EL PAPEL DE LA DATA PROTECTION COMMISSION DE IRLANDA: ENFOQUE, CRÍTICAS Y NUEVAS RESPONSABILIDADES[1]

OSCAR JOSAFAT LEYVA FERZULI
Escuela de Derecho y Gobierno de Dublin City University

EDOARDO CELESTE
Escuela de Derecho y Gobierno de Dublin City University

Cómo citar/Citation
Leyva Ferzuli, O.J. y Celeste, E. (2025).
El papel de la Data Protection Commission de Irlanda:
enfoque, críticas y nuevas responsabilidades.
Revista de Administración Pública, 228, 231-259.
doi: https://doi.org/10.18042/cepc/rap.228.08

Resumen

El artículo analiza el rol de la Data Protection Commission de Irlanda como autoridad de protección de datos, en un contexto marcado por la concentración de grandes empresas tecnológicas en el país. Examina su evolución, limitaciones institucionales y críticas, así como las tensiones entre su función y el entorno económico irlandés. A la luz de nuevas normativas como el Reglamento de Servicios Digitales y el Reglamento de Inteligencia Artificial, se advierte sobre la posible reproducción de las debilidades del Sistema de ventanilla única del Reglamento General de Protección

[1] Este trabajo ha sido posible gracias al apoyo financiero del Máster Europeo en Derecho, Datos e Inteligencia Artificial (EMILDAI) financiado por el programa Erasmus Mundus de la UE. Nos gustaría agradecer a los revisores anónimos de esta revista y a los participantes en el taller «El régimen sancionador del RGDP y su implementación en los sistemas jurídicos nacionales. Los casos de Italia, Irlanda y Portugal» (Universidad de Murcia, 23 de septiembre de 2024, Proyecto PID2022-139265OB-I00 Financiado por MICIU/AEI/10.13039/501100011033/ Y POR FEDER, UE) —en particular a los profesores Julián Valero Torrijos y Magnolia Pardo López— por sus comentarios constructivos a versiones anteriores de este artículo.

de Datos. El texto propone reformas estructurales, en aras de una aplicación más equitativa, coherente y eficaz del derecho digital en la Unión Europea en su búsqueda por recuperar su soberanía digital.

Palabras clave

Data Protection Commission; sistema de ventanilla única; protección de datos; derecho digital; soberanía digital.

Abstract

The article analyses the role of Ireland's Data Protection Commission as a data protection authority, within a context defined by the concentration of major technology companies in the country. It examines the Commission's evolution, institutional limitations, and criticisms, as well as the tensions between its regulatory function and Ireland's economic environment. In light of new regulations such as the Digital Services Act and the Artificial Intelligence Act, the article warns of the potential replication of the weaknesses of the General Data Protection Regulation's One-Stop-Shop mechanism. It proposes structural reforms aimed at ensuring a more equitable, consistent, and effective enforcement of digital law in the European Union, as it seeks to reclaim its digital sovereignty.

Keywords

Data Protection Commission; one-stop-shop; data protection; digital Law; digital sovereignty.

SUMARIO

I. INTRODUCCIÓN. II. HISTORIA DE LA DATA PROTECTION COMMISSION: 1. Origen y evolución: *1.1. Responsabilidades y potestades iniciales. 1.2. Cambios regulatorios.* 2. La actual Data Protection Commission de Irlanda: *2.1. Marco legislativo. 2.2. Composición y potestades. 2.3. El alcance presupuestario de la Data Protection Commission.* III. INTENTANDO ADECUARSE AL MECANISMO DE COHERENCIA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: EL CASO DE IRLANDA: 1. Una mirada al sistema de ventanilla única desde la perspectiva irlandesa. 2. Implicaciones del entorno favorable a las empresas en Irlanda. IV. CASOS DESTACADOS Y CRÍTICAS: 1. El Comité Europeo de Protección de Datos al mando del sistema de ventanilla única. 2. Analizando el enfoque de la Data Protection Commission. 3. ¿Protección de datos vs. crecimiento económico? V. EL PAPEL DE LA DATA PROTECTION COMMISSION A LA LUZ DE LA NUEVA ESTRATEGIA DIGITAL DE LA UNIÓN EUROPEA: 1. Nuevas normativas y responsabilidades: *1.1. Reglamento de Servicios Digitales. 1.2. Reglamento de Inteligencia Artificial* (AI Act). VI. CONCLUSIONES.

I. INTRODUCCIÓN

En la era digital, la protección de los datos personales se ha convertido en una de las preocupaciones más urgentes para los gobiernos, las empresas y los individuos. La Unión Europea (UE) se ha posicionado como líder global en el ámbito de la protección de datos mediante la adopción del Reglamento General de Protección de Datos (RGPD), que establece estándares uniformes y estrictos para la recopilación, el procesamiento y el almacenamiento de datos personales en todos los Estados miembros de la UE. En el centro de este marco regulatorio se encuentra la Data Protection Commission (DPC), la autoridad nacional irlandesa para la protección de datos personales. Bajo el RGPD, esta desempeña un papel crucial como autoridad de control principal para muchas de las mayores empresas tecnológicas del mundo que tienen sus oficinas europeas en la República Irlandesa.

La historia de la DPC está marcada por una evolución gradual, pasando de ser un organismo regulador relativamente modesto a convertirse en una autoridad central con una influencia significativa en el panorama digital de toda la UE. Con el paso de los años, a medida que la economía digital se expandía e Irlanda se convertía en un destino preferido por los gigantes tecnológicos, el papel de la DPC creció en complejidad e importancia. Esta transformación alcanzó su punto culminante con la aplicación del RGPD a partir de 2018, que no solo amplió las competencias de la DPC, sino que también introdujo nuevos desafíos, especialmente en la aplicación de la legislación de protección de datos a través de múltiples jurisdicciones.

La adopción del RGPD representó un cambio trascendental en el entorno regulatorio, tanto en Irlanda como en toda la UE. Introdujo potestades de aplicación más efectivas, amplió el alcance de la supervisión y estableció mecanismos de cooperación transfronteriza entre las autoridades de protección de datos. Sin embargo, la implementación del RGPD también puso de manifiesto las limitaciones de los mecanismos de aplicación existentes, en particular el sistema de ventanilla única, que centraliza la aplicación en manos de la autoridad de control principal del país donde una empresa tiene su establecimiento principal. Para Irlanda, esto significó que la DPC asumiría una gran magnitud de la responsabilidad en la aplicación del RGPD, dada la concentración de empresas tecnológicas en el país.

A medida que la UE sigue desarrollando su estrategia digital, nuevas normativas, como el Reglamento de Servicios Digitales (DSA del inglés Digital Services Act) y el Reglamento de Inteligencia Artificial *(AI Act)* están destinadas a expandir aún más el panorama regulatorio. Estas normativas, al igual que el RGPD, requerirán mecanismos de aplicación robustos para garantizar el cumplimiento en toda la UE. Al respecto, surge una pregunta desde una perspectiva regulatoria: ¿son adecuados los mecanismos existentes, en particular el sistema de ventanilla única y los similares previstos en el DSA y el *AI Act,* para manejar la mayor complejidad y carga de trabajo que traerán estas nuevas regulaciones? La experiencia de la DPC bajo el RGPD sugiere que podrían presentarse desafíos considerables tanto en su rol de supervisión como en su capacidad sancionadora.

El sistema de ventanilla única, aunque innovador en su diseño, ha sido objeto de críticas por sus ineficiencias y la carga desigual que impone a ciertas autoridades de protección de datos, especialmente a la DPC. Además, el papel del Comité Europeo de Protección de Datos (CEPD) en la supervisión de la coherencia en la aplicación del RGPD ha puesto de manifiesto los desafíos para mantener un enfoque uniforme en toda la UE. El CEPD ha tenido que intervenir con frecuencia en casos gestionados por la DPC, a menudo exigiendo medidas de aplicación más estrictas que las inicialmente propuestas. Esta dinámica plantea interrogantes sobre el equilibrio de poder entre las autoridades nacionales y los organismos a nivel de la UE, y si el marco actual respalda adecuadamente las amplias ambiciones digitales de la UE.

En este contexto, la eficacia de la estrategia digital de la UE depende de la capacidad de sus mecanismos de aplicación para adaptarse a las exigencias de un panorama digital en rápida evolución. La experiencia de la DPC bajo el RGPD constituye un estudio de caso fundamental para comprender los posibles desafíos y oportunidades que se avecinan. A medida que la UE avanza con la implementación del DSA, *AI Act* y otras normativas, resulta imprescindible evaluar si los mecanismos existentes son adecuados para cumplir con su propósito o si es necesario un enfoque diferente para alcanzar la visión digital de la UE.

Esta contribución analiza la evolución de las responsabilidades de la DPC, desde una pequeña autoridad nacional hasta convertirse en un regulador con responsabilidades a nivel de toda la UE. Reconstruimos su enfoque regulatorio y las críticas relacionadas. Finalmente, reflexionamos sobre los desafíos generados por la ampliación del ámbito de poder de la autoridad irlandesa a raíz de la expansión de la estrategia digital de la UE.

II. HISTORIA DE LA DATA PROTECTION COMMISSION

El papel de la DPC ha evolucionado sustancialmente a lo largo de los años, reflejando los cambios en el panorama de la protección de datos tanto en Irlanda como en la UE. Con potestades iniciales limitadas, la DPC ha ganado relevancia, especialmente ante los desafíos de la era digital y la posición especial de Irlanda como centro tecnológico digital. Esta sección explora el origen y la evolución de la DPC, centrándose en sus responsabilidades iniciales, potestades y los cambios normativos posteriores.

1. ORIGEN Y EVOLUCIÓN

1.1. Responsabilidades y potestades iniciales

Las preocupaciones de Europa sobre la protección de los datos personales tomaron forma en normas legales vinculantes con la ratificación del Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, promovido por el Consejo de Europa (Convenio 108)[2]. Este primer y único tratado internacional sobre protección de datos serviría posteriormente como base para la Directiva de Protección

[2] Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2018), *Handbook on European Data Protection Law,* Oficina de Publicaciones de la Unión Europea, pág. 24; Consejo de Europa (1981), «Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal» (*ETS 108*), cap. II; P. de Hert y M. Czerniawski (2016), «Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection

de Datos y, más tarde, para el RGPD. Al implementar estos instrumentos legales, el marco de protección de datos de Irlanda deriva de los estándares de protección de datos establecidos por la UE.

El antecesor de la DPC, llamado Data Protection Commissioner, nació con la Ley de Protección de Datos de 1988, tras la transposición al derecho irlandés del Convenio 108, como una autoridad de supervisión equipada con amplias potestades de investigación y aplicación, pero con medios sancionadores escasos[3]. El alcance y las capacidades de ejecución del Data Protection Commissioner eran, en comparación con los estándares actuales, algo limitados. Asimismo, su presupuesto restringido añadía más limitaciones a su capacidad legal[4]. Con la Ley de Protección de Datos de 2003, Irlanda reformó el texto de 1988, transponiendo la Directiva de Protección de Datos a su marco jurídico, pero sin ampliar de manera importante las potestades sancionadoras del Data Protection Commissioner[5]. El marco inicial otorgaba al *Commissioner* la autoridad para realizar investigaciones, emitir advertencias y, cuando fuera necesario, emprender acciones legales contra entidades que violaran las leyes de protección de datos. Sin embargo, esa autoridad no podía imponer sanciones de gran impacto y estaba obligada a recurrir a enfoques alternativos, como la resolución amistosa de conflictos[6].

1.2. Cambios regulatorios

El establecimiento de importantes gigantes tecnológicos en Irlanda puso al Data Protection Commissioner en el centro de atención[7]. Estas circunstancias, junto con los incesantes avances tecnológicos de la era digital, impulsaron a Irlanda a introducir cambios regulatorios en su marco de protección de datos. Uno de los cambios clave llegó con la entrada en vigor del RGPD en 2018, que sustituyó a la Directiva 95/46/CE y estableció un marco más sólido y completo para la protección de datos en toda la UE. El RGPD fue implementado en Irlanda a través de la Ley de Protección de Datos de 2018, adoptada por el Oireachtas, el Parlamento irlandés, el 24 de mayo de 2018[8]. Cabe señalar que la Ley de Protección de Datos de 2018 también dio cumplimiento a la Directiva sobre Protección de Datos en el Ámbito Penal, como se explicará más adelante.

Regulation in its Wider Context», *International Data Privacy Law*, 6(3), págs. 230-243, pág. 232.

3 T. J. McIntyre (2020), «Regulating the Information Society: Data Protection and Ireland's Internet Industry», en D. M. Farrell y N. Hardiman (eds.), *The Oxford Handbook of Irish Politics*, Oxford University Press, pág. 705.

4 *Ibid.,* pág. 706.

5 Ley de Protección de Datos (Reformada) de 2003, sección 10.

6 *Ibid.,* s 9, s 11.

7 McIntyre (2020, pág. 708).

8 Ley de Protección de Datos de 2018.

Los principales cambios regulatorios introducidos por el RGPD desde una perspectiva de supervisión consistieron en el fortalecimiento de las potestades de ejecución, la ampliación del alcance de la supervisión y la introducción de mecanismos de cooperación transfronteriza. El RGPD otorgó a las autoridades de control la potestad de imponer sanciones sustanciales a las organizaciones que infringieran las leyes de protección de datos, con multas que podrían alcanzar hasta 20 millones de euros o el 4% de la facturación anual global de la empresa, lo que sea mayor[9]. Esto supuso un aumento sustancial en comparación con las multas relativamente modestas que eran posibles bajo el marco normativo anterior en Irlanda. En segundo lugar, el RGPD incrementó el alcance de supervisión de las autoridades de control para incluir no solo a los responsables del tratamiento de datos, sino también a los encargados del tratamiento[10], ampliando el rango de entidades sujetas a escrutinio regulatorio. En tercer lugar, la nueva normativa introdujo mecanismos de cooperación entre las autoridades de protección de datos en toda la UE, lo que facilitó un enfoque más coordinado y cohesionado en la aplicación de la normativa de protección de datos[11]. Esto es particularmente importante para gestionar casos que involucran a organizaciones multinacionales que operan en múltiples Estados miembros.

El énfasis del RGPD en la responsabilidad y la transparencia requirió un enfoque más proactivo y comprometido por parte del Data Protection Commissioner, ampliando de manera relevante su mandato tanto *de iure* como *de facto*. Con la entrada en vigor de la Ley de Protección de Datos de 2018 en Irlanda, se dio cumplimiento al RGPD y se transformó la oficina del Data Protection Commissioner en la hodierna DPC, concebida como la autoridad nacional de protección de datos, dotada de los medios necesarios para supervisar y hacer cumplir los estándares de protección de datos consagrados en el RGPD de manera eficiente y efectiva[12]. Estas mejoras regulatorias han dado forma a la autoridad y las potestades actuales de la DPC.

2. LA ACTUAL DATA PROTECTION COMMISSION DE IRLANDA

2.1. Marco legislativo

Actualmente, las potestades de la DPC se definen por las siguientes disposiciones:

---

9 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (2016) OJ L119/1, art. 83(5).

10 *Ibid.,* art. 4(8).

11 *Ibid.,* c 7.

12 Ley de Protección de Datos de 2018, Exposición de Motivos, pág. 2.

— Reglamento General de Protección de Datos (RGPD).
— Ley de Protección de Datos 2018.
— Directiva sobre Protección de Datos en el Ámbito Penal (LED, por sus siglas en inglés).
— Las Leyes de Protección de Datos de 1988 y 2003.
— Las *ePrivacy Regulations* de 2011[13].

Si bien el RGPD regula en general la mayoría de los tratamientos de datos personales por defecto, en Irlanda existen regulaciones adicionales sobre cuestiones específicas, como la justificación y el alcance de las restricciones a los derechos de los interesados, que se detallan en la Ley de Protección de Datos de 2018[14]. Además, la LED establece normas relacionadas con la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de orden público[15]. La LED fue transpuesta al derecho irlandés en las Partes 5 y 6 de la Ley de Protección de Datos 2018[16]. Por su parte, la Directiva sobre Privacidad Electrónica y Comunicaciones Electrónicas[17] y la Directiva 2009/136/EC[18] fueron implementadas mediante *ePrivacy Regulations* de 2011[19]. La DPC es la autoridad encargada de supervisar

[13] Data Protection Legislation, Key Data Protection legislative frameworks applicable from 25 May 2018: https://is.gd/RszIkr. Consultado el 17 de octubre de 2025.

[14] *Ibid.*, Ley de Protección de Datos de 2018, arts. 57, 59 y 61.

[15] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (2016) DO L119/89, considerando (11).

[16] Ley de Protección de Datos de 2018, parte 5.

[17] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (2002) DO L201/37.

[18] Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores (2009) DO L337/11.

[19] Instrumento Estatutario 336 de 2011 Regulaciones de las Comunidades Europeas 2011 (Redes y Servicios de Comunicaciones Electrónicas) (Privacidad y Comunicaciones Electrónicas).

el cumplimiento de los instrumentos legales mencionados en esta sección y, en conjunto, dichas disposiciones legales definen las potestades de esta autoridad.

2.2. Composición y potestades

La composición de la DPC está regulada por el art. 15 de la Ley de Protección de Datos de 2018, que establece que la DPC estará compuesta por los miembros que el Gobierno determine, pero no más de tres. Cada miembro de la Comisión será denominado comisionado de Protección de Datos por un período no inferior a cuatro años ni superior a cinco años desde la fecha de su nombramiento[20]. Actualmente, por la primera vez en su historia, la DPC tiene tres comisionados[21].

Las potestades de la DPC están definidas principalmente por la Ley de Protección de Datos de 2018, con autoridad adicional otorgada a través de los instrumentos legales discutidos en la sección anterior. En consecuencia, la DPC cuenta con la potestad para examinar las reclamaciones de individuos respecto a posibles infracciones de la legislación de protección de datos; realizar investigaciones e indagaciones sobre incumplimientos de dicha legislación y tomar medidas de aplicación cuando sea necesario; promover la concienciación pública sobre los derechos de las personas para proteger sus datos personales según la normativa vigente y, además, mejorar la concienciación y el cumplimiento entre los responsables y encargados del tratamiento mediante la publicación de guías de alta calidad, así como el compromiso proactivo con organizaciones del sector público y privado. De igual manera, ayuda a identificar riesgos para la protección de datos personales y ofrece orientaciones sobre las mejores prácticas para mitigarlos. Coopera también con otras autoridades de protección de datos, incluyendo el intercambio de información, y actúa como autoridad de control principal a nivel de la UE para organizaciones cuyo establecimiento principal en la UE esté en Irlanda[22].

Adicionalmente, la DPC también actúa como autoridad de control para el tratamiento de datos personales en el marco de la LED y desempeña ciertas funciones de supervisión y aplicación relacionadas con el tratamiento de datos personales en el contexto de las comunicaciones electrónicas bajo las *ePrivacy* Regulations de 2011[23]. La DPC también sigue supervisando funciones regulatorias bajo las Leyes de Protección de Datos de 1988 y 2003, abordando reclamaciones e investigaciones relacionadas con períodos anteriores al 25 de

---

20 Ley de Protección de Datos de 2018, parte 2.

21 DPC Welcomes the Appointment of 3rd Commissioner: https://is.gd/87IYu7. Consultado el 17 de octubre de 2025.

22 Ley de Protección de Datos de 2018 (n 8), parte 2 y parte 6, c 2; What we do: https://is.gd/ZB2kEZ. Consultado el 17 de octubre de 2025.

23 DPC, Reporte Anual de 2023 (DPC 2024), págs. 12-14.

mayo de 2018. Asimismo, gestiona categorías específicas de tratamiento, independientemente de si ocurrieron antes o después de esta fecha[24]. Además, más allá de la legislación específica en materia de protección de datos, la DPC es responsable de supervisar el tratamiento de datos personales en virtud de aproximadamente 20 piezas legislativas adicionales en diversas áreas sectoriales, donde se le han asignado funciones específicas de supervisión[25].

2.3. El alcance presupuestario de la Data Protection Commission

La DPC ha enfrentado históricamente restricciones presupuestarias en comparación con sus homólogas de otros Estados miembros de la UE. Sin embargo, el presupuesto de la DPC ha aumentado considerablemente en los últimos años. Por ejemplo, en 2024, el presupuesto se incrementó a 29 millones de euros, lo que representa un aumento ocho veces mayor en comparación con los 3,6 millones de euros asignados en 2015[26]. En cualquier caso, este aumento presupuestario podría seguir siendo insuficiente para que la DPC gestione sus responsabilidades en expansión, especialmente considerando el papel de Irlanda como autoridad de control principal para muchas de las grandes empresas tecnológicas con sede en el país, debido al sistema de ventanilla única establecido por el RGPD[27], según el cual la autoridad de control principal es la de la jurisdicción en la que el responsable o encargado del tratamiento tiene su establecimiento principal[28].

La DPC es responsable de una cantidad desproporcionada de reclamaciones en materia de protección de datos[29]. La posición única de Irlanda da lugar a una carga de trabajo considerable, sobre la cual algunos argumentan que el presupuesto actual aún podría no cubrir completamente[30]. La siguiente tabla muestra los presupuestos y el número de reclamaciones recibidas («RR») de algunas de las

---

24 *Ibid.*

25 *Ibid.*

26 Minister McEntee secures record €3.9bn Budget: https://is.gd/b7zqr3. Consultado el 17 de octubre de 2025.

27 D. M. Brandão (2023), «The One-Stop-Shop and the European Data Protection Board's Role in Combatting Data Supervision Forum Shopping», *International Data Privacy Law*, 13(4), págs. 313-330, pág. 319.

28 GDPR, art. 56.

29 Irish Council for Civil Liberties (2021), «Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities», *ICCL*, págs. 5-7; Key Takeaways from the Irish DPC's 2022 Annual Report: https://is.gd/TTy1a7. Consultado el 17 de octubre de 2025.

30 Irish Council for Civil Liberties (2021).

TABLA 1. *Relación entre presupuesto y reclamaciones de las autoridades de protección de datos*

PAÍS	APD	2017		2024	
		PRESUPUESTO	RR	PRESUPUESTO	RR
Francia	CNIL (Commission Nationale de l'Informatique et des Libertés)	€17M[1]	8,360[2]	€28.2M[3]	15,350[4]
Italia	Garante per la Protezione dei Dati Personali	€21M[5]	5,708 (incluye reclamaciones y reportes)[6]	€50.3M[7]	4,030[8]
España	AEPD (Agencia Española de Protección de Datos)	€14.1M[9]	10,651[10]	€18.7M[11]	18,855[12]
Irlanda	Data Protection Commission (DPC)	€7.5M[13]	2,642[14]	€28.1M[15]	11,091[16]
Alemania	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit[17]	€15.3M[18]	NA[19]	€45.3M[20]	8,670[21]
Países Bajos	Autoriteit Persoonsgegevens	NA[22]	NA[23]	€40M[24]	7.119[25]

1 Commission nationale de l'informatique et des libertés (2018), «38e Rapport Annuel 2017», pág. 3.
2 *Ibid*.
3 Commission nationale de l'informatique et des libertés (2025), «44e Rapport Annuel 2024», pág. 5.
4 *Ibid*.
5 Garante per la protezione dei dati personali (2018), «Relazione Annuale 2017», pág. 196.
6 *Ibid.*, pág. 4.
7 Garante per la protezione dei dati personali (2025), «Relazione Annuale 2024», pág. 244.
8 *Ibid.*, pág. 6. En Italia hubo además alrededor de 90,000 reportes por violación de seguridad de datos personale
9 Agencia Española de Protección de Datos, «Gestión presupuestaria»:https://is.gd/XcYIai. Consultado el 17 de octubre de 2025.
10 Agencia Española de Protección de Datos, «La AEPD recibe por tercer año consecutivo el mayor número de reclamaciones de su historia»: https://is.gd/urQQCt. Consultado el 17 de octubre de 2025.
11 Agencia Española de Protección de Datos, «Gestión presupuestaria»: https://is.gd/XcYIai. Consultado el 17 de octubre de 2025.
12 Agencia Española de Protección de Datos (2025), «Memoria Anual 2024», pág. 100.
13 Data Protection Commissioner (2018), «Annual Report 2017», pág. 5.
14 *Ibid*. 13.
15 DPC (2025), «Annual Report 2024», pág. 17.
16 *Ibid.*, pág. 10.
17 Esta es la autoridad federal alemana, sin embargo, en Alemania existen además autoridades regionales.
18 Bundesrepublik Deutschland (2017), «*Haushaltsgesetz 2017 — Einzelplan 21: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*», Bundesministerium der Finanzen, pág. 21. Esta cifra se refiere a la autoridad federal alemana. Hay estimaciones independientes que indican un total de €53.8M en el año 2016, sumando el presupuesto federal y los presupuestos regionales: Irish Council for Civil Liberties (2023), «5 Years: GDPR's Crisis Point - ICCL Report on EEA Data Protection Authorities», *ICCL*, pág. 7.
19 No hay información suficiente disponible.
20 Bundesrepublik Deutschland (2025), «*Haushaltsgesetz 2024 — Einzelplan 21: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*», *Bundestag*, pág. 21. En 2022 se estimó que el presupuesto acumulado era de 104 millones de euros, sin embargo, no hay información suficiente disponible sobre el presupuesto de 2024: Irish Council for Civil Liberties (2023), «5 Years: GDPR's Crisis Point - ICCL Report on EEA Data Protection Authorities», *ICCL*, pág. 7.
21 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2025), «Tätigkeitsbericht 2024 — 32. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit», *BfDI*, pág. 143.
22 No hay información suficiente disponible.
23 No hay información suficiente disponible.
24 Autoriteit Persoonsgegevens (2025), «Jaarverslag 2024», pág. 37.
25 *Ibid.*, pág. 27.

principales autoridades de control de la UE para el año 2017, antes de la adopción del RGPD, y para el año 2024.

La tabla 1, muestra que la DPC es una de las autoridades de control que ha experimentado uno de los mayores incrementos en financiación en comparación con el período anterior al RGPD. Sin embargo, los presupuestos de las principales autoridades de control siguen siendo más altos en la mayoría de los casos, y solo España mantiene un presupuesto menor que el de la DPC, a pesar de haber recibido también una cantidad importante de reclamaciones en 2024[31]. En el caso de Francia, el presupuesto fue prácticamente igual al de la DPC en el año anterior. En otros casos, se observa que, en comparación con algunas jurisdicciones (por ejemplo, Países Bajos, Alemania e Italia), la DPC cuenta con un presupuesto mucho menor. Además de la cantidad de reclamaciones recibidas, el principal desafío para la DPC es la sofisticación y el carácter técnico de las reclamaciones que está obligada a abordar como autoridad de control principal de las mayores empresas tecnológicas del mundo, lo que podría derivar en la necesidad de un presupuesto aún mayor.

III. INTENTANDO ADECUARSE AL MECANISMO DE COHERENCIA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: EL CASO DE IRLANDA

Irlanda se ha convertido en un centro estratégico para las principales empresas tecnológicas en los últimos años, con muchas de ellas estableciendo sus sedes europeas en el país. Esta tendencia puede atribuirse al entorno empresarial favorable de Irlanda, con tasas impositivas altamente competitivas[32]. Empresas como Google, Facebook, Apple, Microsoft y Twitter (X) han elegido Irlanda como su base para operaciones europeas, aprovechando estos beneficios, lo cual conlleva desafíos significativos, especialmente en la aplicación de las normativas de protección de datos.

---

31 Agencia Española de Protección de Datos (2024), «La AEPD recibe por tercer año consecutivo el mayor número de reclamaciones de su historia», *AEPD*, 11 de abril de 2024, disponible en: https://is.gd/RcBr64.

32 Corporation Tax (CT): https://is.gd/wMk9q7. Consultado el 17 de octubre de 2025; A. Walsh y C. Sanger (2020), «The Historical Development and International Context of the Irish Corporate Tax System: A Report Commissioned by the Irish Department of Finance», *Department of Finance*, pág. 1; Comisionados de Hacienda (2024), «Research & Development (R&D) Corporation Tax Credit - Tax and Duty Manual Part 29-02-03», *Revenue Commissioners*, pág. 5.

1. UNA MIRADA AL SISTEMA DE VENTANILLA ÚNICA DESDE LA PERSPECTIVA IRLANDESA

El RGPD introduce un mecanismo de coherencia diseñado para garantizar que la aplicación de la protección de datos en toda la UE sea coordinada y cohesionada. Este mecanismo exige la cooperación entre las autoridades de control de todos los Estados miembros de la UE[33]. Al fomentar la colaboración, el RGPD busca crear un panorama de aplicación uniforme, evitando discrepancias y garantizando que los estándares de protección de datos se apliquen de manera homogénea.

El núcleo del mecanismo de coherencia del RGPD es el sistema de ventanilla única[34]. Este sistema designa una autoridad de control principal para los casos de tratamiento de datos transfronterizos, lo que simplifica ampliamente el panorama regulatorio para las empresas que operan en varios países de la UE. Según el art. 55(1) del RGPD, la autoridad de control del establecimiento principal del responsable o encargado del tratamiento se designa como la autoridad de control principal. Esto significa que, si una empresa opera en varios Estados miembros de la UE, la autoridad de control del país donde la empresa tiene su establecimiento principal asumirá el liderazgo en la supervisión y aplicación de la normativa.

Aunque el sistema de ventanilla única puede ser muy útil en el tratamiento transfronterizo que involucra a un par de Estados miembros, puede resultar insuficiente e ineficiente cuando se trata del tratamiento de datos que afecta a interesados en varios Estados miembros. Esto se debe a varios factores: enfoques alternativos en los Estados miembros para aplicar las disposiciones de protección de datos, presupuestos desiguales y desproporcionados entre jurisdicciones, diferentes niveles de eficiencia de las autoridades de control en cada jurisdicción y agendas divergentes entre los Estados miembros[35]. De hecho, en muchos casos, las empresas pueden buscar jurisdicciones más permisivas en cuanto a la aplicación de la normativa de protección de datos para establecer su sede principal, una

33 RGPD, art. 60.

34 P. A. de Miguel Asensio (2017), «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *Revista Española de Derecho Internacional*, 69(1), Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales, págs. 88-90.

35 G. Gentile y O. Lynskey (2022), «Deficient by Design? The Transnational Enforcement of the GDPR», *International and Comparative Law Quarterly*, 71, págs. 799-830, pág. 806; Centre for Information Policy Leadership, *The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement* (May 2024), 14: https://is.gd/1eS645. Consultado el 17 de octubre de 2025.

práctica conocida como *forum shopping*[36]. Estas circunstancias pueden dar lugar a una protección desigual del derecho fundamental a la protección de datos en la UE,[37] dependiendo de la autoridad de control encargada de hacer cumplir las disposiciones de protección de datos.

El sistema de ventanilla única es particularmente relevante en el contexto irlandés, dado su entorno corporativo tecnológico, con la presencia de los establecimientos principales de algunas de las mayores empresas tecnológicas del mundo. La DPC actúa con frecuencia como autoridad de control principal en muchos casos importantes de tratamiento de datos transfronterizos. Por ello, la DPC tiene la responsabilidad de hacer cumplir las normativas de protección de datos no solo para los residentes en Irlanda, sino también para los individuos de toda la UE cuando sus datos son tratados por estos gigantes tecnológicos. Esto reviste una gran importancia, ya que la autoridad de control principal puede influir de manera decisiva en los procedimientos de protección de datos, desde el alcance de la investigación hasta la magnitud de las sanciones y su aplicación[38]. Las acciones y decisiones de la DPC en este ámbito pueden tener implicaciones de gran alcance para los estándares de protección de datos a través de la Unión.

2. IMPLICACIONES DEL ENTORNO FAVORABLE A LAS EMPRESAS EN IRLANDA

El entorno favorable a las empresas en Irlanda se caracteriza por varios factores clave que atraen a las empresas tecnológicas. Uno de los más trascendentes es el impuesto de sociedades, que, con un 12,5%, es uno de los más bajos de la UE[39]. Este tipo impositivo, combinado con diversos incentivos fiscales para la investigación y el desarrollo[40], hace de Irlanda un destino atractivo y estratégico para las corporaciones multinacionales. Además, es el único país de habla inglesa que permanece en la UE después del Brexit, junto con Malta. Cabe mencionar que, a partir del 1 de enero de 2024, el tipo impositivo del 12,5% ya no resulta aplicable a las empresas con ingresos superiores a 750 millones de euros (lo que incluye a muchas de las grandes empresas tecnológicas con sede en Irlanda).

---

36 D. Matos Brandão (2023, pág. 322).

37 J. Lin (2024), «More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance», *Columbia Journal of Transnational Law*, pág. 17

38 G. Gentile y O. Lynskey (2022, pág. 809).

39 Corporation Tax (CT): https://is.gd/wMk9q7. Consultado el 17 de octubre de 2025; A. Walsh y C. Sanger (2020), «The Historical Development and International Context of the Irish Corporate Tax System: A Report Commissioned by the Irish Department of Finance», *Departamento de Finanzas*, pág. 1.

40 Revenue Commissioners (2024), «Research & Development (R&D) Corporation Tax Credit - Tax and Duty Manual Part 29-02-03», *Comisionados de Hacienda*, pág. 5.

Como se explicará más adelante en la sección IV.3, Irlanda adoptó el acuerdo de Dos Pilares de la Organización para la Cooperación y el Desarrollo Económicos ('OCDE'), que incluye un tipo impositivo mínimo global efectivo del 15% para las entidades dentro de su ámbito de aplicación. Este se implementará mediante un impuesto complementario, añadido al impuesto de sociedades bajo las normas nacionales, para alcanzar el tipo efectivo del 15%[41].

Aunque este régimen fiscal favorable ha atraído a un número notable de empresas extranjeras, estos beneficios implican una serie de desafíos para Irlanda. El gobierno irlandés debe equilibrar un entorno favorable a los negocios con la necesidad de aplicar estrictamente las leyes de protección de datos bajo el RGPD. La presencia de estos gigantes tecnológicos significa que la DPC desempeña un papel desproporcionadamente grande en la regulación de la protección de los datos dentro de la UE, lo que añade presión tanto sobre la DPC como sobre el gobierno para garantizar el cumplimiento sin desincentivar la inversión empresarial. Estos incentivos fiscales reflejan la intención del gobierno irlandés de atraer y retener la inversión extranjera en el país. Sin embargo, dicha agenda podría entrar en conflicto con el deber de la DPC de hacer cumplir las leyes de protección de datos.

El papel de la DPC irlandesa como autoridad de control principal para muchas de estas empresas tecnológicas la sitúa a la vanguardia de la aplicación del RGPD. Esto ha generado diversas críticas. La DPC ha sido acusada de ser lenta en la investigación y resolución de reclamaciones de protección de datos. Por ejemplo, un informe reveló que, hasta mayo de 2021, el 98% de los 164 casos transfronterizos significativos seguían sin resolverse[42]. Este ritmo lento ha provocado críticas tanto de defensores de la privacidad como de otras autoridades de protección de datos de la UE, quienes argumentan que la ineficiencia de la DPC obstaculiza la eficacia general del RGPD[43].

El enfoque de la DPC en la aplicación de la normativa también ha sido criticado por ser demasiado indulgente. Los críticos argumentan que la DPC prefiere resolver los problemas mediante acuerdos amistosos en lugar de imponer multas, lo que podría reducir el efecto disuasorio de las sanciones del RGPD[44]. Además,

---

41 Minister McGrath notes Ireland's application of effective 15% corporation tax rate for in-scope businesses: https://is.gd/O72Be8. Consultado el 17 de octubre de 2025.

42 Irish Council for Civil Liberties (2021), «Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities», *ICCL*, págs. 5-7; Key Takeaways from the Irish DPC's 2022 Annual Report: https://is.gd/TTy1a7. Consultado el 17 de octubre de 2025.

43 Irish Council for Civil Liberties (2021), «Submission on the GDPR to the Joint Oireachtas Committee on Justice», *ICCL*, págs. 7-10.

44 V. Manancourt (2021), «Ireland frets as criticism over Big Tech links goes mainstream», *Politico*, https://is.gd/xRKFoq. Consultado el 17 de octubre de 2025; Irish DPC Challenges EDPB Jurisdiction in Meta Investigation, https://is.gd/kcqngi.

la DPC solo ha impuesto 35 multas desde la entrada en vigor del RGPD, una cantidad considerablemente baja en comparación con algunas de sus homólogas, como Francia (73 multas), Alemania (218 multas), Italia (446 multas) y España (1.026 multas)[45], este último con un presupuesto incluso menor que el de la DPC, como se analizó antes en este artículo. Esta indulgencia se percibe como influenciada por los beneficios económicos generales que estas empresas tecnológicas aportan a Irlanda, creando un conflicto de intereses que complica el papel de la DPC[46].

De hecho, la eficiencia de la DPC es inferior en comparación con sus homólogas, incluso cuando el presupuesto con el que opera es similar en algunos casos. Esta menor tasa de resolución pone de manifiesto las preocupaciones continuas sobre la capacidad de la DPC para gestionar de manera efectiva su carga de trabajo, incluso con un presupuesto ampliado[47]. Incluso las decisiones más recientes de la DPC, que han resultado en las mayores multas impuestas bajo el RGPD a algunas de estas empresas tecnológicas, han sido objeto de críticas, ya que el CEPD ha tenido que corregir el enfoque inicial de la DPC, como se discutirá en la siguiente sección. En este contexto, la confianza en el sistema de ventanilla única se ha ido perdiendo gradualmente, y algunas autoridades de control nacionales prefieren eludir el mecanismo de coordinación del RGPD en busca de una mayor eficacia[48]. También se han hecho llamamientos a favor de un modelo diferente y centralizado[49], ya que el CEPD ha demostrado su eficacia al intervenir en investigaciones transfronterizas.

La posición estratégica de Irlanda como centro para las principales empresas tecnológicas trae tanto oportunidades como desafíos. Mientras que el entorno favorable a los negocios atrae una inversión extranjera importante, también ejerce una enorme presión sobre la DPC para que aplique eficazmente las normativas del RGPD. Por lo tanto, la DPC no solo está bajo presión por parte de los Esta-

Consultado el 17 de octubre de 2025; Ireland's failure to enforce EU law against Big Tech is slowing down Europe's GDPR enforcement, <https://www.emarketer.com/content/ireland-s-failure-enforce-eu-law-against-big-tech-slowing-down-europe-s-gdpr-enforcement>. Consultado el 17 de octubre de 2025.

45 Statistics: Countries with highest fines (Top 10): https://is.gd/59evXU. Consultado el 17 de octubre de 2025.

46 V. Manancourt (2021).

47 Irish Council for Civil Liberties (2021), «Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights, Submission on the GDPR to the Joint Oireachtas Committee on Justice», *ICCL*, pág. 7; Irish Council for Civil Liberties (2021), «Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities», *ICCL*, pág. 7.

48 D. Matos Brandão (2023, pág. 319).

49 *Ibid.,* pág. 326.

dos miembros de la UE, sino también de las grandes empresas tecnológicas y del propio gobierno irlandés.

IV. CASOS DESTACADOS Y CRÍTICAS

1. EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS AL MANDO DEL SISTEMA DE VENTANILLA ÚNICA

Como se explicó anteriormente, tanto la inacción como la tenue acción de la DPC han sido objeto de críticas, lo cual se ha hecho más evidente en los casos que han tenido que ser resueltos de manera definitiva por el CEPD.

De conformidad con el sistema de ventanilla única, una autoridad de control principal que lleve a cabo una investigación debe someter, sin demora, un proyecto de decisión a las demás autoridades de control interesadas para que emitan su opinión y tomar debidamente en cuenta sus puntos de vista[50]. Además, el RGPD contiene un mecanismo de resolución de disputas mediante el cual, cuando otras autoridades de control planteen una objeción pertinente y fundamentada a un proyecto de decisión de la autoridad de control principal, o esta haya rechazado dicha objeción por considerarla no pertinente o no fundamentada, el CEPD adoptará una decisión vinculante. La autoridad de control principal deberá adoptar su decisión final basándose en la decisión del CEPD[51].

Varios casos han puesto de manifiesto el enfoque de la DPC en la aplicación de la protección de datos como autoridad de control principal, así como la importancia de la potestad del CEPD para intervenir en la protección del derecho fundamental de la UE a la protección de datos. Los más relevantes han tenido como principales actores a empresas como X, Meta y TikTok. La tabla 2 contiene una comparativa con respecto a las sanciones impuestas por la DPC inicialmente y aquellas impuestas derivadas de la intervención del CEPD.

2. ANALIZANDO EL ENFOQUE DE LA DATA PROTECTION COMMISSION

Como se puede observar en el análisis de los casos anteriores, el enfoque de la DPC ha sido inicialmente conservador y cauteloso a la hora de investigar y sancionar a las grandes empresas tecnológicas con sede en Irlanda. Este enfoque es evidente en los proyectos de decisiones iniciales y las sanciones propuestas, que a menudo parecen relativamente indulgentes dada la magnitud e impacto de las violaciones de protección de datos involucradas. En todos los casos, la DPC propuso multas bajas, a pesar del consenso generalizado entre otras auto-

[50] RGPD, art. 60(3).
[51] *Ibid.,* art. 65 (1)(6).

TABLA 2. *Comparación entre sanciones de la DPC y del CEPD*

Caso	Sanción inicial de la DPC	Sanción posterior a la intervención del CEPD
Twitter[1]	Multa administrativa de entre €135.000 y €275.000.	Multa de €450.000[2]
Whatsapp[3]	Multa de entre 30 y 50 millones de euros.	Multa de €225.500.000[4]
Instagram [5]	Multa de entre 202 y 405 millones de euros.	Multa de €405.000.000, más diversas medidas correctivas adicionales[6].
Facebook[7] *(no hay versión disponible en español)*	Multa de entre 28 y 36 millones de euros.	Multa de €210.000.000[8]
Facebook 2[9] *(no hay versión disponible en español)*	Suspensión de transferencias internacionales de datos con los Estados Unidos, pero decidió no imponer una multa administrativa.	Multa de €1.200.000.000[10]
TikTok[11]	Diversas multas: 2. 2 multas de entre 55 y 100 millones de euros por la infracción de los artículos 5(1)(c) y (f) y 25(1) y (2) del RGPD. 3. Multa de entre 110 y 180 millones de euros por la infracción de los artículos 12(1) y 13(1)(e) del RGPD.	Multa de €345.000.000[12]

1 CEPD (2020), Decisión 01/2020 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con Twitter International Company con arreglo al art. 65, apartado 1, letra a) del RGPD.

2 Data Protection Commission announces decision in Twitter inquiry: https://is.gd/UjMZYz. Consultado el 17 de octubre de 2025.

3 CEPD (2021), Decisión vinculante 1/2021 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con WhatsApp Ireland con arreglo al art. 65, apartado 1, letra a), del RGPD.

4 Data Protection Commission announces decision in WhatsApp inquiry: https://is.gd/aSVLaY. Consultado el 17 de octubre de 2025.

5 CEPD (2022), Decisión vinculante 2/2022 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con Meta Platforms Ireland Limited (Instagram) con arreglo al art. 65, apdo. 1, letra a), del RGPD.

6 Data Protection Commission announces decision in Instagram Inquiry: https://is.gd/oJWRhD. Consultado el 17 de octubre de 2025.

7 CEPD (2022), Decisión Vinculante 3/2022 sobre la disputa presentada por la autoridad irlandesa contra Meta Platforms Ireland Limited y su servicio de Facebook (art. 65 del RGPD).

8 DPC (2022), Final Decision in the Matter of LB and Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service, pág.154.

9 CEPD (2023), Decisión Vinculante 1/2023 sobre la disputa presentada por la autoridad irlandesa relativa a las transferencias de datos realizadas por Meta Platforms Ireland Limited para su servicio de Facebook (art. 65 del RGPD).

10 DPC (2023), Final Decision in the Matter of Maximilian Schrems and Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) Regarding Facebook Data Transfers, pág. 214.

11 CEPD (2023), Decisión vinculante 2/2023 sobre la controversia planteada por la AC irlandesa en relación con TikTok Technology Limited (art. 65 del RGPD).

12 DPC (2023), Final Decision in the Matter of TikTok Technology Limited Regarding the Processing of Children's Data, pág.122.

ridades de supervisión europeas de que estas cifras no reflejaban la gravedad de las infracciones.

El enfoque de la DPC podría reflejar una estrategia nacional más amplia para mantener la atractividad de Irlanda como centro de negocios para estos gigantes globales. Al proponer inicialmente multas más bajas y adoptar una postura más reservada, la DPC podría estar buscando equilibrar la aplicación de las leyes de protección de datos con los intereses económicos en juego. Además, este enfoque cauteloso pone de relieve los desafíos inherentes a la regulación de poderosas corporaciones multinacionales. En este contexto, el tamaño del presupuesto desempeña un papel importante. Aquí es donde el papel del CEPD se ha vuelto esencial para la correcta aplicación de la legislación de protección de datos. El CEPD ha intervenido de manera constante, ordenando acciones de aplicación más estrictas y multas más elevadas que las inicialmente propuestas por la DPC. La intervención del CEPD ha garantizado que los resultados finales de estos casos estén más alineados con los principios de sanciones efectivas, proporcionales y disuasorias previstos por el RGPD. Debido a estas circunstancias, han surgido varios argumentos a favor de un modelo de aplicación más centralizado, cuestionando la eficacia del sistema de ventanilla única[52].

El enfoque conservador y cauteloso de la DPC en la investigación y sanción de las grandes empresas tecnológicas refleja una compleja interacción de consideraciones económicas, desafíos regulatorios y la necesidad de una solidez jurídica. Sin embargo, los mecanismos estructurados de cooperación y resolución de disputas dentro del RGPD, ejemplificados por las intervenciones decisivas del CEPD, desempeñan un papel crucial en el fortalecimiento de la integridad de la aplicación de la protección de datos en toda la UE. Esta dinámica garantiza que, incluso si las propuestas iniciales son conservadoras, las acciones regulatorias finales sean lo suficientemente estrictas como para cumplir con los objetivos del RGPD y proteger de manera efectiva los derechos de los interesados.

3. ¿PROTECCIÓN DE DATOS VS. CRECIMIENTO ECONÓMICO?

A la luz del análisis anterior, queda claro que Irlanda se encuentra en una encrucijada donde la aplicación de las normativas de protección de datos y el mantenimiento de su entorno favorable a los negocios aparecen como prioridades en competencia. ¿Cómo puede entonces el país equilibrar ambas? Las complejas implicaciones ejercen una gran presión sobre el gobierno irlandés.

Se podría argumentar que el mandato del Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE) es ineludible y, por lo tanto, el país está obligado a aplicar las normativas de protección de datos con toda la fuerza de la ley. Ambos tratados enfatizan la importancia de proteger los derechos fundamentales, incluida la protección de datos, consagrada en el art.

[52] D. Matos Brandão (2023, pág. 326).

8 de la Carta de los Derechos Fundamentales de la UE (CDFUE). En este mismo sentido, los Reglamentos de la UE son directamente aplicables a los Estados miembros[53] y, como tal, Irlanda está obligada a hacer cumplir adecuadamente el RGPD. En otro ámbito, la comunidad internacional ha adoptado el compromiso de imponer un tipo impositivo mínimo universal del 15% a través del Enfoque de Dos Pilares de la OCDE[54] para abordar los desafíos fiscales de la economía digital. En línea con el Pilar Dos, el 14 de diciembre de 2022, se adoptó la Directiva 2022/2523[55], con la obligación para los Estados miembros de transponerla en su legislación a más tardar el 31 de diciembre de 2023[56]. Irlanda transpuso la Directiva 2022/2523 en la Parte 4A de la Ley de Consolidación Fiscal de 1997 (*Taxes Consolidation Act 1997*), con dicho tipo impositivo aplicable desde el 1 de enero de 2024. Sin embargo, no está claro si esto podría cambiar las circunstancias para Irlanda[57]. A pesar de que las multinacionales, incluidas las grandes empresas tecnológicas con sede en Irlanda, deberán pagar un mínimo del 15% en impuestos de sociedades, este porcentaje sigue siendo bajo en comparación con otros Estados miembros.

Cabe destacar que Irlanda mantendrá su tipo impositivo de sociedades del 12,5% para las empresas que no estén cubiertas por el pilar dos, específicamente aquellas con ingresos inferiores a 750 millones de euros. En consecuencia, más del 99 % de las empresas que operan en Irlanda no estarán sujetas al tipo impositivo mínimo global efectivo del 15%[58]. Además, las políticas fiscales de Irlanda ya han atraído la atención de la Comisión en asuntos de competencia, como en la investigación iniciada sobre la base de las normas sobre ayudas de Estado y el art. 107 del TFUE[59], según el cual un Estado no puede otorgar apoyo gubernamental, salvo en casos excepcionales, cuando las intervenciones del gobierno sean necesarias para una economía bien estructurada y equitativa[60]. En el caso de las ayudas de Estado de Apple, la Comisión Europea concluyó que Irlanda debía recuperar

53 Según el art. 288 de la Versión Consolidada del Tratado de Funcionamiento de la Unión Europea (2012), DO C326/47.

54 OECD/G20 Base Erosion and Profit Shifting Project (2021), «Tax Challenges Arising from Digitalisation of the Economy: Global Anti-Base Erosion Model Rules (Pillar Two)», *OECD Publishing*.

55 Directiva (UE) 2022/2523 del Consejo de 14 de diciembre de 2022 relativa a la garantía de un nivel mínimo global de imposición para los grupos de empresas multinacionales y los grupos nacionales de gran magnitud en la Unión, DO L328/1.

56 *Ibid.,* art. 56.

57 The global corporation tax rate: what are the implications for Ireland? https://is.gd/9CXBEG. Consultado el 17 de octubre de 2025.

58 Minister McGrath notes Ireland's application of effective 15% corporation tax rate for in-scope businesses: https://is.gd/O72Be8. Consultado el 17 de octubre de 2025.

59 TFUE, art. 107.

60 State Aid Overview: https://is.gd/mt388z. Consultado el 17 de octubre de 2025.

13.000 millones de euros por ayudas indebidas otorgadas a Apple[61]. El caso llegó al TJUE, que ha confirmado las conclusiones de la Comisión[62]. Más allá del resultado del caso, pueden observarse ciertas similitudes entre las prácticas anticompetitivas y el enfoque de Irlanda en la aplicación de la protección de datos, en términos de cómo afectan a otros Estados miembros de la UE. De hecho, mientras que otras autoridades de control ejercen una presión constante sobre las empresas multinacionales mediante la aplicación de la legislación de protección de datos, la pasividad y cautela de Irlanda pueden percibirse como una estrategia para posicionarse como un país ideal para el *forum shopping*, con el objetivo de incrementar la inversión extranjera.

Por lo tanto, a través de las medidas fiscales mencionadas anteriormente, combinadas con una débil aplicación de la legislación de protección de datos, Irlanda concentra y se beneficia de la inversión extranjera ofrecida por empresas multinacionales, en contraposición con los esfuerzos onerosos de otros Estados miembros por cumplir estrictamente con la normativa de protección de datos. Por otro lado, el hecho de que Irlanda sea la autoridad de control principal para la mayoría de los casos transfronterizos de protección de datos en la UE implica que el peso de la aplicación de esta normativa no solo recae sobre los hombros de la DPC, sino también sobre los residentes irlandeses. Por ejemplo, si es necesario un presupuesto mayor para abordar adecuadamente estos casos, dicho aumento podría traducirse en una mayor carga fiscal para la población o, al menos, para las corporaciones, lo que podría contradecir el objetivo de atraer y mantener empresas extranjeras.

Irlanda se enfrenta al desafío de equilibrar la aplicación estricta de las normativas de protección de datos con el mantenimiento de un entorno favorable a los negocios para atraer inversión extranjera. Las obligaciones legales del país exigen una aplicación rigurosa de la protección de datos, pero el enfoque de Irlanda parece estar más orientado a fomentar su atractivo como centro para multinacionales. Estas condiciones plantean interrogantes sobre la equidad de las prácticas económicas. Mientras Irlanda navega por estas dinámicas complejas, fortalecer a la DPC parece una tarea imperativa. Más allá de las limitaciones presupuestarias, contar con un organismo verdaderamente fuerte e independiente podría ser el primer paso hacia una solución.

Para abordar los desafíos presentados en la sección anterior, Irlanda debe mejorar las capacidades e independencia de la DPC. Fortalecer los recursos de la DPC, tanto en términos de presupuesto como de independencia y experiencia,

---

61 State aid: Ireland gave illegal tax benefits to Apple worth up to €13 billion: https://is.gd/Qc8Mxuz. Consultado el 17 de octubre de 2025.

62 TJUE (2024), «Caso C-465/20 P», *EUR-Lex*, ECLI:EU:C:2024:724, disponible en: https://is.gd/JapGq8.; European Commission, Remarks by Executive Vice-President Vestager following the Court of Justice rulings on the Apple tax State aid and Google Shopping antitrust cases: https://is.gd/mUjMXY. Consultado el 17 de octubre de 2025.

es esencial para garantizar una aplicación sólida de las leyes de protección de datos[63]. El presupuesto actual de la DPC, aunque ha aumentado visiblemente a lo largo de los años, podría seguir representando un obstáculo para su eficacia, dado el alto volumen de casos complejos que maneja. Es fundamental implementar medidas que aseguren la independencia de la DPC de influencias gubernamentales y corporativas. Esto puede lograrse mediante el establecimiento de marcos legislativos claros que protejan a la DPC de influencias externas, proporcionándole la autonomía necesaria para tomar decisiones imparciales[64]. Irlanda debe emprender reformas integrales para fortalecer a la DPC. Asegurar su independencia, aumentar las asignaciones presupuestarias y mejorar sus capacidades son pasos esenciales. Estas reformas ayudarán a que la DPC aplique los estándares de protección de datos de manera más efectiva, mientras mantiene la reputación de Irlanda como un entorno favorable para los negocios.

V. EL PAPEL DE LA DATA PROTECTION COMMISSION A LA LUZ DE LA NUEVA ESTRATEGIA DIGITAL DE LA UNIÓN EUROPEA

Con la estrategia digital de la UE se están adoptando diversas nuevas normativas para restaurar y preservar su soberanía digital[65]. A la vanguardia de esta estrategia se encuentran el DSA[66] y el *AI Act*[67]. Ambas normativas prevén mecanismos de aplicación similares a los del RGPD y, por ello, es fundamental abordar eficazmente los problemas de aplicación que implica el RGPD para evitar que se

63 Irish Council for Civil Liberties (2021), «Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights, Submission on the GDPR to the Joint Oireachtas Committee on Justice», *ICCL*, pág. 13.

64 F. Brito Bastos y P. Pałka (2023), «Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?», *European Constitutional Law Review*, 19, págs. 487-517, pág. 511.

65 Comisión Europea (2021), «2030 Digital Compass: The European Way for the Digital Decade (Communication)», *COM(2021) 118 final*, pág. 1; E. Celeste (2021), «Digital Sovereignty in the EU: Challenges and Future Perspectives», en F. Fabbrini, E. Celeste y J. Quinn (eds.), «Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty», *Hart*.

66 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un Mercado Único de Servicios Digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), *DO L277/1* (DSA').

67 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) *DO L1689/1 (AI Act)*.

reproduzcan en estas nuevas normativas. Los mismos grandes actores que están sujetos a las disposiciones del RGPD estarán también sujetos a las disposiciones del DSA y del *AI Act,* por lo que podrían surgir complicaciones similares al tratar de aplicar la legislación de la UE.

En el caso del DSA, el Estado Miembro en el que se encuentra el establecimiento principal del proveedor de servicios intermediarios tiene competencias exclusivas para supervisar y aplicar el Reglamento[68]. Por su parte, en el *AI Act,* serán las autoridades nacionales competentes las encargadas de aplicar dicho Reglamento[69]. Aunque las estructuras de aplicación de estas normativas presentan diferencias importantes con el sistema de ventanilla única y el mecanismo de resolución de disputas del RGPD, algunas disposiciones sobre la aplicación son similares y, por lo tanto, podrían plantear las mismas complicaciones. Estas mismas complejidades podrían resonar nuevamente en el caso de Irlanda. El peso completo de la estrategia digital de la UE está a las puertas de Irlanda y parece poco probable que el país pueda enfrentarlo con la misma fuerza requerida.

La aplicación desigual de reglamentos como el RGPD, discutida anteriormente, podría estar obstaculizando los objetivos de la UE de consolidar su firme control sobre el mercado digital. Si se implementan más regulaciones de manera similar, el estandarte de los derechos fundamentales que la UE utiliza como justificación para avanzar en su estrategia digital, junto con el paquete de reglamentos y directivas que ha implementado en los últimos años, podría empezar a tambalearse. La correcta implementación del DSA y del *AI Act* representará los próximos desafíos tanto para Irlanda como para la UE. Por lo tanto, es necesario comprender las diferencias y similitudes que comparten estos mecanismos. Este ejercicio puede arrojar luz sobre cómo abordar la implementación y la aplicación de manera más efectiva.

1. NUEVAS NORMATIVAS Y RESPONSABILIDADES

1.1. Reglamento de Servicios Digitales (DSA)

El DSA establece obligaciones aplicables a los prestadores de servicios intermediarios en línea, particularmente a las plataformas en línea, las plataformas en línea de muy gran tamaño (VLOP, por sus siglas en inglés) y los motores de búsqueda en línea de muy gran tamaño (VLOSE, por sus siglas en inglés) [70]. Su objetivo es garantizar la seguridad de los usuarios, proteger los derechos fundamentales y crear un entorno justo y abierto en las plataformas en línea[71]. Este Reglamento incluye obligaciones generales para los prestadores de servicios,

[68] DSA, art. 56(1).
[69] *AI Act,* considerando (80).
[70] DSA, considerando (41).
[71] The Digital Services Act. https://is.gd/PrfzKO. Consultado el 17 de octubre de 2025.

como la presentación de informes de transparencia, la designación de puntos de contacto con las autoridades, la adecuación de términos y condiciones, y la gestión de notificaciones[72]. También establece obligaciones específicas según el tipo de servicio de intermediación proporcionado, así como obligaciones adicionales para las VLOP y los VLOSE. El DSA exige la creación de autoridades competentes para supervisar y hacer cumplir sus disposiciones, designadas como Coordinadores de Servicios Digitales (CSD)[73]. Estos CSD son designados por cada Estado Miembro y, en conjunto, forman un mecanismo de cooperación con la Comisión Europea y la Junta Europea de Servicios Digitales (JESD)[74].

Los CSD tienen potestades de investigación y aplicación respecto a los prestadores de servicios intermediarios que caen dentro de la competencia de su Estado miembro, así como algunas potestades adicionales relacionadas con servicios de intermediación en su jurisdicción[75]. De manera similar al sistema de ventanilla única del RGPD, el DSA contiene un mecanismo de coherencia para asuntos transfronterizos destinado a lograr una aplicación coordinada y homogénea.

Cuando un CSD tiene razones para sospechar que un proveedor de servicios de intermediación ha infringido el DSA de manera que afecta negativamente a los receptores del servicio en el Estado miembro de dicho CSD, puede solicitar al CSD del Estado miembro donde el prestador tiene su establecimiento principal (CSD del prestador) que evalúe el asunto y tome las medidas de investigación y aplicación necesarias para garantizar el cumplimiento de este Reglamento. A menos que la Comisión haya iniciado una investigación por la misma presunta infracción, y a solicitud de al menos tres CSD que tengan razones para sospechar que un proveedor específico de servicios de intermediación ha infringido este reglamento de manera que afecta negativamente a los receptores del servicio en sus respectivos Estados miembros, la JESD puede solicitar al CSD del prestador que evalúe el asunto y tome las medidas de investigación y aplicación necesarias para garantizar el cumplimiento de este reglamento[76].

El CSD del prestador deberá, a más tardar dos meses después de recibir la solicitud, comunicar al CSD que envió la solicitud y a la JESD la evaluación de la presunta infracción y una explicación de las medidas de investigación o aplicación adoptadas o previstas en relación con esta, para garantizar el cumplimiento de este Reglamento[77]. En caso de que no se reciba dicha comunicación dentro del período indicado, si existe un desacuerdo de la JESD con la determinación, o

72 DSA, arts. 11, 12, 14 y 15.
73 *Ibid.,* art. 49.
74 *Ibid.*
75 *Ibid.,* art. 51.
76 *Ibid.,* art. 58(2)(3).
77 *Ibid.,* art. 58(5).

en los casos mencionados en el art. 60(3), la JESD podrá remitir el asunto a la Comisión Europea[78].

Cuando la Comisión considere que la evaluación o las medidas de investígación o aplicación adoptadas o previstas son insuficientes, comunicará su opinión al CSD del prestador y a la JESD, y solicitará al CSD del prestador que revise el asunto[79]. El CSD del prestador deberá tomar las medidas necesarias para garantizar el cumplimiento de este Reglamento, teniendo en cuenta en la mayor medida posible las opiniones y la solicitud de revisión de la Comisión., y deberá informar las medidas adoptadas a los actores correspondientes[80].

Aunque los mecanismos de supervisión y aplicación contenidos en el DSA difieren del sistema de ventanilla única del RGPD, pueden observarse algunas similitudes. Al igual que en el sistema de ventanilla única, la responsabilidad inicial de supervisar y aplicar el DSA recae en una autoridad de supervisión, en este caso los CSD, del Estado Miembro donde el proveedor de servicios de intermediación tiene su establecimiento principal. Asimismo, el DSA prevé un mecanismo de resolución de disputas mediante el cual la Comisión Europea puede intervenir para corregir o modificar las determinaciones del CSD.

1.2. Reglamento de Inteligencia Artificial (AI Act)

En la UE no puede planificarse, diseñarse ni implementarse un sistema de inteligencia artificial sin una adecuada gobernanza y cumplimiento de la protección de datos[81]. Como tal, el AI Act tiene una relación aún más estrecha con el RGPD, ya que el Reglamento requerirá una autoridad nacional encargada de garantizar su cumplimiento, y la estructura ya implementada para el RGPD podría servir perfectamente como base[82].

De acuerdo con el art. 70 del *AI Act,* cada Estado Miembro deberá establecer o designar, como autoridades competentes nacionales, al menos una autoridad notificante (AN), responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad y para su supervisión[83], y al menos una autoridad

78 *Ibid.,* art. 59.

79 *Ibid.,* art. 59(3).

80 *Ibid.,* art. 59.

81 Véase: R. Herrera de las Heras (2022), «Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil», *Dykinson, S.L.*, pág. 52; M. Janssen y otros (2020), «Data Governance: Organizing Data for Trustworthy Artificial Intelligence», *Government Information Quarterly*, 37(4), 101493.

82 CEPD (2024), «Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework», *CEPD*, pág. 4.

83 AI Act, art. 3(19).

de vigilancia del mercado (AVM) para los fines de este Reglamento. Estas autoridades competentes nacionales deberán ejercer sus potestades de forma independiente, imparcial y sin sesgos, a fin de salvaguardar la objetividad de sus actividades y tareas, y garantizar la aplicación e implementación del *AI Act*[84]. Al igual que el RGPD y el DSA, el *AI Act* crea una autoridad centralizada para facilitar la cooperación y coordinación entre las autoridades nacionales de supervisión, denominado Consejo Europeo de Inteligencia Artificial (CEIA) [85]. Sin embargo, a diferencia del CEPD y la JESD, el CEIA carece de potestades de aplicación, las cuales están conferidas a la Comisión Europea.

Los artículos 79 a 83 del AI Act establecen un procedimiento para tratar con sistemas de IA que puedan presentar un riesgo. Según este procedimiento, una AVM que tenga razones suficientes para considerar que un sistema de IA representa un riesgo para la salud, la seguridad o los derechos fundamentales de las personas deberá llevar a cabo una evaluación del sistema de IA. Si la AVM determina que el sistema de IA no cumple con el Reglamento, deberá solicitar al operador que adopte medidas correctivas o retire el sistema del mercado[86]. Cuando la AVM considere que el incumplimiento no se limita a su territorio nacional, deberá informar a la Comisión y a los demás Estados miembros, sin demora indebida, sobre los resultados de la evaluación y las medidas que ha requerido al operador. Las AVM distintas de la del Estado Miembro que inició el procedimiento deberán informar a la Comisión y a los demás Estados miembros de cualquier medida adoptada y de cualquier información adicional que tengan sobre el incumplimiento del sistema de IA en cuestión, y, en caso de desacuerdo con la medida notificada por la AVM que inició el procedimiento, comunicar sus objeciones. Si, dentro de los tres meses posteriores, ninguna AVM de un Estado Miembro ni la Comisión Europea plantean objeciones a una medida provisional adoptada por una AVM de otro Estado Miembro, dicha medida se considerará justificada[87]. Este mismo procedimiento debe llevarse a cabo también en los casos en que una AVM tenga razones suficientes para considerar que un sistema de IA clasificado por el proveedor como no de alto riesgo, de acuerdo con el art. 6(3), es en realidad de alto riesgo, y para aquellos sistemas de alto riesgo que, aunque cumplan con el AI Act, puedan aún representar un riesgo para la salud, la seguridad de las personas o los derechos fundamentales[88].

De manera similar a los mecanismos de resolución de disputas del RGPD y el DSA, el *AI Act* establece un procedimiento de salvaguardia a nivel de la Unión, mediante el cual se evalúan las medidas adoptadas por las AVM cuando estas han sido objetadas por otras AVM o cuando la Comisión considera que la medida

84 *Ibid.,* art. 70(1).
85 *Ibid.,* art. 66.
86 *Ibid.,* art. 79(2).
87 *Ibid.,* art. 79(3)(7)(8).
88 *Ibid.,* arts. 80(1), 82(1).

contraviene el derecho de la Unión. La Comisión, sin demora indebida, deberá entablar consultas con la AVM del Estado Miembro correspondiente y con el operador u operadores implicados, y evaluará la medida. Sobre la base de los resultados de dicha evaluación, la Comisión decidirá si la medida está justificada y notificará su decisión a la AVM del Estado Miembro en cuestión. Asimismo, la Comisión informará a todas las demás AVM de su decisión. Las AVM estarán vinculadas por la decisión de la Comisión, y la medida adoptada será mantenida o retirada en consecuencia[89].

A la luz de lo anterior, está claro que, para el *AI Act,* es la Comisión quien asumirá el rol del CEPD y de la JESD para el RGPD y el DSA, respectivamente. La Comisión actuará como mediadora y conductora del proceso de resolución de disputas cuando las medidas adoptadas por una AVM sean cuestionadas por otras AVM. Solo en el caso de los modelos de IA de uso general ('GPAI', por sus siglas en inglés)[90], la Comisión, a través de la Oficina de IA, tendrá potestades exclusivas para supervisar y hacer cumplir el *AI Act*[91].

Como puede apreciarse del análisis anterior, se están desplegando mecanismos similares al sistema de ventanilla única y al mecanismo de resolución de disputas del RGPD para garantizar el cumplimiento tanto del DSA como del AI Act. Sin embargo, si los defectos antes advertidos del sistema de ventanilla única no se corrigen antes de la implementación completa de estas dos normativas, estos vicios se transmitirán a la aplicación de ambas legislaciones.

VI. CONCLUSIONES

La trayectoria de la DPC destaca la naturaleza compleja y en constante evolución de la protección de datos en la UE. Como autoridad de control principal para muchas de las mayores empresas tecnológicas del mundo, la DPC ha enfrentado desafíos sustanciales para equilibrar sus responsabilidades con las expectativas que tanto la UE como sus ciudadanos han depositado en ella.

Se han señalado diversas complejidades en la aplicación del sistema de coordinación de la UE. En particular, este articulo se centra en las que surgen de la implementación del RGPD, DSA y *AI Act,* ya que dichas normativas comparten mecanismos de investigación y aplicación similares.

El sistema de ventanilla única del RGPD ha sido evaluado y criticado constantemente por su falta de eficacia frente a los principales actores del ámbito digital, lo que ha puesto a Irlanda en el punto de mira de la UE debido a sus circuns-

89 *Ibid.*, art. 81(1)(2).

90 De conformidad con el art. 3(63) del *AI Act,* los GPAI son modelos de inteligencia artificial que muestran una generalidad significativa y son capaces de desempeñar de manera competente una amplia gama de tareas distintas.

91 *Ibid.,* art. 88.

tancias únicas. Los mecanismos de coordinación y aplicación del DSA y del *AI Act* siguen gran parte del modelo del sistema de ventanilla única y, por lo tanto, podrían plantear preocupaciones similares en estas dos normativas. ¿Se replicarán las complejidades de la aplicación del RGPD en asuntos transfronterizos en toda la estrategia digital europea?

Esta pregunta resulta aún más relevante considerando la manera en que cada Estado Miembro podría determinar las autoridades nacionales de supervisión para el DSA y el AI Act. En el caso del *AI Act,* el CEPD recomendó que la carga de la aplicación recaiga sobre las autoridades nacionales de protección de datos[92]. Aunque el Comité presenta un argumento sólido al señalar que sería prudente aprovechar la experiencia y el conocimiento de las autoridades de protección de datos[93], este razonamiento también podría implicar una carga aún mayor para algunos reguladores ya sobrecargados, como la DPC. Para autoridades nacionales de protección de datos, como la DPC, cumplir con tantas responsabilidades adicionales frente a los mismos grandes actores podría volverse mucho más complicado. Sin las reformas integrales necesarias para fortalecer la DPC, imponer responsabilidades mayores no hará más que empeorar una ya debilitada aplicación de la legislación de la UE y aumentar las preocupaciones de otros Estados miembros y de las autoridades centralizadas de la UE. Si la aplicación de la estrategia digital de la UE sigue recayendo sobre los hombros de Irlanda, los objetivos de la UE podrían verse amenazados.

Compartir las responsabilidades de aplicación entre múltiples autoridades nacionales de protección de datos, cada una con experiencia específica en diferentes áreas regulatorias, podría proporcionar un sistema más equilibrado y efectivo. Este cambio no solo aliviaría la presión sobre la DPC, sino que también garantizaría que las acciones de aplicación se alineen más estrechamente con las particularidades de cada caso y jurisdicción. Este enfoque requeriría reformas significativas, incluyendo un aumento de financiación y recursos para las autoridades nacionales de protección de datos en toda la UE, así como una mayor claridad en la división de responsabilidades entre los organismos nacionales y los de nivel europeo.

Además, las intervenciones del CEPD en los casos gestionados por la DPC han demostrado la importancia de contar con un organismo central fuerte para mantener la coherencia y defender los principios del RGPD. El papel de las autoridades centralizadas en la UE, como el CEPD, la JESD y la Comisión Europea, en la supervisión y coordinación de la aplicación en toda la UE será crucial para garantizar que el DSA, el *AI Act* y otras normativas se implementen de manera efectiva. Sin embargo, el equilibrio entre la supervisión centralizada y la autonomía nacional debe gestionarse cuidadosamente para evitar conflictos y garantizar

92 CEPD (2024), «Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework», *CEPD*, pág. 4.

93 *Ibid.*

que todos los Estados miembros puedan contribuir de manera efectiva al proceso de aplicación.

A medida que la UE avanza con su estrategia digital, es esencial reconocer que el éxito de esta visión no depende únicamente de la solidez de las normativas, sino también de la eficacia de los mecanismos establecidos para aplicarlas. Los desafíos enfrentados por la DPC bajo el RGPD sirven como advertencia de que, sin reformas trascendentales, la UE corre el riesgo de repetir los mismos errores con el DSA y el *AI Act*. Para alcanzar sus ambiciones digitales, la UE debe garantizar que su marco de aplicación sea tanto flexible como resiliente, capaz de adaptarse a las demandas de un panorama digital en constante evolución. El futuro de la protección de datos en la UE requerirá un delicado equilibrio entre la centralización y la descentralización, entre la coherencia y la flexibilidad. Las lecciones aprendidas de la experiencia de la DPC bajo el RGPD deben guiar el desarrollo de nuevas estrategias de aplicación que puedan abordar mejor las complejidades de la era digital. Al fortalecer las capacidades de las autoridades de supervisión, compartir las responsabilidades de aplicación y garantizar que las entidades adecuadas asuman las tareas correctas, la UE puede construir un marco más efectivo y sostenible para proteger los derechos de sus ciudadanos en la era digital.