
This is the **published version** of the bachelor thesis:

Cerezo Piñol, Berta. *Protección de datos personales y soberanía digital : el conflicto entre la Unión Europea y Estados Unidos*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 54 pàg.

This version is available at <https://ddd.uab.cat/record/331929>

under the terms of the  license.



TRABAJO DE FIN DE GRADO

Protección de datos personales y soberanía digital: el conflicto entre la Unión Europea y Estados
Unidos

Autor: Berta Cerezo Piñol

Grado en Derecho

Barcelona, 2025 / 2026

Tutor: Alfredo Ramírez Nárdiz

RESUMEN:

En una sociedad cada vez más digitalizada e interconectada, la protección de los datos personales se ha convertido en una cuestión jurídica de gran relevancia, ya que el intercambio constante de información entre países resulta esencial para la economía y la comunicación global, aunque también genera tensiones entre la protección de los derechos fundamentales y las necesidades de seguridad de los Estados. En este contexto, la Unión Europea entiende la protección de datos como un derecho fundamental desarrollado a través del RGPD, mientras que Estados Unidos mantiene un sistema más fragmentado y sectorial, que otorga amplias facultades de acceso a la información por motivos de seguridad nacional. Estas diferencias se hicieron especialmente evidentes tras los atentados del 11 de septiembre y las revelaciones sobre vigilancia masiva realizadas en 2013, circunstancias que llevaron al Tribunal de Justicia de la Unión Europea a invalidar los acuerdos Safe Harbor y Privacy Shield al considerar que no garantizaban un nivel de protección equivalente al europeo. Como consecuencia, las transferencias internacionales de datos, indispensables para el funcionamiento de la economía digital, pasaron a estar sometidas a mayores exigencias y garantías jurídicas, lo que impulsó la creación del EU-US Data Privacy Framework de 2023 con el objetivo de reforzar la protección de los datos y recuperar la confianza en los intercambios transatlánticos, aunque su suficiencia continúa siendo objeto de debate. Todo ello plantea la necesidad de analizar si este nuevo marco es realmente capaz de garantizar una protección sustancialmente equivalente a la exigida por el Derecho de la Unión y de resolver las diferencias estructurales existentes entre ambos modelos jurídicos.

Palabras clave: Protección de datos; transferencias internacionales de datos; RGPD; Unión Europea; Estados Unidos; privacidad; Schrems I; Schrems II; EU-US Data Privacy Framework.

ABSTRACT:

In an increasingly digital and interconnected society, the protection of personal data has become a fundamental legal challenge, particularly due to the tension between the protection of fundamental rights and the security needs of States. While the European Union regards data protection as a fundamental right developed through the GDPR, the United States maintains a more fragmented and sectoral model, with broad powers of access to information for national security purposes. These differences became more evident after the September 11 attacks and the revelations of mass surveillance in 2013, which led the Court of Justice of the European Union to invalidate the Safe Harbor and Privacy Shield agreements on the grounds that they did not guarantee a level of protection equivalent to the European one. In response, the EU–US Data Privacy Framework was adopted in 2023 with the aim of strengthening safeguards for international data transfers and restoring trust in transatlantic data flows, although its adequacy remains under debate. In this context, the question arises as to whether this new framework is truly capable of guaranteeing a level of protection equivalent to that required under European Union law.

Keywords: Data protection; international data transfers; GDPR; European Union; United States; privacy; Schrems I; Schrems II; EU–US Data Privacy Framework.

A mis padres, por la confianza con la que me hicieron crecer.

Y a mí, por estar a la altura.

1.Introducción

2. Protección de datos y soberanía digital

2.1. Concepto y evolución del derecho a la protección de datos

2.2. Soberanía digital

3. Régimen europeo de protección de datos personales

3.1. Principios del RGPD

- a) Legalidad, equidad y transparencia
- b) Limitación de la finalidad
- c) Minimización de datos
- d) Exactitud
- e) Limitación del plazo de conservación
- f) Integridad y confidencialidad (seguridad)
- g) Responsabilidad proactiva (accountability)

3.2. Derechos del interesado

- 3.2.1. Introducción y marco normativo
- 3.2.2. Derecho de acceso
- 3.2.3. Derecho de rectificación
- 3.2.4. Derecho de supresión (“derecho al olvido”)
- 3.2.5. Derecho a la limitación del tratamiento
- 3.2.6. Derecho a la portabilidad
- 3.2.7. Derecho de oposición
- 3.2.8. Derecho a no ser objeto de decisiones automatizadas

3.3. Transferencias internacionales de datos

4. El marco jurídico de protección de datos en EE. UU.

4.1. Falta de ley federal general

4.1.2. Regulación sectorial

4.2. Papel de las agencias federales y estatales

- 4.2.1. El nivel federal y el papel de la Federal Trade Commission
- 4.2.2. El nivel estatal y la fragmentación territorial
- 4.2.3. Límites estructurales del modelo estadounidense

4.3 El papel regulador de los Estados ante la ausencia de una ley federal

4.3.1. California: la California Privacy Rights Act (CPRA)

4.4. El acceso de las autoridades públicas a los datos por razones de seguridad nacional

- 4.4.1. La sección 702 de la Foreign Intelligence Surveillance Act
- 4.4.2. La Executive Order 12333 y la recopilación masiva de datos
- 4.4.3. Reformas y límites: de la PPD-28 a la Executive Order 14086

5. Conflicto UE–EE. UU.

5.1. Antecedentes: Safe Harbor (2000) y Privacy Shield (2016)

5.2. Jurisprudencia del TJUE: Schrems I (C-362/14) y Schrems II (C-311/18)

- 5.2.1. Schrems I (C-362/14): invalidez del Safe Harbor
- 5.2.2. Schrems II (C-311/18): invalidez del Privacy Shield y control reforzado de las transferencias

6. Conclusión

1.Introducción

El tratamiento y la protección de los datos personales se han convertido en uno de los principales desafíos jurídicos del siglo XXI. En un entorno globalizado e hiperconectado, el flujo transfronterizo de información constituye la base del comercio digital, la comunicación y la innovación tecnológica. Sin embargo, este intercambio masivo de datos plantea importantes tensiones entre la protección de los derechos fundamentales y las necesidades de seguridad y control por parte de los Estados. En este contexto, la Unión Europea ha consolidado un modelo normativo centrado en el reconocimiento de la protección de datos personales como un derecho fundamental, consagrado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea. Por el contrario, el sistema estadounidense mantiene un enfoque sectorial y fragmentado, sin una ley federal general de protección de datos, en el que la privacidad se concibe predominantemente como un interés comercial o de consumo más que como un derecho fundamental.

Esta divergencia de modelos se intensificó tras los atentados del 11 de septiembre de 2001, que marcaron un punto de inflexión en la política de seguridad de Estados Unidos. La aprobación de la USA PATRIOT Act y las sucesivas reformas de la Foreign Intelligence Surveillance Act (FISA) otorgaron amplias facultades a las agencias de inteligencia para acceder a datos personales, incluidos los de ciudadanos extranjeros, sin garantías judiciales efectivas equiparables a las exigidas en el ordenamiento europeo. Esta legislación reforzó un paradigma de vigilancia preventiva y debilitó las salvaguardas tradicionales en materia de privacidad.

Las consecuencias de este giro legislativo se manifestaron a nivel internacional cuando, en 2013, las revelaciones de Edward Snowden sobre los programas de vigilancia masiva desarrollados por la National Security Agency (NSA), en particular PRISM y UPSTREAM, evidenciaron el acceso sistemático a datos de usuarios europeos almacenados en servidores situados en Estados Unidos. A raíz de estas revelaciones, el Tribunal de Justicia de la Unión Europea declaró la invalidez del marco Safe Harbor, en la sentencia del Tribunal de Justicia de 6 de octubre de 2015, asunto C-362/14, Maximilian Schrems/Data Protection Commissioner (Schrems I), al considerar que no garantizaba un nivel adecuado de protección frente a las injerencias de las autoridades públicas estadounidenses. Posteriormente, el mismo Tribunal anuló el marco Privacy Shield en la sentencia del Tribunal de

Justicia de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximilian Schrems (Schrems II), al apreciar que la normativa estadounidense no aseguraba un nivel de protección “sustancialmente equivalente” al exigido por el Derecho de la Unión, ni ofrecía a los interesados europeos mecanismos de tutela judicial efectiva.

De este modo, los atentados del 11 de septiembre no solo transformaron la política de seguridad estadounidense, sino que también redefinieron las relaciones transatlánticas en materia de protección de datos, generando un conflicto jurídico y político que continúa vigente en la actualidad. El EU–US Data Privacy Framework, adoptado mediante la Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023, pretende restaurar la confianza mutua en las transferencias internacionales de datos, si bien su suficiencia sigue siendo objeto de debate tanto en la doctrina como en la jurisprudencia europea.

El presente trabajo tiene como objetivo principal **analizar si el nuevo EU–US Data Privacy Framework garantiza una protección adecuada de los datos personales de los ciudadanos europeos**, conforme a los estándares establecidos por el Reglamento (UE) 2016/679, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y valorar si el marco jurídico estadounidense ofrece garantías suficientes para considerar una verdadera adecuación normativa entre ambas jurisdicciones.

Para alcanzar este propósito, el trabajo se estructura en varios objetivos específicos. En primer lugar, examinar los principios fundamentales del derecho a la protección de datos en el marco europeo, con especial atención al Reglamento (UE) 2016/679 y a su regulación de las transferencias internacionales de datos. En segundo lugar, describir y comparar el sistema estadounidense de protección de datos, analizando su enfoque sectorial y la amplitud de las competencias de acceso a la información por parte de las agencias de inteligencia, especialmente tras las reformas adoptadas a raíz de los atentados del 11 de septiembre de 2001. En tercer lugar, estudiar el contenido, la estructura y las garantías del nuevo EU–US Data Privacy Framework, evaluando si este responde a las deficiencias señaladas por el Tribunal de Justicia de la Unión Europea en la sentencia del Tribunal de Justicia de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximilian Schrems (Schrems II). Finalmente, el trabajo busca

valorar si el marco actual permite transferencias internacionales de datos conformes a los estándares europeos de protección de los derechos fundamentales.

De acuerdo con los antecedentes expuestos y los objetivos planteados, la hipótesis de este trabajo sostiene que el nuevo marco EU–US Data Privacy Framework no resuelve de forma suficiente los problemas estructurales detectados en la sentencia del Tribunal de Justicia de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximilian Schrems (Schrems II). A pesar de los avances formales introducidos por el EU–US Data Privacy Framework en comparación con los mecanismos anteriores (Safe Harbor y Privacy Shield), el nuevo acuerdo no solventa de manera estructural ni suficiente las deficiencias jurídicas apreciadas por el Tribunal de Justicia de la Unión Europea en dicha sentencia, lo que compromete su validez a largo plazo, la protección de los derechos de los ciudadanos europeos y lo expone a una eventual nueva invalidación judicial.

El presente trabajo emplea una metodología jurídico-descriptiva y comparada, con el objetivo de analizar la adecuación del nuevo marco transatlántico de transferencias de datos, el EU–US Data Privacy Framework, a los estándares de protección establecidos por el Derecho de la Unión Europea, en particular por el Reglamento (UE) 2016/679 y por la jurisprudencia del Tribunal de Justicia de la Unión Europea. En primer lugar, se aplicará una metodología de análisis jurídico-descriptivo con el fin de exponer de manera sistemática y estructurada los principios, normas y mecanismos jurídicos que regulan la protección de datos personales en la Unión Europea, especialmente en lo que respecta a las transferencias internacionales de datos. Este análisis incluirá los artículos 44 a 50 del Reglamento (UE) 2016/679, así como las disposiciones del nuevo EU–US Data Privacy Framework y la normativa estadounidense relacionada, en particular la Foreign Intelligence Surveillance Act, sección 702, y la Executive Order 12333. En segundo lugar, se desarrollará un estudio jurisprudencial centrado en el análisis de la sentencia del Tribunal de Justicia de 6 de octubre de 2015, asunto C-362/14, Maximilian Schrems/Data Protection Commissioner (Schrems I) y de la sentencia del Tribunal de Justicia de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximilian Schrems (Schrems II), que constituyen hitos fundamentales en el control judicial de la validez de los mecanismos de transferencia de datos entre la Unión Europea y los Estados Unidos. Este análisis se centrará en los razonamientos jurídicos que condujeron a la invalidez de los marcos

Safe Harbor y Privacy Shield, y servirá como base para evaluar críticamente la solidez jurídica del nuevo EU–US Data Privacy Framework. Asimismo, se empleará la técnica del derecho comparado, confrontando el modelo normativo europeo con el estadounidense en cuanto a principios, garantías y mecanismos de tutela de los derechos de los interesados, lo que permitirá identificar las diferencias estructurales entre ambos sistemas, especialmente en lo relativo al acceso a los datos por parte de los poderes públicos, el control judicial y la protección efectiva de los derechos fundamentales.

2. Protección de datos y soberanía digital

2.1. Concepto y evolución del derecho a la protección de datos

El derecho a la protección de datos personales constituye una de las manifestaciones más recientes y, a la vez, más significativas del desarrollo de los derechos fundamentales en las sociedades contemporáneas altamente digitalizadas. Sus raíces doctrinales y jurisprudenciales se vinculan al derecho a la privacidad recogido, entre otros instrumentos, en el artículo 8 del Convenio Europeo de Derechos Humanos, donde se reconoce el derecho de toda persona al respeto de su vida privada y familiar, su domicilio y su correspondencia. En sus primeras formulaciones, la protección de datos no se concebía como un derecho autónomo, sino más bien como una prolongación del derecho a la intimidad, orientada fundamentalmente a evitar injerencias desproporcionadas por parte de los poderes públicos o de entidades privadas, lo que responde a un estadio inicial de desarrollo del derecho marcado por la tutela de la privacidad frente a los riesgos derivados de la informatización incipiente (Simón Marco, 2020: 91–92).

Sin embargo, el progresivo avance de las tecnologías de la información, unido a la proliferación de bases de datos y a la creciente capacidad de tratar grandes volúmenes de información personal, puso de manifiesto las limitaciones de este enfoque inicial. La automatización del tratamiento de datos y la posibilidad de perfilar comportamientos, hábitos o preferencias individuales generaron riesgos cualitativamente nuevos, que exigían respuestas jurídicas más complejas y específicas. En este contexto surgió el concepto de autodeterminación informativa, formulado por el Tribunal Constitucional Federal alemán en la sentencia de 15 de diciembre de 1983, relativa a la Ley del Censo (Volkszählungsurteil), BVerfGE 65, 1, en la que se afirmó que el individuo debe conservar la capacidad de decidir sobre el uso y la difusión de su información personal. Esta doctrina ejerció una influencia decisiva en la evolución posterior del derecho europeo de protección de datos.

En el ámbito de la Unión Europea, el reconocimiento del derecho a la protección de datos como derecho fundamental autónomo se consolidó con el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que lo distingue expresamente del derecho al respeto de la vida privada y familiar recogido en el artículo 7. Esta disposición incorpora principios esenciales como

la licitud, la lealtad, la exactitud y la limitación de la finalidad en el tratamiento de los datos, así como derechos específicos de los interesados, entre ellos el acceso, la rectificación y la supresión. De este modo, la Unión Europea configuró progresivamente un derecho propio, estructurado en torno a las ideas de control individual y transparencia en el uso de la información personal.

La entrada en vigor del Reglamento (UE) 2016/679, de 27 de abril, supuso, en la práctica, un cambio estructural profundo en el modelo europeo de protección de datos. Este Reglamento, aplicable desde mayo de 2018, estableció un marco jurídico armonizado para todos los Estados miembros y reforzó de manera significativa la posición jurídica de los ciudadanos frente al tratamiento de sus datos personales. Entre sus aportaciones más relevantes cabe destacar la creación de la figura del Delegado de Protección de Datos, prevista en los artículos 37 a 39 del Reglamento (UE) 2016/679; la generalización de las evaluaciones de impacto relativas a la protección de datos, contempladas en el artículo 35 del Reglamento (UE) 2016/679; y la consagración del principio de responsabilidad proactiva, recogido en el artículo 5.2 del Reglamento (UE) 2016/679, que obliga a los responsables del tratamiento no solo a cumplir la normativa, sino también a poder demostrar dicho cumplimiento.

Uno de los ámbitos más complejos y controvertidos del Reglamento (UE) 2016/679 es el relativo a las transferencias internacionales de datos. Conforme a los artículos 44 a 50 del Reglamento (UE) 2016/679, los datos personales solo pueden transferirse fuera de la Unión Europea si el país de destino garantiza un nivel de protección esencialmente equivalente al ofrecido en el ordenamiento europeo o si existen garantías adecuadas, como las cláusulas contractuales tipo.

Las sentencias Schrems I y Schrems II han resultado determinantes para la configuración contemporánea del derecho europeo de protección de datos. En la sentencia del Tribunal de Justicia de 6 de octubre de 2015, Maximilian Schrems contra Data Protection Commissioner, asunto C-362/14, ECLI:EU:C:2015:650, el Tribunal declaró inválido el acuerdo Safe Harbor al considerar que no ofrecía garantías suficientes frente al acceso indiscriminado a los datos personales por parte de las autoridades estadounidenses. Posteriormente, en la sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Ltd y Maximilian Schrems, asunto C-311/18, ECLI:EU:C:2020:559, el Tribunal anuló el Privacy Shield por razones sustancialmente similares, poniendo de relieve que la normativa estadounidense permite accesos desproporcionados a los datos y carece de mecanismos de recurso efectivos para los ciudadanos

europeos. Estas decisiones confirman que la protección de datos trasciende la mera defensa de la intimidad y se proyecta sobre la libertad personal y el control efectivo de la información propia.

El derecho a la protección de datos ha adquirido, además, una dimensión especialmente relevante en el contexto social europeo actual, hasta el punto de convertirse en un presupuesto indispensable para la autonomía individual en la era digital. La Comisión Europea, en el Libro Blanco sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza, COM(2020) 65 final, ha subrayado que la garantía efectiva de este derecho resulta esencial para que los ciudadanos puedan participar en la vida digital de forma libre e informada. Principios como la transparencia, la minimización de datos o la limitación de la finalidad pretenden evitar que la persona quede reducida a un mero objeto de análisis automatizado, reforzando así la idea de autodeterminación informativa, tal y como destaca la doctrina al analizar el modelo europeo de protección de datos como un sistema centrado en el control del individuo sobre su información personal (Palacios González, 2012: 62–63).

La expansión del big data, el perfilado masivo y el uso creciente de sistemas de inteligencia artificial han planteado, asimismo, desafíos adicionales. Estas tecnologías permiten inferir información altamente sensible a partir de datos aparentemente neutros, lo que obliga a interpretar el derecho fundamental a la protección de datos desde una perspectiva dinámica y evolutiva. Parte de la doctrina ha advertido del riesgo de discriminaciones invisibles derivadas de decisiones algorítmicas opacas, especialmente cuando los procesos automatizados carecen de transparencia y control efectivo (Wachter, Mittelstadt y Floridi, 2017: 76–78). El Reglamento (UE) 2016/679, consciente de estas amenazas, incorpora obligaciones como la evaluación de impacto relativa a la protección de datos, prevista en su artículo 35, y la adopción de medidas técnicas y organizativas adecuadas, recordando que la protección de datos debe adaptarse de forma constante a los avances tecnológicos. En esta línea, el propio Tribunal de Justicia, en la citada sentencia de 16 de julio de 2020 (asunto C-311/18), ha subrayado que la protección de datos debe preservar la esencia del artículo 8 de la Carta incluso frente a tratamientos masivos o altamente automatizados.

La relación entre protección de datos y soberanía digital resulta cada vez más evidente. En un contexto marcado por la circulación transfronteriza permanente de información, la capacidad de la Unión Europea para garantizar que los derechos de sus ciudadanos sean respetados más allá de sus fronteras constituye un elemento central de su autonomía normativa. Los casos Schrems pusieron de

relieve la necesidad de contar con instituciones sólidas y con instrumentos jurídicos eficaces que permitan hacer valer los principios europeos incluso frente a grandes potencias tecnológicas globales, como ha señalado la doctrina española al analizar el impacto estructural de dichas sentencias sobre el régimen de transferencias internacionales de datos (De Miguel Asensio, 2015: 7).

El derecho a la protección de datos se ha consolidado, así, como uno de los pilares de la ciudadanía digital europea. Ya no opera únicamente como una garantía defensiva frente a injerencias externas, sino como un derecho que empodera activamente a las personas, permitiéndoles intervenir, controlar y exigir responsabilidad en relación con el uso de su información personal. Este derecho actúa como un contrapeso esencial frente a dinámicas de vigilancia y concentración de poder, y contribuye a mantener el equilibrio entre innovación tecnológica y respeto de los derechos fundamentales. El Supervisor Europeo de Protección de Datos ha insistido en esta idea al afirmar que los procesos de digitalización solo resultan legítimos cuando se desarrollan con transparencia, control judicial efectivo y mecanismos adecuados de supervisión institucional, en su Estrategia “Shaping a Safer Digital Future”, de 2020.

2.2. Soberanía digital

El concepto de soberanía digital alude a la capacidad de los Estados y de entidades supranacionales, como la Unión Europea, para ejercer un control efectivo sobre su infraestructura digital, sus sistemas tecnológicos y los datos que circulan dentro y fuera de su territorio. Se trata de una noción con una marcada dimensión política y jurídica, que adquiere especial relevancia en un contexto caracterizado por la globalización tecnológica y por la creciente concentración de poder en manos de un número reducido de grandes plataformas digitales, muchas de ellas con sede en Estados Unidos.

No obstante, la soberanía digital no constituye un concepto unívoco. Como señala Robles Carrillo, se trata de una categoría compleja que integra dimensiones normativas, tecnológicas y políticas, y que se vincula con la capacidad de la Unión Europea para organizar su modelo digital conforme a sus propios valores y principios jurídicos (Robles Carrillo, 2023: 133-135). En este sentido, no se limita a la producción normativa, sino que implica también una capacidad real de actuación autónoma en el entorno digital.

Esta noción comprende distintas dimensiones interrelacionadas, entre las que destacan el control sobre infraestructuras críticas, la regulación de los servicios digitales, la seguridad de los sistemas de información y, de manera especialmente relevante, la gobernanza de los datos personales. Desde la perspectiva del Derecho de la Unión, estas dimensiones se conectan directamente con la garantía de los derechos fundamentales, en particular con el derecho a la protección de datos reconocido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

En esta línea, la Estrategia Digital Europea subraya la necesidad de que Europa pueda definir su propio modelo digital conforme a sus valores. Uno de los principales factores que ha puesto en cuestión la soberanía digital europea es la existencia de marcos normativos en terceros Estados que permiten el acceso extraterritorial a datos personales. En particular, el CLOUD Act estadounidense ha evidenciado los límites del control europeo cuando los datos son tratados por empresas sometidas a jurisdicciones extranjeras. Esta situación plantea dudas relevantes sobre la protección efectiva de los datos de ciudadanos europeos, especialmente cuando pueden ser objeto de acceso por parte de autoridades públicas sin garantías equivalentes a las exigidas en el Derecho de la Unión.

Esta problemática conecta directamente con el conflicto jurídico entre la Unión Europea y Estados Unidos en materia de transferencias internacionales de datos. De Miguel Asensio señala que uno de los elementos centrales en la invalidez del sistema de Safe Harbor fue precisamente la posibilidad de acceso a los datos por parte de las autoridades estadounidenses sin límites adecuados ni mecanismos efectivos de tutela judicial (De Miguel Asensio, 2015: 8-9). En la misma línea, Schwartz y Peifer destacan que la divergencia entre ambos ordenamientos responde a diferencias estructurales, dado que la Unión Europea concibe la protección de datos como un derecho fundamental, mientras que en Estados Unidos predomina un enfoque sectorial y fragmentado (Schwartz & Peifer, 2017: 117-120).

Ante este escenario, la Unión Europea ha impulsado diversas iniciativas dirigidas a reforzar su autonomía digital. Entre ellas destacan el Reglamento de Servicios Digitales (DSA) y el Reglamento de Mercados Digitales (DMA), que introducen obligaciones reforzadas de transparencia, responsabilidad y control sobre las grandes plataformas digitales. Como señala Barrio Andrés, estos instrumentos forman parte de un esfuerzo más amplio por incrementar la supervisión pública sobre el

ecosistema digital y corregir los desequilibrios generados por los grandes operadores tecnológicos (Barrio Andrés, 2022: 2-3).

Sin embargo, estos avances normativos conviven con una limitación estructural relevante. La Unión Europea se ha consolidado como una potencia reguladora en el ámbito digital, pero no como una potencia tecnológica en sentido estricto. Como señalan Hobbs y Torreblanca, Europa ha destacado por su capacidad para establecer reglas, pero continúa rezagada en el desarrollo de infraestructuras y empresas tecnológicas capaces de competir a escala global (Hobbs & Torreblanca, 2020). Esta asimetría condiciona la efectividad de su modelo jurídico, ya que muchos tratamientos de datos dependen de tecnologías desarrolladas fuera de su ámbito de control.

Desde esta perspectiva, la soberanía digital no puede entenderse únicamente como una cuestión normativa. La existencia de un marco jurídico avanzado no resulta suficiente si no va acompañada de una capacidad material que permita garantizar su aplicación efectiva. En este sentido, la soberanía digital implica la capacidad de la Unión para proteger los derechos fundamentales de sus ciudadanos incluso en un entorno globalizado y tecnológicamente interdependiente.

En definitiva, la soberanía digital europea se configura como una condición necesaria para preservar la autonomía normativa de la Unión y garantizar la efectividad de los derechos fundamentales en la era digital. No se trata de promover un aislamiento tecnológico, sino de asegurar que el desarrollo y uso de las tecnologías digitales se produzca dentro de un marco democrático y respetuoso con los valores del ordenamiento europeo.

3. Régimen europeo de protección de datos personales

3.1. Principios del RGPD

El Reglamento General de Protección de Datos constituye uno de los pilares esenciales del sistema europeo de protección de datos. El artículo 5 del Reglamento (UE) 2016/679 recoge un conjunto de principios que orientan todo tratamiento de datos personales y que reflejan la concepción europea del individuo como sujeto autónomo, digno y con capacidad de decidir sobre su información, tal y como ha puesto de relieve la doctrina española al analizar el modelo europeo de protección de datos desde una perspectiva de derechos fundamentales (Palacios González, 2012: 62–63). Esta estructura normativa se inserta en un marco más amplio de derechos, especialmente los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que consagran la protección de datos como un derecho autónomo. La Comisión Europea, en el Libro Blanco sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza, COM(2020) 65 final, ha recordado que estos principios no se limitan a ordenar un proceso técnico, sino que cumplen una función profundamente democrática, al permitir que las personas participen en el entorno digital con confianza y transparencia.

a) Legalidad, equidad y transparencia

Este primer principio exige que cualquier tratamiento se base en una de las condiciones de licitud previstas en el artículo 6 del Reglamento (UE) 2016/679, como el consentimiento del interesado, el cumplimiento de una obligación legal, el interés legítimo, la necesidad contractual o el ejercicio de una tarea realizada en interés público, y que dicho tratamiento sea leal, evitando prácticas engañosas o sorpresivas. La transparencia, por su parte, obliga a informar de manera clara, accesible y comprensible sobre la finalidad del tratamiento, los destinatarios, los plazos de conservación o los derechos del interesado, de conformidad con el artículo 5.1.a del Reglamento (UE) 2016/679. La doctrina ha subrayado que la transparencia constituye un elemento esencial para que el interesado pueda ejercer un control efectivo sobre su información personal (Palacios González, 2012: 64). En el ámbito de las instituciones públicas, como universidades o administraciones, ello implica diseñar

políticas de privacidad comprensibles y procesos informativos que permitan a la ciudadanía conocer de forma efectiva qué sucede con sus datos personales.

b) Limitación de la finalidad

El Reglamento General de Protección de Datos exige que los datos personales se utilicen únicamente para los fines concretos para los que fueron recogidos y que dichos fines sean legítimos, específicos y explícitos. El artículo 5.1.b del Reglamento (UE) 2016/679 impide la reutilización de los datos para propósitos incompatibles, salvo supuestos específicos como los fines de archivo en interés público, la investigación científica o los fines estadísticos, siempre que se apliquen las garantías adecuadas, conforme al artículo 89 del Reglamento (UE) 2016/679. Este principio responde a una idea fundamental del sistema europeo: el control sobre la finalidad del tratamiento constituye un mecanismo central para evitar la expansión ilimitada y no justificada del uso de la información personal.

c) Minimización de datos

El principio de minimización obliga a limitar la recogida de datos a aquellos que sean adecuados, pertinentes y estrictamente necesarios para cumplir la finalidad prevista. Este principio se encuentra estrechamente vinculado con la proporcionalidad y con la prevención de riesgos innecesarios derivados del tratamiento masivo de información personal. La doctrina ha advertido que la recopilación excesiva de datos incrementa significativamente el riesgo de perfilado indebido y de discriminaciones invisibles derivadas de decisiones automatizadas (Wachter, Mittelstadt y Floridi, 2017: 76–78). En la práctica, la minimización exige revisar de manera crítica los formularios, eliminar campos superfluos y cuestionar si cada dato solicitado resulta realmente imprescindible para la finalidad perseguida.

d) Exactitud

El principio de exactitud garantiza que los datos personales sean correctos y estén actualizados. El artículo 5.1.d del Reglamento (UE) 2016/679 exige adoptar todas las medidas razonables para rectificar o suprimir sin demora la información inexacta, en conexión con el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679. La relevancia de este principio fue

subrayada por el Tribunal de Justicia de la Unión Europea en la sentencia de 20 de diciembre de 2017, Peter Nowak contra Data Protection Commissioner, asunto C-434/16, en la que se reconoció que incluso un examen corregido puede constituir un dato personal y que cualquier error factual puede afectar directamente a los derechos del interesado. Este pronunciamiento evidencia que la exactitud no es un mero formalismo administrativo, sino una garantía sustantiva vinculada a la equidad, a la buena administración y a la protección efectiva de los derechos fundamentales.

e) Limitación del plazo de conservación

El Reglamento General de Protección de Datos impone que los datos personales no se conserven más tiempo del necesario para la finalidad del tratamiento. El considerando 39 del Reglamento (UE) 2016/679 recuerda que los plazos de conservación deben limitarse a lo estrictamente necesario, mientras que el artículo 5.1.e del Reglamento (UE) 2016/679 exige suprimir o anonimizar los datos personales cuando dejan de ser útiles para la finalidad inicial. La aplicación de este principio implica definir políticas internas de conservación, establecer calendarios de supresión y realizar revisiones periódicas, evitando la acumulación de datos personales que ya no cumplen una función legítima desde la perspectiva del derecho fundamental a la protección de datos.

f) Integridad y confidencialidad (seguridad)

La seguridad constituye un elemento esencial para proteger los datos personales frente a accesos no autorizados, alteraciones ilícitas o pérdidas accidentales. El artículo 32 del Reglamento (UE) 2016/679 obliga a los responsables del tratamiento a adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, tales como el cifrado, la seudonimización, los controles de acceso, las auditorías de seguridad o los planes de contingencia. El Supervisor Europeo de Protección de Datos ha advertido que, sin un nivel adecuado de seguridad, no puede hablarse de una protección efectiva del derecho fundamental a la protección de datos, en su Opinión 1/2020 sobre la Estrategia Europea de Datos. Este principio adquiere especial relevancia en ámbitos como el educativo, el sanitario o el administrativo, en los que se tratan categorías especiales de datos personales o información especialmente sensible.

g) Responsabilidad proactiva (accountability)

La responsabilidad proactiva constituye uno de los elementos vertebradores del Reglamento General de Protección de Datos. El artículo 5.2 del Reglamento (UE) 2016/679 exige que el responsable del tratamiento no solo cumpla la normativa, sino que sea capaz de demostrar dicho cumplimiento. Este principio implica un cambio de enfoque respecto de modelos anteriores, al desplazar la protección de datos desde una lógica meramente reactiva hacia una obligación permanente de diligencia, planificación y control por parte del responsable.

En la práctica, la responsabilidad proactiva exige la adopción de medidas organizativas y documentales que permitan acreditar el respeto efectivo de los principios del RGPD. Entre ellas se incluyen la llevanza de registros de las actividades de tratamiento, conforme al artículo 30 del Reglamento (UE) 2016/679, la realización de evaluaciones de impacto relativas a la protección de datos cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, según lo dispuesto en el artículo 35 del Reglamento (UE) 2016/679, la revisión periódica de los protocolos internos y la formación del personal. Asimismo, en los supuestos legalmente previstos, resulta obligatoria la designación de un Delegado de Protección de Datos, de acuerdo con el artículo 37 del Reglamento (UE) 2016/679. De este modo, el principio de responsabilidad proactiva transforma el régimen jurídico de protección de datos en un sistema dinámico que exige una supervisión continua y una mejora constante de las prácticas organizativas, con el objetivo de garantizar una protección efectiva y demostrable del derecho fundamental a la protección de datos personales.

Los principios del Reglamento General de Protección de Datos no se comprenden plenamente sin atender al papel de las autoridades de control. El Comité Europeo de Protección de Datos, la Agencia Española de Protección de Datos y la Autoritat Catalana de Protecció de Dades desempeñan funciones esenciales de supervisión, interpretación y garantía de una aplicación coherente del Reglamento (UE) 2016/679 en sus respectivos ámbitos de competencia. Las directrices adoptadas por el Comité Europeo de Protección de Datos, en particular, contribuyen a aclarar la interpretación de conceptos clave como el consentimiento, la minimización de datos o la evaluación de impacto relativa a la protección de datos, convirtiéndose en instrumentos fundamentales para asegurar una aplicación homogénea del Derecho de la Unión. En conjunto, estos principios funcionan como un sistema integrado que sitúa a la persona en el centro de todo tratamiento de datos personales. En

universidades, administraciones públicas y demás entidades del sector público, su correcta aplicación no supone únicamente cumplir con la ley, sino promover un entorno digital seguro, fiable y respetuoso con los derechos fundamentales.

3.2. Derechos del interesado

3.2.1. Introducción y marco normativo

El Reglamento General de Protección de Datos reconoce a los interesados un conjunto de derechos que constituyen la dimensión más tangible del derecho fundamental a la protección de datos. Estos derechos, recogidos en los artículos 12 a 22 del Reglamento (UE) 2016/679, permiten que la persona sea algo más que un sujeto pasivo frente al tratamiento de su información personal, convirtiéndola en protagonista del proceso y reforzando la idea de autodeterminación informativa que inspira el modelo europeo, tal y como se desprende de la propia configuración normativa del RGPD y de su orientación hacia el control efectivo del interesado sobre sus datos. Su fundamento jurídico se encuentra en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, que dotan al derecho a la protección de datos de autonomía conceptual y de un estatus constitucional dentro del ordenamiento jurídico de la Unión.

La finalidad de estos derechos es doble: por un lado, permitir que el individuo conserve el control sobre su información personal y, por otro, asegurar que los principios establecidos en el artículo 5 del Reglamento (UE) 2016/679 se respeten de manera efectiva a lo largo de todo el ciclo del tratamiento. La Agencia Española de Protección de Datos ha destacado que el ejercicio de los derechos de los interesados constituye un elemento esencial para garantizar la efectividad práctica del RGPD y para reforzar la confianza de la ciudadanía en el entorno digital. El ejercicio de estos derechos es gratuito, salvo en los supuestos de solicitudes manifiestamente infundadas o excesivas, conforme a lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679, y debe resolverse en el plazo máximo de un mes, prorrogable cuando la solicitud sea especialmente compleja. En la práctica, estos derechos constituyen la principal vía a través de la cual las personas pueden comprobar, rectificar, suprimir o limitar el impacto del tratamiento de sus datos personales en su vida cotidiana.

3.2.2. Derecho de acceso

El derecho de acceso, regulado en el artículo 15 del Reglamento (UE) 2016/679, permite al interesado conocer si sus datos personales están siendo objeto de tratamiento y, en caso afirmativo, obtener una copia de dichos datos junto con información esencial sobre el tratamiento realizado. Esta información comprende, entre otros extremos, la finalidad del tratamiento, las categorías de datos personales tratados, los destinatarios o categorías de destinatarios, el plazo previsto de conservación, la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y las garantías aplicables en caso de transferencias internacionales de datos.

Este derecho posee un marcado carácter empoderador, ya que permite al individuo comprender qué datos existen sobre él, cómo se han obtenido y con qué lógica se utilizan. Un ejemplo cotidiano sería el de una estudiante que solicita a su universidad una copia de su expediente académico o de comunicaciones administrativas que contengan sus datos personales. La jurisprudencia del Tribunal de Justicia de la Unión Europea ha contribuido a reforzar una interpretación amplia del derecho de acceso; en particular, la sentencia de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak contra Data Protection Commissioner, reconoció que incluso los comentarios de un examinador constituyen datos personales, confirmando así que el ámbito de protección del RGPD no se limita a información puramente objetiva, sino que incluye también valoraciones y apreciaciones vinculadas a una persona identificada o identificable.

3.2.3. Derecho de rectificación

El derecho de rectificación, reconocido en el artículo 16 del Reglamento (UE) 2016/679, permite al interesado obtener sin dilación indebida la corrección de los datos personales inexactos que le conciernan, así como la actualización o completación de aquellos datos que resulten incompletos. Este derecho no se limita a la subsanación de errores manifiestos, sino que incluye también la modificación de información que, como consecuencia del transcurso del tiempo, haya dejado de reflejar fielmente la situación real del interesado. Un ejemplo habitual es la actualización del domicilio de un paciente o de un estudiante, con el fin de garantizar que las comunicaciones y notificaciones oficiales se practiquen correctamente.

La efectividad de este derecho exige que los responsables del tratamiento adopten procedimientos internos adecuados para garantizar la exactitud de los datos personales. El Comité Europeo de

Protección de Datos ha subrayado que los responsables deben implementar medidas organizativas que permitan la revisión y actualización periódica de la información tratada, así como mecanismos de verificación cuando resulte necesario, en sus directrices interpretativas sobre los derechos de los interesados. De este modo, el derecho de rectificación se configura como una garantía esencial para evitar perjuicios derivados del uso de información errónea y para asegurar un tratamiento leal y conforme a los principios del Reglamento (UE) 2016/679.

3.2.4. Derecho de supresión (“derecho al olvido”)

El derecho de supresión, previsto en el artículo 17 del Reglamento (UE) 2016/679, permite al interesado solicitar la eliminación de sus datos personales cuando estos ya no sean necesarios para la finalidad para la que fueron recogidos, cuando se haya retirado el consentimiento en el que se basaba el tratamiento, cuando este resulte ilícito o cuando exista una obligación legal de proceder a su supresión. Su manifestación más conocida es el denominado “derecho al olvido digital”, consolidado por la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, asunto C-131/12, que impuso a los motores de búsqueda la obligación de desindexar contenidos cuando su difusión resulte incompatible con los derechos fundamentales del interesado.

Un ejemplo práctico de aplicación de este derecho sería la retirada de fotografías personales publicadas en un blog institucional una vez finalizado un proyecto concreto, especialmente cuando las personas afectadas consideran que ya no existe una razón legítima que justifique el mantenimiento de dicha información accesible de forma pública.

3.2.5. Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento, reconocido en el artículo 18 del Reglamento (UE) 2016/679, permite conservar los datos personales sin que sean objeto de tratamiento activo más allá de lo estrictamente necesario. Este derecho actúa como una suerte de suspensión temporal del tratamiento, aplicable en aquellos supuestos en los que el interesado considera que existe un problema en relación con sus datos personales, pero no desea o no procede su supresión inmediata.

Los supuestos más habituales de ejercicio de este derecho incluyen la impugnación de la exactitud de los datos personales, el tratamiento ilícito cuando el interesado se opone a la supresión, o la necesidad de conservar los datos para la formulación, el ejercicio o la defensa de reclamaciones legales. Un ejemplo ilustrativo sería la limitación temporal del tratamiento de un expediente académico mientras se resuelve un recurso administrativo relativo a su contenido, impidiendo su utilización para otros fines durante dicho periodo.

3.2.6. Derecho a la portabilidad

El derecho a la portabilidad de los datos, reconocido en el artículo 20 del Reglamento (UE) 2016/679, permite al interesado recibir los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica, así como transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado inicialmente. La finalidad de este derecho es facilitar la movilidad de los usuarios y reforzar su control sobre la información personal, reduciendo situaciones de dependencia tecnológica o institucional.

Este derecho resulta aplicable únicamente cuando el tratamiento se basa en el consentimiento del interesado o en la ejecución de un contrato y se realiza por medios automatizados, de conformidad con lo dispuesto en el artículo 20.1 del Reglamento (UE) 2016/679. Un ejemplo práctico de su ejercicio sería la transferencia del historial académico de un estudiante entre universidades europeas en el marco de un programa de movilidad como Erasmus+, siempre que el tratamiento de dichos datos se lleve a cabo de forma automatizada y con base en una relación contractual o en el consentimiento del interesado.

3.2.7. Derecho de oposición

El derecho de oposición permite al interesado oponerse al tratamiento de sus datos personales cuando este se base en el cumplimiento de una misión realizada en interés público o en el interés legítimo del responsable del tratamiento. Este derecho se reconoce en el artículo 21 del Reglamento (UE) 2016/679 y exige que la oposición se fundamente en motivos relacionados con la situación particular del interesado. En estos casos, el responsable deberá cesar en el tratamiento de los datos personales, salvo que acredite la existencia de motivos legítimos imperiosos que prevalezcan sobre

los intereses, derechos y libertades del interesado, o que el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.

Este derecho adquiere un carácter absoluto cuando el tratamiento tenga por finalidad el marketing directo, ya que basta con que el interesado manifieste su oposición para que los datos personales no puedan seguir utilizándose con fines publicitarios, conforme a lo dispuesto en el artículo 21.2 del Reglamento (UE) 2016/679. Un ejemplo práctico sería el de un trabajador que se opone a que su empresa utilice sus datos personales para la elaboración de perfiles automatizados de productividad basados en intereses legítimos de la organización, obligando al responsable a interrumpir dicho tratamiento salvo que concurran razones legalmente justificadas.

3.2.8. Derecho a no ser objeto de decisiones automatizadas

El derecho a no ser objeto de decisiones individuales automatizadas se reconoce en el artículo 22 del Reglamento (UE) 2016/679, y permite al interesado no quedar sujeto a decisiones basadas exclusivamente en el tratamiento automatizado de datos personales, incluido el perfilado, cuando dichas decisiones produzcan efectos jurídicos sobre la persona o le afecten significativamente de modo similar. Este derecho tiene como finalidad evitar que decisiones relevantes (como la concesión de un préstamo, la admisión a un puesto de trabajo o una evaluación laboral) se adopten sin una intervención humana significativa que permita valorar las circunstancias concretas del caso.

Aunque el propio Reglamento prevé determinadas excepciones, como los supuestos en los que la decisión sea necesaria para la ejecución de un contrato, esté autorizada por el Derecho de la Unión o de los Estados miembros, o se base en el consentimiento explícito del interesado, estas excepciones deben ir acompañadas de garantías adecuadas para proteger los derechos y libertades de la persona afectada, tales como el derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión.

La relevancia de este derecho ha sido confirmada recientemente por el Tribunal de Justicia de la Unión Europea en la sentencia de 7 de diciembre de 2023, Schufa Holding AG, asunto C-634/21, en la que el Tribunal subrayó la necesidad de un control especialmente riguroso de los sistemas de evaluación crediticia automatizada, advirtiendo de los riesgos de resultados injustos o

discriminatorios cuando decisiones de impacto significativo se adoptan sin salvaguardias suficientes ni supervisión humana efectiva.

3.3. Transferencias internacionales de datos

En la sociedad digital contemporánea, la circulación transfronteriza de información se ha convertido en una práctica habitual y, en muchos sectores, prácticamente inevitable. El uso generalizado de servicios de computación en la nube, la externalización de funciones tecnológicas o la gestión de plataformas digitales complejas implica, con frecuencia, que los datos personales se transfieran fuera del Espacio Económico Europeo. Esta realidad, aunque funcionalmente necesaria para el funcionamiento de numerosas organizaciones, plantea un riesgo que no puede minimizarse: que la protección de los derechos de las personas se debilite una vez que los datos abandonan el marco jurídico europeo, especialmente cuando se transfieren a entornos normativos menos garantistas.

Consciente de este riesgo, el Reglamento (UE) 2016/679 establece un régimen específico para las transferencias internacionales de datos personales, regulado en los artículos 44 a 50 del Reglamento (UE) 2016/679. La lógica que subyace a este sistema es inequívoca: el hecho de que los datos se transfieran a un tercer país no puede traducirse en una pérdida de protección para el interesado. En este sentido, el RGPD exige que toda transferencia internacional garantice un nivel de protección esencialmente equivalente al existente dentro de la Unión Europea, estándar que no admite interpretaciones meramente formales y que ha sido reafirmado por la jurisprudencia del Tribunal de Justicia de la Unión Europea, en la sentencia de 6 de octubre de 2015, asunto C-362/14, Maximilian Schrems contra Data Protection Commissioner.

Este estándar, lejos de constituir una exigencia abstracta, impone una protección efectiva y real en la práctica. Así lo ha puesto de manifiesto de forma reiterada el Tribunal de Justicia de la Unión Europea, cuya jurisprudencia ha resultado decisiva en la configuración del régimen de transferencias internacionales. En particular, en las sentencias de 6 de octubre de 2015, asunto C-362/14 (Schrems I), y de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner contra Facebook Ireland Ltd y Maximilian Schrems (Schrems II), el Tribunal subrayó que la evaluación del nivel de protección de un tercer país no puede limitarse a un análisis normativo, sino que debe atender también a las prácticas de las autoridades públicas, al alcance de sus poderes de acceso a los datos personales y

a la existencia de mecanismos efectivos de control y tutela judicial. Esta interpretación refuerza la idea de que la protección de datos no se agota en la letra de la ley, sino que depende de su aplicación material.

El punto de partida normativo lo establece el artículo 44 del Reglamento (UE) 2016/679, que opera como una auténtica cláusula general del sistema: toda transferencia de datos personales a un tercer país u organización internacional solo será lícita si el responsable o el encargado del tratamiento cumple las disposiciones del Reglamento y si se preserva el nivel de protección exigido por el Derecho de la Unión. De este modo, el RGPD proyecta sus garantías más allá del territorio europeo, acompañando a los datos personales allí donde se encuentren, lo que evidencia la vocación extraterritorial del modelo europeo de protección de datos.

Sobre esta base, el Reglamento articula un sistema jerarquizado de mecanismos de legitimación. En primer lugar, se sitúan las decisiones de adecuación, previstas en el artículo 45 del Reglamento (UE) 2016/679, que constituyen el instrumento que ofrece mayor seguridad jurídica tanto para los responsables del tratamiento como para los interesados. Mediante este mecanismo, la Comisión Europea declara que un tercer país garantiza un nivel de protección sustancialmente equivalente al europeo, permitiendo así la realización de transferencias internacionales sin necesidad de autorizaciones adicionales. No obstante, la experiencia práctica, especialmente en relación con Estados Unidos, ha puesto de relieve las limitaciones de este instrumento, ya que tanto el Safe Harbor como el Privacy Shield fueron invalidados por el Tribunal de Justicia al no ofrecer garantías suficientes frente al acceso de las autoridades públicas a los datos personales, en las sentencias C-362/14 y C-311/18.

Cuando no existe una decisión de adecuación, el Reglamento General de Protección de Datos permite las transferencias internacionales siempre que se establezcan garantías adecuadas, de conformidad con el artículo 46 del Reglamento (UE) 2016/679. Entre estas garantías destacan las cláusulas contractuales tipo y las normas corporativas vinculantes, instrumentos especialmente relevantes para los grupos empresariales multinacionales. Sin embargo, tras la sentencia Schrems II, el uso de estos mecanismos exige un análisis concreto del marco jurídico del país de destino y, cuando resulte necesario, la adopción de medidas técnicas complementarias (como el cifrado efectivo o la seudonimización) destinadas a mitigar los riesgos derivados de accesos no autorizados.

Esta exigencia introduce una carga adicional de diligencia para los responsables del tratamiento, que ya no pueden apoyarse de forma automática en instrumentos contractuales estandarizados.

Solo de manera excepcional, el artículo 49 del Reglamento (UE) 2016/679 admite determinadas derogaciones que permiten transferencias internacionales sin decisión de adecuación ni garantías específicas, como el consentimiento explícito del interesado o la necesidad de ejecutar un contrato. Estas derogaciones están concebidas para situaciones puntuales y no pueden convertirse en mecanismos habituales para flujos recurrentes de datos personales, tal y como ha subrayado el Comité Europeo de Protección de Datos en sus Directrices 2/2018 sobre las derogaciones del artículo 49 del RGPD, que insisten en una interpretación estricta y restrictiva de estas excepciones.

En la práctica, este régimen plantea desafíos relevantes tanto para organizaciones públicas como privadas, especialmente en un contexto marcado por la concentración tecnológica, la dependencia de proveedores globales y la inestabilidad geopolítica. Garantizar la continuidad de los flujos internacionales de datos resulta imprescindible para el funcionamiento de numerosas actividades económicas y administrativas, pero dicha necesidad no puede prevalecer sobre la exigencia de proteger de forma efectiva el derecho fundamental a la protección de datos personales, que constituye uno de los pilares del ordenamiento jurídico europeo.

4. El marco jurídico de protección de datos en EE. UU.

4.1. Falta de ley federal general

El modelo estadounidense de protección de datos personales se ha desarrollado de forma muy distinta al europeo. Mientras que en la Unión Europea la protección de datos se configura como un derecho fundamental autónomo, en Estados Unidos la privacidad no responde a una construcción unitaria. Como explica Solove, la privacidad debe entenderse como un conjunto de problemas jurídicos diversos que el Derecho aborda de manera fragmentaria según el tipo de daño o riesgo implicado (Solove, 2010:1–6). Esta aproximación ayuda a comprender por qué no existe en Estados Unidos una ley federal general equivalente al Reglamento (UE) 2016/679.

En lugar de una norma transversal aplicable a todo tratamiento de datos personales, el sistema estadounidense se articula a través de leyes sectoriales. La lógica subyacente no es la afirmación abstracta de un derecho fundamental, sino la corrección de prácticas específicas. En este sentido, Solove critica la simplificación del argumento del “nothing to hide”, señalando que reducir la privacidad a la ocultación de conductas ilícitas ignora sus dimensiones estructurales y democráticas (Solove, 2011: 1–3).

Desde una perspectiva comparada, Schwartz y Peifer explican que la diferencia entre ambos sistemas no es meramente técnica, sino conceptual. La Unión Europea ha desarrollado una cultura jurídica basada en el “rights talk”, donde el individuo es concebido como titular de derechos frente al tratamiento de sus datos. En contraste, en Estados Unidos predomina un “marketplace discourse”, centrado en la protección del consumidor dentro del mercado de la información (Schwartz & Peifer, 2017: 121–123). En sus propias palabras, el derecho estadounidense de la privacidad de datos se enfoca en la protección de los “privacy consumers” en un entorno comercial (Schwartz & Peifer, 2017: 122).

Asimismo, Schwartz destaca que el modelo estadounidense descansa en una regulación sectorial y en mecanismos de aplicación reactivos, en lugar de en principios generales coherentes aplicables a todo tratamiento (Schwartz, 2012: 1625–1628). Este enfoque fragmentado explica la centralidad de la

Federal Trade Commission como autoridad que actúa principalmente frente a prácticas engañosas o incumplimientos de compromisos empresariales.

Desde la doctrina europea, Blasi Casagran subraya que el sistema estadounidense responde a una lógica funcional orientada a facilitar los flujos económicos, lo que condiciona su compatibilidad con el estándar europeo de protección “esencialmente equivalente” (Blasi Casagran, 2017:198–201). En términos similares, Sobrino García destaca que la comparación entre ambos modelos debe partir del reconocimiento de sus fundamentos jurídicos distintos, especialmente en lo relativo a la concepción del derecho a la protección de datos (Sobrino García, 2020: 69–73).

En definitiva, la ausencia de una ley federal general en Estados Unidos no constituye simplemente una laguna normativa, sino el reflejo de una tradición jurídica diferente, basada en la regulación sectorial, la autorregulación empresarial y mecanismos de ejecución ex post.

4.1.2. Regulación sectorial

La inexistencia de una ley federal integral no implica, sin embargo, la ausencia de regulación en materia de privacidad y protección de datos en Estados Unidos. El ordenamiento estadounidense ha desarrollado históricamente un enfoque sectorial, articulado a través de normas específicas que protegen determinados tipos de información o sectores económicos concretos. Como señala Barrio Andrés, el marco federal vigente constituye un “intrincado puzle regulatorio” caracterizado por su falta de uniformidad, obsolescencia y deficiente técnica normativa (Barrio Andrés, 2022:186–187).

En efecto, a nivel federal no existe una única ley que regule de forma exhaustiva el uso de los datos personales de los ciudadanos. En su lugar, se han aprobado normas dirigidas a ámbitos específicos. Este modelo se estructura, fundamentalmente, en dos grandes bloques: por un lado, leyes que protegen tipos concretos de información; por otro, legislación sectorial aplicable a determinados sectores económicos (Barrio Andrés, 2022 :187–188).

En el ámbito de la protección de menores en el entorno digital, la Children’s Online Privacy Protection Act (COPPA) regula la recopilación y el tratamiento de datos personales de niños menores de 13 años, imponiendo obligaciones específicas a los operadores de servicios en línea dirigidos a este

colectivo (Barrio Andrés, 2022:187). Se trata de una norma focalizada en una categoría especialmente vulnerable, pero cuyo alcance se limita a ese ámbito concreto.

En materia sanitaria, la Health Insurance Portability and Accountability Act (HIPAA) establece estándares federales para la protección de la información médica confidencial. La norma restringe la divulgación de datos sanitarios identificables y exige medidas de seguridad específicas a hospitales y proveedores de servicios médicos (Barrio Andrés, 2022:188). No obstante, su ámbito subjetivo es limitado, ya que solo se aplica a determinadas entidades cubiertas por la norma, dejando fuera a numerosos actores digitales que también tratan datos de salud.

En el sector financiero, la Gramm-Leach-Bliley Act (GLBA) regula el tratamiento de información personal por parte de bancos e instituciones financieras, incorporando obligaciones de confidencialidad respecto de la denominada “información personal no pública” (Barrio Andrés, 2022: 188). De forma complementaria, la Fair Credit Reporting Act (FCRA) disciplina la recopilación y utilización de información crediticia, reconociendo a los consumidores derechos de acceso y corrección respecto de sus informes de solvencia (Barrio Andrés, 2022: 188).

Por su parte, en el ámbito educativo, la Family Educational Rights and Privacy Act (FERPA) protege los registros académicos de los estudiantes, limitando su divulgación sin consentimiento (Barrio Andrés, 2022: 188). Sin embargo, su ámbito también es sectorial y no cubre otros tratamientos de datos personales que puedan producirse fuera del contexto estrictamente educativo.

Este conjunto normativo confirma que el sistema estadounidense no carece de regulación en materia de privacidad, sino que la articula desde una lógica funcional y sectorial. La protección se activa en función del tipo de dato o del sector implicado, y no a través de un marco general aplicable a todo tratamiento de datos personales. Ello genera una falta de uniformidad que complica el cumplimiento normativo y deja amplias zonas grises en la tutela efectiva de los ciudadanos (Barrio Andrés, 2022: 189–190).

Esta característica estructural explica, en gran medida, las dificultades para alcanzar una convergencia plena con el modelo europeo, basado en una regulación transversal y en la configuración de la protección de datos como derecho fundamental autónomo.

4.2. Papel de las agencias federales y estatales

El sistema estadounidense de protección de datos no solo se caracteriza por la ausencia de una ley federal general, sino también por una estructura institucional descentralizada y sectorial. A diferencia del modelo europeo, que se articula en torno a autoridades de control independientes con competencias generales y funciones preventivas, en Estados Unidos la supervisión del tratamiento de datos se distribuye entre diversas agencias con competencias limitadas al ámbito material que regulan.

Desde una perspectiva comparada, Schwartz y Peifer explican que el sistema estadounidense no se construye sobre una lógica de derechos fundamentales garantizados por una autoridad especializada, sino sobre una estructura regulatoria orientada al mercado, donde la protección de la privacidad se integra dentro del discurso de protección del consumidor (“marketplace discourse”) (Schwartz & Peifer, 2017: 121–122). Esta diferencia conceptual tiene una traducción institucional clara.

4.2.1. El nivel federal y el papel de la Federal Trade Commission

En el plano federal, no existe una autoridad equivalente a las autoridades de control europeas previstas en el RGPD. La protección de los datos personales se encuentra repartida entre agencias sectoriales, pero en la práctica la Federal Trade Commission (FTC) ha asumido un papel central respecto al sector privado.

La intervención de la FTC se fundamenta principalmente en la Section 5 del Federal Trade Commission Act, que le permite actuar frente a prácticas comerciales desleales o engañosas. Como señala Schwartz, la FTC ha construido su actuación en materia de privacidad sobre la base del incumplimiento de compromisos empresariales o de prácticas engañosas, lo que sitúa la protección de datos dentro de la lógica del enforcement del mercado más que dentro de un sistema general de garantías (Schwartz, 2012: 1625–1627).

Este modelo presenta una característica esencial: su naturaleza eminentemente *ex post*. La actuación de la FTC se activa tras la existencia de una infracción o una práctica engañosa, pero no implica un control preventivo sistemático del tratamiento de datos. En este sentido, Solove advierte

que el Derecho estadounidense tiende a reaccionar frente a abusos concretos más que a estructurar un sistema preventivo de protección frente a riesgos sistémicos (Solove, 2011: 21–23).

Desde la doctrina europea, Blasi Casagran destaca que esta forma de supervisión limita la capacidad del sistema estadounidense para garantizar una protección estructural equivalente a la europea, ya que no existe un órgano con competencia general para evaluar de manera preventiva los riesgos derivados del tratamiento masivo de datos (Blasi Casagran, 2017:198–200).

4.2.2. El nivel estatal y la fragmentación territorial

La ausencia de una regulación federal integral ha impulsado la intervención de los Estados federados. La aplicación de las normas estatales suele recaer en los attorneys general, que actúan como autoridades de enforcement en sus respectivos territorios.

Este fenómeno ha generado un marco normativo heterogéneo dentro del propio territorio estadounidense. Como señala Sobrino García, la protección de la privacidad en Estados Unidos se ha desarrollado de forma desigual, dependiendo tanto del sector regulado como del ámbito territorial de aplicación (Sobrino García, 2020:71–73).

Desde la perspectiva comparada, Schwartz y Peifer subrayan que esta pluralidad institucional refuerza el carácter fragmentado del sistema, en contraste con el modelo europeo, que apuesta por una arquitectura institucional coordinada y basada en autoridades independientes (Schwartz & Peifer, 2017:122–123).

La consecuencia práctica es que el nivel de protección puede variar en función del Estado de residencia del interesado y del tipo de actividad desarrollada, lo que dificulta la consolidación de un estándar nacional coherente.

4.2.3. Límites estructurales del modelo estadounidense

Del análisis conjunto del nivel federal y estatal se desprenden varios límites estructurales. En primer lugar, la fragmentación institucional dificulta la aplicación uniforme de estándares de privacidad. En segundo lugar, el predominio del enforcement ex post reduce la capacidad del sistema para anticipar riesgos derivados de tratamientos masivos o automatizados.

En este sentido, Barrio Andrés subraya que el modelo estadounidense carece de instrumentos equivalentes a los mecanismos preventivos europeos, como las evaluaciones de impacto o la supervisión previa de tratamientos de alto riesgo, lo que limita su capacidad para gestionar riesgos estructurales asociados al uso intensivo de datos (Barrio Andrés, 2022: 186–188).

Desde la perspectiva de las transferencias internacionales, esta debilidad institucional resulta especialmente relevante. Como explican Schwartz y Peifer, el debate transatlántico no gira únicamente en torno a normas sustantivas, sino también en torno a la existencia de mecanismos efectivos de supervisión y control (Schwartz & Peifer, 2017: 117). La estructura institucional estadounidense constituye, por tanto, uno de los elementos centrales en la evaluación europea del nivel de protección “esencialmente equivalente”.

4.3 El papel regulador de los Estados ante la ausencia de una ley federal

En ausencia de una ley federal general de protección de datos, los Estados federados han asumido progresivamente la iniciativa regulatoria en materia de privacidad. Según el State Privacy Legislation Tracker de Bloomberg Law (2025), actualmente veinte Estados de los Estados Unidos han promulgado leyes integrales de privacidad de datos (comprehensive data privacy laws), configurando un modelo descentralizado de protección que contrasta con el enfoque uniforme del Reglamento General de Protección de Datos en la Unión Europea.

Entre los Estados que han aprobado legislación integral se encuentran: California, Colorado, Connecticut, Virginia, Utah, Texas, Indiana, Iowa, Montana, Tennessee, Florida, Oregon, Delaware, New Hampshire, New Jersey, Kentucky, Rhode Island, Minnesota, Nebraska y Maryland. Esta expansión normativa refleja una tendencia clara hacia la generalización de derechos del consumidor en materia de privacidad, aunque bajo un enfoque predominantemente comercial y no basado en la configuración de un derecho fundamental autónomo.

No obstante, la proliferación legislativa no ha eliminado la fragmentación estructural del sistema, ya que cada Estado establece criterios propios de aplicación, umbrales cuantitativos, régimen sancionador y autoridades competentes.

A continuación, se analiza de forma más detallada el modelo de California, como referente pionero y más avanzado de la nueva generación de leyes estatales.

4.3.1. California: la California Privacy Rights Act (CPRA)

La California Privacy Rights Act (CPRA), vigente desde el 1 de enero de 2023, constituye una reforma y ampliación de la anterior California Consumer Privacy Act (CCPA) de 2018. Actualmente representa el régimen estatal más desarrollado en materia de privacidad en Estados Unidos y suele considerarse el modelo de referencia dentro del proceso de expansión legislativa estatal.

La CPRA reconoce a los residentes de California una serie de derechos sobre su información personal. Entre ellos se encuentran el derecho a acceder a los datos que les conciernen, a corregir información inexacta, a solicitar la supresión de sus datos personales y a obtener una copia de los mismos. Asimismo, la norma permite a los consumidores oponerse a la venta o compartición de su información personal y limitar el uso de datos personales sensibles. De este modo, se refuerza la posición jurídica del individuo frente a las entidades que recopilan y explotan información en el entorno digital. Junto a la ampliación de los derechos de los consumidores, la CPRA introduce obligaciones adicionales para las empresas, especialmente en materia de transparencia y tratamiento responsable de la información. La ley exige que las entidades informen adecuadamente sobre la recopilación y uso de datos personales y, en determinados supuestos, obtengan el consentimiento del interesado, particularmente cuando se trate de categorías sensibles de información.

Uno de los elementos más significativos de esta reforma es la creación de la California Privacy Protection Agency (CPPA), autoridad administrativa independiente encargada de la supervisión y aplicación de la norma. La existencia de un organismo especializado con potestad sancionadora distingue a California de otros Estados y lo aproxima, en cierta medida, al modelo europeo basado en autoridades independientes de control. No obstante, pese a su mayor sofisticación institucional y a la amplitud de los derechos reconocidos, la CPRA mantiene una lógica centrada en la protección del consumidor dentro del mercado digital. La protección de datos no se configura como un derecho fundamental autónomo, sino como un instrumento de equilibrio en las relaciones entre consumidores y empresas en el ámbito comercial.

4.4. El acceso de las autoridades públicas a los datos por razones de seguridad nacional

Uno de los elementos estructurales que explican la persistente tensión entre el modelo europeo y el estadounidense de protección de datos es el régimen de acceso de las autoridades públicas a la información personal por motivos de seguridad nacional. Desde la perspectiva de la Unión Europea, el problema no radica en la existencia de mecanismos de vigilancia en sí mismos (presentes en todos los Estados democráticos) sino en su alcance material, en la amplitud de las facultades conferidas a los servicios de inteligencia y, especialmente, en la insuficiencia de los mecanismos de control y recurso disponibles para las personas no estadounidenses.

La jurisprudencia del Tribunal de Justicia de la Unión Europea, particularmente en los asuntos Schrems I y Schrems II, ha dejado claro que el estándar exigible para autorizar transferencias internacionales no se limita a la existencia formal de normas de protección, sino que requiere un nivel de tutela “esencialmente equivalente” al garantizado por el Derecho de la Unión. Esta exigencia afecta de manera directa al análisis de la normativa estadounidense en materia de vigilancia (Cañabate Pérez, 2024: 125).

4.4.1. La sección 702 de la Foreign Intelligence Surveillance Act

La Section 702 de la Foreign Intelligence Surveillance Act (FISA) constituye uno de los pilares del sistema de inteligencia estadounidense. Esta disposición permite la recopilación de información dirigida a personas no estadounidenses situadas fuera del territorio de Estados Unidos, cuando la finalidad sea la obtención de inteligencia exterior. Sobre esta base jurídica se han articulado programas como PRISM o UPSTREAM, que permiten acceder a comunicaciones electrónicas gestionadas por grandes proveedores de servicios digitales.

El problema central, desde la óptica europea, reside en que esta vigilancia no se fundamenta en un control judicial individualizado respecto de cada persona afectada, sino en autorizaciones programáticas. Como señalan Rubinstein y Margulies, el control ejercido por el Foreign Intelligence Surveillance Court se centra en la legalidad general del programa y no en la protección individualizada de los derechos de las personas cuyos datos pueden verse afectados (Rubinstein y Margulies, 2022: 389-392). Esta configuración difiere sustancialmente del estándar europeo de necesidad y proporcionalidad, que exige una evaluación concreta y limitada al caso específico.

El Tribunal de Justicia, en *Schrems II*, consideró que la normativa estadounidense no establecía límites suficientemente claros ni proporcionaba garantías efectivas frente al acceso de las autoridades públicas a los datos transferidos desde la Unión. En particular, subrayó la amplitud de las facultades conferidas por la Section 702 FISA y la ausencia de mecanismos efectivos de tutela judicial para los ciudadanos europeos (Dimović, 2024: 89-91).

Desde una perspectiva doctrinal comparada, Blasi Casagran ha destacado que esta configuración normativa responde a una lógica funcional orientada a la seguridad nacional y no a una construcción sistemática basada en la garantía de derechos fundamentales (Blasi Casagran, 2020: 53). Ello explica la dificultad estructural de alcanzar una equivalencia sustancial con el modelo europeo.

4.4.2. La Executive Order 12333 y la recopilación masiva de datos

Junto a la FISA, la Executive Order 12333 constituye otro elemento clave del sistema estadounidense de vigilancia. A diferencia de la Section 702, esta orden ejecutiva regula actividades de inteligencia que se desarrollan fuera del marco del tribunal especializado en vigilancia, lo que implica un nivel de supervisión judicial aún más limitado.

Diversos análisis han puesto de relieve que la Executive Order 12333 permite la recopilación masiva de comunicaciones internacionales mediante técnicas automatizadas, con un filtrado posterior basado en criterios de inteligencia. Este modelo de “bulk collection” ha sido considerado especialmente problemático desde la perspectiva europea, ya que la recopilación se produce con carácter previo a cualquier evaluación individualizada de necesidad (Dimović, 2024: 90-92).

El Tribunal de Justicia consideró que este tipo de recopilación masiva no satisface el principio de proporcionalidad tal como se interpreta en el Derecho de la Unión, en la medida en que no se limita estrictamente a lo necesario para alcanzar un objetivo legítimo (Cañabate Pérez, 2024: 140). La crítica no se dirige únicamente a la amplitud del acceso, sino también a la falta de transparencia y a la dificultad de impugnar estas prácticas desde el exterior.

Como ha señalado Schwartz, la expansión tecnológica de las capacidades de recopilación de datos exige mecanismos de control especialmente robustos para evitar abusos estructurales. Sin embargo,

el modelo estadounidense ha evolucionado históricamente priorizando la flexibilidad operativa de los servicios de inteligencia.

4.4.3. Reformas y límites: de la PPD-28 a la Executive Order 14086

Tras las revelaciones de Edward Snowden, Estados Unidos adoptó la Presidential Policy Directive 28 (PPD-28), que introdujo ciertos principios de minimización y límites en el uso de datos obtenidos mediante vigilancia masiva, incluyendo referencias a la protección de personas no estadounidenses. No obstante, el TJUE consideró en *Schrems II* que estas garantías no eran suficientes, especialmente por la ausencia de un mecanismo de recurso efectivo (Dimović, 2024: 92).

En respuesta a esta situación, la Executive Order 14086, adoptada en 2022, pretende reforzar las salvaguardas aplicables a las actividades de inteligencia. Esta orden incorpora de manera explícita los principios de necesidad y proporcionalidad en la recopilación de señales de inteligencia, estableciendo que dichas actividades deberán limitarse a objetivos legítimos claramente definidos (Dimović, 2024: 92-93).

Además, la orden ejecutiva introduce un mecanismo de recurso en dos niveles: en primer lugar, una revisión por parte de la Civil Liberties Protection Officer (CLPO) y, en segundo lugar, la posibilidad de acudir ante la Data Protection Review Court (DPRC). Este diseño pretende responder a la exigencia europea de ofrecer un recurso efectivo e independiente.

Sin embargo, la doctrina ha mostrado reservas importantes respecto a la efectividad real de este sistema. Dimović subraya que tanto la CLPO como la DPRC se integran en la estructura del poder ejecutivo, lo que suscita dudas sobre su independencia (Dimović, 2024: 96-97). Asimismo, el carácter confidencial de los procedimientos y la posibilidad de emitir respuestas que no confirmen ni nieguen la existencia de vigilancia limitan la transparencia del sistema.

Desde una perspectiva crítica, Cañabate Pérez sostiene que el nuevo marco puede interpretarse como una solución funcional orientada a permitir la continuidad de las transferencias transatlánticas, pero que no altera sustancialmente la lógica estructural del sistema estadounidense de vigilancia (Cañabate Pérez, 2024: 125). En términos similares, Blasi Casagran destaca que mientras no se produzca una reforma legislativa de alcance general que limite estructuralmente las facultades de

acceso por razones de seguridad nacional, la brecha con el modelo europeo persistirá (Blasi Casagran, 2020:56).

5. Conflicto UE–EE. UU.

5.1. Antecedentes: Safe Harbor (2000) y Privacy Shield (2016)

El origen del conflicto jurídico entre la Unión Europea y Estados Unidos en materia de transferencias internacionales de datos personales se encuentra en la distinta concepción que ambos ordenamientos mantienen sobre la protección de datos. En el ámbito europeo, la protección de los datos personales se ha configurado progresivamente como un verdadero derecho fundamental, mientras que en el sistema estadounidense ha prevalecido tradicionalmente un enfoque sectorial y fragmentado. Esta divergencia explica que, desde finales del siglo XX, la transferencia de datos personales desde la Unión Europea a Estados Unidos se convirtiera en un problema jurídico de primer orden, al no existir en este último país un nivel de protección que pudiera considerarse equiparable al europeo (Tulac, 2024: 157).

En este contexto, la Directiva 95/46/CE estableció como regla general que la transferencia de datos personales a un tercer país solo podía llevarse a cabo si este garantizaba un “nivel adecuado de protección”, exigencia que obligaba a la Comisión Europea a valorar las condiciones normativas existentes en el Estado de destino (Ni Loideain, 2016: 8). Precisamente tras esa valoración, la Comisión entendió que Estados Unidos no ofrecía, con carácter general, una protección suficiente, lo que impulsó a ambas partes a negociar una solución específica para permitir los flujos transatlánticos de datos (Tulac, 2024:158). Blasi Casagran subraya que el concepto de “nivel adecuado de protección” introducido por la Directiva 95/46/CE no implica una identidad normativa entre ordenamientos, sino la exigencia de un estándar sustancialmente equivalente que garantice de forma efectiva los derechos fundamentales de los ciudadanos europeos. No obstante, la autora advierte que esta evaluación presenta una elevada complejidad práctica, ya que obliga a valorar no solo las normas formales del tercer Estado, sino también su aplicación efectiva y los mecanismos de control existentes (Blasi Casagran, 2017: 195).

Fruto de esas negociaciones, en el año 2000 se adoptó el sistema conocido como *Safe Harbor*, articulado a través de la Decisión 2000/520/CE. Este mecanismo descansaba sobre un sistema de principios de privacidad al que las empresas estadounidenses podían adherirse voluntariamente mediante autocertificación. Su finalidad era permitir la transferencia de datos personales de

ciudadanos europeos a entidades estadounidenses sin necesidad de autorizaciones adicionales en cada caso, facilitando así el funcionamiento del mercado digital y de los servicios transatlánticos basados en datos (Ni Loideain, 2016:8). En la misma línea, Tulac explica que *Safe Harbor* introdujo reglas destinadas a facilitar el almacenamiento, análisis y utilización en Estados Unidos de datos personales de ciudadanos europeos en el marco de servicios emergentes de la sociedad de la información, como redes sociales o servicios digitales de contenidos (Tulac, 2024:158).

Sin embargo, desde muy pronto comenzaron a manifestarse importantes dudas sobre la solidez real de este sistema. Desde una perspectiva crítica, Blasi Casagran señala que Safe Harbor se configuró como una solución pragmática, pero jurídicamente débil, al basarse en compromisos unilaterales de las empresas estadounidenses sin una supervisión pública equivalente a la existente en la Unión Europea, lo que comprometía la garantía efectiva de los derechos de los interesados (Blasi Casagran, 2017: 198). En esta misma línea, Compagnucci recuerda que el sistema descansaba en gran medida en los “commitments” y en la “self-certification” de las empresas participantes, lo que planteaba problemas evidentes de control y cumplimiento material (Compagnucci, 2024: 6). A ello se añadía la preocupación de que el respeto formal de los principios Safe Harbor resultaba insuficiente para asegurar una protección real en entornos digitales complejos, como ya había advertido el Article 29 Working Party al exigir la incorporación de salvaguardas adicionales (Compagnucci, 2024: 6).

La situación se volvió especialmente crítica tras las revelaciones de Edward Snowden en 2013 sobre los programas de vigilancia masiva desarrollados por la NSA. A partir de ese momento, quedó en evidencia que las autoridades estadounidenses podían acceder a datos personales transferidos desde la Unión Europea mediante programas como PRISM, incluidos aquellos tratados por empresas adheridas a Safe Harbor. En este sentido, Tulac señala que la NSA obtuvo derechos de acceso e interceptación sobre datos mantenidos por dichas empresas, entre ellas Facebook (Tulac, 2024: 158), mientras que Compagnucci destaca que una parte significativa de las compañías certificadas en el marco del sistema aparecía vinculada a programas de vigilancia, lo que contribuyó decisivamente a cuestionar su viabilidad (Compagnucci, 2024: 6). En esta misma línea, Blasi Casagran pone de relieve que estas revelaciones evidenciaron una incompatibilidad de fondo entre el ordenamiento estadounidense y las exigencias europeas en materia de protección de datos,

especialmente por la amplitud de las facultades de acceso de las autoridades públicas y la ausencia de garantías efectivas para los ciudadanos no estadounidenses (Blasi Casagran, 2017: 200).

Este contexto desembocó en el asunto Schrems I (C-362/14). Maximilian Schrems impugnó ante la autoridad irlandesa de protección de datos la transferencia de sus datos personales por Facebook Ireland a servidores situados en Estados Unidos, alegando que el ordenamiento estadounidense no garantizaba una protección adecuada frente al acceso de las autoridades públicas. Según explica Compagnucci, Schrems sostuvo que normas como la *Foreign Intelligence Surveillance Act*, especialmente su sección 702, y la *Executive Order 12333* no aseguraban una protección suficiente frente a las actividades de vigilancia estatal (Compagnucci, 2024: 6). Ni Loideain, por su parte, destaca que la sentencia Schrems fue decisiva porque el Tribunal de Justicia precisó que la “adecuación” exigida por el Derecho de la Unión no significa identidad absoluta de sistemas, pero sí exige una protección de los derechos fundamentales “esencialmente equivalente” a la garantizada en el ordenamiento europeo (Ni Loideain, 2016: 1).

La sentencia de 6 de octubre de 2015 declaró inválida la decisión de adecuación relativa a Safe Harbor. El Tribunal entendió que la Comisión no había constatado de forma suficiente la existencia en Estados Unidos de límites efectivos al acceso de las autoridades públicas a los datos personales ni de remedios judiciales eficaces para los ciudadanos europeos. Puccio resume esta idea con claridad al señalar que la decisión fue anulada porque no contenía hallazgos sobre la existencia en Estados Unidos de normas y prácticas que limitaran la injerencia en los derechos a la privacidad y a la protección de datos, ni sobre la disponibilidad de recursos judiciales efectivos para los individuos afectados (Monteleone y Puccio, 2018: 3). En términos similares, Tracol recuerda que el Tribunal exigió que la Comisión declarase motivadamente que el tercer país garantiza de hecho, en virtud de su derecho interno o de sus compromisos internacionales, un nivel de protección de los derechos fundamentales esencialmente equivalente al del ordenamiento de la Unión, algo que no se había acreditado en el caso estadounidense (Tracol, 2020: 6). Blasi Casagran destaca que la sentencia Schrems I supuso un punto de inflexión en la interpretación del concepto de adecuación, al exigir un control más riguroso por parte de la Comisión Europea y reforzar el papel de las autoridades nacionales de protección de datos como garantes efectivos de los derechos fundamentales (Blasi Casagran, 2017: 202).

La consecuencia inmediata de la invalidez de *Safe Harbor* fue una fuerte inseguridad jurídica para las empresas que dependían de las transferencias transatlánticas de datos. Puccio destaca que, tras la sentencia, más de 4.000 empresas estadounidenses tuvieron que recurrir a otros instrumentos de transferencia, como las “*Binding Corporate Rules*” o las “*Standard Contractual Clauses*”, que resultaban más limitados y gravosos (Monteleone y Puccio, 2018: 3). Tulac coincide en que la caída de *Safe Harbor* tuvo efectos económicos y operativos inmediatos, pues obligó a las empresas a solicitar autorizaciones especiales o a rediseñar sus infraestructuras de tratamiento, incrementando costes y retrasos en las transferencias (Tulac, 2024: 158).

Precisamente para hacer frente a esa situación, la Comisión Europea y las autoridades estadounidenses negociaron un nuevo marco de transferencia que desembocó, en julio de 2016, en la adopción del *EU-US Privacy Shield*. Este nuevo instrumento trató de presentarse como una versión reforzada del modelo anterior. Compagnucci explica que el *Privacy Shield* se articuló sobre cuatro grandes pilares: una mayor transparencia para las empresas, límites más estrictos y una supervisión más intensa, más posibilidades de recurso y mecanismos de resolución alternativa de controversias, así como una revisión anual conjunta entre autoridades europeas y estadounidenses (Compagnucci, 2024: 7). Del mismo modo, Tulac expone que el *Privacy Shield* introdujo nuevos estándares orientados a garantizar mejor la protección del flujo de datos personales hacia Estados Unidos (Tulac, 2024: 158). Puccio añade que el nuevo marco fue adoptado en julio de 2016 para sustituir a *Safe Harbor* y restaurar un instrumento de transferencia que permitiera el flujo comercial de datos entre ambas orillas del Atlántico, pero advierte que, aunque en su primer año más de 3.000 empresas se suscribieron al sistema y la FTC activó ya varios procedimientos por incumplimiento, persistían importantes preocupaciones acerca de su suficiencia material (Monteleone y Puccio, 2018:3). En efecto, la autora subraya que, pese a su diseño más detallado, seguían existiendo dudas sobre si el *Privacy Shield* ofrecía una protección duradera y satisfactoria, especialmente tras el escándalo Facebook/Cambridge Analytica y a la vista de las objeciones formuladas por el Parlamento Europeo y por los órganos de protección de datos (Monteleone y Puccio, 2018:3).

No obstante, pese a las mejoras introducidas, persistieron dudas relevantes sobre la solidez del nuevo marco. Así, Blasi Casagran advierte que las limitaciones al acceso de las autoridades estadounidenses a los datos personales no resultaban suficientemente claras ni vinculantes, y

cuestiona la efectividad real de los mecanismos de recurso previstos para los ciudadanos europeos (Blasi Casagran, 2017: 210). En términos coincidentes, Tulac señala que el Privacy Shield no logró corregir plenamente los problemas estructurales ya identificados en Safe Harbor, dado que la legislación estadounidense continuaba permitiendo prácticas de vigilancia masiva sobre la base de la FISA 702, la Executive Order 12333 y la Presidential Directive 28, sin controles adecuados desde la perspectiva europea (Tulac, 2024: 159). Por su parte, Tracol añade que, aunque la decisión relativa al Privacy Shield ofrecía una mayor información sobre el sistema estadounidense, en Schrems II tanto el Abogado General como el Tribunal concluyeron que este no cumplía con las exigencias del Derecho de la Unión en materia de protección de datos (Tracol, 2020: 6).

Así, aunque el *Privacy Shield* nació como una respuesta institucional a la caída de *Safe Harbor*, lo cierto es que nunca llegó a disipar por completo las dudas sobre la compatibilidad del sistema estadounidense de vigilancia con el estándar europeo de protección de datos. Por eso, como señala Puccio, la incertidumbre jurídica de fondo no desapareció con el nuevo acuerdo y el riesgo de una nueva impugnación ante el Tribunal de Justicia siguió presente desde sus primeros años de vigencia (Monteleone y Puccio, 2018: 3). Esa previsión terminó confirmándose en 2020, cuando el Tribunal de Justicia, en Schrems II, declaró inválido también el Privacy Shield.

En consecuencia, los antecedentes de *Safe Harbor* y *Privacy Shield* muestran que el problema de las transferencias de datos entre la Unión Europea y Estados Unidos no ha sido coyuntural, sino estructural. Como han puesto de relieve tanto la doctrina como la jurisprudencia, el verdadero núcleo del conflicto reside en la imposibilidad de considerar adecuado un sistema que no limita de forma suficientemente estricta la injerencia de los poderes públicos en los datos personales transferidos ni garantiza a los ciudadanos europeos remedios equivalentes a los previstos en el Derecho de la Unión (Ni Loideain, 2016: 1; Monteleone y Puccio, 2018: 3; Tulac, 2024: 158-159).

La invalidez sucesiva de ambos marcos no solo generó inseguridad jurídica para empresas y operadores económicos, sino que puso de manifiesto la dificultad de conciliar la libre circulación transatlántica de datos con el nivel de protección de derechos fundamentales exigido por la Unión Europea. En este sentido, Blasi Casagran subraya que los distintos intentos de articular mecanismos de transferencia entre la Unión Europea y Estados Unidos han respondido en gran medida a necesidades económicas y políticas, más que a una verdadera convergencia jurídica entre ambos

sistemas, lo que explica la fragilidad estructural de estos instrumentos frente al control del Tribunal de Justicia (Blasi Casagran, 2017: 214). De ahí que, tras Schrems II, se abriera una nueva etapa de incertidumbre normativa en la que, como señalan Corrales Compagnucci, Minssen, Seitz y Aboy, la anulación del Privacy Shield y la subsistencia de las SCC generaron importantes riesgos de responsabilidad e inseguridad jurídica para las organizaciones que dependen de las transferencias de datos UE-EE. UU., poniendo de relieve la necesidad de reconstruir un marco jurídicamente sólido para estas transferencias (Corrales Compagnucci, Minssen, Seitz y Aboy, 2020: 2).

5.2. Jurisprudencia del TJUE: Schrems I (C-362/14) y Schrems II (C-311/18)

5.2.1. Schrems I (C-362/14): invalidez del Safe Harbor

Para comprender con mayor precisión el alcance de esta evolución resulta necesario analizar de forma sistemática la jurisprudencia del Tribunal de Justicia comenzando por la sentencia Schrems I. En la sentencia del 6 de octubre de 2015 (asunto C-362/14) se declaró inválida la Decisión 2000/520/CE de la Comisión Europea, que establecía el régimen denominado Safe Harbor. Este sistema permitía la transferencia de datos personales desde la Unión Europea a empresas estadounidenses adheridas a determinados principios, bajo la premisa de que ofrecían un nivel de protección adecuado.

El litigio se originó a partir de una reclamación presentada por Maximilian Schrems ante la autoridad irlandesa de protección de datos, en la que se cuestionaba la transferencia de sus datos personales por parte de Facebook Ireland a servidores situados en Estados Unidos. La controversia se centraba en determinar si el ordenamiento estadounidense garantizaba un nivel de protección sustancialmente equivalente al exigido por el Derecho de la Unión.

Del análisis de la sentencia se desprende que el Tribunal identifica diversos elementos incompatibles con dicho estándar. En primer lugar, constata la existencia de posibilidades de acceso generalizado a los datos personales por parte de las autoridades públicas estadounidenses, especialmente con fines de seguridad nacional, sin limitaciones claras ni criterios de proporcionalidad. Este aspecto resulta especialmente relevante, ya que implica una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (Canata, 2016: 5).

En segundo lugar, la sentencia pone de relieve la ausencia de mecanismos efectivos de tutela judicial para los ciudadanos europeos, lo que impedía garantizar el derecho a un recurso efectivo frente a posibles vulneraciones de sus datos personales. Este elemento adquiere una importancia central en el razonamiento del Tribunal, al evidenciar que la protección ofrecida por el sistema estadounidense no alcanzaba el nivel exigido por el ordenamiento de la Unión.

Asimismo, el TJUE destaca que el sistema Safe Harbor se basaba en un modelo de autocertificación empresarial sin mecanismos de control suficientes, lo que debilitaba la efectividad real de las garantías previstas (Monteleone & Puccio, 2018:3). A partir de estos elementos, puede observarse que el Tribunal no se limita a cuestionar aspectos concretos del sistema, sino que pone en duda su estructura general.

En consecuencia, el Tribunal concluye que el régimen no aseguraba un nivel de protección adecuado, al permitir injerencias en los derechos fundamentales sin garantías suficientes ni control efectivo. La invalidez de la decisión de la Comisión no solo supuso la desaparición del Safe Harbor, sino que evidenció la necesidad de someter los mecanismos de transferencia internacional a un control mucho más riguroso desde la perspectiva de los derechos fundamentales.

5.2.2. Schrems II (C-311/18): invalidez del Privacy Shield y control reforzado de las transferencias

La sentencia de 16 de julio de 2020 (asunto C-311/18) volvió a examinar la validez de los mecanismos de transferencia de datos hacia Estados Unidos, en este caso en relación con la Decisión (UE) 2016/1250 relativa al Privacy Shield, adoptada tras la anulación del Safe Harbor. En continuidad con Schrems I, el Tribunal parte de la premisa de que las transferencias internacionales solo son lícitas si el país de destino garantiza un nivel de protección sustancialmente equivalente al de la Unión Europea.

A partir de este criterio, el Tribunal identifica nuevamente deficiencias estructurales en el sistema estadounidense que impiden alcanzar dicho nivel de protección. En primer lugar, constata que la normativa estadounidense permite el acceso a los datos personales por parte de las autoridades públicas en condiciones que no respetan el principio de proporcionalidad, al no limitarse a lo

estrictamente necesario. Este elemento, ya presente en Schrems I, se consolida como uno de los ejes centrales del razonamiento del Tribunal (Tracol, 2020: 6).

En segundo lugar, el Tribunal analiza el mecanismo del Ombudsperson previsto en el Privacy Shield y concluye que no constituye un sistema de tutela independiente ni garantiza un recurso efectivo para los ciudadanos europeos. De este modo, se refuerza la idea de que no basta con la existencia formal de mecanismos de control, sino que estos deben ser efectivos y ofrecer garantías equivalentes a las del Derecho de la Unión (Zalnieriute & Churches, 2021 :4).

Uno de los aspectos más relevantes de esta sentencia es que el TJUE no se limita a declarar la invalidez del Privacy Shield, sino que introduce un enfoque más exigente respecto a los instrumentos de transferencia. En este sentido, aborda la validez de las cláusulas contractuales tipo (Standard Contractual Clauses, SCC) y confirma su validez formal, pero condiciona su utilización a que, en la práctica, se pueda garantizar un nivel de protección equivalente.

De este modo, la sentencia desplaza el análisis desde un control puramente formal hacia un control material de las transferencias internacionales. En consecuencia, las autoridades de control deben suspender o prohibir las transferencias cuando consideren que no se cumplen las garantías exigidas (Tracol, 2020). Esto implica que la legalidad de las transferencias ya no depende únicamente del instrumento jurídico utilizado, sino también del contexto normativo del país de destino.

En definitiva, Schrems II supone un refuerzo significativo del estándar europeo de protección de datos, al exigir un examen más riguroso y caso por caso de las transferencias internacionales. La sentencia consolida así una línea jurisprudencial iniciada en Schrems I, en la que el Tribunal asume un papel central en la protección de los derechos fundamentales frente a las injerencias derivadas de la transferencia de datos a terceros Estados.

5.3. El nuevo EU–US Data Privacy Framework (2023)

Como ya hemos visto, la regulación de las transferencias internacionales de datos entre la Unión Europea y los Estados Unidos ha estado marcada por una tensión estructural persistente derivada de la divergencia entre ambos modelos de protección de la privacidad. Mientras que el sistema europeo se fundamenta en la protección de datos como derecho fundamental, el modelo estadounidense

presenta un enfoque sectorial y fragmentado, lo que dificulta el reconocimiento de un nivel de protección equivalente (Cañabate Pérez, 2024:124). Esta divergencia ha sido, además, uno de los factores determinantes en la inestabilidad de los mecanismos de transferencia transatlánticos, como demuestra la sucesiva invalidez de Safe Harbor y Privacy Shield.

En este contexto, el 10 de julio de 2023 la Comisión Europea adoptó una nueva decisión de adecuación relativa al denominado EU-US Data Privacy Framework (en adelante DPF), con el objetivo de restablecer un marco jurídico para las transferencias de datos personales tras la sentencia Schrems II. Este instrumento constituye el tercer intento de articular un régimen estable para los flujos de datos entre ambas jurisdicciones, reflejando la relevancia económica y estratégica de estas transferencias en la economía digital global (Savin, 2023: 159).

Desde el punto de vista normativo, el DPF se integra en el sistema del Reglamento (UE) 2016/679, que permite las transferencias internacionales cuando el país tercero garantiza un nivel de protección “esencialmente equivalente”. Este estándar implica que los derechos de los interesados deben mantenerse efectivos incluso tras la transferencia, siendo responsabilidad del exportador garantizar dicha equivalencia (Batlle & van Waeyenberge, 2024: 191).

La adopción del nuevo marco responde directamente a las deficiencias señaladas por el Tribunal de Justicia en Schrems II. En particular, el Tribunal había cuestionado dos aspectos fundamentales del ordenamiento estadounidense: por un lado, la amplitud de los programas de vigilancia de las autoridades públicas y, por otro, la inexistencia de mecanismos efectivos de tutela judicial para los ciudadanos europeos. En este sentido, el DPF introduce mejoras relevantes, como la incorporación de los principios de necesidad y proporcionalidad en las actividades de inteligencia y la creación de un nuevo sistema de recurso, articulado en torno al Data Protection Review Court (en adelante DPRC) (Savin, 2023 :160-161).

Asimismo, el nuevo marco mantiene un elemento estructural ya presente en los regímenes anteriores: la adhesión voluntaria de las empresas estadounidenses mediante un sistema de autocertificación supervisado por autoridades administrativas como la Federal Trade Commission. Este modelo, sin embargo, ha sido objeto de críticas doctrinales debido a su dependencia de

mecanismos de autorregulación empresarial, cuya eficacia ya fue cuestionada en el pasado (Rahimzadeh, 2023: 30).

Desde una perspectiva crítica, diversos autores han señalado que, aunque el DPF introduce mejoras formales, persisten importantes dudas sobre su capacidad real para garantizar un nivel de protección equivalente al europeo. En particular, se ha cuestionado que las reformas introducidas mediante la Executive Order 14086 no modifican sustancialmente la legislación estadounidense en materia de vigilancia, como la Foreign Intelligence Surveillance Act (FISA), lo que podría comprometer la compatibilidad del sistema con los estándares europeos (Batlle & van Waeyenberge, 2024:195-196).

Igualmente, el nuevo mecanismo de tutela (el DPRC) ha suscitado críticas en cuanto a su naturaleza jurídica y grado de independencia. Aunque se presenta como un órgano destinado a garantizar un recurso efectivo, parte de la doctrina cuestiona si puede considerarse un verdadero órgano jurisdiccional en el sentido exigido por el artículo 47 de la Carta de Derechos Fundamentales de la Unión Europea. A ello se añade la falta de transparencia en determinados procedimientos y la limitada información que reciben los afectados sobre posibles actividades de vigilancia.

En este contexto, el Parlamento Europeo ha llegado a considerar que el DPF no alcanza plenamente el estándar de “equivalencia esencial”, lo que pone de manifiesto la persistencia de incertidumbre jurídica en esta materia. Esta incertidumbre se ve reforzada por la naturaleza del propio instrumento, basado en compromisos del poder ejecutivo estadounidense, lo que plantea dudas sobre su estabilidad a largo plazo (Batlle & van Waeyenberge, 2024:193).

En definitiva, el EU-US Data Privacy Framework representa un nuevo intento de equilibrar la libre circulación internacional de datos con la protección de los derechos fundamentales en el entorno digital. No obstante, la persistencia de diferencias estructurales entre ambos sistemas, las limitaciones del control sobre las actividades de vigilancia y las dudas sobre la efectividad de los mecanismos de recurso permiten anticipar que este marco podría volver a ser objeto de control por el Tribunal de Justicia, manteniendo abierta la posibilidad de un futuro “Schrems III”.

6. Conclusión

A la luz del análisis realizado, resulta difícil sostener una visión optimista sobre la evolución del marco transatlántico de protección de datos. Lejos de avanzar hacia una solución estable, la relación entre la Unión Europea y Estados Unidos en esta materia parece atrapada en una dinámica repetitiva: se diseñan nuevos mecanismos jurídicos que, con el tiempo, terminan siendo cuestionados por no resolver las deficiencias de fondo. En este sentido, el EU-US Data Privacy Framework no puede entenderse como una solución definitiva, sino más bien como un intento adicional (probablemente provisional) de mantener un equilibrio que sigue siendo jurídicamente frágil.

El objetivo de este trabajo ha sido analizar si este nuevo marco permite garantizar un nivel de protección adecuado conforme a los estándares del Derecho de la Unión Europea. A partir del estudio realizado, la respuesta es clara: en el momento actual, resulta difícil afirmar que se alcance un nivel de protección plenamente equivalente en el sentido exigido por el RGPD y por la jurisprudencia del Tribunal de Justicia. Aunque el Data Privacy Framework introduce mejoras respecto a los mecanismos anteriores, estas no parecen suficientes para superar los problemas estructurales ya identificados en Schrems I y Schrems II.

El núcleo del problema sigue estando, en gran medida, intacto. Por un lado, el acceso a los datos personales por parte de las autoridades públicas estadounidenses continúa siendo amplio y, en ciertos aspectos, poco transparente. Es cierto que la Executive Order 14086 incorpora referencias a los principios de necesidad y proporcionalidad, pero no parece que se haya producido una modificación sustancial del marco normativo en materia de vigilancia. Normas como la Foreign Intelligence Surveillance Act (FISA) siguen vigentes, lo que permite cuestionar si, en la práctica, el nivel de protección ofrecido puede considerarse equivalente al europeo. Desde la perspectiva del Derecho de la Unión, donde cualquier injerencia en los derechos fundamentales está sometida a límites muy estrictos, esta cuestión sigue siendo especialmente problemática.

Por otro lado, los mecanismos de tutela de los ciudadanos europeos continúan generando dudas relevantes. La creación del Data Protection Review Court representa una mejora respecto a la situación anterior, pero no despeja completamente las incertidumbres. Parte de la doctrina ha señalado que no resulta evidente que este órgano pueda considerarse un tribunal independiente en

sentido estricto, ni que garantice un nivel de protección equivalente al exigido por el artículo 47 de la Carta de Derechos Fundamentales de la Unión Europea. En este sentido, la cuestión no se limita a la existencia formal de un mecanismo de recurso, sino a su efectividad real como vía de protección frente a posibles vulneraciones.

La combinación de estos dos elementos, un acceso amplio por parte de las autoridades y unos mecanismos de tutela discutibles, permite entender por qué resulta complicado sostener que el estándar de “equivalencia esencial” se cumple plenamente. El Data Privacy Framework introduce avances, pero todo apunta a que estos responden más a una lógica de ajuste que a una verdadera transformación del sistema. Por ello, la idea de que este nuevo marco pueda consolidarse como una solución estable a largo plazo resulta, como mínimo, cuestionable.

En este contexto, la posibilidad de una futura impugnación (un eventual “Schrems III”) no puede afirmarse con certeza, pero sí puede considerarse una hipótesis razonable. No solo desde una valoración personal, sino también a la luz de parte de la doctrina, que advierte de que, si no se producen cambios estructurales en el modelo estadounidense, los problemas identificados por el Tribunal de Justicia podrían reproducirse. En este sentido, más que una predicción, se trata de una conclusión coherente con la evolución que ha seguido esta materia en los últimos años.

Además, esta problemática adquiere una dimensión aún mayor si se sitúa en el contexto tecnológico actual. La digitalización creciente, el desarrollo del Big Data, la inteligencia artificial y la expansión de los servicios en la nube hacen que el volumen de datos personales que se transfieren internacionalmente no deje de aumentar. Esto implica que cualquier debilidad en el sistema de protección no solo se mantiene, sino que puede tener un impacto cada vez más amplio. Cuanto mayor es la dependencia de estos flujos de datos, mayor es también la necesidad de que existan garantías sólidas y efectivas.

Ahora bien, este análisis no puede centrarse únicamente en las carencias del modelo estadounidense. También obliga a reflexionar sobre las limitaciones del propio modelo europeo. La Unión Europea ha construido uno de los sistemas normativos más avanzados en materia de protección de datos, basado en la consideración de este derecho como un derecho fundamental y en

la exigencia de altos estándares de protección. Sin embargo, esta fortaleza normativa no siempre se traduce en una capacidad real de control en el entorno digital.

En este sentido, resulta evidente que Europa se encuentra en una posición más fuerte desde el punto de vista jurídico que desde el tecnológico. La dependencia de infraestructuras, plataformas y servicios digitales desarrollados fuera de la Unión limita, en la práctica, la efectividad de las normas europeas. Esto plantea una cuestión clave, la protección de los datos personales no depende únicamente de la calidad de la regulación, sino también de la capacidad de aplicarla en un entorno globalizado donde los principales actores no están bajo control europeo.

Por ello, si realmente se pretende garantizar una protección efectiva, no basta con seguir perfeccionando el marco normativo. Es necesario avanzar también en el plano tecnológico. Esto implica apostar por la innovación, fomentar el desarrollo de infraestructuras propias y reforzar la soberanía digital europea. Sin este tipo de medidas, el modelo europeo corre el riesgo de quedarse fuerte en teoría, pero limitado en la práctica.

Desde una perspectiva propositiva, esto exige un doble esfuerzo. Por un lado, sería necesario que el sistema estadounidense evolucionara hacia un modelo más coherente y garantista, con límites más claros al acceso por parte de las autoridades públicas y con mecanismos de tutela judicial plenamente efectivos. Por otro lado, la Unión Europea debe complementar su fortaleza normativa con una estrategia tecnológica sólida que le permita reducir su dependencia y reforzar la aplicación real de sus estándares.

En definitiva, el EU-US Data Privacy Framework representa un nuevo intento de equilibrar la libre circulación de datos con la protección de los derechos fundamentales. Sin embargo, no resuelve las diferencias estructurales existentes entre ambos sistemas. Mientras estas diferencias persistan, cualquier solución será, en mayor o menor medida, provisional.

Bibliografía

Battle, S., & van Waeyenberge, A. (2024). EU–US data privacy framework: A first legal assessment. *European Journal of Risk Regulation*, 15, 191–200. <https://doi.org/10.1017/err.2023.67>

Barrio Andrés, M. (2022). Avanzando en la soberanía digital europea: Los reglamentos DSA y DMA. *Análisis del Real Instituto Elcano (ARI)*, 43, 1–10.

Barrio Andrés, M. (2022). La regulación del derecho a la protección de datos en los Estados Unidos: Hacia un RGPD norteamericano. *Cuadernos de Derecho Transnacional*, 14(2), 186–193.

Blasi Casagran, C. (2017). Nuevo régimen jurídico para la transferencia de datos entre la UE y los Estados Unidos: ¿Es compatible con la normativa europea de protección de datos? *Revista General de Derecho Europeo*, 42, 192–217.

Blasi Casagran, C. (2020). *Transferencias internacionales de datos personales*, 5-31.

Canata, A. (2016). The data transfer from EU to US under the EU data protection rules: *The consequences of the Schrems case*.

Cañabate Pérez, J. (2024). La transferencia internacional de datos personales a Estados Unidos: El “transatlantic clash” de dos culturas de privacidad. En J. A. Fernández Amor (Dir.), *Digitalización, empresa y derecho* 123–152. Atelier.

Corrales Compagnucci, M. (2024). The EU-US Data Privacy Framework: Is the Dragon Eating its Own Tail? *Perspectives in Law, Business and Innovation*, 17-39..pdf

Corrales Compagnucci, M., Minssen, T., Seitz, C., & Aboy, M. (2020). Lost on the high seas without a safe harbor or a shield? Navigating cross-border data transfers in the pharmaceutical sector after Schrems II. *European Pharmaceutical Law Review*, 4(3), 153–160.

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: Las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, 31.

Dimović, Z. (2024). Analysing the EU data privacy implications resulting from Executive Order 14086: A legal perspective. *Lexonomica*, 16(1), 85–110.

González, M. D. P. (2012). El poder de autodeterminación de los datos personales en Internet. IDP. *Revista de Internet, Derecho y Política*, 14, 61–74.

López Aguilar, J. F. (2023). Transparencia, un derecho europeo, y su relación con otros bienes constitucionalmente relevantes. *Revista Española de la Transparencia*, 17.

Marco, J. M. S. (2020). Evolución del derecho a la protección de datos y disrupción tecnológica: ¿Estamos vallando el campo? *CEFLegal. Revista Práctica de Derecho*, 89–120.

Monteleone, S., & Puccio, L. (2018). *The privacy shield: Update on the state of play of the EU–US data transfer rules*. European Parliamentary Research Service.

Ni Loideain, N. (2016). The end of safe harbour: Implications for EU digital privacy and data law. *Computer Law & Security Review*, 19(8).

Rahimzadeh, V. (2023). The ethical data practices framework and its implications for data privacy relations between the United States and the European Union. *The American Journal of Bioethics*, 23(11), 29–33.

Robles Carrillo, M. (2023). La articulación de la soberanía digital en el marco de la Unión Europea. *Revista de Derecho Comunitario Europeo*, 75, 133–171.

Rubinstein, I. S., & Margulies, P. (2022). Risk and rights in transatlantic data transfers: EU privacy law, U.S. surveillance, and search for common ground. *Connecticut Law Review*, 54(2), 395–455.

Savin, A. (2023). *The new framework for transatlantic data transfers*. CBS Law Research Paper No. 23-01. <https://ssrn.com/abstract=4494289>

Schwartz, P. M. (2012). Information privacy in the cloud. *University of Pennsylvania Law Review*, 161, 1623–1661.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, 106(1), 115–178.

Sobrino-García, I. (2020). Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Solove, D. J. (2010). *Understanding privacy*. Harvard University Press.

Sury, U. (2023). EU–U.S. data privacy framework. *Informatik Spektrum*, 46, 58–60. <https://doi.org/10.1007/s00287-022-01515-7>

Torreblanca, J. I., & Hobbs, C. (2020). La soberanía digital de Europa: *De regulador a superpotencia en la era de la rivalidad entre Estados Unidos y China*. Los Libros de la Catarata.

Tracol, X. (2020). Schrems II: The return of the privacy shield. *Computer Law & Security Review*, 39, 105484.

Tulac, B. R. (2024). Third time's the charm? The EU–US data privacy framework. *EURINT – European Union and International Affairs*, 11(1), 157–177.

Zalnieriute, M., & Churches, G. (2021). Rejecting the transatlantic outsourcing of data protection in the face of unrestrained surveillance. *Cambridge Law Journal*, 80(1), 8–11.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the GDPR. *International Data Privacy Law*, 7(2), 76–99.