarrollar.

El primero es que la CLOUD Act[24] (la norma que permite acceder a los datos en poder de empresas estadounidenses, estén donde estén los servidores) sigue plenamente en vigor pese a la decisión de adecuación de 2023. Aquí conviene recordar el artículo 48 del RGPD. Esta norma responde a una pregunta muy concreta: ¿qué debe hacer una empresa europea cuando un juez o una autoridad de un tercer país le ordena entregar datos personales? La respuesta del Reglamento es que esa orden extranjera, por sí sola, no basta: para que pueda cumplirse sin infringir el Derecho europeo, tiene que apoyarse en un acuerdo internacional entre ese país y la Unión o sus Estados miembros (típicamente, un tratado de asistencia judicial). Dicho de otro modo, el Derecho europeo no reconoce eficacia directa a los requerimientos de tribunales o autoridades extranjeros: exige que pasen por el cauce pactado entre Estados.

Es precisamente en la tensión entre el artículo 48 y la CLOUD Act donde se localiza el núcleo del conflicto de leyes que la decisión de adecuación no llega a resolver: los operadores de cloud estadounidenses (que copan el mercado mundial) pueden verse compelidos por su propio ordenamiento a entregar datos que el ordenamiento europeo le prohíbe entregar sin amparo en un tratado.

El segundo es que, pese a la promulgación de la RISAA, no se haya producido modificación ni análisis alguno de la Comisión sobre su impacto en lo recogido en la decisión de adecuación, como si el marco se hubiera congelado en el momento de su adopción y resultara inmune a la evolución legislativa posterior.

El tercero es que el sistema parta de un modelo voluntario para las entidades privadas que deseen recibir datos, basado en una autocertificación que, una vez inscrita, deviene obligatoria; de modo que la autorregulación (básica en el sistema estadounidense)

---

[21] Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities,, de 7 de octubre de 2022.
[22] Reforming Intelligence and Securing America Act (RISAA), de abril de 2024, que reautorizó y modificó la sección 702 de la FISA.
[23] Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023.
[24] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), de 2018.

sigue plenamente vigente. La adecuación no se predica, así, de los Estados Unidos como ordenamiento, sino del subconjunto de empresas que han decidido adherirse, lo que traslada al exportador la carga de verificar, transferencia a transferencia, que su contraparte figura efectivamente en la lista y mantiene la certificación.

El cuarto, y más delicado, es la naturaleza del órgano de protección. El Data Protection Review Court (DPRC) no es, pese a su nombre, un tribunal en sentido estricto, sino un órgano administrativo de revisión situado dentro del poder ejecutivo, que opera como segundo nivel del mecanismo de reparación tras la actuación del Civil Liberties Protection Officer. Esta fue, precisamente, la cuestión central de la sentencia del Tribunal General de 3 de septiembre de 2025, Latombe c. Comisión, que desestimó el recurso de anulación contra la Decisión 2023/1795[25]. El Tribunal consideró que el nombramiento y cese de sus miembros, junto con la prohibición de injerencia del Fiscal General y de las agencias de inteligencia, aseguran su independencia, y que, conforme a Schrems II, basta con un control judicial a posteriori, sin necesidad de autorización previa de una autoridad independiente para cada recogida de datos. La sentencia, sin embargo, ha sido recurrida en casación ante el Tribunal de Justicia, de modo que el debate no está cerrado; y no sería la primera vez que una solución aparentemente consolidada acaba siendo anulada años después.

A ello se añade el quinto elemento, llamativo por su amplitud: las condiciones de acceso a los datos en poder de empresas estadounidenses con fines «civiles o regulatorios», que escapan en buena medida al perímetro de las garantías reforzadas, pensadas sobre todo para la inteligencia de señales.

A la fragilidad estructural del marco se ha sumado, además, un elemento sobrevenido especialmente relevante: el debilitamiento del Privacy and Civil Liberties Oversight Board (PCLOB), que perdió su quórum operativo tras el cese de varios de sus miembros desde la llegada del Presidente Trump a la Casa Blanca. Dado que ese organismo desempeñaba una función de supervisión decisiva en la arquitectura de garantías sobre la que se asienta la decisión de adecuación, varias autoridades europeas han recomendado a las empresas diseñar *estrategias de salida* del marco. El dato es elocuente: cuando las propias autoridades aconsejan preparar la retirada de un mecanismo, es porque su solidez se percibe como provisional.

Conviene, en fin, situar este andamiaje en su contexto político más reciente, porque es el que mejor explica su fragilidad. El Marco de Privacidad de Datos no descansa en ningún acuerdo nuevo, sino que sigue apoyándose en la decisión de adecuación de 2023 y en la Executive Order 14086; pero su suerte se ha entrelazado, desde 2025, con la del gran pacto comercial transatlántico. En el acuerdo marco alcanzado en Turnberry en julio de 2025, la Comisión sostuvo formalmente que la modificación de su normativa digital «no estaba sobre la mesa»[26]; y, sin embargo, la presión estadounidense por desregular —escenificada en las amenazas arancelarias frente a las legislaciones de servicios y de mercados digitales— no ha cesado, y ha empezado a

[25] Sentencia del Tribunal General de la Unión Europea de 3 de septiembre de 2025, asunto T-553/23, Latombe c. Comisión, recurrida en casación ante el Tribunal de Justicia.
[26] Declaración conjunta UE-EE. UU. sobre el acuerdo marco comercial alcanzado en Turnberry el 27 de julio de 2025

materializarse en la propuesta de «Digital Omnibus», a la que volveremos, que ablanda el propio Reglamento.

El resultado es que la continuidad del marco de transferencias depende cada vez menos de un juicio de equivalencia y cada vez más de la negociación comercial, en un momento, además, de máxima inestabilidad de sus cimientos estadounidenses: la reautorización de la sección 702 de la FISA decayó en abril de 2026 y solo se mantiene viva mediante prórrogas de corta duración, mientras la capacidad de supervisión del PCLOB pende de lo que resuelva el Tribunal Supremo sobre la facultad presidencial de cesar a los miembros de los órganos independientes[27].

Como corolario de todo lo anterior, y llevado a un supuesto práctico, resulta llamativo que la Agencia Española de Protección de Datos haya considerado a Microsoft un proveedor seguro a efectos de la transferencia, cuando en Francia se han restringido las aplicaciones de dicha compañía para la Administración por razones de seguridad en el tratamiento de la información. El último acuerdo con los Estados Unidos en esta materia presenta, en fin, no pocos elementos que recuerdan a las operaciones reconstructivas de la cirugía estética: corrige la apariencia sin alterar la estructura.

XI. La aportación de garantías adecuadas

La decisión de adecuación es el instrumento más sencillo, pero no el único. El artículo 46 del Reglamento habilita la transferencia cuando el responsable o el encargado ofrecen garantías adecuadas, a condición de que los interesados dispongan de derechos exigibles y de acciones legales efectivas en el país de destino.

Este es, de hecho, el marco que opera en la práctica en la mayor parte de los supuestos, precisamente porque la mayoría de los grandes flujos (y, en particular, los dirigidos a los Estados Unidos cuando el importador no está certificado) no se amparan en una decisión de adecuación, sino en estos instrumentos. Conviene, por ello, distinguir con nitidez dos categorías que el texto separa: las garantías que no requieren autorización previa de la autoridad de control (apartado 2 del artículo 46) y las que sí la requieren, recogidas en el apartado 3.

Siguiendo el orden del propio artículo 46, apartado 2, el primer instrumento es el de los **acuerdos jurídicamente vinculantes y exigibles entre autoridades u organismos públicos**. Se trata de instrumentos pensados para la cooperación entre Administraciones (por ejemplo, en el ámbito tributario, aduanero o de la seguridad social), en los que el carácter público de ambas partes permite articular compromisos de protección con fuerza obligatoria y mecanismos de reparación para los interesados.

El segundo instrumento son las **normas corporativas vinculantes (binding corporate rules o BCR**). Imaginemos un grupo multinacional con matriz en Madrid

[27] La reautorización de la sección 702 de la FISA, contenida en la RISAA, decayó en abril de 2026; el Congreso aprobó una prórroga de cuarenta y cinco días que la mantiene en vigor hasta mediados de junio de 2026. La capacidad operativa del PCLOB depende de lo que resuelva el Tribunal Supremo en *Trump v. Slaughter* sobre los límites de la facultad presidencial de cesar a los miembros de órganos de supervisión independientes.

y filiales en la India, Brasil y los Estados Unidos, que necesita mover datos de empleados y clientes entre todas ellas a diario. Firmar cláusulas contractuales para cada par de filiales sería farragoso; las BCR ofrecen una alternativa: un código interno de protección de datos, único para todo el grupo, que la matriz se compromete a aplicar en cualquier país donde el grupo opere. Son, en esencia, el «reglamento de protección de datos» propio de una empresa multinacional, que viaja con los datos allá donde estos vayan dentro del grupo.

El artículo 47 del Reglamento fija lo que ese código debe contener como mínimo, y sus exigencias pueden agruparse, en lo esencial, en torno a cuatro ejes.

i) El primero es que las normas sean jurídicamente vinculantes: no basta con una declaración de buenas intenciones, sino que han de obligar de verdad, tanto puertas adentro, a todas las filiales y a sus empleados, como puertas afuera, frente a los ciudadanos cuyos datos se tratan.

ii) El segundo es que incorporen los principios sustantivos de protección: que los datos se usen solo para la finalidad prevista (no, por ejemplo, para revenderlos), que se recojan únicamente los necesarios, que se mantengan exactos y actualizados, que no se conserven más tiempo del preciso, que estén protegidos frente a accesos indebidos y que no se reenvíen a terceros ajenos al grupo sin garantías.

iii) El tercero es el reconocimiento a los interesados de derechos realmente exigibles: cualquier afectado debe poder reclamar ante la autoridad de control de su país y ante los tribunales y obtener una indemnización si se vulneran sus derechos, aunque la infracción se haya cometido en una filial al otro lado del mundo.

iv) Y el cuarto, especialmente relevante, es que la entidad establecida en la Unión, la matriz madrileña de nuestro ejemplo, asume la responsabilidad por las infracciones cometidas por los miembros del grupo situados fuera de ella: si la filial india incumple, responde la matriz europea, de modo que el ciudadano siempre tiene un interlocutor solvente y al alcance de los tribunales europeos.

Las BCR no surgen, además, de forma automática. Antes de poder emplearse, deben ser aprobadas por la autoridad de control competente —la Agencia Española de Protección de Datos, en el caso de un grupo con matriz en España— a través del mecanismo de coherencia, que asegura un criterio uniforme en toda la Unión y que incluye un dictamen previo del Comité Europeo de Protección de Datos. Es, por su solidez, el instrumento idóneo para los grandes grupos multinacionales, que con una sola herramienta cubren todos sus flujos internos. Pero esa misma solidez tiene un precio: son el mecanismo más lento y costoso de implantar, pues su elaboración y aprobación pueden prolongarse durante años, lo que los pone fuera del alcance de la mayoría de las empresas. Y arrastran, sobre todo, una limitación que volveremos a encontrar: por muy detalladas que sean, las BCR obligan a las empresas del grupo, pero no pueden vincular a las autoridades del tercer país. Si la ley estadounidense o india permite a sus servicios de inteligencia acceder a los datos, ningún código interno lo

impedirá; de ahí que su empleo no exima de evaluar igualmente ese riesgo de acceso estatal.

El tercer instrumento, y el de uso más extendido con diferencia, son las **cláusulas contractuales tipo adoptadas por la Comisión**. Si las BCR son el reglamento interno de un gran grupo, las cláusulas tipo son el contrato estándar al alcance de cualquiera: una pyme española que contrata el alojamiento de su base de clientes con un proveedor de nube extracomunitario no negocia nada complejo, sino que incorpora a su contrato el modelo de cláusulas ya aprobado por la Comisión, en su variante de responsable a encargado. Mediante la Decisión de Ejecución (UE) 2021/914, de 4 de junio de 2021, se aprobó un nuevo conjunto que sustituyó a las cláusulas anteriores y cuyo periodo transitorio concluyó a finales de 2022. Su gran novedad es la estructura modular: cuatro módulos que cubren, respectivamente, las transferencias entre responsables, de responsable a encargado, entre encargados y de encargado a responsable, de modo que un mismo instrumento se adapta a la posición de cada parte. Incorporan, además, una cláusula de acoplamiento que permite la adhesión de nuevas partes y, sobre todo, integran en su clausulado las exigencias derivadas de Schrems II: la obligación de evaluar si la legislación y la práctica del país de destino impiden cumplir las cláusulas, y la de notificar, impugnar y minimizar los requerimientos de acceso de las autoridades públicas. Las cláusulas confieren a los interesados derechos como terceros beneficiarios y se rigen por el Derecho de un Estado miembro que los reconozca. Comparten, no obstante, el mismo límite estructural que ya señalamos a propósito de las normas corporativas: vinculan únicamente a las partes que las suscriben y no pueden, por su propia naturaleza contractual, obligar a las autoridades públicas del tercer país. De ahí que, cuando el ordenamiento de destino habilita accesos que el contrato no puede neutralizar, las cláusulas resulten insuficientes si no se acompañan de medidas suplementarias.

A estos instrumentos se añaden las cláusulas tipo adoptadas por una autoridad de control y aprobadas por la Comisión, de uso aún incipiente, que ofrecen una alternativa de redacción autorizada para sectores o supuestos específicos.

Cierran el primer grupo los códigos de conducta y los mecanismos de certificación. Concebidos en los artículos 40 a 43 del Reglamento como instrumentos de autorregulación supervisada, pueden operar también como herramientas de transferencia cuando van acompañados de compromisos vinculantes y exigibles del responsable o encargado en el tercer país de aplicar las garantías adecuadas, incluidas las relativas a los derechos de los interesados. Son, hasta la fecha, los menos utilizados —su puesta en marcha exige una infraestructura de aprobación, adhesión y supervisión que aún está madurando—, pero ofrecen un potencial considerable para sectores enteros que comparten un mismo tipo de tratamiento.

Frente a todos ellos, el apartado 3 del artículo 46 reúne las garantías que sí requieren autorización previa de la autoridad de control competente: las cláusulas contractuales ad hoc, negociadas entre las partes al margen de los modelos aprobados, y los acuerdos administrativos entre autoridades públicas que incorporen derechos exigibles para los interesados. Esta es la razón por la que no cabe afirmar, sin más, que toda garantía adecuada quede sometida a un régimen de autorización administrativa previa de la Agencia Española de Protección de Datos: las cláusulas tipo, que son el instrumento de

uso más extendido, no la precisan, y en ello reside buena parte de su atractivo práctico. La autorización se reserva para los instrumentos que, por apartarse de los modelos o por su naturaleza interadministrativa, exigen un control individualizado.

Ahora bien, tras Schrems II, el recurso a cualquiera de estas garantías ha dejado de ser automático. El exportador, auxiliado en su caso por el importador, debe realizar una evaluación de impacto de la transferencia (Transfer Impact Assessment) con arreglo a la metodología en seis pasos de las Recomendaciones 01/2020 del Comité Europeo de Protección de Datos: conocer y cartografiar las transferencias; identificar el instrumento del artículo 46 en que se apoyan; evaluar si ese instrumento es efectivo a la luz de la legislación y la práctica del país de destino; identificar y adoptar, en su caso, medidas suplementarias; cumplir las formalidades procedimentales que estas exijan; y reevaluar el conjunto a intervalos apropiados.

Las medidas suplementarias se ordenan en tres categorías. Las técnicas (cifrado robusto con claves retenidas en la Unión, seudonimización efectiva o tratamiento dividido entre jurisdicciones) son las únicas capaces de neutralizar un acceso masivo por parte de los servicios de inteligencia, pues operan sobre el dato mismo y no sobre la voluntad de las partes. Las contractuales (obligaciones de transparencia sobre los requerimientos recibidos, deberes de impugnación, auditorías) y las organizativas (políticas internas, gobernanza, informes de transparencia) refuerzan el marco, pero no bastan por sí solas cuando el importador está jurídicamente compelido a facilitar el acceso. Y cuando ninguna medida resulta suficiente, la conclusión que impone el sistema es drástica: la transferencia debe suspenderse.

Conviene cerrar este epígrafe con una observación crítica. Todo el peso de esta evaluación recae sobre el exportador, que con frecuencia es una pequeña o mediana empresa sin medios para auditar el sistema jurídico de un tercer país. El resultado es una asimetría difícilmente sostenible: se exige al eslabón más débil de la cadena que garantice lo que ni siquiera la Comisión consigue asegurar mediante sus decisiones de adecuación. Es, una vez más, la distancia entre el Derecho formal y el Derecho practicado; y es también la confirmación de que, en la transferencia real, el vehículo y el ordenamiento que lo gobierna pesan más que la voluntad de las partes.

XII. Las excepciones para situaciones específicas

Junto a los mecanismos anteriores, que cabe considerar ordinarios, el artículo 49 contempla una serie de excepciones que permiten la transferencia en circunstancias específicas cuando no existe ni decisión de adecuación ni garantías adecuadas. Su naturaleza es la de un último recurso, y de ahí derivan dos consecuencias que el Comité Europeo de Protección de Datos ha subrayado con firmeza:[28] su interpretación es restrictiva y su aplicación ha de ser ocasional y no repetitiva. No pueden, por tanto, convertirse en la vía ordinaria para canalizar transferencias estructurales o masivas; quien lo intente desnaturaliza el sistema y se expone a la sanción. Existe, además, un

[28]Comité Europeo de Protección de Datos, Directrices 2/2018 sobre las excepciones del artículo 49 del RGPD, que subrayan su carácter excepcional y de interpretación restrictiva.

orden de prelación: solo cuando no caben la adecuación ni las garantías del artículo 46 procede acudir a estas excepciones.

La primera de ellas es el consentimiento explícito del interesado, prestado tras haber sido informado de los riesgos que la transferencia comporta por la ausencia de decisión de adecuación y de garantías adecuadas. Las exigencias son severas: el consentimiento ha de ser explícito, específico para la transferencia concreta, informado en cuanto a sus riesgos, libre y revocable en cualquier momento. Estas notas hacen del consentimiento una base frágil para los flujos empresariales: difícilmente puede considerarse libre el que se obtiene en una relación de desequilibrio, por ejemplo, la laboral y, por su carácter revocable y singular, resulta inadecuado para transferencias repetitivas o sistemáticas.

La segunda y la tercera giran en torno al contrato. Se admite la transferencia necesaria para la ejecución de un contrato entre el interesado y el responsable, o para la adopción de medidas precontractuales solicitadas por aquel; y también la necesaria para la celebración o ejecución de un contrato celebrado, en interés del interesado, entre el responsable y un tercero. En ambos casos el elemento decisivo es el juicio de necesidad, interpretado de modo estricto: debe existir un vínculo objetivo y estrecho entre la transferencia y la finalidad contractual, de manera que aquella resulte verdaderamente imprescindible y no una mera comodidad de gestión. Por eso el Comité ha negado que esta excepción ampare, por ejemplo, la externalización de un tratamiento en un proveedor extracomunitario elegido por el responsable por razones de conveniencia: ahí la transferencia no es necesaria para el contrato con el interesado, sino para el modelo de negocio del responsable.

La cuarta excepción son las razones importantes de interés público, reconocidas por el Derecho de la Unión o de los Estados miembros. Conviene precisar su alcance: lo que ha de ser público es el interés perseguido, no la condición de las partes. El considerando 112 del Reglamento ofrece ejemplos ilustrativos, como el intercambio internacional de datos entre autoridades de competencia, tributarias o de supervisión, o la cooperación en materia de salud pública.[29] No es, por tanto, una cláusula de cierre para cualquier finalidad que una Administración considere conveniente, sino una excepción anudada a intereses públicos cualificados y expresamente reconocidos.

La quinta es la formulación, el ejercicio o la defensa de reclamaciones, en el marco de procedimientos judiciales, administrativos o extrajudiciales. Es una excepción de notable relevancia práctica, pero también de contornos delicados: en ella se inscriben, por ejemplo, las solicitudes de exhibición documental masiva propias del proceso estadounidense (el llamado e-discovery), que con frecuencia chocan frontalmente con el artículo 48 del RGPD. La excepción no puede convertirse, pues, en una puerta trasera para satisfacer requerimientos extranjeros que el ordenamiento europeo solo admitiría a través de los cauces de la asistencia jurídica mutua.

[29]Considerando 112 del RGPD, que ilustra los supuestos de razones importantes de interés público —por ejemplo, el intercambio internacional de datos entre autoridades de competencia, tributarias o de supervisión, o en el ámbito de la salud pública.

La sexta protege los intereses vitales del interesado o de otras personas cuando aquel se encuentre física o jurídicamente incapacitado para prestar su consentimiento. Es la excepción de las situaciones límite (una urgencia médica de quien viaja, una catástrofe, una operación humanitaria) y su fundamento no es la conveniencia, sino la imposibilidad material de recabar la voluntad del afectado. No ampara, por ello, la transferencia de datos de quien está en condiciones de consentir, por delicada que sea su situación.

La séptima es la transferencia realizada desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, esté destinado a facilitar información al público. Su lógica es que la publicidad legal del registro relativiza la expectativa de confidencialidad; pero la excepción es de alcance limitado: no autoriza la extracción masiva ni la transferencia íntegra del registro, sino la comunicación puntual y conforme a las condiciones de consulta legalmente previstas.

A estas excepciones se añade, en fin, una derogación residual y de aplicación verdaderamente excepcional: la transferencia que, no siendo repetitiva, afecta solo a un número limitado de interesados, resulta necesaria para los intereses legítimos imperiosos del responsable (que no prevalezcan sobre los intereses o derechos del interesado) y va acompañada de las garantías apropiadas que el propio responsable haya valorado y documentado. Es esta la única que obliga al responsable a informar a la autoridad de control y a comunicar al interesado tanto la transferencia como los intereses legítimos imperiosos perseguidos. Conviene, por tanto, evitar la afirmación, inexacta como regla general, de que las excepciones del artículo 49 queden sometidas a un régimen de comunicación previa a la autoridad de control: solo esta cláusula de cierre la impone, y precisamente por su carácter de último de los últimos recursos.

Por último, no debe olvidarse el límite del apartado 3 del artículo 49: las excepciones basadas en el consentimiento, en el contrato y en el contrato celebrado en interés del interesado, así como la derogación residual, no resultan aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos. La advertencia es coherente con el conjunto del sistema: cuanto más débil es el título habilitante, más estrecho es su perímetro de aplicación.

XIII. La dimensión aplicativa y sancionadora

El régimen descrito no es un mero ejercicio teórico. Su aplicación se ha traducido en la sanción más elevada dictada hasta la fecha al amparo del RGPD: la impuesta a Meta por la autoridad irlandesa el 22 de mayo de 2023, por importe de 1.200 millones de euros, precisamente por transferencias a los Estados Unidos efectuadas mediante cláusulas contractuales tipo que no garantizaban el nivel de protección exigido.[30] Es este, y no otro, el mejor ejemplo de la distancia entre el Derecho formal y el Derecho practicado: el incumplimiento del capítulo V no es una infracción menor, sino una de

[30] Decisión de la Data Protection Commission irlandesa, de 22 de mayo de 2023, que impuso a Meta una sanción de 1.200 millones de euros —la mayor dictada hasta la fecha al amparo del RGPD— por transferencias a los Estados Unidos efectuadas con cláusulas contractuales tipo.

las que mayor exposición sancionadora generan. La cuantía no es anecdótica: traslada al mercado la señal de que la transferencia internacional es un punto de riesgo de primer orden, también económico.

A la vertiente sancionadora se suma, además, una vertiente resarcitoria de creciente importancia. En enero de 2025, el Tribunal General, en el asunto *Bindl c. Comisión*, condenó por primera vez a la propia Comisión a indemnizar a un particular por una transferencia ilícita de datos a los Estados Unidos, apreciando un daño moral derivado de la pérdida de control sobre los datos personales[31]. La relevancia del precedente trasciende el caso concreto: si una eventual invalidación del marco de transferencias diera lugar a reclamaciones de esta naturaleza, la exposición de los responsables podría multiplicarse por la vía de las acciones colectivas. El incumplimiento del capítulo V deja de ser, así, un riesgo meramente sancionador para convertirse también en un riesgo indemnizatorio de alcance potencialmente masivo.

Conviene situar esta decisión en su contexto institucional. El mecanismo de ventanilla única hace recaer la competencia en la autoridad de control principal (en el caso de las grandes tecnológicas, con frecuencia la irlandesa, lo que ha suscitado críticas por la lentitud y la heterogeneidad de la respuesta sancionadora. La sanción a Meta fue, de hecho, fruto de la intervención del Comité Europeo de Protección de Datos a través del mecanismo de coherencia, que corrigió al alza la propuesta inicial. Esta arquitectura explica buena parte de la distancia entre la contundencia del estándar y la desigualdad de su aplicación efectiva.

La preocupación por el acceso de autoridades extranjeras, por lo demás, ha desbordado ya el ámbito de los datos personales. El Reglamento de Datos (*Data Act*) ha incorporado, en su artículo 32, salvaguardias frente al acceso de autoridades de terceros países a los datos no personales en poder de proveedores de servicios de tratamiento, en un esquema deliberadamente paralelo al del artículo 48 del RGPD.[32] La señal regulatoria es clara: el problema del vehículo —quién controla la infraestructura y a qué legislación queda sujeta— se ha convertido en el eje de la política europea de datos, también más allá del dato personal. La protección de datos deja de ser una materia aislada para integrarse en una estrategia más amplia de autonomía sobre la infraestructura digital.

XIV. Inteligencia artificial y transferencia internacional de datos

El siguiente paso es el análisis del impacto de la inteligencia artificial en la transferencia internacional de datos. Un problema de extremada importancia si tenemos en cuenta cómo funciona la IA y el origen de sus actores máximos (China y Estados Unidos). Cuando un usuario europeo introduce un dato personal en un modelo alojado fuera de la Unión, no se limita a depositarlo en una infraestructura pasiva: lo

[31] Sentencia del Tribunal General de la Unión Europea de 8 de enero de 2025, asunto T-354/22, *Bindl c. Comisión*.

[32] Reglamento (UE) 2023/2854 (Reglamento de Datos o *Data Act*), cuyo artículo 32 establece salvaguardias frente al acceso de autoridades de terceros países a datos no personales, en un esquema paralelo al del artículo 48 del RGPD.

entrega a un sistema que lo procesa, lo combina con otros, infiere a partir de él y, en ocasiones, lo retiene en su propia configuración. El proveedor de inteligencia artificial es, por ello, el vehículo de la transferencia en su forma más intensa que condensa todos los problemas examinados hasta aquí.

Hay que empezar con una cuestión práctica: determinar cuándo el uso de la IA genera transferencia internacional de datos. De entrada, con el entrenamiento, derivado de los conjuntos de datos masivos que utilizan los modelos, que se suelen captar de forma indiscriminada y que suelen afectar a datos personales. El segundo es derivado de la inferencia: cada consulta que se dirige a un modelo alojado en un tercer país constituye, en sí misma, una puesta a disposición de datos personales y, por tanto, una transferencia internacional.

La armonización entre norma y técnica resulta prácticamente imposible. La dificultad de valorar la equivalencia a que hecho referencia antes, la dificultad de suprimir y rectificar datos choca con una realidad técnica incómoda: una vez que un dato ha contribuido a fijar los parámetros de un modelo, extraerlo de sus pesos es extraordinariamente difícil, cuando no imposible, de modo que el derecho al olvido se enfrenta a un objeto que no olvida. Y la inferencia de categorías especiales puede producirse en un servidor situado fuera de la Unión, combinando el problema del capítulo V con el de las decisiones automatizadas del artículo 22 del Reglamento.

Frente a este cuadro, el marco normativo presenta un vacío significativo. El Reglamento de Inteligencia Artificial ordena el sistema pero no regula la transferencia internacional de datos personales, que sigue rigiéndose por el capítulo V del Reglamento General de Protección de Datos. Sobre un mismo sistema de inteligencia artificial recaen a la vez tres normativas que persiguen fines distintos y que no terminan de encajar: el Reglamento de Inteligencia Artificial, que vela por la seguridad del producto; la parte sustantiva del Reglamento General de Protección de Datos, que vela por la licitud del tratamiento y los derechos de la persona; y el capítulo V de este último, que controla la salida de los datos fuera de la Unión. Cada una mira el problema desde su ángulo y presume que del resto se ocupan las demás, de modo que el aspecto más delicado (el dato personal que viaja a un tercer país a bordo de un modelo de inteligencia artificial) acaba cayendo en una zona de intersección que ninguna cubre por entero.

El caso de DeepSeek ilustra todo lo anterior y enlaza con la ausencia de decisión de adecuación respecto de China. Tras la irrupción de su modelo a comienzos de 2025, las autoridades europeas reaccionaron con rapidez y encuadraron el problema, precisamente, en clave de transferencia: el Garante italiano bloqueó el tratamiento de datos de los usuarios italianos, y el comisionado de Berlín declaró ilícito el envío de datos a China, subrayando la falta de decisión de adecuación, el amplio acceso de las autoridades chinas y la ausencia de recursos efectivos para los afectados, hasta el punto de pedir a Apple y Google que retiraran la aplicación. El caso revela dos cosas: que la herramienta última de protección ya no es solo la sanción, sino el bloqueo a través de las tiendas de aplicaciones —lo que convierte a esas plataformas en ejecutores de facto del Derecho europeo—, y que la aplicación extraterritorial tiene límites palpables, pues el uso de DeepSeek siguió creciendo pese a toda la presión regulatoria: la norma existe, se invoca y hasta se ejecuta, y aun así el ciudadano sigue entregando sus datos. Es la

distancia entre el Derecho formal y el practicado en su forma más aguda. Y apunta hacia donde sopla la corriente: la inteligencia artificial se ha convertido en el principal argumento para rebajar el estándar (la propuesta de «Digital Omnibus» quiere amparar el entrenamiento de modelos como interés legítimo y estrechar la noción misma de dato personal), de modo que, también aquí, la protección cede ante la conveniencia tecnológica. El problema de la IA no es un capítulo aparte: es donde se anudan todos los hilos de este trabajo.

XV. Consideraciones finales

El problema al que nos enfrentamos es el de la competencia de ordenamientos y la presión para que el consenso se construya a la baja, como mecanismo para incrementar la apropiación de beneficios por parte de las empresas que gestionan los datos. En el ámbito europeo se reciben numerosas presiones, derivadas de ese lugar común según el cual Europa no progresa ni innova como consecuencia del RGPD, frente al supuesto "dinamismo" estadounidense o asiático.

Ese proceso no es una hipótesis: está sucediendo. La propuesta de "Digital Omnibus", que pretende, entre otros extremos, redefinir a la baja el concepto mismo de dato personal, ha merecido un dictamen conjunto crítico del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos, de 10 de febrero de 2026, por restringir esa noción en contra de la jurisprudencia del Tribunal de Justicia.[33] Es, en cierto modo, el segundo movimiento del *Bolero* de Ravel: si Europa cede, los requisitos se equipararán a la baja para reiniciar después, bajo acordes aún más tenues, un nuevo desarrollo. Y el ciclo Schrems I — Schrems II — Latombe, hoy en casación, recuerda que la melodía no se ha detenido: cada acuerdo transatlántico se construye sabiendo que será impugnado, y cada impugnación se resuelve sabiendo que el equilibrio es provisional.

El núcleo del problema, creo, no debe situarse en el texto normativo, sino en el lugar donde realmente residen los aspectos básicos de la protección: una política pública de protección de datos orientada a la ciudadanía. Conviene, además, no perder de vista la dimensión estructural que aquí se ha defendido a lo largo de todo el trabajo: en una transferencia internacional ordinaria no hay dos sujetos, sino tres (emisor, receptor y vehículo) y a menudo cuatro. Mientras el análisis jurídico siga razonando en clave bilateral, el Derecho formal continuará alejándose del Derecho practicado, y la protección equivalente seguirá siendo, en demasiados casos, una equivalencia sobre el papel. El recorrido por las decisiones de adecuación, por las garantías adecuadas del artículo 46 y por las excepciones del artículo 49 confirma esa intuición: en todos esos planos, el factor determinante acaba siendo el ordenamiento que gobierna la infraestructura por la que el dato circula.

[33] Dictamen conjunto del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos, de 10 de febrero de 2026, sobre la propuesta de "Digital Omnibus", crítico con la redefinición del concepto de dato personal.

Recordemos, en fin, que al otro lado del Atlántico tenemos un *dataholic*;[34] en Asia, de forma más sutil y callada, otro tanto; y en el fondo de la *dark web*, todos aquellos archivos que creímos borrados de nuestros dispositivos. Somos nosotros quienes decidimos. Solo en Francia, por el momento, se ha empezado a desarrollar un debate público sobre esta cuestión —aunque se quede, en parte, en la dimensión fiscal—, vinculando la protección de los datos personales a la soberanía digital de los Estados. No podemos olvidar el dato de que ingentes cantidades de información se trasladan a diario desde Europa a los Estados Unidos, pues las grandes empresas que dominan la infraestructura están domiciliadas en aquel país. Decidir sobre los datos es, también, decidir sobre la soberanía.

De esta doble regla conviene retener una consecuencia que suele generar confusión. Que una empresa de fuera de la Unión quede sometida al Reglamento -por ofrecer servicios a personas que están en Europa o por seguir su comportamiento- no significa que pase a estar "dentro" de Europa a efectos de la circulación de datos. Son dos cuestiones diferentes: una cosa es *si* el Reglamento se aplica a esa empresa, y otra distinta es *qué requisitos* deben cumplirse para enviarle datos desde la Unión. Pensemos en una empresa estadounidense que ofrece una aplicación a usuarios españoles: el Reglamento es derecho aplicable, sí, pero cuando una empresa europea le remite datos personales sigue habiendo una transferencia internacional que exige sus propias garantías.

Dicho de otro modo, el artículo 3 decide si el Reglamento entra en juego; y solo después, el capítulo V impone las cautelas para enviar los datos al exterior, cautelas que pueden ser exigibles incluso cuando quien los recibe está, él mismo, sujeto al Reglamento. Por eso el Comité Europeo de Protección de Datos insiste en no mezclar ambos planos.

El RGPD no ha sido especialmente minucioso al configurar las normas de conflicto que delimitan el alcance de su contenido. Se trata de una cuestión relevante en la medida en que ningún Estado está dispuesto a dejar de aplicar su propia normativa, lo que genera solapamientos y, en ocasiones, conflictos abiertos de leyes -señaladamente con las legislaciones de seguridad nacional de terceros países, a las que más adelante volveremos-. El resultado es un espacio de fricción en el que un mismo dato puede quedar simultáneamente reclamado por dos ordenamientos con exigencias incompatibles.

A este marco hay que añadir los Tratados comerciales de nueva generación, que incluyen cláusulas de protección de datos concebidas para que no constituyan un factor de limitación del comercio. Tampoco en ellos está concretado el régimen de protección aplicable; o, para ser más exactos, no se ha producido una concreción de la normativa aplicable, que en ocasiones se remite a acuerdos ulteriores, como sucede en el Tratado con México.[35] Por último, no puede olvidarse el régimen que pudiera derivarse de los

---

[34] Tomo la expresión de Morozov en el *Frankfurter Allgemeine Zeitung* de 24 de julio de 2013: "My name is America and I'm a dataholic".

[35] Sobre la conexión entre protección de datos y comercio internacional, véase Otero García-Castrillón, C., "Protección de datos en la economía digital. Una aproximación desde la regulación del comercio internacional", en

acuerdos alcanzados en el marco de la Organización Mundial del Comercio, que pueden añadir aspectos concretos a la regulación.

Como puede verse, un problema de derechos fundamentales como este plantea, ya de entrada, serias dificultades de conocimiento para la ciudadanía; dificultades que alcanzan incluso a la identificación de los órganos ante los que cabe recabar protección.

Rodríguez Pineau, E. y Torralba Mendiola, E. (dirs.), *La protección de las transferencias transnacionales de datos*, Thomson Reuters Aranzadi, 2021, páginas 33 y siguientes.

Sobre el autor

Julio V. González García

Catedrático de Derecho Administrativo en la Universidad Complutense de Madrid desde 1992. Ha sido Secretario General de la UCM y del Grupo Correos. Investigador en Harvard Law School y en el Instituto Universitario Europeo de Fiesole. Sus áreas de especialización incluyen la contratación pública, los bienes públicos, la regulación económica, el Derecho bancario y el Derecho europeo.

ECOSISTEMA EDITORIAL

Global Politics and Law · globalpoliticsandlaw.com
Blog académico de referencia en Derecho Público. Más de 400 artículos y una década de análisis riguroso sobre Derecho Administrativo, regulación y gobernanza pública.

Documentos de trabajo · globalpoliticsandlaw.com/working-papers/
Serie de working papers de investigación, disponibles en acceso abierto.

La Trastienda · globalpoliticsandlaw.com/la-trastienda/
Newsletter de análisis de Derecho Público. Una publicación quincenal para quienes quieren entender el Derecho que mueve las instituciones.