DOI: https://doi.org/10.69592/2952-1955-N7-DIC-2025-ART-6

# Protección de datos y personas trabajadoras: un estudio a las conclusiones de la STJUE de 27 de junio de 2024, c-768/21

DATA PROTECTION AND EMPLOYEES: AN ANALYSIS OF THE CJEU JUDGMENT OF 27 JUNE 2024 (CASE C-768/21)

**Arturo Montesdeoca Suárez**
Profesor Ayudante Doctor en la Universidad de Las Palmas de Gran Canaria
Las Palmas de Gran Canaria, Canarias, España
https://orcid.org/0000-0002-1519-4923
arturo.montesdeoca@ulpgc.es

**Enviado el 24 de septiembre de 2025; aceptado el 27 de noviembre de 2025.**



**Resumen**: En esta aportación doctrinal se profundiza el alcance del deber de actuación de las autoridades nacionales de protección de datos ante una infracción del RGPD a partir de la sentencia del TJUE de 27 de junio de 2024 (C-768/21). En este sentido, se examina si la constatación de una vulneración de la normativa conlleva necesariamente la adopción de medidas correctoras, en particular, la imposición de sanciones administrativas, o si cabe una apreciación discrecional basada en los principios de proporcionalidad y eficacia. Asimismo, se analiza la exigencia de dolo o negligencia como presupuesto de culpabilidad para la imposición de multas, y se valora el papel de las medidas preventivas adoptadas por el responsable del tratamiento. Finalmente, se analiza la relación entre la infracción del RGPD y el derecho a la indemnización del afectado.

**Palabras clave**: protección de datos personales, RGPD, multas administrativas, autoridades de control, proporcionalidad.

***Abstract:*** *In this doctrinal contribution, the scope of the duty of national data protection authorities to act upon a breach of the GDPR is examined, based on the judgment of the CJEU of 27 June 2024 (C-768/21). In this regard, the analysis focuses on whether the finding of a violation of the regulation necessarily entails the adoption of corrective measures—particularly the imposition of administrative sanctions—or whether a discretionary assessment based on the principles of proportionality and effectiveness is permissible. The requirement of intent or negligence as a prerequisite for culpability in the imposition of fines is also addressed, along with the role of preventive measures adopted by the data controller. Finally, the relationship between the GDPR infringement and the data subject's right to compensation is analyzed.*

***Keywords:*** *personal data protection, GDPR, administrative fines, supervisory authorities, proportionality.*

# I. Introducción

La cuestión prejudicial europea se integró en el ordenamiento jurídico europeo desde el primer tratado constitutivo *ex* art. 41 del Tratado de la Comunidad Europea del Carbón y del Acero (TCECA), y ha ido evolucionando, sufriendo ciertas modificaciones en su configuración. Así pueden señalarse, el art. 177 del Tratado de la Comunidad Económica Europea (TCEE), art. 234 del Tratado de la Comunidad Europea (TCE) y, finalmente, el art. 267 del Tratado de Funcionamiento de la Unión Europea (TFUE)[1].

Además, la cuestión prejudicial también encuentra acomodo en el art. 93 y ss. del Reglamento de Procedimiento del Tribunal de Justicia, en el que se disponen aspectos tan relevantes en el proceso como: a) una exposición concisa del objeto del litigio y de los hechos pertinentes, según se hayan constatado por el órgano jurisdiccional remitente, o al menos una exposición de los datos fácticos en que se basan las cuestiones; b) el texto de las disposiciones nacionales que puedan ser aplicables al asunto y, en su caso, la jurisprudencia nacional pertinente; c) la indicación de las razones que han llevado al órgano jurisdiccional remitente a preguntarse sobre la interpretación o la validez de determinadas disposiciones del Derecho de la Unión, así como de la relación que a su juicio existe entre dichas disposiciones y la normativa nacional aplicable en el litigio principal.

Del contenido y regulación de la cuestión prejudicial puede constatarse el denominado proceso de «diálogo entre jurisdicciones»[2], justificado por la necesaria uniformidad en la

1 Esta evolución histórico-jurídica se examina en Macías Castaño, J.M. (2014). *La cuestión prejudicial europea y el Tribunal Constitucional. El asunto Melloni*, Barcelona, Atelier, pp. 31 y ss.

2 Me remito a los siguientes estudios que abordan la cuestión, Soca Torres, I. (2016). *La cuestión prejudicial europea. Planteamiento y competencia del tribunal de justicia*, Barcelona, Bosch Procesal, p. 25 yss. Lousada Arochena, J.F. (2021). *La cuestión prejudicial ante el Tribunal de Justicia vista desde un órgano judicial español*, Granada, Laborum Ediciones, p. 41 y ss.

aplicación del derecho de la UE[3]. A este respecto, la STJUE *Schwarze* (C-16/65), señaló que «el órgano jurisdiccional y el Tribunal de Justicia deben cooperar directa y recíprocamente, dentro del ámbito de sus propias competencias, a la elaboración de una resolución con el fin de garantizar la aplicación uniforme del Derecho comunitario en todos los Estados miembros; que decidir en otro sentido equivaldría a permitir que los propios órganos jurisdiccionales nacionales se pronuncien sobre la validez de los actos comunitarios».

A partir de esta vía procesal, el TJUE ha llevado a cabo una prolífera actividad interpretativa sobre la adecuación de los marcos jurídicos nacionales con el europeo. Un buen ejemplo es el caso del derecho a la protección de datos personales, consagrado en el art. 8 del Convenio Europeo de Derechos Humanos de 1950 (CEDH) que reconoce el derecho al respeto de la vida privada y familiar, interpretado posteriormente por el Tribunal Europeo de Derechos Humanos (TEDH) como una garantía frente al tratamiento indebido de información personal. A este instrumento se añadió el Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, primer tratado internacional jurídicamente vinculante en la materia, cuyo objetivo fue asegurar el respeto de los derechos y libertades fundamentales de las personas frente al tratamiento automatizado de datos personales; su Protocolo de enmienda de 2018 (Convenio 108+) amplió su alcance y reforzó los mecanismos de supervisión. Posteriormente, se ha reconocido en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE). A partir de estos preceptos se configura un marco normativo europeo robusto en la materia, desarrollado principalmente, en estos momentos, por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), aplicable directamente en todos los Estados miembros desde el 25 de mayo de 2018.

El RGPD tiene como finalidad garantizar la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos, estableciendo los principios rectores del tratamiento (licitud, lealtad, transparencia, minimización, exactitud, limitación de la finalidad y seguridad). En el ámbito laboral, el artículo 88 RGPD habilita a los Estados miembros para establecer disposiciones más específicas a fin de garantizar la protección de los derechos y libertades de los trabajadores, en particular respecto al tratamiento de datos en el contexto de las relaciones laborales, incluyendo el control empresarial y la gestión de recursos humanos.

A nivel nacional, el artículo 18.4 de la Constitución Española (CE) reconoce el derecho fundamental a la protección de datos personales, cuyo desarrollo legislativo se articula a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Esta norma complementa y adapta el RGPD al ordenamiento español, incorporando en su Título X un conjunto de derechos digitales de las personas asociados al ámbito del derecho del trabajo.

3 Sobre su importancia en el ordenamiento comunitario, un sector doctrinal ha llegado a concluir que la cuestión prejudicial constituye un instrumento relevante en el sistema de control jurisdiccional dadas las características del modelo de organización jurisdiccional de la UE, Mangas Martín, A. Liñán Nogueras, D.J. (2012). *Instituciones y derecho de la Unión Europea*, 7.º Edición, Madrid, Tecnos, p. 457.

El derecho a la protección de datos personales ha sido construido como señala la doctrina[4], tanto por obra del TC a nivel nacional y por el TJUE a nivel comunitario[5]. En este sentido, puede constatarse que el TJUE ha desempeñado una función crucial en la interpretación y armonización de la aplicación de la normativa europea. Precisamente, en el objeto de este estudio, sobre el derecho fundamental a la protección de datos personales previsto y consagrado en un amplio abanico normativo europeo que ha ido evolucionando conforme a los retos tecnológicos planteados en sociedad[6]. De hecho, esta labor interpretativa de gran valor permite compartir la apreciación doctrinal[7] por la cual se estima que el TJUE se ha convertido en un *«auténtico juez garante de la privacidad ante la evolución tecnológica global»*. Esta opinión se respalda con la hemeroteca judicial por la cual puede evidenciarse que, a partir de supuestos relevantes como las sentencias *Lindqvist* (C-101/01), *Digital Rights Ireland* (C-293/12 y C-594/12) y *Google Spain* (C-131/12), entre otros, se ha materializado una línea jurisprudencial sólida sobre la normativa de protección de datos personales. Una actuación que continúa hasta nuestros días con la interpretación por el TJUE de los preceptos del RGPD, consolidándose una nueva doctrina jurisprudencial acorde al marco jurídico y actualizada a los nuevos retos tecnológicos que se plantean en referencia a la salvaguarda de este derecho fundamental[8]; por tales razones, se ha estimado oportuno llevar a cabo una aproximación a esta jurisprudencia con repercusión directa en el marco de las relaciones laborales[9].

En definitiva, el objetivo propuesto en las siguientes líneas no es otro que, precisamente, analizar la STJUE de 27 de junio C-768/21, desde una triple perspectiva dado el interés que ofrece este pronunciamiento sobre el derecho a la protección de datos personales.

---

4 Un repaso histórico-jurídico y a la evolución del derecho a la protección de datos personales en la jurisprudencia en Piñar Mañas, J.L. (2003). «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», *Cuadernos de Derecho Público*, núm. 19-20, pp. 54 y ss. Polo Roca, A. (2020). «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado», *Revista de Derecho Político*, núm. 108, pp. 173 y ss.

5 *Vid., in extenso* en Piñar Mañas, J.L., Recio Gayo, M. (2018). *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer España.

6 En concreto, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Carta de Derechos Fundamentales de la Unión Europea —en concreto su art. 8—, y ahora el 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.

7 Rallo Lombarte, A. (2017). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet, *UNED- Teoría y Realidad Constitucional*, núm. 39, p. 584.

8 López Aguilar, J.F. (2017). «La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EE. UU.», *Revista de Teoría y realidad constitucional*, núm. 39, p. 561.

9 Ante este reto, voces laboralistas critican que el RGPD como el RIA no se encuentran adaptados al marco de las relaciones laborales, *vid*., en Todolí Signes, A. (2024). «Democracia en el trabajo y codeterminación ante el uso de la IA en la empresa: algo más que negociar el algoritmo», *Revista Crítica de Relaciones de Trabajo, Laborum*, núm. extra-2, p. 231.

## II. Los hechos probados sobre los que versa la cuestión prejudicial

El TJUE resolvió la cuestión prejudicial planteada por el Tribunal de lo Contencioso-Administrativo de Wiesbaden (Alemania), conforme al artículo 267 del Tratado de Funcionamiento de la Unión Europea (TFUE), en el marco del litigio entre TR y el Estado federado de Hesse (Land Hessen).

La controversia principal versaba sobre la interpretación de los artículos 57.1, letras a) y f); 58.2 y 77.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD), 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. Y, en particular, se discutía la legalidad de la decisión del Comisionado para la Protección de Datos y la Libertad de Información del Estado de Hesse (HBDI), al no adoptar medidas correctoras frente a la entidad Sparkasse X, pese a la existencia de una posible infracción del RGPD.

En cuanto a los hechos relevantes, el 15 de noviembre de 2019, Sparkasse X notificó al HBDI, en cumplimiento del artículo 33 del RGPD, una violación de la seguridad de los datos personales bajo su responsabilidad. Dicha violación consistió en accesos reiterados e injustificados por parte de un empleado de la entidad a los datos personales de TR. No obstante, Sparkasse X no informó a la persona afectada, es decir, a TR, de dicha vulneración, lo cual podría constituir una infracción del artículo 34 del RGPD.

Posteriormente, al tener conocimiento de los accesos indebidos a sus datos personales, TR presentó el 27 de julio de 2020 una reclamación ante el HBDI con fundamento en el artículo 77 del RGPD, denunciando la omisión de comunicación de la violación conforme al artículo 34 del citado Reglamento.

Durante la tramitación del expediente, Sparkasse X justificó su actuación alegando que, conforme a las indicaciones de su delegado de protección de datos, la violación no implicaba un «riesgo elevado para los derechos y libertades» de la persona afectada, por lo que no procedía su notificación individual. Además, la entidad adoptó medidas disciplinarias internas contra el empleado responsable de los accesos indebidos.

El HBDI, tras valorar las alegaciones presentadas y concluir que los datos personales no habían sido difundidos a terceros ni utilizados en perjuicio de TR, determinó que no se había producido una infracción del artículo 34 del RGPD, por lo que decidió no imponer ninguna medida correctora.

Disconforme con dicha decisión, TR interpuso recurso ante el Tribunal de lo Contencioso-Administrativo de Wiesbaden, alegando una aplicación incorrecta del RGPD por parte del HBDI. A su juicio, este último debería haber ejercido su potestad sancionadora imponiendo una multa a Sparkasse X, en virtud de los artículos 5, 12.3, 15.1, letra c), y 33.1 y 33.3 del RGPD. Según el recurrente, el HBDI no tenía la facultad de abstenerse de actuar, sino únicamente la de elegir entre las diferentes medidas correctoras previstas en el artículo 58 del RGPD.

El Tribunal de lo Contencioso-Administrativo de Wiesbaden planteó ante el Tribunal de Justicia de la Unión Europea (TJUE) una cuestión prejudicial orientada a dilucidar si, una vez constatada una vulneración del Reglamento General de Protección de Datos (RGPD), la autoridad de control competente está imperativamente obligada a ejercer alguna de las facultades correctoras previstas en el artículo 58.2 del mismo, tales como la imposición de una sanción administrativa; o si, por el contrario, puede legítimamente abstenerse de actuar, en función de las particularidades del caso y de una apreciación fundada de los hechos.

Desde la perspectiva del demandante TR, la función de las autoridades de protección de datos no se limita a una mera supervisión pasiva, sino que implica el deber de restablecer la legalidad en el ámbito del tratamiento de datos personales, conforme a lo previsto en el artículo 58.2 del RGPD. En tal sentido, una vez identificada una infracción, la autoridad debería intervenir, aunque conserve autonomía para seleccionar la medida más adecuada y proporcional, atendiendo a la naturaleza, gravedad y circunstancias de la infracción.

No obstante, el órgano remitente muestra reservas frente a esta interpretación, que considera excesivamente restrictiva del margen de apreciación conferido a las autoridades de control. A juicio del tribunal alemán, el RGPD también admite que, en ciertos escenarios, la autoridad pueda optar por no aplicar ninguna medida correctora, siempre que fundamente su decisión en una evaluación exhaustiva y razonada de la situación, y especialmente si las medidas adoptadas voluntariamente por el responsable del tratamiento resultan suficientes para corregir o prevenir ulteriores incumplimientos.

Bajo este contexto interpretativo, y con el objetivo de clarificar el alcance exacto de las obligaciones que recaen sobre las autoridades nacionales en materia de control y sanción, el Tribunal de Wiesbaden acordó suspender el procedimiento interno y elevar la siguiente cuestión prejudicial al TJUE:

¿Deben interpretarse los artículos 57, apartado 1, letras a) y f), y 58, apartado 2, letras a) a j), en relación con el artículo 77, apartado 1, del [RGPD], en el sentido de que, cuando la autoridad de control constate actividades de tratamiento de datos que vulneran los derechos del interesado, estará obligada siempre a intervenir con arreglo al artículo 58, apartado 2, [de dicho Reglamento]?

# III. La fundamentación jurídica del TJUE

En cuanto a la fundamentación jurídica llevada a cabo por el TJUE para dilucidar el conflicto, puede estructurarse por el interés del tema, en varios epígrafes que se encuentran estrechamente interrelacionados y permiten obtener una valoración final completa del asunto en cuestión.

## 1. El acceso indebido por las personas trabajadoras a datos personales

En primer lugar, debe señalarse que el conflicto se inicia con el acceso indebido a datos personales por parte de la persona trabajadora; es aquí, por tanto, cuando se inicia el recorrido judicial de este asunto. Esta actuación se inserta en el concepto *de «violación de seguridad»*, que de conformidad con el art. 4.12 RGPD es *«toda violación de la seguridad que ocasione la*

*destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos»*.

En este caso, y ante un manifiesto y contrastado acceso no autorizado a datos personales, el RGPD indica cuáles son las actuaciones que seguir al respecto. Por un lado, la notificación de una violación de seguridad de los datos personales a la autoridad de control *ex* art. 33 RGPD. Por otro, la comunicación de una violación de la seguridad de los datos personales al interesado *ex* art. 34, que serán analizadas posteriormente.

De conformidad con los hechos probados, la entidad adoptó las medidas disciplinarias oportunas contra la persona trabajadora una vez que constató la magnitud del incidente. Sin embargo, esta actuación quizás se podría haber evitado a través de actuaciones preventivas como pueden ser la adopción de protocolos internos, medidas técnicas o de diseño que permitan identificar accesos no autorizados, y, con mayor interés la formación. Sobre esta materia, se quiere resaltar el valor fundamental que adquiere la formación del personal en materia de protección de datos personales, precisamente, en entidades como las entidades bancarias en las que se tratan a gran escala datos personales con diferentes características.

Como primera apreciación, el RGPD no incluye ninguna referencia expresa a la formación obligatoria por parte del responsable a quienes traten bajo sus indicaciones, datos personales. Esta previsión sí que se incorpora expresa y obligatoriamente en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento de Inteligencia Artificial). A tenor de su art. 4 se prevé la «alfabetización en IA», de tal forma que *«los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas»*. Si bien es cierto que el RGPD no incluye ninguna previsión directa y expresa, esta obligación puede derivar de otras obligaciones impuestas al responsable del tratamiento de datos personales, como puede ser, la adopción de una actuación proactiva, mediante la adopción de medidas técnicas y organizativas adecuadas a fin de garantizar un tratamiento de datos personales de conformidad con los parámetros señalados por el RGPD *ex* arts. 24, 25, 32 y 39 RGPD.

Por consiguiente, la formación en materia de protección de datos personales constituye una actuación de diligencia debida a nivel interno por las organizaciones en un ejercicio de exteriorización a las personas trabajadoras de su deber de colaboración en el cumplimiento normativo cuando desempeñan sus funciones. De esta manera, las entidades que adopten este tipo de medidas, es decir, la adopción e implementación de programas formativos periódicos y adaptados a los riesgos específicos de cada entidad y/o puesto de trabajo de las personas trabajadoras, podrán justificar, mitigar y minimizar las posibilidades de sufrir una sanción económica por la autoridad de control en casos como el aquí reseñado, por fugas, brechas o accesos indebidos a datos personales. Todo ello fruto de un compromiso claro y diligente con las acciones preventivas y proactivas en el cumplimiento de las obligaciones impuestas por el RGPD[10]. Esta cuestión se corrobora a través de la revisión de varios

10 En esta línea, el GT29 indica que «inmediatamente después de tener conocimiento de una violación, es de vital importancia que el responsable del tratamiento no trate solo de contener el incidente,

expedientes de la AEPD, de los que se puede concluir que la formación y las acciones de concienciación pueden adquirir un papel relevante en el procedimiento sancionador. Por ello, se destaca que los programas formativos deben ser específicos, adaptados a las particularidades operativas como los riesgos de la entidad, la acreditación del número de personas asistentes y del nivel de los formadores, así como el carácter (obligatorio o voluntario) de las formaciones a razón de la responsabilidad asumida por las personas trabajadoras.

En suma, esta actuación conecta con las previsiones del régimen de infracciones o sanciones al que una persona trabajadora puede exponerse y que, en su caso, puede ser la sanción más grave, es decir, el despido disciplinario. La incorporación de las personas trabajadoras a una empresa mediante la formalización del contrato de trabajo implica para ambas partes el cumplimiento recíproco de los derechos y deberes que les impone el ET. Entre estos deberes, destaca el principio general de buena fe contractual. En este sentido, el artículo 5.a) del ET establece que los trabajadores deben *«cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia»*.

Por su parte, desde la perspectiva empresarial, el art. 54.2.d) ET prevé como causa de extinción del contrato por decisión unilateral del empleador, en el marco de un despido disciplinario, *«la transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo»*. De hecho, ya pueden encontrarse ejemplos en la jurisdicción social (STSJ de Galicia 6192/2024, de 17 de septiembre[11], STSJ de Cataluña 5331/2023 de 27 de septiembre[12], STSJ de Comunidad Valenciana 2070/2021, de 22 de junio[13] y STSJ de Madrid 689/2018, de 26 de octubre[14]) avalando el despido disciplinario de la persona trabajadora transgresora de la buena fe contractual sobre esta materia, es decir, la vulneración de las políticas internas sobre acceso y gestión de datos personales.

Por lo tanto, este puede ser un terreno en el que los CC puedan incorporar y prever expresamente un régimen sancionador más claro y explícito en este tipo de incumplimiento sobre protección de datos personales. De momento, y con carácter general, las aportaciones identificadas en CC suelen derivar en apreciaciones generales asociadas al incumplimiento de disposiciones legales de las empresas, fraude, deslealtad y abuso de confianza en las gestiones encomendadas o genéricas, referidas a cualquier otro incumplimiento de los deberes laborales y que causen un perjuicio grave y notorio a la entidad.

---

sino que también evalúe el riesgo que podría derivarse del mismo. Hay dos razones importantes para ello: en primer lugar, conocer la probabilidad y la gravedad potencial del impacto en la persona ayudará al responsable del tratamiento a adoptar medidas eficaces para contener y poner remedio a la violación; en segundo lugar, le ayudará a determinar si la notificación a la autoridad de control es necesaria y, en su caso, a las personas afectadas». Por lo tanto, estima necesario que se evalúe el tipo de violación, la naturaleza, el carácter sensible y el volumen de datos personales, la facilidad de identificación de las personas, gravedad de las consecuencias para las personas, características particulares de las personas, características particulares del responsable del tratamiento, así como el número de personas afectadas. Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, pp. 25-29.

11 ECLI:ES:TSJGAL:2024:6192.

12 ECLI: ES:TSJCAT:2023:9206.

13 ECLI: ES:TSJCV:2021:7805.

14 ECLI: ES:TSJM:2018:10344.

## 2. La actuación inspectora de la Agencia Nacional de Protección de datos y la interpretación de la imposición de multas administrativas al responsable del tratamiento de datos personales

En segundo lugar, el TJUE continúa desgranando jurídicamente el contenido de la cuestión planteada, en estos momentos, respecto a la intervención de la autoridad de control a efectos de imponer multas administrativas con arreglo a los arts. 57.1 a) y f), 58.2 a) a j) y 77.1 RGPD.

En cuanto al ejercicio de las funciones de supervisión, no queda lugar a dudas que las autoridades nacionales de control están legitimadas para verificar el cumplimiento del RGPD en virtud del artículo 8.3 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), así como de los artículos 51.1 y 57.1, letra a), del propio RGPD (apartado 31). En particular, el artículo 57.1, letra f), establece la obligación de cada autoridad de control de tramitar y resolver las reclamaciones que formulen las personas afectadas, así como de informar sobre el resultado de la investigación con la debida diligencia.

En consecuencia con lo anterior, una vez que la autoridad de control, tras el procedimiento de investigación y el análisis de las alegaciones presentadas por las partes, constate la existencia de una infracción del RGPD, se encuentra legalmente habilitada para adoptar las medidas correctoras pertinentes. Estas medidas no tienen otro resultado que llevar a cabo una restauración del cumplimiento normativo transgredido. Esta potestad se inserta dentro del marco del poder corrector conferido *ex* art. 58.2 RGPD, por el que se le habilita requerir al responsable o encargado del tratamiento actuaciones concretas o, en su caso, imponer sanciones administrativas en los términos del artículo 83 del RGPD[15].

En este supuesto, se ha podido constatar que el Comisionado para la Protección de Datos y la Libertad de Información del Estado de Hesse (HBDI) tramitó la reclamación interpuesta por la parte reclamante, informándole del resultado de la investigación. Si bien es cierto, el HBDI reconoció que se había producido una vulneración de la seguridad de los datos personales por parte de una empleada de la entidad *Sparkasse* X, por el contrario, no atendió positivamente para la reclamante que era necesario adoptar una medida correctora con a tenor del art. 58.2 RGPD.

El razonamiento del TJUE para alcanzar esta conclusión es que, de conformidad con el art. 58.2 RGPD, las autoridades de control disponen de un margen de apreciación para seleccionar, atendiendo a las circunstancias del caso concreto, la medida más adecuada. En efecto, el artículo 83.2 del RGPD establece que la imposición de sanciones administrativas debe basarse en una valoración individualizada, teniendo en cuenta factores como la naturaleza, gravedad y duración de la infracción, así como los criterios establecidos en las letras a) a k) *ex* art. 83.2 RGPD[16].

15 Ortega Giménez, A. (2024). «El Tribunal de Justicia de la UE y la imposición de multas administrativas por infracción del Reglamento General de Protección de Datos (Casos Nacionalinis visuomenės Sveikatos Centras y Deutsche Wohnen)», *Diario la Ley*, núm. 10581, pp. 12-13.

16 Recio Gayo, M. (2017). «Las sanciones en el RGPD: comentarios a las Directrices del Grupo de trabajo del artículo 29», *Diario la Ley*, núm. 12, pp. 7-8.

El TJUE realiza varias precisiones relevantes sobre esta actuación sancionadora respecto a la responsabilidad que recae sobre el responsable del tratamiento de datos personales. En cuanto a la autoridad de control, esta entidad puede, excepcionalmente, decidir no imponer medidas correctoras incluso en presencia de una infracción. No obstante, no se trata de una actuación general sino individualizada para cada caso, de tal manera que existirán situaciones que podrán permitir excepcionar esta responsabilidad. La pregunta, en este sentido, sería, ¿bajo qué criterios o situaciones podría darse lugar la excepción de responsabilidad? Para el TJUE existen varios elementos como puede ser la ausencia de reiteración, la adopción inmediata de medidas técnicas y organizativas por parte del responsable del tratamiento, y la garantía de que no se volverá a producir la deficiencia, conforme a los artículos 24.2 y 24.5 del RGPD.

Esta flexibilidad interpretativa encuentra justificación legal en los fines perseguidos por los artículos 58.2 y 83 del RGPD, cuyo contenido está referido a una actuación proporcionada y ajustada al principio de eficacia. Por consiguiente, la imposición de sanciones podría, en determinadas situaciones, generar una carga desproporcionada; por ello, el apercibimiento puede considerarse una respuesta más adecuada a los fines del RGPD.

En definitiva, el TJUE concluye que corresponde al órgano jurisdiccional nacional valorar si la autoridad de control ha actuado dentro de los márgenes de apreciación conferidos por el artículo 58.2 del RGPD y si ha cumplido la diligencia debida a lo largo del procedimiento.

Estrechamente relacionada con la imposición de la multa administrativa, puede reseñarse la doctrina del TJUE recaída en dos sentencias de 5 de diciembre de 2023, C-683/21 y C-807/21. En esencia, lo que se plantea en estos pronunciamientos judiciales es si, de conformidad con el art. 83 RGPD *«debe interpretarse en el sentido de que solo puede imponerse una multa administrativa con arreglo a esa disposición si se demuestra que el responsable del tratamiento, que es a la vez una persona jurídica y una empresa, cometió, de forma intencionada o negligente, una infracción contemplada en los apartados 4 a 6 de dicho artículo»*.

El TJUE para dar respuesta a esta duda lleva a cabo una interpretación conjunta de los arts. 58.2 y 83 RGPD. Por una parte, el art. 58.2 i) RGPD dispone que las autoridades de control podrán, con arreglo al art. 83.2 RGPD, imponer una multa administrativa*, «además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular»*. Por lo que, se entiende que la imposición de la multa administrativa revierte un carácter adicional o sustitutivo de otras formas como puede ser la advertencia, apercibimiento u órdenes (apartado 71 C-807/21). Por otra, no se desconoce que el régimen sancionador previsto por el RGPD desprende que *«las multas administrativas deben ser efectivas, proporcionadas y disuasorias»* ex art. 83.1 RGPD, ya que *«contribuyen a reforzar la protección de las personas físicas en lo que respecta al tratamiento de datos personales y constituyen, por ende, un elemento clave para garantizar el respeto de los derechos de dichas personas, de conformidad con la finalidad del citado Reglamento de asegurar un elevado nivel de protección de esas personas en lo que respecta al tratamiento de los datos personales»*.

Asimismo, el art. 83.2 RGPD recoge las condiciones generales para la imposición de multas administrativas; entre ellos, la letra b) recoge la *«intencionalidad o negligencia en la infracción»*. Con ello, *sensu contrario*, si no media la denominada «intencionalidad o negligencia» no puede imponerse una sanción ya que no media culpabilidad o actuación voluntaria o negligente por parte del responsable del tratamiento de datos personales (apartado 75). Este

razonamiento radica en que el legislador europeo ha considerado que la imposición de sanciones económicas no debe producirse en ausencia de culpabilidad, y, por ende, de permitir la imposición de multas sin requerir una conducta dolosa o negligente sería contrario a los fines de armonización del RGPD[17] y podría provocar desigualdades entre operadores económicos de distintos Estados miembros, vulnerando los principios de coherencia normativa y libre competencia, como subrayan los considerandos 9 y 13 RGPD (apartado 74).

Con todo ello, el TJUE determina que a tenor del art. 83 del RGPD no se permite la imposición de multas administrativas por infracciones recogidas en sus apartados 4 a 6 si no se demuestra que dichas infracciones han sido cometidas con dolo o negligencia por parte del responsable del tratamiento. De tal forma que, la existencia y probatura de la culpabilidad se erige como un requisito indispensable para legitimar la imposición de la sanción económica correspondiente.

## 3. La satisfacción procesal de resarcimiento de daños por vulneración del derecho fundamental a la protección de datos personales de sus titulares

En tercer lugar, y estrechamente relacionado con los puntos anteriores, puede abordarse la posibilidad de reclamar daños al responsable o encargado del tratamiento por una vulneración de los parámetros del RGPD en relación con el tratamiento de datos personales.

No debe perderse de vista que en esta etapa de la sociedad 4.0 se comienza a constatar un mayor riesgo para los datos personales bien por los errores propios en la actividad llevada a cabo o bien ante la creciente e insaciable actividad de quienes se dedican a proferir ciberataques a cambio de recompensas económicas de rescate de datos. Por tanto, pueden darse situaciones dispares, en tanto en cuanto, inclusive cuando se adopten y se cumplan las previsiones legales, puede materializarse el efecto lesivo indeseado para el derecho a la protección de datos personales. De este modo, puede estarse de acuerdo con que las empresas pueden adoptar férreas y solventes medidas de seguridad[18] y, pese a ello, sufrir este tipo de ataques que merman su actividad como su reputación corporativa pese a los esfuerzos adoptados[19]. En suma, los potenciales afectados, es decir, los titulares de tales datos personales inician el procedimiento de resarcimiento de daños inmateriales causados por dicha transgresión.

17 Recio Gayo, M. (2017). «Las sanciones en el RGPD: comentarios a las Directrices del Grupo de trabajo del artículo 29», ob. cit., p.8.

18 Téngase en cuenta que, a tenor de la Disposición Adicional Primera de la LOPDGDD, en el ámbito del sector público deben adoptarse medidas de seguridad concretas y materializadas en el Esquema Nacional de Seguridad, regulados en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

19 De hecho, la falta de adopción de las medidas de seguridad ex art. 32 RGPD ocupó en los inicios el foco de actuación en las actuaciones sancionadoras dadas las comprobaciones e infructuosas acciones comprobadas por las entidades. Padín Vidal, A. (2019). «Sanciones por incumplimiento del RGPD en la Unión Europea», *La Ley Privacidad*, núm. 2, pp. 5-6.

Sobre esta materia, el art. 82 RGPD dispone que *«toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos»*. Y, en su apartado tercero, se prevé una excepción de responsabilidad por los daños y perjuicios causados por incumplimiento del RGPD *«si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios»*. Por lo tanto, el RGPD ya prevé el derecho a la indemnización y responsabilidad de responsable y/o encargado, así como las posibilidades de exonerar dicha culpabilidad o responsabilidad[20]. No obstante, y pese a las diferentes vías de resarcimiento de este tipo de daños, la doctrina civilista reitera las lagunas que existen aún en la coordinación entre las acciones indemnizatorias previstas a nivel europeo (RGPD) y en el ordenamiento jurídico español (disposiciones del Código Civil y de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen)[21].

En aras de desentrañar esta problemática cuestión, puede acudir a la doctrina del TJUE, ya que en varias de sus sentencias (STJUE de 20 de junio de 2024, C-590/22[22] y asuntos acumulados C-182/22 y C-189/22[23]) se han aportado conclusiones muy sugerentes y clarificadoras al respecto.

20 Ortega Giménez, A. (2024). «El Tribunal de Justicia de la UE y la imposición de multas administrativas por infracción del Reglamento General. *ob.cit*., pp. 12-13.

21 Sobre la cuestión me remito a un exhaustivo análisis en Rubí Puig, A. (2019). «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español», *Derecho Privado y Constitución*, núm. 34, 197-232.

22 El Amtsgericht Wesel (Tribunal de lo Civil y Penal de Wesel) decidió suspender el procedimiento y plantear al Tribunal de Justicia las cuestiones prejudiciales siguientes: 1) ¿Es suficiente para que exista un derecho a indemnización por daños y perjuicios con arreglo al artículo 82, apartado 1, del [RGPD] que se haya infringido una disposición [de este Reglamento] que protege a quien reclama o es necesario que, además de la infracción de las disposiciones como tal, se haya producido un perjuicio añadido para dicha persona? 2) Para que exista, conforme al Derecho de la Unión, un derecho a indemnización por daños y perjuicios inmateriales con arreglo al artículo 82, apartado 1, del RGPD, ¿es preciso que se haya producido un perjuicio de cierta entidad? 3)En particular, para que exista un derecho a indemnización por daños y perjuicios inmateriales con arreglo al artículo 82, apartado 1, del RGPD, ¿es suficiente que quien reclama tema que, como consecuencia de infracciones de las disposiciones del RGPD, sus datos personales hayan llegado a manos de terceros, sin que esto pueda establecerse positivamente? 4) ¿Resulta conforme con el Derecho de la Unión que el órgano jurisdiccional nacional, a la hora de cuantificar la indemnización por daños y perjuicios inmateriales con arreglo al artículo 82, apartado 1, del RGPD, recurra por analogía a los criterios del artículo 83, apartado 2, segunda frase, del RGPD, que por su redacción son aplicables únicamente a las multas administrativas? 5) ¿Debe cuantificarse el derecho a una indemnización por daños y perjuicios inmateriales con arreglo al artículo 82, apartado 1, del RGPD atendiendo también al hecho de que con la cuantía del derecho reconocido se logre un efecto disuasorio o se impida la «comercialización» de las infracciones de dicho Reglamento (aceptación calculada de multas administrativas y de pagos en concepto de indemnización por daños y perjuicios)? 6) ¿Es conforme con el Derecho de la Unión que a la hora de cuantificar un derecho a indemnización por daños y perjuicios inmateriales con arreglo al artículo 82, apartado 1, del RGPD se tengan en cuenta las infracciones simultáneas de las disposiciones nacionales que tienen por objeto la protección de los datos personales, pero que no son actos delegados o de ejecución adoptados de conformidad con dicho Reglamento o Derecho de los Estados miembros que especifique las normas de dicho Reglamento?.

23 El Amtsgericht München (Tribunal de lo Civil y Penal de Múnich) decidió, en los asuntos C-182/22

Por un lado, una de las cuestiones prejudiciales planteadas, la segunda (asuntos acumulados C-182/22 y C-189/22), pretende obtener respuesta a la interrelación entre la gravedad, culpabilidad y dolo en el incumplimiento de los parámetros del RGPD con la estimación y cuantificación de la indemnización por daños y perjuicios inmateriales sufridos por la persona titular de los datos personales. El TJUE responde a ello remitiendo al ordenamiento jurídico interno de los estados miembros, a fin de que sean los jueces nacionales quienes determinen conforme a las normas internas el alcance de la reparación pecuniaria (apartado 27). A este respecto, la reparación debe respetar en todo caso, los principios de equivalencia y efectividad, de modo que una indemnización pecuniaria basada en esta disposición debe considerarse total y efectiva si permite compensar íntegramente los concretos daños y perjuicios sufridos como consecuencia de la infracción del RGPD, sin que sea necesario, a efectos de tal compensación íntegra, imponer el pago de indemnizaciones de carácter punitivo (STJUE C-300/21 apartado 58).

Por otro, en cuanto a la valoración de la indemnización el TJUE ha precisado que, de conformidad con el art. 82.1 RGPD, la mera infracción de los parámetros del RGPD no constituye un derecho indemnizatorio directo. De este modo, debe acreditarse una relación de causalidad y acreditarse por la persona que reclama dicha indemnización, el padecimiento

y C-189/22, suspender los procedimientos y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales, redactadas en términos idénticos en ambos asuntos: 1) ¿Debe interpretarse el artículo 82 del [RGPD] en el sentido de que el derecho a indemnización no tiene carácter sancionador, en particular no cumple una función disuasoria general o especial, ni siquiera en cuanto a su cuantificación, sino que cumple una función estrictamente indemnizatoria y, en ciertos casos, de desagravio? 2) En cuanto a la cuantificación de la indemnización de los perjuicios inmateriales, ¿se ha de considerar que el derecho a indemnización cumple también una función de desagravio individual (en este caso, en el sentido del interés particular del perjudicado por ver sancionado el comportamiento dañoso) o cumple solamente una función indemnizatoria (en este caso, en el sentido de compensar el perjuicio sufrido)? En caso de que la indemnización de los perjuicios inmateriales cumpla tanto una función indemnizatoria como de desagravio: ¿En cuanto a su cuantificación se ha de considerar que la función indemnizatoria goza de una preferencia sistemática o, al menos, de una preferencia en cuanto relación regla-excepción, respecto a la función de desagravio? ¿Implica esto que la función de desagravio solo entra en juego en caso de infracciones dolosas o por negligencia grave? En caso de que la indemnización de los perjuicios inmateriales no cumpla una función de desagravio: ¿Solo pueden considerarse agravantes en la cuantificación de la indemnización las infracciones cometidas mediando dolo o negligencia grave que contribuyan causalmente al perjuicio? 3) Respecto a la cuantificación de la indemnización de los perjuicios inmateriales, ¿debe entenderse que existe una jerarquía sistemática o, al menos, una jerarquía en cuanto a relación regla-excepción, con arreglo a la cual el perjuicio experimentado a causa de una violación de la seguridad de los datos tiene menos importancia que los daños y perjuicios sufridos como consecuencia de lesiones corporales? 4) En caso de que deba partirse del principio de que existe un daño, ¿está facultado el órgano jurisdiccional nacional, en atención a su escasa gravedad, para conceder una indemnización materialmente reducida y que, en ciertos casos, pueda ser percibida por el perjudicado, o con carácter general, como meramente simbólica? 5) Respecto a la valoración de las consecuencias de la indemnización de los perjuicios inmateriales, ¿debe entenderse que solo existe una usurpación de identidad en el sentido del considerando 75 del [RGPD] cuando un infractor ha utilizado efectivamente la identidad del interesado, haciéndose pasar por él de cualquier manera, o existe tal usurpación de identidad desde el momento en que un infractor dispone de datos que permiten identificar al interesado?

de unos daños inmateriales por el incumplimiento o infracción normativa cometida. Además, que estos daños inmateriales no son de menor importancia que unas lesiones corporales.

En cuanto a la cuantificación de los daños, el TJUE aporta claridad al asunto al determinar que, a tenor del art. 82.1 y en relación con el art. 82.6 RGPD, la indemnización por daños y perjuicios inmateriales puede alcanzar un régimen de mínimos en aquellos supuestos en los que carezcan de gravedad. Por tanto, los daños no deben alcanzar un régimen de mínimos para obtener la ansiada indemnización, sin perjuicio de que esta valoración les corresponde a los jueces nacionales.

Y, estrechamente relacionado se encuentran los parámetros de cálculo, el TJUE descarta la posibilidad de utilizar las cantidades de las multas administrativas *ex* art. 83 RGPD para la indemnización de daños y perjuicios *ex* art. 82 RGPD. El TJUE advierte que esta posibilidad debe ser descartada ya que el RGPD no integra disposición alguna referida a establecer la determinación del importe de la indemnización por daños y perjuicios (apartado 40 C-590/22). Además, el derecho de indemnización reconocido *ex* art. 82 RGPD no cumple una función disuasoria o punitiva (apartado 41 C-590/22), por lo que no puede aplicarse «*mutatis mutandis*» los criterios de fijación del importe de las multas administrativas *ex* art. 83 RGPD.

# IV. Fallo judicial

La jurisprudencia europea analizada trasciende del ámbito estrictamente administrativo del control de datos personales para proyectarse también sobre la disciplina del Derecho del Trabajo. En este contexto, la STJUE de 27 de junio de 2024 (C-768/21) refuerza la necesidad de que las empresas actúen bajo los principios de proporcionalidad, finalidad legítima y diligencia proactiva, conforme a los artículos 5 y 24 del RGPD.

Por ello, el TJUE señaló que «los artículos 57, apartado 1, letras a) y f), 58, apartado 2, y 77, apartado 1, del 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),

deben interpretarse en el sentido de que, en caso de que se constate una violación de la seguridad de datos personales, la autoridad de control no está obligada a adoptar una medida correctora, en particular una multa administrativa, en virtud del citado artículo 58, apartado 2, cuando tal intervención no sea adecuada, necesaria o proporcionada para subsanar la deficiencia constatada y garantizar el pleno respeto de dicho Reglamento».

El reconocimiento de este margen de apreciación de las autoridades nacionales, delimitado por el principio de proporcionalidad, permite extraer una lectura «laboralmente sensible» del RGPD, respecto al parámetro de exigencia de culpabilidad (dolo o negligencia) para imponer sanciones a las empresas ya que asumen la condición de responsable del tratamiento de los datos personales.

En consecuencia, el fallo refuerza el deber de diligencia proactiva del empleador en la aplicación de las medidas técnicas y organizativas previstas en el artículo 24 RGPD, de modo que la ausencia

de tales medidas o su implementación deficiente pueda considerarse una forma de negligencia sancionable. Al mismo tiempo, la sentencia invita a las autoridades de control a ponderar la gravedad real del incumplimiento y la conducta previa del responsable, promoviendo un modelo de cumplimiento preventivo más que meramente reactivo en la gestión de datos en el entorno laboral. Entre ellas, puede estar como se ha comprobado, la necesidad de evaluar la responsabilidad disciplinaria de las personas trabajadoras en relación con la gestión de datos personales.

# V. Conclusiones

La doctrina del TJUE en materia de protección de datos, en un primer momento sobre la Directiva 95/46/CE y, en estos momentos sobre el RGPD, ha resultado ser prolífera y esclarecedora de diferentes aristas que conforman este derecho fundamental. En esta ocasión, la intención ha sido esclarecer una temática —la vulneración del derecho a la protección de datos personales— desde una triple perspectiva por el interés que la materia adquiere en esta etapa tecnológica que augura una continuidad en la conflictividad ante las innegables agresiones futuras que la tecnología plantea a este derecho fundamental.

La STJUE 27 de junio de 2024 (C-768/21) brinda la posibilidad al lector la posibilidad de iniciar su abordaje jurídico desde esta triple perspectiva. De este modo, una primera aproximación permite comprobar el protagonismo que asumen las autoridades de control en cuanto a la aplicación del principio de proporcionalidad y el margen de discrecionalidad respecto a las potenciales sanciones a imponer ante incumplimientos de los parámetros del RGPD.

Esta discrecionalidad no debe confundirse con una merma en el rigor o espíritu del RGPD, sino más bien, una interpretación flexible y acorde con el principio de proporcionalidad en aras de alcanzar el verdadero propósito de la normativa europea. Con ello se está haciendo referencia a una interpretación basada en la probabilidad del riesgo y las consecuencias de su materialización como criterios para determinar las responsabilidades asumidas por responsables y/o encargados del tratamiento de datos personales. Una responsabilidad que deberá ser valorada conforme a una actitud primordial del responsable del tratamiento como es la proactividad en la adopción de cuantas medidas técnicas y organizativas fueran necesarias para mitigar los riesgos pese a como se ha comentado, de la dificultad y los retos asumidos en la lucha contra la ciberseguridad.

En esta innegable labor de protección del derecho fundamental a la protección de datos personales, puede estarse de acuerdo con que la interpretación del TJUE sobre el contenido normativo del RGPD ha sido proporcional en cuanto a la atribución de responsabilidades como en el reconocimiento de la reparación del daño causado. A este respecto, se ha delimitado un aspecto controvertido como es la concurrencia de culpabilidad, dolo o negligencia como criterios imprescindibles para atribuir una responsabilidad frente a meras infracciones sin repercusión para los derechos de las personas. Con ello se está descartando el carácter automático del régimen sancionador causando perjuicios y cargas desproporcionadas a los verdaderos objetivos que pretende alcanzar el RGPD; fortalecer la cultura preventiva de los riesgos asociados al tratamiento y el compromiso con el cumplimiento normativo.

Y en cuanto a los derechos de los interesados, no puede afirmarse que se haya auspiciado una pérdida o desprotección en cuanto al resarcimiento de los daños y perjuicios ocasio-

nados por la infracción del RGPD. Al contrario, se impone el criterio o doctrina civilista de acreditación de los daños y perjuicios causados, alejada de la automaticidad y requiriendo una actividad probatoria que justifique frente a las hipotéticas reclamaciones infundadas de derecho; de esta forma, se refuerzan los principios de equivalencia y efectividad.

Por consiguiente, la posible indemnización reparadora no adquiere un carácter punitivo, sino más bien compensatorio, alejada de las posibles sanciones administrativas que puedan imponerse por la vulneración normativa de origen. Y, en suma, sin tomar como referencia los montantes económicos previstos para las sanciones administrativas, ya que los parámetros gradualistas de las indemnizaciones deben adoptarse por los jueces nacionales a partir de las disposiciones internas. Así, la tutela judicial efectiva se garantiza en tanto en cuanto las personas pueden acudir ante la jurisdicción en su estado miembro articulando la actividad probatoria correspondiente, a fin de obtener un resarcimiento inclusive a régimen de mínimos. Por ello, la indemnización debe garantizar el acceso a una reparación proporcional, efectiva y justa del daño causado.

# VI. Bibliografía

**Jääskinen, N**. (2024). «Robo de datos personales registrados en una aplicación de negociación con valores: TJ, Sala Tercera, 20 jun. 2024. Asuntos. C-182/22 y C-189/22: JU, SO y Scalable Capital GmbH», *La Ley Unión Europea*, núm. 129.

**Jääskinen, N**. (2023). «Solo una infracción culpable del Reglamento General de Protección de Datos puede dar lugar a la imposición de una multa administrativa: TJ, Gran Sala, S 5 dic. 2023. Asunto: C–683/21: Nacionalinis visuomenės sveikatos centras», *La Ley Unión Europea*, núm. 121.

**Jääskinen, N**. (2023). «Poderes de las autoridades de control para imponer medidas correctivas a una persona jurídica: necesidad de que la infracción sea intencionada o negligente: TJ, Gran Sala, S 5 dic. 2023. Asunto C-807/21: Deutsche Wohnen», *La Ley Unión Europea*, núm. 121.

**Jääskinen, N**. (2023). «El temor a un potencial uso indebido de datos personales puede constituir por sí solo un daño o perjuicio inmaterial: TJ, Sala Tercera, S 14 dic. 2023. Asunto C–340/21: Natsionalna agentsia za prihodite», *La Ley Unión Europea*, núm. 121.

**Jääskinen, N**. (2023). «Derecho a indemnización por los daños y perjuicios causados por un tratamiento de datos en infracción del Reglamento de tratamiento de datos personales (TJ 3.ª S 4 May. 2023, as. C-300/21: Österreichische Post): TJ, Sala Tercera, S 4 May. 2023. Asunto C-300/21: Österreichische Post», *La Ley Unión Europea*, núm. 115.

**López Aguilar, J.F**. (2017). «La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU», *Revista de Teoría y realidad constitucional*, núm. 39.

**Lousada Arochena, F**. (2021). *La cuestión prejudicial ante el tribunal de justicia vista desde un órgano judicial español*, Granada, Laborum.

**Macías Castaño, J.M**. (2014). *La cuestión prejudicial europea y el Tribunal Constitucional. Asunto Melloni*, Barcelona, Atelier.

**Mangas Martín, A. Liñán Nogueras, D.J**. (2012). *Instituciones y derecho de la Unión Europea*, 7.º Edición, Madrid, Tecnos.

**Ortega Giménez, A**. (2024). «El Tribunal de Justicia de la UE y la imposición de multas administrativas por infracción del Reglamento General de Protección de Datos (Casos Nacionalinis visuomenės Sveikatos Centras y Deutsche Wohnen)», *Diario la Ley*, núm. 10581.

**Padín Vidal, A**. (2019). «Sanciones por incumplimiento del RGPD en la Unión Europea», La Ley Privacidad, núm. 2.

**Piñar Mañas, J.L**. (2003). «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», *Cuadernos de Derecho Público*, núm. 19-20.

**Piñar Mañas, J.L., Recio Gayo, M**. (2018). *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer España

**Polo Roca, A**. (2020). «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado», *Revista de Derecho Político*, núm. 108.

**Pouget Bastida, M.A**. (2017). *Cuestión Prejudicial Comunitaria y Tutela Judicial Efectiva*, Pamplona, Thomson Reuters Aranzadi.

**Rallo Lombarte, A**. (2017). «El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet», *UNED- Teoría y Realidad Constitucional*, núm. 39.

**Recio Gayo, M**. (2017). «Las sanciones en el RGPD: comentarios a las Directrices del Grupo de trabajo del artículo 29», *Diario la Ley*, núm. 12.

**Rubí Puig, A**. (2019). «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español», *Derecho Privado y Constitución*, núm. 34.

**Soca Torres, I**. (2016). *La cuestión prejudicial europea. Planteamiento y competencia del tribunal de justicia*, Barcelona, Bosch Procesal.

**Todolí Signes, A**. (2024). «Democracia en el trabajo y codeterminación ante el uso de la IA en la empresa: algo más que negociar el algoritmo», *Revista Crítica de Relaciones de Trabajo*, *Laborum*, núm, extra-2.

# VII. Anexo sentencias

- STSJ de Galicia 6192/2024, de 17 de septiembre.
- STSJ de Cataluña 5331/2023 de 27 de septiembre.
- STSJ de Comunidad Valenciana 2070/2021, de 22 de junio.
- STSJ de Madrid 689/2018, de 26 de octubre.
- STJUE de 5 de mayo de 2023, C-300/21.
- STJUE de 5 de diciembre de 2023, C-807/21.
- STJUE de 5 de diciembre de 2023, C-683/21.
- STJUE de 14 de diciembre de 2023, C-340/21.
- STJUE de 20 de junio de 2024, C-590/22.
- STJUE de 20 de junio de 2024, C-182/22 y C-189/22.
- STJUE de 27 de junio de 2024, C-768/21.