ESTUDIOS

Incluye
Papel + Digital

ASPECTOS LEGALES DE LA CIBERSEGURIDAD

LAURA GRANDE PÉREZ
IRENE GONZÁLEZ PULIDO
DIRECTORAS

Cátedra Internacional en Ciberseguridad CyberChain
VNiVERSiDAD D SALAMANCA
Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
ARANZADI

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/publicaciones

Primera edición: marzo 2026

Depósito Legal: M-3984-2026
ISBN versión impresa con complemento electrónico: 978-84-1085-679-0
ISBN versión electrónica: 978-84-1085-680-6

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

Índice General

Página

Página

Algunos aspectos problemáticos sobre la responsabilidad civil por infracción del derecho a la protección de datos en casos de ciberataque

Felipe Oyarzún Vargas*
Universidad Carlos III de Madrid

SUMARIO: 1. INTRODUCCIÓN. 2. ¿CUÁL ES EL PLAZO DE PRESCRIPCIÓN POR LOS DAÑOS DERIVADOS POR UN CIBERATAQUE? 3. EN CUANTO AL CRITERIO DE IMPUTACIÓN EN CASOS DE CIBERATAQUES: ¿RÉGIMEN OBJETIVO O SUBJETIVO? 4. EN CUANTO A LA CAUSALIDAD: ¿EL HECHO DE UN TERCERO (COMO UN HACKER) EXONERA DE RESPONSABILIDAD AL RESPONSABLE DEL TRATAMIENTO? 5. EN CUANTO AL DAÑO RESARCIBLE: ¿QUÉ DAÑOS SE PUEDEN PRODUCIR POR UNA BRECHA DE SEGURIDAD? 6. CONCLUSIONES.

1. INTRODUCCIÓN

El Reglamento General de Protección de Datos (RGPD) es el que ha establecido las bases que dotan de contenido el derecho de las personas a la protección de sus datos personales en Europa. En cuanto a los remedios en caso de infracción, de la lectura de la normativa es posible distinguir entre la tutela jurídica privada y la tutela jurídica pública en la protección de los datos personales[1]. La primera se cristaliza a través del establecimiento de la responsabilidad civil del responsable o encargado del tratamiento como

* Este trabajo ha sido realizado en el marco del Proyecto de I+D+i PID2022-142468NB-I00, sobre "Pago de lo indebido y enriquecimiento injustificado: las bases del sistema", financiado por la Agencia Estatal de Investigación (AEI).

1. De Miguel Asensio, P. "Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos", *Revista La Ley Unión Europea*, Nº 115, 2023, p. 2.

una de las consecuencias que se derivan de la vulneración a la protección de los datos personales (art. 82 del RGPD[2]). La segunda establece un derecho a presentar una reclamación ante una autoridad de control, la cual es competente para sancionar las conductas contrarias al RGPD (Art. 77 del RGPD).

Así, una de las posibles consecuencias de la vulneración de la protección de datos personales es la responsabilidad civil. En la actualidad es el art. 82 del RGPD —el cual es directamente aplicable en cada Estado miembro y obligatorio en todos sus elementos (Art. 288 del Tratado de Funcionamiento de la Unión Europea)[3]— el fundamento legal de las acciones indemnizatorias por las infracciones al derecho de protección de datos personales en España[4], reemplazando al antiguo art. 19 de la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[5]. Esto resulta una diferencia con otros países de la Unión Europea, que han incluido una regla de responsabilidad en su Derecho interno[6].

Ahora bien, es preciso indicar que esta regla tiene una serie de problemas para su aplicación. En primer lugar, el art. 82 del RGPD se trata de un

---

2. Art. 82.1. del RGPD indica 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*".
3. Plaza Penadés, J., "Protección de datos e indemnización por daños en la reciente jurisprudencia del TJUE", en Herrador Guardia, M (Dir.), *Daño y resarcimiento.* Sepin, Madrid, 2024, p. 398.
4. Rubí Puig, A., "Daños por infracciones del derecho a la protección de datos personales: el remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil*, vol. V, n.º 4, 2018, p. 57.
5. La derogada LOPD de 1999 establecía lo siguiente: "*Artículo 19. Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria*".
6. Véase la situación en otros ordenamientos jurídicos europeos en Moreno Martínez, J.A., "El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores", en Ataz López, J; Cobacho Gómez, J.A. (coords), *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*, Vol. 3, Aranzadi, Pamplona, 2021, p. 542 y ss.

remedio privado que está inserto en una normativa que posee un protagonismo elevado del Derecho público y regulatorio[7]. El diseño normativo del régimen de protección de datos contiene una serie de actuaciones que pueden realizarse sin la concurrencia de la persona que ha visto lesionado su derecho a la protección de datos personales[8].

En segundo lugar, constituyendo el objeto central de este trabajo, existe una escueta regulación de la responsabilidad civil en materia de protección de datos. En este sentido, el RGPD se caracteriza por una ausencia de regulación de diferentes aspectos de la responsabilidad civil, cuestión que ha sido mantenida (y acentuada) por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). Por una parte, el RGPD dispone de una cláusula general de responsabilidad, pero en su normativa omite una serie de aspectos propios de este mecanismo (por ejemplo: el criterio de imputación, el plazo de prescripción, entre otros), mientras que, por otra parte, la LOPD no contiene prácticamente ninguna norma sobre esta materia[9].

A partir de esa insuficiencia, las normas sustantivas y procesales de Derecho interno de cada Estado tienen la tarea de colmar las lagunas existentes. No obstante, la falta de previsión legal por parte del legislador europeo sobre la responsabilidad civil en este tipo de casos puede llevar a que los países de la UE resuelvan problemas idénticos mediante soluciones diferentes[10].

La situación descrita no solamente genera interrogantes que afectan el atractivo de la acción indemnizatoria para ser ejercida en nuestro ordenamiento jurídico, sino que también contrasta con la creciente producción de ciberataques en España[11]. No resulta una novedad indicar que, en la era

7. En igual sentido, De Barrón Arniches, P., "Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela", *Revista de Derecho Civil* (2024), vol. 11, n.º 1, 2024, p. 182; Rubí Puig, A., "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", *Revista Derecho Privado y Constitución*, n.º 34, 2019, p. 201.
8. Rubí Puig, *op. cit*., 2019, p. 207.
9. En rigor, la vigente LOPD se limita a señalar exclusivamente que, en los casos en que pueda existir responsabilidad del encargado, el responsable del tratamiento deberá responder solidariamente junto con él (art. 30.2 LOPD, lo cual sigue lo establecido en el art. 82.4 del RGPD).
10. Rubí Puig, *op. cit*., 2019, p. 203.
11. Consultado en: https://cincodias.elpais.com/smartlife/lifestyle/2024-09-17/espana-quinto-pais-mas-ciberataques-recibe.html (Fecha última consulta: 7 de mayo de 2025).

digital, la protección de datos personales se ha convertido en un tema crucial debido al aumento de violaciones de seguridad[12].

Con base en este diagnóstico, resulta relevante identificar e investigar acerca de algunos de los aspectos problemáticos de la responsabilidad civil por infracción del derecho a la protección de datos en casos de ciberataque.

2. ¿CUÁL ES EL PLAZO DE PRESCRIPCIÓN POR LOS DAÑOS DERIVADOS POR UN CIBERATAQUE?

Uno de los ejemplos de lagunas normativas en el ámbito de protección de datos es la prescripción de la acción indemnizatoria. Sobre este punto, ni el RGPD ni la LOPD disponen de una regla al respecto. A causa de la ausencia de un plazo en la regulación y reflejo de las problemáticas que se pueden generar en estas materias, es posible ofrecer más de una respuesta al respecto.

Algunos autores han indicado que, a falta de plazo en la normativa especial, por defecto se tendrán que aplicar las normas de derecho interno[13]. Apelando a las normas de Derecho interno, es preciso realizar algunas distinciones.

Inicialmente, se debe distinguir si es una lesión producida por un ente público o uno privado. Con base en el art. 82.6 del RGPD, las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro de acuerdo con el art. 79.2 del RGPD[14]. Así, en el caso de que la víctima ejerza una acción ante tribunales españoles, deberá presentar su demanda en una sede distinta según cual sea la naturaleza del ente que ha sido el responsable del

12. De acuerdo con el INCIBE, las brechas de seguridad son "*violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos*". Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf (Fecha última consulta: 7 de mayo de 2025).

13. Rubí Puig, A., "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil*, Vol. 5, Nº 4, 2018, p. 82.

14. Art. 79.2 RGPD establece que "*Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos*".

tratamiento de los datos personales. Si es un ente privado, se deberá presentar una acción ante la jurisdicción civil; en cambio, si es un ente público, deberá presentar su acción ante la jurisdicción contencioso-administrativa[15].

En los casos en que el responsable del tratamiento sea un ente privado, se ha mencionado que el art. 82 es la regla de responsabilidad civil en el ordenamiento jurídico español. Aplicando las normas generales, se puede apuntar que los daños en estas materias suelen producirse al margen de lo establecido en el contrato, motivo por el cual las acciones tienden a seguir el marco extracontractual[16]. Por este motivo, buena parte de la doctrina nacional se inclina por la aplicación del régimen extracontractual para este tipo de casos. En consecuencia, el plazo para ejercer la acción sería de un año desde que la persona que ha sido lesionada en su derecho a protección de datos ha tenido conocimiento (art. 1968.2 del Código Civil)[17]. No obstante, también se debe mencionar que existen autores que consideran posible aplicar la tutela contractual, siendo posible considerar el incumplimiento como parte del contenido del contrato en virtud del art. 1258 del CC[18]. En esta hipótesis, el plazo de prescripción sería el de las acciones personales que no tengan plazo especial (cinco años desde que pueda exigirse el cumplimiento de la obligación, art. 1964.2 del Código Civil). Incluso, se ha indicado que el plazo de prescripción puede variar de acuerdo con el contenido del derecho civil de cada una de las Comunidades Autónomas (así, por ejemplo, en Cataluña serían diez años en la responsabilidad contractual y tres años en la responsabilidad extracontractual, arts. 120-20 y 120-21 del Código Civil de Cataluña[19]).

En los casos en que el responsable del tratamiento sea un ente público, la vigente LOPD no contiene una regla de responsabilidad, a diferencia de

15. En igual sentido, Santos Morón, M.J., "Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD", *Cuadernos de Derecho Transnacional*, 16(2), 2024, p. 1406; López del Moral Echeverría, J.L, "Derecho al resarcimiento por los perjuicios derivados de infracciones en materia de protección de datos (Comentario al artículo 82 RGPD)", en Troncoso Reigada. A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*, Vol. 2, Civitas, Pamplona, 2021, p. 3073.
16. En igual sentido, Moreno Martínez, *op. cit*., 2021, p. 522.
17. Véase el Informe Jurídico 00148/2019 de la Agencia Española de Protección de Datos (AEPD), p. 26.
18. Busto Lago, J.M., "La responsabilidad civil y su función de tutela del derecho a la protección de los datos personales: una visión desde el derecho de la Unión Europea", *Revista Jurídica da UFERSA*, Vol. 5, Nº. 10, 2021, p. 30.
19. Por ejemplo, Rubí Puig defiende un plazo de diez años de la acción del art. 82 del RGPD en Cataluña, Rubí Puig, *op. cit*., 2019, p. 225.

su antecesora. En este aspecto, el art. 19 de la antigua LOPD establecía una remisión normativa a la legislación reguladora del régimen de responsabilidad patrimonial de las Administraciones públicas. Sin embargo, dicha remisión en la actualidad no existe, de forma tal que surge una pregunta en cuanto a cuál debiese ser la normativa aplicable en el caso de que sea un ente público el responsable del tratamiento de datos personales.

Pese a la ausencia de referencias en la legislación vigente y a pesar de que el art. 19 de la antigua LOPD está derogado, existe una parte de la doctrina que indica que se debe aplicar en estos casos la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP)[20]. En consecuencia, en estos casos la indemnización se exigirá de acuerdo con la LRJSP ante la jurisdicción contencioso-administrativa[21]. Por tanto, estos autores defienden la idea de que, cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá con arreglo a la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. Siguiendo esta idea, la prescripción de la acción indemnizatoria en estos supuestos sería de un año de producido el hecho o el acto que motive la indemnización o se manifieste su efecto lesivo (art. 67 de Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas).

Del panorama descrito, resulta evidente que la cantidad de plazos disponibles afecta a la consolidación de un régimen de protección de los datos personales desde la perspectiva del derecho de daños. Sería conveniente unificar esta materia, estableciendo un régimen igualitario de protección centrado en la figura del responsable del tratamiento y estableciendo causales de interrupción, como en otras materias de nuestro ordenamiento jurídico[22], sin importar si el responsable del tratamiento es un ente privado o público, o si el daño es contractual o extracontractual, o si el territorio donde se ha sufrido el daño dispone de un plazo especial de prescripción. Esto resulta más urgente en casos de ciberataques, donde las víctimas pueden

20. Por ejemplo, Plaza Penadés, *op. cit.*, 2024, p. 403; Moreno Martínez, *op. cit.*, 2021, p. 552.
21. López del Moral, *op. cit.*, 2021, p. 3073.
22. Por ejemplo, esto es así en materia de competencia desleal. Concretamente, el art. 74.3 de la Ley de Competencia Desleal establece que la prescripción se interrumpe si una autoridad de la competencia inicia una investigación o un procedimiento sancionador en relación con una infracción del Derecho de la competencia relacionada con la acción de daños. La interrupción terminará un año después de que la resolución adoptada por la autoridad de competencia sea firme o se dé por concluido el procedimiento de cualquier otra forma. A diferencia de la LDC (art. 74.3), la LOPD no establece una interrupción de la prescripción por el inicio de una investigación por parte de la autoridad administrativa.

ser múltiples, no estando siempre en condiciones similares o en una misma comunidad autónoma.

3. EN CUANTO AL CRITERIO DE IMPUTACIÓN EN CASOS DE CIBERATAQUES: ¿RÉGIMEN OBJETIVO O SUBJETIVO?

De la lectura del art. 82 del RGPD no es posible señalar *a priori* si se está en presencia de un régimen objetivo o subjetivo de responsabilidad. Al respecto, se debe advertir que el asunto no se ha caracterizado por su desarrollo. Un ejemplo de esto es que, hasta hace poco, no existían sentencias del Tribunal de Justicia de la Unión Europea (TJUE) que se refiriesen a la responsabilidad civil en materia de protección de datos[23]. Sin embargo, a fines de 2023 fue resuelta una cuestión prejudicial por el TJUE que precisamente abordó diferentes cuestiones relativas a la responsabilidad civil a causa de una brecha de seguridad producida por un ciberataque de un tercero[24]. Posterior a esa sentencia, el TJUE se ha manifestado en más de una ocasión sobre el contenido del art. 82 del RGPD.

Por su parte, la doctrina no es uniforme al momento de calificar si la responsabilidad establecida en el art. 82 del RGPD es objetiva o subjetiva. Una buena parte de la doctrina nacional ha considerado que el criterio de imputación de responsabilidad civil en materia de protección de datos es objetivo, con base en distintos argumentos[25]. En contraste, otros autores dentro de la doctrina española se han manifestado en el sentido opuesto, es decir, han indicado que el régimen de responsabilidad del RGPD es subjetivo[26].

23. La primera sentencia en la que TJUE se refirió a este asunto fue la STJUE, de 4 de mayo de 2023 (Asunto C-300/21, *RW c. Österreichische Post AG*, ECLI:EU:C:2023:370).

24. STJUE, de 14 de diciembre de 2023 (Asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986). En este caso, la Agencia Nacional de Recaudación búlgara sufrió un ciberataque que generó la publicación en Internet de los datos personales de millones de personas. Un gran número de afectados interpusieron acciones contra la Agencia Nacional de Recaudación, exigiendo un resarcimiento por los daños morales que habían sufrido por el temor a un potencial uso indebido de sus datos personales.

25. Martín Faba, J.M., "Novedades en materia de indemnización y protección de datos personales", *Revista CESCO De Derecho De Consumo*, Nº49, 2024, pp. 145-146; Moreno Martínez, *op. cit*., 2021, p. 538; Grimalt Servera, P., "Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen. Tutela civil versus tutela administrativa", en Castilla Barea, M; González Pacanowska, I. (coords.), *Protección de datos personales*, Tirant Lo Blanch, Valencia, 2020, p.364; Rubí Puig, *op. cit*., 2018, p. 62.

26. Busto Lago, *op. cit*., 2021, p. 33; Nieto Garrido, E., "Derecho a indemnización y responsabilidad", en Piñar Mañas, J.L. (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 561-562.

En rigor, se ha señalado que se está en presencia de un sistema subjetivo de responsabilidad, pero con una inversión de la carga de la prueba de la culpa.

Esta última posición ha sido la adoptada por el TJUE en sus últimos pronunciamientos sobre la responsabilidad civil en el ámbito de la protección de datos. En este aspecto, el asunto C-667/21 ("*Krankenversicherung Nordrhein*") indica expresamente que el art. 82 establece un régimen de responsabilidad por culpa en que la carga de la prueba recae sobre el responsable del tratamiento[27]. Por tanto, se presume la culpa del responsable del tratamiento de datos personales. En esta sentencia, el TJUE ha indicado que un régimen de responsabilidad objetiva no garantizaría la consecución del objetivo de seguridad jurídica perseguida por el legislador y no respetaría el equilibrio entre los intereses de los responsables del tratamiento y los derechos de las personas cuyos datos se tratan[28].

La doctrina establecida en el asunto C-667/2021, ha sido ratificada por el TJUE en otras sentencias. Así, en los asuntos C-687/21 ("*MediaMarktSaturn*"[29]), C-741/21 ("*Juris*"[30]) se ha considerado que la culpa se presume salvo que el responsable demuestre que no es responsable del hecho generador del daño. En otras palabras, se establece un régimen de responsabilidad por culpa con inversión de la carga de la prueba.

Pese a las sentencias citadas, la cuestión dista de estar resuelta. Es posible encontrar matices y reparos en lo que ha sido la postura del TJUE en sus últimas sentencias. En este sentido, se ha manifestado que lo que se invierte no es la prueba de la culpa, sino que la prueba de la infracción[31]. La inversión de la carga de la prueba es sobre la infracción, pues será el responsable, en función de sus respectivas obligaciones, quien deba acreditar que se han cumplido con las obligaciones contenidas en el RGPD[32]. Por su parte, el propio TJUE presenta inconsistencias en su argumentación. Por ejemplo, en *Juris*, el TJUE, luego de establecer que la responsabilidad era subjetiva con inversión de la prueba de la culpa, se contradice ya que establece que, en casos de violación de seguridad de los datos personales, el responsable

27. STJUE, de 21 de diciembre de 2023 (Asunto C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2024:1051), apartados 94 y 103.
28. STJUE, *Krankenversicherung Nordrhein* (cit.), ap. 100.
29. STJUE, de 25 de enero de 2024 (Asunto C-687/21, *MediaMarktSaturn,* ECLI:EU:C:2024:72), ap. 52.
30. STJUE, de 11 de abril de 2024 (Asunto C-741/21, *GP contra juris GmbH*, ECLI:EU-:C:2024:288), ap. 46.
31. Santos Morón, *op. cit*., 2024, p. 1419.
32. López del Moral, *op. cit*., 2021, p. 3068.

podrá exonerarse si demuestra que no existe una relación de causalidad entre el eventual incumplimiento del RGPD y los daños y perjuicios sufridos por el interesado[33]. Es decir, vuelve a apelar a criterios estrictamente causales y no hace referencia a la prueba de la diligencia para exonerar de responsabilidad al responsable del tratamiento.

También existen posturas intermedias acerca de este punto. Santos Morón distingue según se esté en presencia de una obligación de medios o una obligación de resultado en el RGPD. Para esta autora, el criterio de imputación subjetivo con inversión de la carga de la prueba de la infracción se aplicará cuando se trate de una obligación de medios, que exige la apreciación de culpa en el caso concreto. En cambio, en el caso en que la obligación que incumbe al responsable del tratamiento sea una obligación de resultado, en ese caso solamente se podrá exonerar demostrando que el hecho causante del daño no le es imputable[34].

Como se observa, no es un tema pacífico donde exista una posición unánime. Hasta antes de los pronunciamientos del TJUE, se veía un predominio de la idea de que la responsabilidad era objetiva[35]. En cambio, siguiendo el criterio establecido por el TJUE en sus últimas sentencias, en la actualidad prevalece el enfoque de una responsabilidad subjetiva con inversión de la prueba de la infracción. En este contexto, será clave conocer los primeros pronunciamientos del Tribunal Supremo sobre la aplicación del RGPD en este punto[36].

---

33. STJUE, *GP contra juris GmbH* (cit.), ap. 51.
34. Santos Morón, *op. cit.*, 2024, p. 1421. Es posible encontrar opiniones similares referidas a la antigua LOPD. Al respecto, se ha dicho que "*a la hora de aplicar el artículo 19 LOPD, la Ley no determina si la responsabilidad es objetiva o subjetiva, sin embargo, parece que por norma general lo que habrá que analizar es si el incumplimiento es imputable a un sujeto determinado y si el titular de los datos tiene o no el deber de soportarlo*", en Aberasturi Gorriño, U., "El derecho a la indemnización en el artículo 19 de la Ley orgánica de Protección de Datos de Carácter Personal", *Revista Aragonesa de Administración Pública*, Nº 41-42, 2013, p. 191. También se debe destacar lo señalado por el Abogado General Campos Sánchez-Bordona, dado que, a pesar de dar argumentos que finalmente defienden una responsabilidad objetiva, señala que no cree que el RGPD se ajuste plenamente a ninguno de los dos modelos en puridad. Véase la nota al pie 55 del ap. 72 de las Conclusiones del Abogado General sobre el Asunto C-667/21, presentadas el 25 de mayo de 2023.
35. En la doctrina comparada, véase Menezes Cordeiro, A., "Civil Liability for Processing of Personal Data in the GDPR". *European Data Protection Law Review (EDPL)*, Nº. 4, 2019, p. 498.
36. Es posible encontrar en alguna sentencia dictada por un tribunal español afirmando que la responsabilidad establecida en el RGPD no es objetiva. Véase SAP Madrid (Sección 20ª), de 28 de junio de 2024 (JUR\2024\308163).

4. EN CUANTO A LA CAUSALIDAD: ¿EL HECHO DE UN TERCERO (COMO UN HACKER) EXONERA DE RESPONSABILIDAD AL RESPONSABLE DEL TRATAMIENTO?

La causalidad siempre es un requisito para la concurrencia de responsabilidad, ya sea un régimen objetivo como subjetivo. En cuanto a la relación causal en el ámbito de protección de datos, se discute si un ciberataque por un tercero (como un hacker) exime de responsabilidad al responsable del tratamiento. Sobre este punto, cabe señalar que uno de los pilares fundamentales del RGPD es la seguridad. En este sentido, el responsable del tratamiento de datos está obligado a implementar medidas técnicas y organizativas adecuadas y eficaces que se ajusten a los requisitos establecidos por el RGPD, con el objetivo de asegurar un nivel de protección apropiado[37]. Esta obligación implica que dicho responsable debe identificar y evaluar los riesgos asociados al tratamiento de los datos personales, y adoptar las medidas necesarias para reducirlos. Conforme al artículo 5.1.f) del RGPD, este tratamiento debe llevarse a cabo de forma que se garantice su seguridad, protegiéndolos contra accesos no autorizados o ilícitos, así como contra su pérdida, destrucción o alteración accidental, todo ello mediante la aplicación de mecanismos de protección apropiados.

No se debe entender este mandato de seguridad que recae sobre los responsables del tratamiento como una responsabilidad a todo evento. En efecto, el TJUE ha señalado que el RGPD exige al responsable del tratamiento adoptar medidas técnicas y organizativas destinadas a evitar, en la medida de lo posible, cualquier violación de la seguridad de los datos personales[38]. Es decir, el responsable del tratamiento de los datos personales no está obligado a impedir toda violación de seguridad, sino que debe adoptar las medidas adecuadas para que las violaciones no se produzcan. Desde esta perspectiva, el legislador europeo ha entendido que es imposible eliminar todos los riesgos que surgen en la protección de los datos personales; por ese motivo, permite al responsable de datos aportar prueba de que las medidas adoptadas eran las apropiadas. El TJUE ha indicado que los jueces de cada Estado miembro deben valorar el carácter apropiado de las medidas técnicas y organizativas, teniendo en cuenta el caso concreto, considerando los riesgos asociados y apreciando si la naturaleza, el contenido y la adopción de esas medidas están adaptados a estos riesgos[39].

37. Véase tanto los arts. 24 y 32 como los considerandos 74 y 83 del RGPD.
38. STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), ap. 30.
39. STJUE, *MediaMarktSaturn* (cit.), ap. 38.

Con base en lo expuesto, el acceso no autorizado por parte de un tercero o una comunicación no autorizada de datos personales no basta para concluir que las medidas adoptadas por el responsable no eran las adecuadas. Así, no es suficiente que haya ocurrido un ciberataque para concluir que se está en presencia de un incumplimiento de la obligación de seguridad por parte de responsable. Se deberá valorar, para determinar el carácter apropiado de las medidas, tanto el análisis de riesgos que entrañe el tratamiento como la adecuación de las medidas a los riesgos teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento[40].

En virtud de los artículos 5.2, 24.1 y 32.1 del RGPD, la carga de la prueba de que los datos personales se tratan de modo que se garantiza una seguridad adecuada incumbe al responsable de tratamiento[41]. En consecuencia, cuando la infracción tenga relación con la falta de implementación de medidas de seguridad adecuadas, se produce una inversión de la carga de la prueba. Martín Faba justifica esta inversión señalando que los interesados no tienen conocimiento suficiente ni acceso a la información referida a la implementación de las medidas de seguridad que ha adoptado el responsable del tratamiento[42].

5. EN CUANTO AL DAÑO RESARCIBLE: ¿QUÉ DAÑOS SE PUEDEN PRODUCIR POR UNA BRECHA DE SEGURIDAD?

Las violaciones de seguridad de los datos personales pueden llegar a producir daños patrimoniales o extrapatrimoniales para las personas físicas[43]. Cabe advertir que no toda vulneración de seguridad de los datos será causa suficiente para que proceda la responsabilidad en el caso concreto[44], siendo insuficiente la mera infracción del RGPD para obtener un resarcimiento[45]. Por tanto, será

40. STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartados 30 y 42.
41. STJUE, *MediaMarktSaturn* (cit.), ap. 42-43; STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), ap. 52 y 57.
42. Martín Faba, *op. cit*., 2024, p. 137.
43. El art. 4.12 del RGPD define la violación de la seguridad de los datos personales como aquella "*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*".
44. Esto es una diferencia, por ejemplo, con lo regulado en la Ley Orgánica 1/1982, la cual indica en su art. 9.3 que la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. Es decir, el daño se presume ante la prueba de la infracción a la normativa, cuestión que no ocurre en el ámbito de datos personales.
45. Véase STS (Civil) de 19 de marzo de 2024 (JUR\2024\92465). En doctrina, Plaza Penadés, *op. cit*., 2024, p. 413.

siempre necesario que el interesado acredite los daños que ha sufrido como consecuencia de la vulneración en el tratamiento de sus datos personales[46].

Como ha sido dicho, el art. 82 del RGPD establece un resarcimiento tanto de los daños patrimoniales como de los extrapatrimoniales a causa de infracciones en el tratamiento de los datos personales. Ahora bien, a partir de la amplitud que establece esta cláusula general de daños, conviene preguntarse cuáles son los daños indemnizables y qué criterios se pueden utilizar para distinguir entre aquellos que deben ser resarcidos y los que no en situaciones de brechas de seguridad.

Antes de los primeros pronunciamientos del TJUE en estos asuntos, se consideraba que una brecha de seguridad no era causal suficiente para activar el mecanismo de la responsabilidad civil, sino que servía exclusivamente para notificar a la autoridad competente y a las personas afectadas[47].

Eso se ha modificado mediante la STJUE del asunto C-340/21 la cual se refiere, entre otras cuestiones, a la aplicación y extensión del artículo 82 del RGPD en este tipo de casos. Concretamente, el TJUE ha considerado que el temor a un potencial uso indebido de datos personales puede constituir por sí solo un daño extrapatrimonial resarcible al amparo del art. 82 del RGPD. Adicionalmente, en varias sentencias posteriores el TJUE ha reiterado que la mera pérdida de control puede ocasionar una violación de la seguridad de los datos personales que puede causar al interesado daños y perjuicios resarcibles al amparo del art. 82 del RGPD, por mínimos que sean[48]. El TJUE ha sostenido que una vez acreditada una infracción al RGPD, éste no distingue entre: (i) los supuestos de daños morales que alega el interesado a causa de un uso indebido de sus datos personales por terceros que ya se ha producido en la fecha de la acción indemnizatoria; (ii) de los supuestos en los que esos daños morales están relacionados con el temor que experimenta ese interesado a que tal uso pueda producirse en el futuro[49].

---

46. El TJUE lo ha señalado en varias ocasiones, por ejemplo: STJUE, *GP y juris GmbH*, (cit.), ap. 34-35; STJUE, *Österreichische Post AG* (cit.), ap. 42; STJUE, *MediaMarktSaturn* (cit.), ap. 58; STJUE, *Krankenversicherung Nordrhein* (cit.), ap. 82; STJUE, *GP contra juris GmbH* (cit.), ap. 34. Esto también se observa en sentencias dictadas por tribunales españoles, véase STS (Civil) de 19 de marzo de 2024 (JUR\2024\92465); ATS (Sección 1ª) de 17 de enero de 2019 (JUR\2019\35381); STSJ Andalucía (Sala de lo Social, Sección 1ª) de 10 de enero de 2024 (JUR\2024\104740); SAP Madrid (Sección 20ª), de 28 de junio de 2024 (JUR\2024\308163).
47. Plaza Penadés, *op. cit*., 2024, p. 413.
48. STJUE, *GP contra juris GmbH* (cit.), ap. 42. STJUE, *MediaMarktSaturn* (cit.), ap. 66.
49. STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), ap. 79.

En consecuencia, el TJUE ha sido proclive a indemnizar los daños morales puros y ha establecido una regla "*de minimis*" mediante la cual se impone la idea de que no se debe exigir ningún umbral de gravedad de los daños sufridos, siendo estos resarcibles por mínimos que sean. No obstante, es importante destacar que no toda molestia puede considerarse un daño resarcible[50]. Lo señalado tiene especial trascendencia en el contexto de la ciberdelincuencia, dado que si toda persona afectada —aunque solo sea mínimamente— por una infracción tuviera derecho a una indemnización de los daños morales, existirían importantes consecuencias para los responsables del tratamiento de datos personales. Lo descrito se representa con mayor fuerza en los casos del sector público, los cuales son financiados con fondos públicos limitados y deben servir a intereses colectivos, incluida la mejora de la seguridad de los datos personales[51]. Por estos motivos, resulta necesario hacer unas distinciones para el desarrollo de la materia en el ordenamiento jurídico español.

Inicialmente, el RGPD permite una acción por daño moral autónomo, sin que sea necesaria la prueba de algún daño patrimonial[52]. En este sentido, el ordenamiento jurídico español, a diferencia de otros ordenamientos jurídicos europeos, la indemnización del daño moral no es una cuestión que sea objeto de debate[53]. Al respecto, conviene destacar que en nuestro Derecho se reconoce la indemnizabilidad del daño moral puro[54], el cual se conceptualiza como aquel perjuicio "*resultante de la lesión de bienes de la personalidad o de un hecho dañoso cuyas consecuencias se limitan al ámbito puramente moral o espiritual de la víctima*"[55]. Como expone Martín Casals, un ejemplo de este tipo de daños es

50. Santos Morón, *op. cit*., 2024, p. 1414.
51. Véase la cita 39 de las Conclusiones del Abogado General sobre el Asunto C-340/21, presentadas el 27 de abril de 2023.
52. Martín Faba, *op. cit*., 2024, p. 141; Rubí Puig, *op. cit*., 2018, p. 74.
53. En cuanto a los diferentes tratamientos que recibe el daño extrapatrimonial en los diversos sistemas jurídicos europeos, véase las reflexiones de Zimmermann, R., "30. Comparative Report (Categories 11-13)", en Winiger. B. et al. (eds.), *Digest of European tort law. Volume 2: Essential Cases on Damages*, De Gruyter, Viena, 2011, pp. 706 y ss.
54. Martín Casals, M., "La 'modernización' del derecho de la responsabilidad extracontractual", en Asociación de Profesores de Derecho Civil (eds.), *Cuestiones actuales en materia de responsabilidad civil. XV Jornadas de la Asociación de Profesores de Derecho Civil, A Coruña, 8 y 9 de abril de 2011*, Editum, Murcia, 2011, p. 119; Martín Casals, M., "Principis per a una proposta de regulació de la responsabilitat extracontractual al Codi Civil de Catalunya", en Institut de Dret Privat Europeu i Comparat de la Universitat de Girona (ed.), *Contractes, responsabilitat extracontractual i altres fonts d'obligacions al Codi civil de Catalunya: materials de les Setzenes Jornades de Dret Català a Tossa*, Girona: Documenta Universitaria, 2012, p. 302; Del Olmo García, P., "Art. 1902", en Cañizares Laso, A. (dir.), *Comentarios al Código Civil. Tomo V*. Primera Edición. Tirant Lo Blanch, Valencia, 2023, p. 8446.
55. Santos Morón, *op. cit*., 2024, p. 1412.

la angustia por el miedo de sufrir un daño que finalmente no se materializa (el caso de "falsos positivos")[56]. Se trata de casos que envuelven únicamente padecimientos emocionales, psíquicos, son daños que derivan de casos de "*perjuicios intangibles y que no acompañan a una pérdida patrimonial, a lesiones personales o a la muerte de la víctima del accidente, son daños reales*"[57].

Ahora bien, aunque en España se acepta la indemnización de distintas hipótesis de daños extrapatrimoniales, lo cierto es que de esto no se debe colegir que cualquier daño moral deba ser resarcido[58]. De acuerdo con Rubí Puig, resulta cuestionable que cualquier exposición a un riesgo sea transformable en un daño moral puro[59]. Como expone Santos Morón, la doctrina "*de minimis*" establecida por el TJUE debería ser entendida en el sentido de que no cabe fijar "*a priori*" un nivel mínimo de gravedad para entender que se está ante un daño indemnizable. Para esta autora, los jueces nacionales de cada Estado miembro, atendiendo las circunstancias concretas, podrán determinar si las consecuencias negativas pueden ser consideradas o no como un daño resarcible[60].

Además, cabe agregar que le corresponderá a la víctima acreditar la existencia de ese daño moral puro. Desde esta perspectiva, el riesgo puramente hipotético no debería dar lugar a indemnización[61]. Siguiendo a Plaza Penadés, el daño moral debe estar fundado en hechos objetivos y no meras conjeturas[62]. En el ámbito de protección de datos personales, no existirá *per se* un resarcimiento por vulneración de los datos personales, puesto que ello dependerá de la naturaleza de los datos y las circunstancias concurrentes de cada caso en particular[63].

---

56. Martín Casals, *op. cit*., 2011, p. 119; Martín Casals, *op. cit*., 2012, p. 302.
57. Gómez Ligüerre, C., "Capítulo I. El concepto de daño moral", en Gómez Pomar, F.; Marín García, Ignacio (Dirs.), *El daño moral y su cuantificación*, Tercera edición, Bosch La Ley, Barcelona, 2023, p. 40.
58. Del Olmo García, P., "Capítulo 2. Epígrafe 1.2. El daño extrapatrimonial", en Soler Presas. A.; Del Olmo García, P. (coords.), *Practicum Daños*, Thomson Reuters, Cizur Menor, 2019, p. 202.
59. Rubí Puig, A., "Inteligencia artificial y daños indemnizables", en Asociación de Profesores de Derecho Civil (eds.), D*erecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, Pamplona, 2024, p. 650.
60. Santos Morón, *op. cit*., 2024, p. 1414.
61. Martín Faba tiene esta posición respecto al riesgo hipotético de un uso indebido por un tercero. Para este autor, "*el riesgo puramente hipotético de uso indebido podría darse cuando es razonable esperar que ningún tercero ha tenido conocimiento de los datos personales en cuestión. Tampoco parece que se genere daño moral alguno cuando los datos revelados de manera no autorizada son de un tipo cuyo uso indebido es inocuo, como el nombre o la dirección postal*". Véase Martín Faba, *op. cit*., 2024, p. 141.
62. Plaza Penadés, *op. cit.* 2024, p. 422.
63. Santos Morón, *op. cit*., 2024, p. 1412.

Por último, sobre los daños indemnizables debe señalarse que existe una ausencia de normas comunes en el Derecho de la Unión Europea que se refieran a la cuantificación de los daños, motivo por el cual le corresponde a cada ordenamiento jurídico aplicar sus propias normas referidas a esta materia[64]. Particularmente en el caso de los daños morales, existe una dificultad para determinar los criterios para cuantificar éstos en materias de protección de datos dada la ausencia de regulación tanto del RGPD como de la LOPD. Al respecto, se pueden observar algunos pronunciamientos por parte del TJUE que pueden servir de orientación a nuestro Derecho para cuantificar los daños derivados de una brecha de seguridad. En efecto, este tribunal ha sostenido que el temor debe estar fundado, habida cuenta las circunstancias del caso y del interesado[65]. En otro de sus últimos pronunciamientos, el TJUE ha indicado que el criterio de que un riesgo meramente hipotético de un uso indebido por un tercero no puede dar lugar a una indemnización, lo cual puede ocurrir cuando ningún tercero ha tenido conocimiento de los datos personales de que se trate[66]. Otra posibilidad para calcular los daños morales sufridos en estas materias, podría ser la aplicación por analogía de los criterios contenidos en otros preceptos de nuestro ordenamiento jurídico para tal efecto, como los establecidos en el ámbito de derecho al honor[67] o en la propiedad intelectual[68], es decir, las circunstancias del caso y la gravedad de la lesión[69]. Trasladando estos criterios al ámbito de protección de datos, se tendría que valorar el tipo de dato personal afectado en el caso concreto, puesto que no es lo mismo un dato relativo a la salud de la víctima que otro tipo de dato[70].

64. STJUE, *GP contra juris GmbH* (cit.), ap. 58. También STJUE *Österreichische Post AG* (cit.), ap. 54; STJUE, *MediaMarktSaturn* (cit.), ap, 47-50; STJUE, *Krankenversicherung Nordrhein* (cit.), ap. 83 y 101.
65. STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), ap. 85.
66. STJUE, *MediaMarktSaturn* (cit.), ap. 68.
67. El art. 9.3 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, establece que "*La indemnización se extenderá al daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido*".
68. Véase el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. Concretamente, el art. 140.2 de esta normativa indica que "*En el caso de daño moral procederá su indemnización, aun no probada la existencia de perjuicio económico. Para su valoración se atenderá a las circunstancias de la infracción, gravedad de la lesión y grado de difusión ilícita de la obra*".
69. Es posible observar esta propuesta en Busto Lago, *op. cit*., 2021, p. 51.
70. Martín Faba (2024), *op. cit*., 2024, p. 141.

6. CONCLUSIONES

La escueta regulación vigente en materia de responsabilidad civil por infracción del derecho a la protección de datos personales, particularmente en casos de ciberataques, genera una serie de incertidumbres sobre la aplicación de este remedio. Las lagunas jurídicas o vacíos normativos en esta materia están presentes tanto en el RGPD como en la LOPD. La ausencia de regulación (sumado al predominio del Derecho público en el diseño institucional) repercute en la protección efectiva de los derechos de los titulares de los datos en supuestos de daños por infracciones al RGPD.

La aplicación directa del artículo 82 del RGPD en el ordenamiento jurídico español, sin desarrollo complementario por parte de la LOPD, genera un marco de responsabilidad incierto. A modo de ejemplo, se han expuesto algunas controversias existentes en el desarrollo e implementación del régimen de responsabilidad civil por daños por infracciones del derecho a la protección de datos personales, con especial énfasis en los supuestos de ciberataque. En este sentido, se ha apuntado a ciertos aspectos problemáticos en torno a la prescripción de la acción indemnizatoria (cuál es el plazo), al criterio de imputación (si es objetivo o subjetivo), la incidencia de factores externos como la intervención de terceros (hackers) a efectos de establecer la causalidad en estos casos y en la determinación de los daños resarcibles (con especial énfasis en la determinación de los daños morales). Cada uno de estos puntos refleja tensiones entre principios de protección eficaz del derecho fundamental a la protección de datos y garantías propias del derecho de daños.

La jurisprudencia del TJUE ha comenzado a ofrecer orientaciones relevantes, aunque todavía incipientes, sobre el alcance de la responsabilidad civil en este ámbito. Su estudio permite advertir una tendencia hacia una interpretación expansiva del artículo 82 del RGPD, favorable a los afectados, aunque queda pendiente una sistematización coherente por parte del legislador nacional y europeo.

A la luz de lo anterior, se impone la necesidad de un desarrollo normativo más preciso que aborde los elementos esenciales de la responsabilidad civil por violación del derecho a la protección de datos en casos de ciberataque. Este desarrollo debe considerar tanto la especificidad técnica del entorno digital como los principios del derecho civil, con el fin de establecer un marco jurídico que garantice la seguridad jurídica, la prevención de daños y la reparación efectiva.

El Reglamento Europeo de Inteligencia Artificial: ¿una regulación ética y eficaz de los sistemas de gestión de riesgos?

Carlos Álvaro Peris

Doctorando en Derecho
Universidad de Valencia

SUMARIO: 1. LOS SISTEMAS DE GESTIÓN DE RIESGOS Y LA CIBERSEGURIDAD. 2. LA REGULACIÓN DE LOS SISTEMAS DE GESTIÓN DE RIESGOS EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL. 2.1. *Análisis normativo.* 2.2. *Análisis técnico.* 2.3. *Análisis ético*. 3. LA COMPLEMENTARIEDAD DE LOS SISTEMAS DE COMPLIANCE PENAL. 4. CONCLUSIONES.

1. LOS SISTEMAS DE GESTIÓN DE RIESGOS Y LA CIBERSEGURIDAD

Las empresas representan el mayor núcleo de creación de actividad económica. Sin duda, esta actividad conlleva riesgos de todo tipo: financieros, legales, operativos… Por tanto, dichas entidades deben contar con un sistema de gestión de riesgos que contemple un enfoque integral, es decir, que sea capaz no solo de identificar, sino también de mitigar, todos los riesgos que surgen en sus distintas áreas[1]. La tecnología ha invadido por completo nuestras vidas, de forma y manera que la mayoría de nuestro tejido empresarial hoy en día ha sido, o está siendo, digitalizado e invadido por la inteligencia artificial[2]. Antiguamente la contabilidad se

1. MORA NAVARRO, O. E., "Gestión de riesgos: un desafío para las organizaciones", *Administración & Desarrollo*, Vol. 52, núm. 1, 2022, p. 7.
2. ÁLVARO PERIS, C., "Atribución de responsabilidad penal en delitos cometidos con uso de sistemas de inteligencia artificial a la luz del nuevo reglamento europeo", *La Ley Penal*, núm. 170, 2024, p. 2.

llevaba en libros físicos, la documentación de los proveedores o clientes se almacenaba en archivadores y las reuniones se anotaban en una agenda. En cambio, en la actualidad, la contabilidad se lleva a través de un programa informático, la documentación de los proveedores o clientes está almacenada en la nube y las reuniones se anotan en un calendario o agenda virtual. Si bien la digitalización ha traído incalculables avances y beneficios, no está exenta de riesgos. Uno de ellos es el posible robo o pérdida de esos datos cuyo almacenamiento hemos confiado a una determinada plataforma en la nube.

De esta manera, en los últimos años numerosas empresas han sido víctimas de distintos ciberataques. Los criminales consiguen el acceso al espacio virtual donde estas almacenan sus datos y una vez recabados pueden llegar incluso a pedirles una cantidad monetaria a cambio de no vender o hacer públicos dichos datos valiosos para la competencia. Este tipo de ciberataques son conocidos como «fugas de información deliberadas»[3]. Además, la ausencia de procedimientos que protejan aquellas actividades de especial importancia o riesgo representa una de las posibles causas organizativas por las que pueden darse esas fugas de información deliberada[4]. Por tanto, ante este contexto resulta necesario que todas las empresas mínimamente digitalizadas implementen un sistema de gestión de riesgos para poder hacer frente a estas situaciones.

2. LA REGULACIÓN DE LOS SISTEMAS DE GESTIÓN DE RIESGOS EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

En primer lugar, centraremos nuestra investigación en torno a los sistemas de gestión de riesgos que en base al Reglamento Europeo de Inteligencia Artificial deben implementar todas aquellas empresas que sean proveedoras de sistemas de IA de alto riesgo. El objetivo principal de este estudio consiste en contrastar las hipótesis acerca de si la regulación propuesta por la Unión Europea para estos sistemas resulta ética y eficaz. Para ello estudiaremos el marco normativo que impera en dicha materia con el fin de realizar posteriormente dos análisis: uno técnico que nos permita averiguar si dicha regulación conllevará sistemas de gestión de riesgos eficaces y otro análisis

3. INCIBE, *Ciberamenazas contra entornos empresariales*, Instituto Nacional de Ciberseguridad, 2020.
4. INCIBE, *Cómo gestionar una fuga de información*, Instituto Nacional de Ciberseguridad, 2016.

ético que nos permita averiguar si con dicha regulación obtendremos sistemas de gestión de riesgos éticos.

2.1. ANÁLISIS NORMATIVO

Primero, antes de establecer el marco normativo, debemos exponer el marco teórico. Para ello debemos aclarar, entre otras cosas, qué entendemos por sistema de gestión de riesgos. Según SIMÓN CASTELLANO, un sistema de gestión de riesgos puede definirse como "*un conjunto de procesos, políticas, procedimientos y herramientas diseñadas para identificar, evaluar, mitigar y monitorear los riesgos que enfrenta una organización en el logro de sus objetivos*"[5]. Además, los riesgos que pretende abordar la presente investigación hacen referencia a aquellos que puedan ocasionar los sistemas de IA de alto riesgo. El apartado 1 del artículo 3 del Reglamento Europeo de IA define estos sistemas, en términos generales, como "*un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*". Posteriormente, el artículo 6 nos aclara que dichos sistemas de IA serán considerados de alto riesgo cuando estemos ante alguno de los contemplados en el anexo III o se den las siguientes dos condiciones:

> *a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y*
>
> *b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.*

Por tanto, siempre que estemos ante un sistema de IA que encaje en la definición del artículo 3 y cumpla con los requisitos establecidos en el

5. SIMÓN CASTELLANO, P., "Los sistemas de gestión de riesgos como obligación específica para los sistemas de inteligencia artificial de alto riesgo en el artículo 9 del Reglamento", en COTINO HUESO, L.; SIMÓN CASTELLANO, P. (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Cizur Menor (Navarra), 2024, p. 535.

artículo 6 para ser considerado de alto riesgo, el proveedor de dicho sistema estará obligado a implementar un sistema de gestión de riesgos, tal y como establecen los artículos 8 y 9 de dicho Reglamento. Seguidamente, habiendo expuesto qué entendemos por sistema de IA de alto riesgo, así como por sistema de gestión de riesgos, debemos dar paso al marco normativo que nos permitirá analizar si la regulación europea asegura o no la implementación de unos sistemas de gestión de riesgos eficaces y éticos. En relación con los aspectos técnicos de dichos sistemas, el marco normativo se encuentra principalmente formado por normativa internacional. La ISO 31010:2010 establece distintas técnicas de apreciación del riesgo, la ISO 27001:2023 fija una serie de requisitos que debenrían cumplir los sistemas de gestión de la seguridad de la información y la ISO 27005:2024 establece una serie de directrices para la gestión de riesgos de seguridad de la información. Además, se debe tener en cuenta los estándares exigidos en torno a la protección de datos (ISO 29100:2011, relativa a la protección de información de identificación personal; ISO 29134:2017, que establece directrices para la evaluación de impacto; e ISO 29151:2017, que representa un código de buenas prácticas para la protección de información de identificación personal). Finalmente, cabría destacar las guías específicas sectoriales, como la ISO 27015:2012, dirigida al sector financiero, o la ISO 27019:2020, orientada al sector de la energía. Por tanto, para analizar si un sistema de gestión de riesgos cumple con los estándares técnicos internacionales, debemos atender al marco normativo que acabamos de describir, teniendo en cuenta no solo las normativas en torno a la gestión del riesgo, sino también aquellas que giran alrededor de la protección de datos, así como si existiera alguna normativa específica para alguno de los sectores en los que opera la empresa.

En relación con los estándares éticos, existen dos principales referencias. La primera corresponde a las directrices éticas para una IA fiable[6]. Este grupo de expertos establece tres componentes que deben darse en toda la cadena de la IA para considerarse como fiable: debe ser lícita, robusta y ética. Por ello, adquiere especial relevancia el capítulo I en el que se identifican los principios éticos que deben respetarse en el desarrollo, despliegue y utilización de los sistemas de IA[7]. Además, desde el punto de vista de la doctrina mayoritaria, estas directrices han sido un referente dentro de la comunidad de inteligencia artificial para la estandarización de los princi-

6. Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial, *Directrices éticas para una IA fiable*, Comisión Europea, 2018.

7. *Ibid*., pp. 11-17.

Papel + Digital

ESTUDIOS

Acceso online a Biblioteca Digital Legalteca:
consulte página inicial de esta obra

El presente libro colectivo sobre «Aspectos legales de la ciberseguridad» recoge un estudio integral e interdisciplinar de los principales desafíos y de la normativa desarrollada en esta materia. El lector encontrará un estudio sobre los diferentes aspectos jurídicos, pudiendo comprender el alcance y la importancia del cumplimiento legal, incluso desde una perspectiva de la prevención. Podrá analizar los principales retos que se plantean con respecto a la protección de datos personales y las responsabilidades que se podrían derivar ante la injerencia de este derecho. Asimismo, el carácter disruptivo de la obra lo marca el análisis de la regulación de la inteligencia artificial, los estudios sobre la gobernanza algorítmica de la ciberseguridad y el planteamiento de los desafíos ciberjurídicos en la era post-cuántica.

ISBN: 978-84-1085-679-0

AENOR GESTIÓN DE LA CALIDAD ISO 9001 ER-0280/2005
IQNET RECOGNIZED CERTIFICATION
AENOR GESTIÓN AMBIENTAL ISO 14001 GA-2005/0100

Cátedra Internacional en Ciberseguridad CyberChain
VNiVERSiDAD D SALAMANCA

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ARANZADI