# Responsabilidad por daños causados por productos inteligentes defectuosos a personas vulnerables

## Daños a niñas, niños y adolescentes, mayores, personas con discapacidad y personas con menor alfabetización digital


Inmaculada Sánchez Ruiz de Valdivia
(Directora)

María del Mar Méndez Serrano
Abigail Quesada Páez
(Coordinadoras)





Esta publicación es parte del Proyecto I+D+i «PID2023-151441OB-I00», financiado por MICIU/AEI/10.13039/501100011033 y por FEDER, UE

PRY015/23 (CSN-2023 Ciber-Clear)

CSN Consejo de Seguridad Nuclear

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:** 2026

**Depósito Legal:** M-14969-2026
**ISBN versión impresa:** 978-84-1085-901-2
**ISBN versión electrónica:** 978-84-1085-902-9

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

# *Índice general*

*Página*

*Página*



PARTE I

## DAÑOS POR PRODUCTOS INTELIGENTES DEFECTUOSOS A PERSONAS VULNERABLES: PREVENCIÓN DE RIESGOS, CARGA DE LA PRUEBA, ASEGURAMIENTO Y REPARABILIDAD

CAPÍTULO I

### DEFECTOS DE SEGURIDAD «UNIVERSAL» EN LA DIRECTIVA POR PRODUCTOS DEFECTUOSOS: PROTECCIÓN FRENTE A LA HIPERVULNERABILIDAD COGNITIVA EN ENTORNOS DIGITALES DE NIÑAS, NIÑOS, ADOLESCENTES, PERSONAS MAYORES Y PERSONAS CON DISCAPACIDAD

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*



PARTE II

## DAÑOS POR PRODUCTOS INTELIGENTES DEFECTUOSOS A NIÑAS, NIÑOS Y ADOLESCENTES (PERSONAS MENORES)

CAPÍTULO XI

### DEL OSITO DE PELUCHE AL *SMART TOY*: PROTECCIÓN DEL MENOR Y SEGURIDAD DEL JUGUETE

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*



PARTE IV

**COMUNICACIONES**

CAPÍTULO XXIV

**VULNERABILIDAD DE LAS PERSONAS MAYORES Y PRODUCTOS INTELIGENTES DEFECTUOSOS EN EL CUIDADO DE LA SALUD: RESPUESTAS REGULATORIAS**

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Página*

*Capítulo I*

# Defectos de seguridad «universal» en la Directiva por productos defectuosos: protección frente a la hipervulnerabilidad cognitiva en entornos digitales de niñas, niños, adolescentes, personas mayores y personas con discapacidad[1]

INMACULADA SÁNCHEZ RUIZ DE VALDIVIA
*Catedrática de Derecho Civil*
*UGR*

«El eslabón más débil en la cadena
de seguridad siempre es la persona».
*Bruce Schneier*[2]

SUMARIO: I. SEGURIDAD «UNIVERSAL» ONLINE: LA ADICIÓN TECNOLÓGICA Y LA HIPERVULNERABILIDAD COGNITIVA EN ENTORNOS DIGITALES, A DEBATE. *1. Tecnología en expansión y en tensión: vulnerabilidad tecnológica e hipervulnerabilidad cognitiva. 2. Seguridad «universal»: mi propuesta doctrinal: Por una seguridad online para todas las*

1. Este trabajo es parte del Proyecto de I+D+I financiado por el MICIN: «Robótica, Inteligencia Artificial y Mayores: oportunidades y desafíos» (PID2023-1514410B-100).

2. Bruce Schneier es uno de los expertos en seguridad informática más influyentes del mundo, conocido por su trabajo en criptografía, análisis de vulnerabilidades y divulgación sobre riesgos tecnológicos. Es criptógrafo y tecnólogo en seguridad de reconocimiento internacional. Nació el 15 de enero de 1963 en Nueva York. Es profesor en la Harvard Kennedy School y afiliado al Berkman Klein Center. Fue conocido como *«gurú de la seguridad»* por *The Economist*.

*personas. También para las más vulnerables.* II. LA SEGURIDAD DEL PRODUCTO: UNA HERRAMIENTA PARA FRENAR EL RIESGO DE DEPENDENCIA EMOCIONAL Y MITIGAR LA HIPERVULNERABILIDAD COGNITIVA DE LAS PERSONAS VULNERABLES. *1. El legislador europeo se ocupa y preocupa por una IA «confiable». 2. De la era analógica (Directiva por productos defectuosos 85/374/CEE) a la era digital (Directiva 2024/2853). El derecho de daños y la seguridad. 3. ¿Qué tienen que ver los defectos de seguridad con la dependencia tecnológica? La vulnerabilidad actúa como freno «natural» a una dependencia tecnológica excesiva y a ciegas. 4. La irrupción de productos dotados de sistemas de IA tensiona el derecho de consumo y el derecho de daños.* III. CONDENADAS META Y YOUTUBE POR CREAR DISEÑOS ADICTIVOS EN SUS PLATAFORMAS: EMPRESAS TECNOLÓGICAS DECLARADAS RESPONSABLES DE DAÑAR LA SALUD MENTAL DE SUS USUARIAS/OS MÁS VULNERABLES (HIPERVULNERABLES DIRÍA YO). *1. Planteamiento. 2. El uso compulsivo de redes sociales, a diferencia del uso compulsivo de videojuegos on-line, aún no ha sido calificado como enfermedad por la OMS. La indemnización de los daños causados a la salud mental.* 2.1. Planteamiento. 2.2. La Directiva por productos defectuosos indica que son resarcibles (únicamente) los daños a la salud psicológica reconocidos médicamente. 2.3. Dañar la salud mental en el entorno digital es un defecto de seguridad del producto, cada día más. 2.4. Defectos de seguridad y sentencias condenatorias de Meta (propietaria de Facebook, Instagram y WhatsApp) y YouTube por crear diseños adictivos en sus plataformas que dañan la salud mental de sus usuarias/os. 2.4.1. La desprotección de menores y la sobreexposición sexual en redes sociales. Primera sentencia/Caso de Nuevo México que condena a Meta (375 millones de dólares). 2.4.2. La adición tecnológica a redes sociales de una niña californiana. Segunda Sentencia/caso de los Ángeles: condenas Meta y YouTube por crear adicción a redes sociales. IV. DEFECTOS DE SEGURIDAD DE LOS PRODUCTOS Y PERSONAS VULNERABLES EN LA DIRECTIVA POR PRODUCTOS DEFECTUOSOS: POR UNA «SEGURIDAD UNIVERSAL». *1. La seguridad «universal» como un principio jurídico implícito en la Directiva (UE) 2024/2583. 2. La convergencia entre «la seguridad universal» y la «responsabilidad civil» por productos defectuosos. 3. ¿Qué se entiende por producto defectuoso?* 3.1. Introducción. 3.2. El acierto de ampliar la definición de producto permite incluir a los productos en la era digital. 3.3. Tipos de defectos que reconoce la Directiva. *4. Seguridad exigible y Seguridad esperable: una distinción que constituye una pieza esencial en el engranaje de activación el régimen de responsabilidad por productos defectuosos.* 4.1. Introducción. 4.2. El caso *Boston Scientific* (C-503/13 y C-504/13): la vulnerabilidad como parámetro de seguridad que «refuerza el estándar de seguridad». 4.3. ¿Qué entiende el TJUE del caso *Boston Scientific* (C-503/13 y C-504/13) por

## I. SEGURIDAD «UNIVERSAL» ONLINE: LA ADICIÓN TECNOLÓGICA Y LA HIPERVULNERABILIDAD COGNITIVA EN ENTORNOS DIGITALES, A DEBATE

### 1. TECNOLOGÍA EN EXPANSIÓN Y EN TENSIÓN: VULNERABILIDAD TECNOLÓGICA E HIPERVULNERABILIDAD COGNITIVA

La expansión de productos inteligentes en hogares, guarderías, centros educativos, residencias, geriátricos, hospitales y hogares es una realidad innegable. Juguetes inteligentes (smart toys)[3], móviles y plataformas de redes sociales (Facebook, Instagram, Wasaph, Titok, Youtube), asistentes digitales como chatbos, robots quirúrgicos (Da vinchi), robots conversaciones, vehículos autónomos, implantes tecnológicos en el cuerpo o en el cerebro, órganos artificiales inteligentes, cámaras y sensores inteligentes, weareables, asistentes de voz, dispositivos médicos conectados, y, un largo etc.; han transformado, profundamente, nuestra vida cotidiana y el día a día de las personas ofreciendo comodidad, conectividad, accesibilidad, inmediatividad y nuevas formas de interacción social. También es una realidad que, la seguridad y salud, (también) la seguridad de los derechos fundamentales de nuestros seres más queridos e indefensos (como la de nuestras nietas y nietos (aunque, aún yo no la/os tengo), nuestras hijas e hijos (niñas, niños y adolescentes)[4], nuestras madres y padres y, las personas con algún tipo de discapacidad —física, auditiva, visual o intelectual— está en juego.

La tecnología se ha vuelto tan central en la vida cotidiana que no es algo exclusivo de niñas, niños o adolescentes. También de ella, dependen cada día más, aunque de manera distinta, las personas mayores y, las personas con algún tipo de discapacidad, física o intelectual. La razón, resulta evidente: la tecnología facilita la vida, personaliza la salud, previene y detecta caídas, enfermedades (como el Alzheimer), previene, también, el posible deterioro cognitivo. Además, aporta una sensación de conexión con la familia que se vuelve muy valiosa e imprescindible a una determinada edad porque evita su propia soledad (no deseada); convirtiéndose en una herramienta en el apoyo, cuidado y atención de las limitaciones y enfermedades propias de la edad y, en su caso, de la falta

3. El informe *Smart AI Toys Market Research Report-Forecast to 203*5, advierte que el mercado global de juguetes inteligentes con IA alcanzó un valor aproximado de 7,69 mil millones de dólares en 2024, estimándose que podría llegar a 25 mil millones de dólares en 2035, lo que supone una tasa de crecimiento anual compuesta del 11,3 %. Sobre el particular, puede consultarse la siguiente URL: https://www.grandviewresearch.com/industry-analysis/smart-toys-market-report (fecha de consulta: 01 febrero 2026).
4. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025, dir.). *Era digital y personas mayores, con discapacidad y menores: vulnerabilidades y oportunidades*, ed., Aranzadi LA LEY, Madrid, 2025. (ISBN versión impresa: 978-84-1085-004-0/ ISBN versión digital: 978-84-1085-005-7).

de capacidad[5]. Pero la dependencia a productos o plataformas dotadas de IA no tiene que ser, necesariamente nociva siempre que sea equilibrada. Las bondades que ofrece la tecnología cada día son mayores: mitiga la soledad (no deseada) de personas mayores y con discapacidad, detecta y previene enfermedades (infecciones de orina, depresiones, Alzheimer), caídas, evita el aislamiento social, facilita la movilidad de personas con discapacidad. Pero, también es cierto que existe, en la actualidad, lo que podríamos denominar hipervulnerabilidad cognitiva de niñas, niños, adolescentes, personas mayores, personas con discapacidad y personas con bajo o escaso nivel de alfabetización digital frente a productos inteligentes.

La hipervulnerabilidad cognitiva, no es una característica inherente a la persona, sino el resultado de un entorno digital que, al no ser universalmente accesible, sitúa a ciertos colectivos en una clara posición de clara desventaja. De hecho, recientemente, los defectos de seguridad —entendidos como diseños adictivos, falta de protección infantil y ausencia de advertencias— han sido considerados causas directas del daño de dependencia emocional sufrido por menores. Por esta razón, Meta y YouTube han sido condenadas: no por el contenido que otros publican, sino por cómo diseñaron y construyeron sus plataformas. Hasta ahora existen 2 sentencias condenatorias, la primera en México y la segunda en California pero es más que probable que haya muchas más. Tratándose de colectivos especialmente vulnerables, la cuestión no es sólo determinar quién responde cuando la tecnología se insegura. Esto, es, cuando la tecnología falla sino determinar la razón por la que se produce dicho fallo de seguridad-que puede ser, o bien de fabricación, diseño, actualización o faltas de advertencias del riesgos o falta de información—; así como, también, aclarar y tomar postura acerca de cuál es «el estándar de información exigible» y «el estándar de seguridad exigible y esperable» tomando en consideración que la capacidad de determinados colectivos es más limitada a la hora de entender, comprender, evitar y anticipar el riesgo para evitar el daño a su seguridad y salud teniendo en cuenta la sobreexposición que las tecnologías emergentes causa en sus derechos más fundamentales (como, la discriminación, la explotación de vulnerabilidades debidas a la edad, discapacidad[6], o una situación social o económica de exclusión, o los daños que puedan sufrir a veces (incluso) de carácter personal). ciertos gru-

5. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). *Inteligencia Artificial, Robótica Asistencia y Tecnologías inclusivas en la atención y Cuidado de las Personas Mayores, con o sin discapacidad: gerontotecnología, biotecnología, neuro tecnología, ratificación y longevidad*, ed., Aranzadi LA LEY, Madrid, 2025. ISBN versión impresa: 978-84-1085-477-2/ISBN versión digital: 978-84-1085-478-9.

6. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025), «Personas con Alzheimer: oportunidades que ofrece la inteligencia artificial y la robótica asistencia en la era digital», en Era Digital y Personas Mayores, Con discapacidad y Menores (dir. SÁNCHEZ RUIZ DE VADIVIA), ed. Aranzadi LA LEY, Madrid, 2025, pp. 67-118. (ISBN versión impresa: 978-84-1085-004-0/ ISBN versión digital: 978-84-1085-005-7).

pos de personas consumidoras y usuarias presentan mayor riesgo de desarrollar dependencia tecnológica a los productos dotados de IA porque estos productos inteligentes están «diseñados para que favorezcan» conductas adictivas; similares a otras adicciones comportamentales como las que crean los videojuegos, o el tabaquismo; ofreciendo notificaciones constantes, recompensas inmediatas y facilitando y personalizando la atención de quienes más queremos. Según los expertos, entre los síntomas que experimentan quienes están expuestos a dicha dependencia tecnológica, cabría resaltar los siguientes: ansiedad, irritación, insomnio, dificultad para concentrarse, aumento de síntomas de depresión y un largo etc. Las consecuencias, también, son inevitables: aislamiento social, alteraciones del sueño y sustitución de actividades saludables por el uso del móvil, del chatbots o de los productos inteligentes a los que estén, usualmente «enganchados». La actitud preventiva para evitar la dependencia tecnológica resulta esencial: enseñarles a usar la tecnología de forma crítica y equilibrada, formarles e informarles así como educarles sobre los riesgos y hábitos saludables, ponerles límites estableciendo horarios sin pantallas y, espacios libres de dispositivos con acceso a internet así como, también, ofrecerles un adecuado acompañamiento digital o una intervención psicológica cuando se detecte algún tipo de *adición tecnológica* resulta esencial.

## 2. SEGURIDAD «UNIVERSAL»: MI PROPUESTA DOCTRINAL: POR UNA SEGURIDAD ONLINE PARA TODAS LAS PERSONAS. TAMBIÉN PARA LAS MÁS VULNERABLES

El acierto de que el régimen de responsabilidad por productos defectuosos contenido en la nueva Directiva de 2024/2583 haya evolucionado desde un modelo centrado en la «persona *consumidora media, razonable y perspicaz*» hacia un modelo dirigido a proteger a «todas las personas» (incluyendo, a niñas, niños y adolescentes, mayores y personas con discapacidad o bajo nivel formativo en lo digital, en «todas las fases del ciclo de la vida del producto»; es indudable. Este enfoque, más humano y protector supone poner en el centro de la tecnología a «la persona» para que la tecnología sea «confiable» a niñas, niños, adolescentes, personas mayores, personas con discapacidad o con bajo nivel de alfabetización digital. El objetivo final es lograr que los productos, entornos y servicios dotados de IA sean más «seguros» y eviten «riesgos de seguridad y salud» y «riesgos para los derechos fundamentales» que tome en consideración su especial hipervulnerabilidad. Tratándose de colectivos especialmente vulnerables, la cuestión no es sólo determinar quién responde cuando la tecnología falla o determinar la razón por la que se produce dicho fallo —que puede ser, o bien de fabricación, diseño, actualización o faltas de advertencias del riesgos o falta de información—; sino la de aclarar y tomar postura acerca de cuál es «el estándar de información exigible» y «el estándar de seguridad exigible y esperable» tomando en consideración que la capacidad de determinados colectivos es más limitada a

la hora de entender, comprender, evitar y anticipar el riesgo para evitar el daño a su seguridad y salud teniendo en cuenta la sobreexposición que las tecnologías emergentes causa en sus derechos más fundamentales (como, la discriminación, la explotación de vulnerabilidades debidas a la edad, discapacidad[7], o una situación social o económica de exclusión, daños a los datos personales

La «seguridad» no puede depender del «usuario medio», porque los productos inteligentes interactúan con perfiles muy diversos, y un fallo puede causar daños más o menos graves, en atención a la mayor o menor vulnerabilidad de quienes son las personas que los utilizan. En materia de accesibilidad, felizmente el legislador de la proyectada reforma de la Ley de Dependencia y Discapacidad lo ha tenido muy claro. No ha dudado en incorporar el término «universal» a la accesibilidad de los entornos, productos y servicios digitales a fin de evitar la discriminación y la discapacidad digital a la que están condenadas las personas dependientes y con discapacidad[8]. Además, la «seguridad» no solo es una herramienta para *evitar el daño*. Puede servir, también como herramienta capaz de prevenir la *«discriminación» y capaz de lograr la «accesibilidad» e «inclusión» asegurando que los productos, servicios y entornos digitales sean más accesibles.* Puede llegar a ser un instrumento, incluso, que ayude a *prevenir los sesgos algorítmicos discriminatorios*, así como los r*iesgos no sólo físicos o funcionales sino, también, los emocionales, cognitivos y socia*les. En mi opinión, la «falta de seguridad» de estos productos inteligentes no es debida (y es imputable) al producto, en sí mismo considerado. Porque no son las máquinas, o los robots, o los juegues inteligentes, o los chatbots los que fallan. Lo que falle en muchas ocasiones, es el «diseño» (en muchas ocasiones, adictivo), «la información», la «falta de formación», la «falta de accesibilidad del producto» o la «falta de advertencias de los riesgos» o «el uso excesivo de los mismos»; lo que provoca que los productos inteligentes produzcan daños a los colectivos vulnerables. Seamos conscientes, por tanto, de que lo que resulta evitable, evaluable y panificable es «gestionar» el riesgo. Solo así, será posible «prevenirlo». Y el riesgo de estos productos inteligentes es que en numerosas ocasiones son utilizados por colectivos especialmente vulnerables.

---

7. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025), «Personas con Alzheimer…», *cit.,* 67 y ss., y, SANCHEZ RUIZ DE VALDIVIA, I. (2025). «Inteligencia Artificial y Personas con discapacidad: algunos retos y logros pendientes», en Retos pendientes de la discapacidad (A. Castro Girona Martínez y F. Cabello de Alba Jurado (Coordinadores), Ed., Fundación Notariado y Fundación Aequitas, pp. 286-30.
8. Es consciente de que, de no haberlo así, el efecto inmediato hubiera supuesto un trato discriminatorio y su consiguiente «discapacidad digital» —un término relacional con la falta de adaptación de los entornos, servicios y productos digitales—. Idea sobre la que he reflexionado, en profundidad en mi anterior trabajo, SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). La (des) protección de las Personas Mayores: personas consumidoras vulnerables (también) en lo digital, Aranzadi LA LEY, Madrid. (ISBN versión impresa: 978-84-1085-473-4/ISBN versión digital: 978-84-1085-474-5).

El concepto de seguridad «universal», que propongo, realmente no es un concepto jurídico positivizado en nuestro derecho español. Es una propuesta doctrinal que sugiero que sea tenida en cuenta a la hora de trasponer a nuestro ordenamiento español la Directiva). El objetivo que persigo resulta evidente: que los productos inteligentes (IoT, IA, *software* integrado) sean diseñados, fabricados y actualizados por fabricantes y productores para que sean seguros para *todas* las personas, incluidas las más vulnerables (insisto: las niñas, niños o adolescentes, las personas menores, mayores, tengan o no discapacidad personas con nivel bajo de alfabetización digital). En mi opinión, la Directiva (UE) 2024/2583 ofrece herramientas suficientes como para que el legislador, en la trasposición de la Directiva positivice a nuestro ordenamiento jurídico, añada el término «seguridad universal». La Directiva «moderniza» el régimen de responsabilidad por daños por productos defectuosos preexistente tratando de dar respuesta al desafío que comportan los productos, en general, y en particular los dotados de IA. Bajo esta concepción la responsabilidad por productos defectuosos pasaría a concebirse como un mecanismo de garantía y seguridad para proteger a las personas vulnerables frente a los riesgos de los productos inteligentes. Un *mecanismo capaz de garantizar*, que los *fabricantes, productores y diseñadores de productos dotados de inteligencia artificial están llamados a garantizar un nivel mínimo de seguridad (re)diseñando sus productos para evitar que sean adictivos*; lo que significa que *la responsabilidad civil funciona como presión jurídica* para que ese nivel o estándar de seguridad (más elevado) se cumpla y el sistema proteja a todas «todas» las personas consumidoras y usuarias.

## II. LA SEGURIDAD DEL PRODUCTO: UNA HERRAMIENTA PARA FRENAR EL RIESGO DE DEPENDENCIA EMOCIONAL Y MITIGAR LA HIPERVULNERABILIDAD COGNITIVA DE LAS PERSONAS VULNERABLES

### 1. EL LEGISLADOR EUROPEO SE OCUPA Y PREOCUPA POR UNA IA «CONFIABLE»

El legislador europeo es consciente, desde hace años ya, que es preciso proteger a las personas consumidoras vulnerables y a los fabricantes de productos inteligentes apostando por «una IA confiable». Para lograrlo, ha trazado un doble senda dirigida a prevenir y, en su caso, reparar los posibles daños que los riesgos de seguridad y salud y los riesgos para los derechos fundamentales ocasionen: (i) por un lado, *y con carácter preventivo* (*ex antes*) ha fijado estándares de seguridad para todos los productos puestos en el mercado y, de forma más específica, para los que incorporan sistemas de IA (imponiendo obligaciones de seguridad e información dirigidas al público, en general, contenidas en el Reglamento de Seguridad del Producto de 2023 —Reglamento (UE) 2023/2859 (DO L de 5.7.2024)— y, prohibiendo e imponiendo obligaciones para productos

especialmente arriesgados, en el Reglamento de Inteligencia Artificial de 2024. Por otro lado, y en segundo lugar (ii) y *con carácter resarcitorio (ex post)*, ha modernizado la responsabilidad objetiva por productos defectuosos, incorporando de manera expresa el *software*, los sistemas IA y el entorno digital. De los daños a los derechos fundamentales que puedan ocasionar los productos inteligentes se ha ocupado otras normativas más sectoriales como Reglamento de protección de datos[9], las Directivas antidiscriminatorias por razón de raza[10] o sexo[11], entre otras).

El nuevo régimen de responsabilidad por productos defectuosos contenido en la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, que debe ser traspuesto, a nuestro ordenamiento jurídico español, a más tardar, antes del 9 de diciembre de 2026 (conforme a los dispuesto en su art. 22) trata de adaptar la regulación existente a la economía circular imperante en la era digital[12] y a los productos que incorporan sistemas de Inteligencia Artificial derogando, sustituyendo y modernizando la regulación actualmente contenida en la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985 (transpuesta, a nuestro ordenamiento español, a través de la Ley 22/1994, de 6 de julio, de responsabilidad civil por los daños causados por productos defectuosos y, compilada en los arts. 128 a 149 del Real Decreto Legislativo 1/2007, de Defensa General de Consumidores y Usuarios). El limitado ámbito legal de aplicación de los daños indemnizables con arreglo a la Directiva 2024/2853 invita a una modernización del concepto de «seguridad». Un proceso, el de diseñar y fabricar productos, servicios y entornos más seguros, que depende de muchos factores: fundamentalmente, de la educación digital, de la formación, del diseño, del error humano, y de la falta o no de accesibilidad por parte de quienes los usan. También, de los hábitos (las horas que las personas usuarias le dediquen al uso

9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos (DOUE L 119/1, 4.5.2016).
10. Por ejemplo, la Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico (DOCE L 180/22, 19.7.2000, que prohíbe la discriminación racial en el empleo, la educación, la seguridad social, la salud y el acceso a bienes y servicios, incluida vivienda.
11. Directiva (UE) 2023/970 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023 por la que se refuerza la aplicación del principio de igualdad de retribución entre hombres y mujeres por un mismo trabajo o un trabajo de igual valor a través de medidas de transparencia retributiva y de mecanismos para su cumplimiento (DOUE L 132/21, 17.5.2023).
12. MARTÍN CASALS, M. (2024). «Líneas generales de la Nueva Directiva europea de responsabilidad por los daños causados por productos defectuosos». *Revista Actualidad Jurídica*, n.º 50, pp.37-40.

de la tecnología), de las advertencias, de las actualizaciones y especialmente, de la información facilitada a las personas usuarias. Especialmente, a las más vulnerables.

En mi opinión, el «deber de información» debe elevarse a estándares razonables teniendo en consideración las necesidades de colectivos hipervulnerables, cognitivamente hablando. Solo así, es posible «reequilibrar» la asimetría informativa que existe entre las partes contractuales con el objetivo de prevenir (evitar) efectos dañinos para que estos sistemas inteligentes no fallen. De hecho, en materia de ciberseguridad, ha quedado demostrado que los fallos más críticos no suelen originarse en debilidades criptográficas o en deficiencias de hardware, sino por la inadecuada interacción humana con los sistemas en IA. La falta accesibilidad, la existencia de patrones oscuros o de diseños altamente adictivos es lo que los sobreexpone. De hecho, es una realidad, que los ciberdelincuentes priorizan la explotación de debilidades/fragilidades humanas (como la edad o la discapacidad), para realizar manipulación psicológica: patrones oscuros, o sobrecarga informativa debida, también, a la falta de destrezas digitales, actúan como «catalizadores de vulnerabilidades» dirigidos a poner en entredicho los desafíos éticos y legales de estos productos inteligentes. Y es que, por «daños de seguridad» debemos entender las consecuencias negativas que afectan no sólo a la *integridad física y funcional de las personas usuarias de estos productos, servicios y entornos digitales sino, también, los daños a la integridad emocional (psicológica), social y digital* (riesgos a los que las personas especialmente vulnerables están sobreexpuestos a riesgos de seguridad y riesgos contra los derechos fundamentales). Y es que, resulta, en mi opinión, fundamental *prevenir este tipo de daños* y, en su caso *repararlos* a fin de lograr *entornos, servicios y productos digitales e inteligentes más seguros y menos discriminatorios para quienes por razón de la edad o debido a su falta de capacidad en lo digital están más sobreexpuestos*.

## 2. DE LA ERA ANALÓGICA (DIRECTIVA POR PRODUCTOS DEFECTUOSOS 85/374/CEE) A LA ERA DIGITAL (DIRECTIVA 2024/2853). EL DERECHO DE DAÑOS Y LA SEGURIDAD

Producido un fallo de seguridad o un daño a la seguridad, salud o a los derechos fundamentales de los colectivos más vulnerables, como son las niñas, niños, adolescentes, personas mayores y personas con discapacidad; la cuestión no es solo determinar quién responde cuando la tecnología falla, sino si cual es el estándar de seguridad exigible y esperable y si dicho estándar debe adaptarse a las necesidades específicas de estos usuarios, reforzando su protección frente a productos inteligentes defectuosos.

La nueva Directiva europea constituye una de las reformas más profundas del régimen europeo de responsabilidad por productos defectuosos desde hace varias décadas. No sólo deroga la anterior (la Directiva 85/374/CEE), sino que

establece un marco jurídico adaptado a los desafíos tecnológicos contemporáneos, especialmente los derivados de: (i) productos digitales (ii) *software* y actualizaciones (iii) inteligencia artificial (iv) economía circular y (v) cadenas de suministro globales[13] Su objetivo central es «garantizar un nivel elevado de protección de "todas" las personas consumidoras en un mercado digital donde los riesgos ya no provienen solo de defectos materiales, sino también de fallos digitales, de ciberseguridad o decisiones automatizadas que sesgan y discriminan a colectivos vulnerables». Realmente el marco normativo vigente hasta ahora no estaba preparado para responder al reto que comporta incorporar entornos, servicios y productos inteligentes en nuestro día a día. La Directiva 85/374/CEE se creó en un contexto analógico, en el que el producto era un bien físico y el fabricante tenía un control delimitado sobre el objeto que ponía en circulación. La propia Comisión Europea reconoció en su Informe de 2018 de evaluación de la Directiva 85/374/CEE[14], «los problemas a los que nos enfrentamos en la actualidad difieren en cierta medida de los que existían en el mundo predominantemente analógico de 1985. Nos encontramos inmersos en otra revolución tecnológica. La economía y los propios productos están aumentando gradualmente su interconexión, su digitalización, su autonomía y su inteligencia. Necesitamos una respuesta coherente y global ante estos retos, tal como se describe en la iniciativa sobre inteligencia artificial[15]». Pero, también es cierto, tal ay como se ha advertido ya que la defectuosa calidad técnica del texto se advierte ante el hecho de que la Directiva no cita de manera expresa el concepto inteligencia artificial —término que sí se menciona extensamente en el preámbulo sin aparecer en el articulado, probablemente por su regulación separada en el Reglamento de Inteligencia Artificial[16]—.

13. MARTÍN CASALS, M. (2024). «Líneas generales de la Nueva Directiva europea de responsabilidad por los daños causados por productos defectuosos». *Revista Actualidad Jurídica*, n.º 50, pp.37-40.
14. COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre la aplicación de la Directiva del Consejo relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos (85/374/CEE), 7 mayo 2018, disponible eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0246&from=FR. (fecha de consulta: 9 de diciembre de 2025).
15. En este tema se debe tomar en consideración: Unión Europea. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, 12 de julio de 2024, núm. 2024/1689, pp. 1-144. Disponible en la siguiente URL: https://www.boe.es/doue/2024/1689/L00001-00144.pdf1 (fecha de consulta: 12.05. 2024).
16. En este sentido, con acierto CARRASCO PERERA, A.F. (2024). «Análisis de la nueva Directiva de responsabilidad por daños causados por productos defectuosos. Síntesis y crítica de la regulación más contenida en la Directiva 2024/2853». Disponible en https://

La complejidad técnica inherente a los productos inteligentes dificulta que las víctimas puedan probar el defecto o el nexo causal y los mecanismos probatorios previstos pueden resultar insuficientes para quienes parten de una situación de mayor desventaja. Reconociendo, por tanto, las bondades como los desafíos que ofrecen las disciplinas tecnológicas emergentes; la humanidad estamos llamada a dar respuestas, lo más humanas posibles, a los desafíos que comporta dar respuesta a la posible dependencia tecnológica y los daños que puedan ocasionar el uso de plataformas, servicios y entornos digitales a niñas, niños, adolescentes, personas mayores y personas con discapacidad porque está en juego su privacidad, intimidad y la propia seguridad de sus datos. Desde esta perspectiva, la regulación de la responsabilidad por productos defectuosos no es solo un debate técnico-jurídico, sino una cuestión que incide directamente en la dignidad, la seguridad, la discriminación y la autonomía de los colectivos más vulnerables por ser los que mayor dependencia tecnológica tienen.

## 3. ¿QUÉ TIENEN QUE VER LOS DEFECTOS DE SEGURIDAD CON LA DEPENDENCIA TECNOLÓGICA? LA VULNERABILIDAD ACTÚA COMO FRENO «NATURAL» A UNA DEPENDENCIA TECNOLÓGICA EXCESIVA Y A CIEGAS

Cuando un sistema inteligente (producto, servicio o entorno) falla —sea lo que sea lo que falle: un algoritmo, el software, la red, el sistema IA o el dispositivo— nos recuerda algo esencial: «que no podemos depender al 100% de algo que puede fallar, sesgar o discriminar a un determinado colectivo en cualquier momento». Sin fallos, la tecnología parecería perfecta; y ahí sí que nos volveríamos absolutamente dependientes de ella. El hecho de que seamos conscientes de que el sistema dotado de IA pueda fallar, es lo que nos obliga (y está bien que así suceda) a que «supervisemos», «verifiquemos» sus decisiones autónomamente adoptadas. Nos obliga a que «no deleguemos decisiones críticas (esenciales) sin pensar ni revisarlas antes». Lo que significa que, los *defectos actúan como un recordatorio permanente* de que el *juico humano sigue siendo necesario*.

Los posibles defectos o fallos de un sistema IA nos recuerdan que ningún sistema inteligente (producto, servicio o entorno), por muy inteligente que sea, puede reemplazar el juicio humano. Porque toda tecnología tiene fallos: «fallos» que llamaremos, «de seguridad». Cada vulnerabilidad descubierta (por razón de la edad —en niñas, niños, adolescentes o mayores— o por razón de la falta de capacidad —la que discrimina a las personas con discapacidad—) «nos obliga» (o, en mi opinión, debería de «obligar») a: *mejorar los protocolos de seguridad*, a a*ctualizar los sistemas para que se adapten y sean más accesibles a quienes los*

centrodeestudiosdeconsumo.com/images/Analisis_de_la_nueva_Directiva_de_responsabilidad_por_danos.pdf, pp.1 (fecha de consulta: 12.05. 2024).

*utilizan*, o *diseñar defensas más robustas, especialmente para las personas usuarias más vulnerables.* Sin «fallos» de seguridad, el sistema inteligente se estancaría porque el ser humano confiaría «a ciegas» en la t*ecnología* o en el *producto inteligente*. Sin embargo, precisamente son los «fallos de seguridad» lo que hace el que ser humano no se fie a «ciegas» de la tecnología y que sea consciente de que sí o sí tendrá que «supervisarla». En definitiva, la vulnerabilidad actúa como un freno «natural» a la «dependencia tecnológica excesiva».

## 4. LA IRRUPCIÓN DE PRODUCTOS DOTADOS DE SISTEMAS DE IA TENSIONA EL DERECHO DE CONSUMO Y EL DERECHO DE DAÑOS

El concepto de daños causados por productos, servicios y entornos digitales defectuosos, dotados de sistemas de Inteligencia Artificial (IA) abarca numerosos prismas[17]: desde los (i) *riesgos de exposición o dependencia tecnológica (daños emocionales, daños morales puros o daños psicológicos, declarados o no enfermedades) (ii) daños* ocasionados *por* un *uso malicioso del tratamiento de datos* (ciberataques, contenidos falsos) (iii) *fallos del sistema inteligente* (sesgos algorítmicos discriminatorios en contra de la edad o de la falta de capacidad, la pérdida de control o de datos) (iv) *riesgos sistémicos* (desempleo, privacidad, falta de accesibilidad); (v) *brechas en dispositivos inteligentes* (cámaras, smart TVs, relojes o electrodomésticos que pueden ser vulnerables a ataques si no están bien configurados); (vi) contraseñas débiles o por defecto (uno de los errores humanos más frecuentes y peligrosos); (vii) *Software sin actualizar* (no instalar parches abre la puerta a ataques de día cero); v*ulnerabilidades de software y, dependencia de servicios centralizados* (como, por ejemplo, caídas de proveedores como Google), y un largo etc. La dificultad de atribuir responsabilidad, en estos, casos en los que la complejidad y autonomía de la IA se une al «efecto de caja negra» y a un diseño adictivo que provoca cierta dependencia en sus usuarios resulta evidente. El hecho de que los sistemas basados en IA puedan operar de forma autónoma y adoptar decisiones independientes viene a dificultar la depuración de las responsabilidades en el ámbito de las reclamaciones por responsabilidad civil por productos defectuosos, como he advertido en otro lugar[18]. Y es que, un «fallo de seguridad» puede afectar a millones de usuarias/os siendo presa más fácil de engaños y estafas especialmente las niñas, niños, adolescentes (menores, en definitiva), las personas mayores y las persona scon discapacidad porque son personas hipervulnerables[19] cognitivamente hablando, por razón

17. SÁNCHEZ RUIZ DE VALDIVIA, I. (2013). *Cuestiones Actuales sobre responsabilidad civil,* ed., Thomson Reuters Aranzadi. ISBN 978-84-90059-075-1.
18. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). La (des) protección de las Personas Mayores: personas consumidoras vulnerables (también) en lo digital, Aranzadi LA LEY, Madrid. (ISBN versión impresa: 978-84-1085-473-4/ISBN versión digital: 978-84-1085-474-5).
19. SANCHEZ RUIZ DE VALDIVIA, I. (2025). «Hipervulnerabilidad de las personas mayores tras la transformación digital (también) del sector bancario: automatización (crédito

de la edad o de la capacidad. Consciente de ello, me propongo demostrar cómo las empres tecnológicas son responsables de diseñar productos, servicios y entornos digitales adictivos que dañan la salud mental con el objetivo de lograr mayores beneficios económicos aprovechándose de su especial vulnerabilidad. Estos «fallos de seguridad» debidos, a veces, al diseño adictivo o a la falta de información real al usuario final. Su edad, unida a su falta de capacidad, o su falta de alfabetización digital; su dependencia funcional, sus limitaciones cognitivas y, probablemente, la falta de alfabetización, apoyo y/o acompañamiento digital; los convierte en flanco fácil de amenazas digitales, patrones oscuros, estafas digitales y compras y captación de uso adictivo y compulsivo en redes sociales y en comercio on-line.

La irrupción de productos dotados de sistemas de inteligencia artificial está tensionando las categorías clásicas del Derecho de consumo y del Derecho de daños. La noción tradicional de consumidor vulnerable se queda corta frente a los nuevos riesgos, defectos de seguridad y daños lo que exige (re)pensar las categorías tradicionales de «consumidor vulnerable», «defectos de seguridad», «defecto de información» y el propio «concepto de daño, de defecto». Y es que, cuando un sistema basado en inteligencia artificial integrado en un juguete, un robot conversacional, un dispositivo médico, una plataforma como YouTube, o un vehículo autónomo falla, las consecuencias no son iguales para toda/os la/os usuarias/os. Son los colectivos más vulnerables los que se encuentran en una posición de especial inferioridad. Su capacidad para comprender, anticipar o evitar los riesgos derivados de estos productos es diversa. En muchas ocasiones, más limitada.

## III. CONDENADAS META Y YOUTUBE POR CREAR DISEÑOS ADICTIVOS EN SUS PLATAFORMAS: EMPRESAS TECNOLÓGICAS DECLARADAS RESPONSABLES DE DAÑAR LA SALUD MENTAL DE SUS USUARIAS/OS MÁS VULNERABLES (HIPERVULNERABLES DIRÍA YO)

### 1. PLANTEAMIENTO

La dependencia tecnológica que causan algunos productos inteligentes, como videojuegos, móviles, robots, Chatbots, y el uso de algunas plataformas de redes sociales, como Instagram, Facebook o YouTube es real. Se ha constatado ya, el daño a la «salud mental» que el uso de estos productos y servicios inteligentes produce ante colectivos tan vulnerables como nuestras nietas y nietos (aunque, aún yo no la/os tengo), nuestras hijas e hijos (niñas, niños y adolescentes), nuestras madres y padres o las personas con discapacidad física, auditiva, visual o intelectual; está en juego.

---

scoring), datificación y daños por productos inteligentes defectuosos a personas vulnerables», ISSN 0210-0444, ISSN-e 2695-6314, Año n.º 100, N.º 812, 2025 (Ejemplar dedicado a: Centenario), pp. 3999-4048.

## 2. EL USO COMPULSIVO DE REDES SOCIALES, A DIFERENCIA DEL USO COMPULSIVO DE VIDEOJUEGOS ON-LINE, AÚN NO HA SIDO CALIFICADO COMO ENFERMEDAD POR LA OMS. LA INDEMNIZACIÓN DE LOS DAÑOS CAUSADOS A LA SALUD MENTAL

### 2.1. Planteamiento

A diferencia del *trastorno por uso compulsivo de videojuegos* que, desde 2018-2019 está reconocido como enfermedad por la OMS, el *trastorno que el uso compulsivo de redes sociales* no tiene una categoría propia en la Clasificación Internacional de Enfermedades. Sin embargo, existen evidencias ya de que puede convertirse en un patrón problemático con efectos similares a una adicción, especialmente en colectivos vulnerables cono niñas, niños, adolescentes (lo que ha sido condenado ya). También, en personas mayores o personas que adolecen de algún tipo de discapacidad).

La salud mental está protegida a nivel mundial, por la OMS, que define la «salud» como el bienestar físico, mental y social. En efecto, en 2018-2019, incluyó como enfermedad el «uso compulsivo de videojuegos» (que es distinto que jugar mucho) consciente de que dicho uso puede generar efectos comparables a otras adicciones conductuales: (i) aislamiento social (ii) problemas de sueño (iii) bajo rendimiento académico o laboral (iv) cambios emocionales (ansiedad, irritabilidad) y (v) deterioro de relaciones personales. La OMS lo define como un patrón de comportamiento persistente o recurrente relacionado con los videojuegos —en línea o fuera de línea— que presenta tres elementos clave: (i) pérdida de control sobre el tiempo, frecuencia o duración del juego (ii) prioridad creciente del juego sobre otras actividades importantes (estudio, trabajo, relaciones, autocuidado), y (iii) continuación del juego a pesar de consecuencias negativas claras

Pero lo cierto es que, la mayoría de las personas que juegan a ciertos videojuegos con conexión on-line —incluidos quienes juegan muchas horas— no tienen dicho trastorno. Para que se considere un trastorno, este patrón debe causar un deterioro significativo en la vida personal, social, familiar, educativa o laboral. Además, debe mantenerse durante al menos 12 meses (salvo casos muy graves). Y es que, el diagnóstico del trastorno requiere evaluación profesional y un impacto real en la vida cotidiana. Impacto en la salud mental y en el día a día de miles (millones) de niñas, jóvenes y adolescentes.

### 2.2. La Directiva por productos defectuosos indica que son resarcibles (únicamente) los daños a la salud psicológica reconocidos médicamente

Para determinar si los daños a la salud mental que causa el uso compulsivo de redes sociales resultan o no resarcibles, habrá que estar a lo que indica, sobre el particular, la nueva Directiva (UE) 2024/2853 sobre responsabilidad por los daños causados por productos defectuosos.

Dicha directiva, dispone que el derecho a la indemnización que establece sólo le será de aplicación a determinados tipos de daños entre los que incluye la «muerte o lesiones corporales, incluidos los daños a la salud psicológica *reconocidos médicamente*» [art. 6.1 a) DRPD]. Lo que significa, que para determinar si estamos ante un daño psíquico que constituye un daño corporal (para que resulte indemnizable) resulta preciso atender a si dicho daño emocional se halla reconocido (o no) como enfermedad en la «Clasificación Internacional de Enfermedades» de la Organización Mundial de la Salud» (CIE-11, OMS 1992) [20] o en el «Manual diagnóstico y estadístico de los trastornos mentales» de la Asociación Estadounidense de Psiquiatría (DSM-5-TR, 2022) [21]. Dos sistemas clasificatorios de enfermedades ampliamente reconocidos y utilizados en el ámbito internacional para el diagnóstico de los trastornos mentales de la edad adulta y también de la niñez y adolescencia[22] que no siempre resulta coincidentes. Prueba de ello es que el primero de los sistemas citados, el CIE ha reconocido ya como enfermedad, «el trastorno por uso de videojuegos on-line» (gaming disorder) y sin embargo, el DSM aún no lo ha tipificado como tal.

La dependencia tecnológica a redes sociales puede causar daños emocionales**,** pero estos solo adquieren relevancia jurídica cuando adquieren relevancia clínica materializándose en un trastorno mental reconocido por la CIE-11 o el DSM-5-TR. Lo que significa, que según la nueva Directiva por productos defectuosos, el «daño emocional» no es una enfermedad ni en la CIE-11 ni en el DSM-5-TR por lo que para que resulte debe demostrarse que ese daño emocional: (i) haya producido un trastorno mental clínicamente identificable (ii) ese trastorno está reconocido en la CIE-11 o DSM-5-TR y (iii) exista relación causal entre el hecho dañoso y el trastorno.

### 2.3. Dañar la salud mental en el entorno digital es un defecto de seguridad del producto, cada día más

Cuando hablamos de plataformas digitales, videojuegos, móviles, productos, servicios o entornos digitales e inteligentes; el concepto de «seguridad» se debe

20. OMS, CIE-11. Clasificación Internacional de Enfermedades, 11.ª revisión. Estandarización mundial de la información de diagnóstico en el ámbito de la salud, que puede consultarse en https://icd.who.int/es (Fecha de consulta: 15.4.2025).
21. En su versión española: AMERICAN PSYCHIATRIC ASSOCIATION, *Manual diagnóstico y estadístico de los trastornos mentales: DSM-5-TR: texto revisado*, Madrid: Editorial Médica Panamericana, 2024.
22. Mientras que la CIE-11 es una clasificación de todas las enfermedades y sólo destina un capítulo a los trastornos mentales, el DSM-5-TR (2023) se dedica exclusivamente a sentar los criterios para describir síntomas para diagnosticarlos y contiene un último apartado en que se recogen trastornos que tienen una cierta relevancia, pero que todavía no son considerados como enfermedades.

«ampliar» dando cobertura, también al uso compulsivo y a la dependencia tecnológica que puedan, estos dispositivos, ocasionar.

Dañar la salud mental en el entorno digital puede ser un defecto de seguridad cuando el producto digital no hayan sido diseñado, actualizado o cuando no haya advertido de los riesgos que su uso conlleva. Cuando no haya protegido razonablemente a sus usuarias/os frente a riesgos psicológicos previsibles y médicamente diagnosticados como enfermedad. Esto abre la puerta a responsabilidad por: (i) plataformas de redes sociales (ii) videojuegos online (iii) apps de IA (iv) sistemas de recomendación, como Chatbot, y (v) dispositivos conectados con funciones digitales. El daño ocasionado a la salud mental, puede ser un defecto de seguridad**,** siempre que el daño mental: (i) sea consecuencia de un riesgo del producto **(**ii) ese riesgo no haya sido suficientemente prevenido, controlado o advertido y (iii) el producto no ofrezca la seguridad que el público puede esperar razonablemente**.** Con esta visión moderna de «daño de seguridad» de la Directiva se amplía expresamente la noción de seguridad para incluir a los riesgos psicológicos derivados del entorno digital; especialmente en productos conectados, servicios digitales integrados y sistemas basados en IA.

Veamos por qué puede (y debe) considerarse un defecto de seguridad de estos productos inteligentes. La Directiva 2024/2853 introduce tres ideas clave que permiten considerar que el daño a la salud mental sea considerado un defecto de seguridad:

En primer lugar, *la Directiva no se limita, en su ámbito de aplicación, a otorgar indemnización a los daños físicos (únicamente)*. Habla de «daños a la salud, incluidos los daños mentales» como daños indemnizables. Por tanto, si un producto digital causa: (i) ansiedad (ii) estrés grave (iii) trastornos derivados de exposición a contenidos (iv) adicción tecnológica, y (v) deterioro psicológico por diseño manipulativo, por ejemplo; dichos daños entran dentro del ámbito de la seguridad del producto y serán indemnizables cuando la enfermedad que los cause esté médicamente diagnosticada según los criterios de clasificación de enfermedades**.** Tal y como he dicho, con anterioridad, Ahora bien. El «daño emocional», no está reconocido como enfermedad ni en la CIE-11 ni en el DSM-5-TR. Solo adquiere relevancia clínica o pericial si se traduce en un trastorno mental concreto reconocido por estas clasificaciones (p. ej., trastorno de ansiedad, depresión, estrés postraumático, etc.). Esta advertencia resulta fundamental, a los efectos de determinar (o n o) la responsabilidad civil (o, en su caso, penal o laboral, penal), porque:

- No basta alegar «daño emocional»: debe acreditarse un trastorno diagnosticable CIE-11 o DSM-5-TR (es decir, según on los dos sistemas de clasificación y diagnóstico más importantes del mundo en el ámbito de la salud y la psicología —que son los que proporcionan un lenguaje común

y estandarizado para que los profesionales médicos identifiquen, clasifiquen y registren enfermedades y trastornos)—.

- Los tribunales suelen exigir informes periciales que vinculen el daño emocional con un diagnóstico clínico reconocido.

Debe tenerse en cuenta que, la Clasificación Internacional de Enfermedades (CIE-11) no reconoce el «daño emocional» como una enfermedad ni como una categoría diagnóstica autónoma. La CIE-11 clasifica trastornos mentales específicos (ansiedad, depresión, estrés postraumático, trastornos disociativos, etc.), pero no incluye una categoría genérica denominada «daño emocional». La CIE-11 no incluye «daño emocional» como diagnóstico**.** La clasificación solo reconoce trastornos mentales específicos**,** como: (i) trastornos depresivos (ii) trastornos de ansiedad (iii) trastornos relacionados con estrés (incluido TEPT) (iv) trastornos disociativos y (v) trastornos de adaptación. Y, la DSM-5-TR tampoco reconoce el «daño emocional» como trastorno diagnosticado. El manual contiene trastornos mentales definidos**,** con criterios diagnósticos precisos (ansiedad, depresión, trastornos de personalidad, trauma, etc.), pero no contempla una categoría diagnóstica llamada «daño emocional». El DSM-5-TR organiza los trastornos en categorías clínicas específicas y no incluye un diagnóstico genérico de «daño emocional». Y es que, tal y como he indicado ya, la CIE-11, a diferencia de la DSM-5 TR, incluye como enfermedad el «Trastorno por uso de videojuegos»**,** dentro del capítulo de trastornos debidos a comportamientos adictivos. Tiene dos subtipos:

- 6C51.0 - Predominantemente en línea.
- 6C51.1 - Predominantemente fuera de línea.

El subtipo 6C51.0, se aplica cuando la conducta adictiva se desarrolla principalmente en entornos conectados, como videojuegos online, plataformas multijugador, mundos virtuales, etc. Dicho trastorno se caracteriza por:

- Pérdida de control sobre el tiempo y la frecuencia de juego.
- Prioridad creciente del juego sobre otras actividades.
- Persistencia del comportamiento pese a consecuencias negativas.
- Deterioro significativo en lo social, académico, laboral o personal.
- Duración mínima: 12 meses (salvo gravedad extrema).

En segundo lugar, *los productos digitales deben ser seguros también en su dimensión psicológica*. Es decir, la Directiva exige evaluar la seguridad considerando: (i) la interacción con servicios digitales (ii) las actualizaciones (iii) los algoritmos y los riesgos derivados de su diseño adictivo (iv) los riesgos deriva-

dos de su conectividad y los comportamientos previsibles de los usuarios, elevando el estándar de seguridad para los colectivos especialmente vulnerables como son las niñas, niños, adolescentes, personas mayores y personas con discapacidad. Luego, si un producto digital (red social, app, plataforma, videojuego, IA) genera riesgos psicológicos previsibles y el fabricante no los mitiga; hay defecto de seguridad.

Junto a la Directiva por productos defectuosos, la Digital Services Act (DSA) de 2024 sí incluye la salud mental como un «riesgo sistémico» —lo que marca un cambio profundo en cómo la Unión Europea regula a las grandes plataformas digitales—. Aunque el DSA no clasifica enfermedades**,** sí reconoce que las plataformas pueden generar efectos psicológicos adversos**,** incluyendo patrones de uso compulsivo. Por otro lado, en nuestro país, la propia Ley Orgánica de Protección Integral a la Infancia y la Adolescencia frente a la Violencia digital (LOPIVI) —Ley 8/2021, de 4 de junio— considera la salud mental parte de la protección frente a violencia digital. Con acierto advierte que la salud mental parte de la protección frente a violencia digital, dando respuesta a riesgos como: (i) el acoso (ii) el grooming (iii) la exposición a contenido dañino y (iv) la adicción a redes. Por tanto, y aunque el DSA no usa literalmente la expresión «adicción a plataformas», sí exige evaluar riesgos derivados del impacto de los algoritmos y sistemas de recomendación sobre el bienestar psicológico. Por riesgo sistémico, se debe entender, el riesgo que causa en los derechos fundamentales y en el bienestar mental y físico de quienes son sus usuaria**s**/os. El DSA obliga a las plataformas en línea de muy gran tamaño (VLOP) y a los motores de búsqueda de muy gran tamaño (VLOSE) a evaluar y mitigar riesgos que sus servicios puedan generar para la sociedad. Entre esos riesgos, el Reglamento incluye explícitamente: (i) efectos negativos en el bienestar mental y físico de los usuarios y (ii) riesgos para los menores, incluyendo exposición a contenidos dañinos y diseño adictivo de plataformas. De hecho, la Agencia Española de Protección de Datos (AEPD) ha empezado a aplicar el DSA y otras normativas (como protección de datos y derechos de los menores) para sancionar prácticas que: (i) exponen a menores a contenidos perjudiciales (ii) utilizan algoritmos que afectan al bienestar psicológico, y (iii) no protegen adecuadamente a usuarios vulnerables. *La propia AEPD destaca que el DSA exige tener en cuenta* el bienestar mental y físico, especialmente de los menores, en el diseño de plataformas y algoritmos.

En tercer lugar, el defecto de seguridad existe cuando el producto no ofrece la seguridad que el público puede esperar. Lo que significa, que el producto, entorno o servicio digital es defectuoso: ***(i)*** cuando falten controles parentales, (ii) cuando esté diseñado con algoritmos que fomentan un uso compulsivo, (iii) cuando exponga a sus usuarios a un uso no controlado de contenidos dañinos, (iv) cuando adolezca de advertencias claras, (v) cuando el diseño sea adictivo o manipulativo («dark patterns») y, (vi) cuando tiene fallos en la moderación de contenidos que generan daño psicológico.

Por tanto, si el riesgo era previsible **y** evitable (cuestión sobre la que ahondaré con determinen**,** el producto será defectuoso. Sobre dicha distinción (riesgos previsible y evitable) ahondaré más adelante.

### 2.4. Defectos de seguridad y sentencias condenatorias de Meta (propietaria de Facebook, Instagram y WhatsApp) y YouTube por crear diseños adictivos en sus plataformas que dañan la salud mental de sus usuarias/os

La relación directa entre los *defectos de seguridad* y las sentencias condenatorias contra Meta y YouTube es que los tribunales concluyeron que las plataformas eran inseguras por diseño, y que esos fallos estructurales —no simples errores aislados— causaron daños reales a menores**,** especialmente en su salud mental y bienestar.

A partir del fallo judicial que cuenta la historia de una niña californiana que empezó a entrar en internet con apenas seis años de edad, viendo vídeos en YouTube se ha (re)abierto un serio debate sobre los defectos de seguridad, los daños a la salud mental que causan la dependencia tecnológica y la posible responsabilidad de las plataformas a la hora de diseñar sus productos. La niña Californiana Kally, con nueve años, ya usaba su primer iPhone propio Instagram; con 10 años, TikTok (llamado entonces Musical.ly), y con 11 años, Snapchat. Durante su infancia y ya, en la adolescencia, llegaba a pasar hasta 16 horas al día en dichas aplicaciones. No sabía estar sin teléfono móvil. Y si sus padres le restringían el uso del mismo, tenía ataques de pánico y agresividad; mostrando una clara adicción al móvil y a las plataformas digitales con las que interactuaba. En realidad, este caso, representa a la perfección lo que están viviendo y padeciendo millones (mejor dicho, billones) de niñas y niños de todo el mundo. Pero este, en concreto, se ha hecho viral y ha acaparado la atención de todos los periódicos del mundo no sólo por lo impactante que es la historia de esta niña, sino porque esta niña, hoy ya mujer, ha logrado una sentencia ejemplarizante en contra de Meta y YouTube que las condena a pagarle 6 millones de dólares y porque ejemplifica (a la perfección) lo que hoy está sucediendo hoy en buena parte del mundo: la preocupación de padres y madres, abuelas y abuelos frente a la dependencia tecnológica de sus hijas e hijos, nietas y nietos es una realidad. Aunque los lobbys tecnológicos son conscientes de los riesgos de seguridad que comportan estos productos tecnológicos frente a colectivos tan vulnerables, por razón de la edad, las arcas y los bolsillos de la industria tecnológica acaparan las redes sociales utilizando compañas de marketing agresivas que encuentran presa fácil, precisamente, entre las personas usuarias que por razón de su edad (menores o mayores) o su discapacidad son más fáciles de engañar, adictivamente hablando, o de engañar.

El mensaje lanzado a la industria tecnológica, a través de esta segunda sentencia pionera que condena a indemnizar a Meta y YouTube es muy claro y evi-

dente: los jurados de California están dispuestos a responsabilidad a las empresas tecnológicas de redes sociales por el impacto de sus decisiones de diseño en contra de la salud mental de sus usuarias. La suerte de Kaley, a quien, recientemente —después de 20 años de lucha en los juzgados de California (EE.UU.)—, se le ha dado la razón a través de una sentencia pionera —no es la suerte de un millar de niñas y niños que hoy se encuentra pendientes de un veredicto parecido—. ¿Sucederá, con estos procesos pendientes en EE.UU. lo mismo que sucedió con las tabacaleras de EE.UU., en los años 90, que recuerden firmaron el pago de 30 billones de euros para evitar juicios condenatorios porque sus productos creaban adición a la población?

Pero la madre de Kaley, como tantas madres y padres, abuelas y abuelos, están más que nunca preocupadas e indignadas por la adición y sobreexposición de hijas e hijos, nietas y nietos. Incluso, también, de algunas madres y padres. Consideran, como la madre de Kaley, que las redes sociales —por medio de patrones oscuros— están dañando su salud mental. Que han cambiado el modo en que funciona el cerebro de quienes no pueden dejar el móvil, la Tablet, o las redes sociales. Ahora son más conscientes que nunca de que «el diseño de las plataformas es adictivo». Es decir, que su «enganche» afecta, incluso a su memoria a largo plazo (que no la tienen, porque lo importante para ellas y ellos es lo inmediato). Está preocupados porque, en cualquier reunión u ocasión, sus hijas e hijos no saben vivir ni estar sin su teléfono móvil. Porque, incluso, son capaces de emprender una batalla quijotesa para no perder su móvil —algo que los padres y madres usamos, a veces, para «negociar» o imponer «un castigo»; conscientes de que reaccionarán para conseguir seguir enganchados a internet y las redes sociales.

#### *2.4.1. La desprotección de menores y la sobreexposición sexual en redes sociales. Primera sentencia/Caso de Nuevo México que condena a Meta (375 millones de dólares)*

El pasado 24 de marzo de 2026, el tribunal de Nuevo México **(**First Judicial District Court of New Mexico), dictó el caso (*State of New Mexico v. Meta Platforms, Inc.*) dictó la fue la primera sentencia condenataria (que conozco) de EE.UU. en la que el jurado determinó que Meta (propietaria de Facebook, Instagram y WhatsApp) no había protegido, adecuadamente, a una menor **(**permitiendo riesgos como contacto con depredadores y afectación a la salud mental) sobreexponiéndola, a través de las redes sociales, a una posible explotación sexual; por lo que le impuso una sanción de 375 millones de dólares. El motivo, en el que se fundamentó fue el siguiente: el uso de prácticas engañosas, priorizar beneficios sobre seguridad infantil y sobreexponerlas a una posible explotación sexual a través de las redes sociales[23].

23. El País, 25/03/2026. Meta y YouTobe pierden el juicio sobre la adición de los menores a redes sociales y son declaradas negligentes» (noticia disponible, publicada en la siguien-

### *2.4.2. La adición tecnológica a redes sociales de una niña californiana. Segunda Sentencia/caso de los Ángeles: condenas Meta y YouTube por crear adicción a redes sociales*

Un día después de haberse dictado la sentencia en Nuevo México, un juzgado de los Ángeles (EE.UU.) declaró culpables a Meta **(**propietaria de Facebook, Instagram y WhatsApp) y YouTube por «diseñar plataformas adictivas» que afectaron a la salud mental de Kally, una joven Californiana. El 25 de marzo se dictó sentencia condenatoria exigiendo a indemnizarle 3 millones de dólares a una niña Californiana. De dicha cantidad, Meta debía de responder, en un 70% y YouTube en un 30%. El argumento clave, en esta segunda ocasión, fue diferente: se centró en el «diseño de las apps»: *un diseño que estaba pensado para enganchar a las personas menores usuarias.*

El abogado de la familia de Kally, llegó a comparar su adicción con «un golpe químico», que afectaba a su cerebro. Kaley pasó por depresión, ansiedad y sufrió problemas de dismorfia corporal. El veredicto del juzgado ha sido muy claro pero (también) algo desalentador al ver la sanción impuesta —comparativamente hablando mucho menor que la impuesta a Meta en Nuevo México—: Meta (propietaria de Facebook[24], Instagram y WhatsApp) tendrá que pagarle un 70% y YouTube, un 30%. Lejos de asumir cualquier tipo de responsabilidad, Meta ha afirmado, a través de un comunicado que respeta el veredicto pero no está «de acuerdo con él» y «está estudiando nuestras opciones legales». Después de haber sido *declaradas culpables de generar adicción entre la/os menores y de engancharles en sus plataformas*, Meta y YouTube (lobbys tecnológicos) han dejado muy clara su prioridad: obtener beneficios económicos frente a la seguridad de las personas que usan sus plataformas. Las posibles adiciones o problemas de salud mental nos les preocupan en exceso.

> Ambas plataformas deberán pagar seis millones de dólares entre las dos Kally (K.G.M.), en concepto de indemnización por daños morales y otros perjuicios económicos. ¿Por qué digo que es más ejemplarizante que otra cosa? En una primera fase se las condenó a pagar tres millones de dólares en daños compensatorios, asignando a Meta el 70% de la responsabilidad

---

te URL: https://elpais.com/tecnologia/2026-03-25/meta-y-youtube-pierden-el-juicio-sobre-la-adiccion-de-los-menores-a-redes-sociales-y-son-declaradas-negligentes.html (fecha de consulta: 25.03.2026).

24. El creador de el creador de Facebook, Mark Zuckerberg, insistió en que la/os menores de 13 años tienen prohibido acceder a Instagram y les achacó cierta responsabilidad: «Creo que hay un grupo de personas, potencialmente un número significativo, que mienten sobre su edad para usar nuestros servicios». Afirmó que su objetivo no era enriquecerse, puesto que donaba «casi todo a obras benéficas», y su intención era «dar miles de millones a la investigación científica». «Cuanto mejor le vaya a Meta, más capaces seremos de investigar».

> por el perjuicio sufrido por la demandante —lo que supone una parte de 2,1 millones de dólares— y a YouTube el 30% restante, es decir, 900.000 dólares. Y, en una segunda fase, los integrantes del jurado añadieron otros tres millones de dólares en daños punitivos —desglosados de la misma manera— tras concluir que ambas empresas habían actuado con «malicia», «conducta abusiva» o «fraude». Concluyeron que Meta y YouTub eran «negligentes en el diseño y funcionamiento» de sus plataformas y que esa negligencia fue un factor central en el daño causado a la demandante.

Siendo criticable, que lo es a mi juicio, el importe de la condena sugiero que nos quedemos con los términos en los que se dicta la sentencia, porque son, en mi opinión, un claro mensaje lanzado a la industria tecnológica y extrapolable al resto de productos inteligentes dirigidos hoy a la población más vulnerables: menores, mayores y personas con discapacidad. Dice la sentencia:

- Que ambas empresas sabían que sus servicios representaban un peligro para los menores,
- Que no advirtieron adecuadamente a sus usuarias/os de ese peligro y,
- Que un operador razonable de una plataforma sí lo habría hecho.

Estas tres afirmaciones (fundamentales, en mi opinión) constituyen un claro mensaje para las empresas tecnológicas. Les están diciendo que cuando lancen un producto al mercado digital eviten, razonablemente, adicciones y consecuencias perjudiciales en la salud. También en la salud mental y psicológica de las personas usuarias de sus productos. Pero, además, estas sentencias pioneras abren la puerta a nuevas demandas masivas contra redes sociales, mayor regulación sobre diseño adictivo y protección infantil y, responsabilidad legal directa por daños psicológicos y riesgos en menores.

Lo cierto es que estos dos primeros fallos judiciales reconocen, por vez primera y de manera oficial, que el diseño de redes sociales puede causar daño; lo que podría transformar la industria tecnológica. A raíz de estas sentencias condenatorias me pregunto si dichas plataformas de redes sociales rediseñarán (o no) sus productos para evitar los riesgos de dependencia emocional y tecnológica; ¿estarán dispuestos a percibir menos rendimientos económicos y lanzar un marketing menos agresivo, de cara al usuario/a? En mi opinión, y a la vista de la sanción impuesta en la que constituye la segunda sentencia constituye un tirón de orejas a la industria tecnológica: una sentencia más ejemplarizante que real. El importante de la multa —6 mil dólares— lo dice todo. Es, realmente irrisorio. ¿Qué representan 6 millones de dólares para estas dos empresas tecnológicas? Es indecente imponer una multa tan escasa, después de reconocer que son culpables de la salud mental de una menor —y ser conscientes de que lo son de la de millones de menores de todo el mundo—. Indecente porque son conscientes

de su negligencia (yo diría, consciencia y hasta dolo) a la hora de lanzar estos productos que causan adicción a quienes los usan. Y yo me pregunto (insisto): ¿Qué son 6 millones de dólares para Meta y YouTube —dos de las empresas de la industria tecnológica de venta de publicidad más ricas del mundo? Las diferencias en la condena son, cuanto menos llamativas: Seis millones de dólares (importe de la multa de la sentencia de Los Ángeles) frente a 375 millones de dólares (importe de la multa de Nuevo México), me parece en realidad, una indecencia más de lo que está sucediendo, lamentablemente, con la adición y fala de protección de las niñas, los niños y los adolescentes. Dejaré para el final, analizar el impacto que estas sentencias condenatorias causarán en Europa y en España una vez analice, con el detenimiento necesario los defectos de seguridad de los productos y las personas vulnerables.

## IV. DEFECTOS DE SEGURIDAD DE LOS PRODUCTOS Y PERSONAS VULNERABLES EN LA DIRECTIVA POR PRODUCTOS DEFECTUOSOS: POR UNA «SEGURIDAD UNIVERSAL»

### 1. LA SEGURIDAD «UNIVERSAL» COMO UN PRINCIPIO JURÍDICO IMPLÍCITO EN LA DIRECTIVA (UE) 2024/2583

Uno de los cambios más relevantes que presenta la Directiva (UE) 2024/2853 de productos defectuosos es que introduce una regla general, conforme a la cual el producto es defectuoso cuando «no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional» (art. 7.1 h). A través de esta afirmación se convierte, en mi opinión, en regla general: que la seguridad «exigible» y «esperable» lo sea con carácter «universal».

Aunque la Directiva (UE) 2024/2583 no usa la expresión «seguridad universal», sí incorpora elementos que la favorecen**.** Es cierto que la idea de «seguridad universal» (o *universal safety*) no aparece como término literal en la Directiva, pero considero que si aparece como «principio jurídico implícito»: «Los productos deben ser seguros para *todas* las personas que los utilicen, incluidas aquellas con vulnerabilidades específicas». Este «principio» se «integra» directamente en la «evaluación del defecto» y en el estándar de seguridad esperable» porque se amplía la noción de producto defectuoso (acertadamente a mi juicio) tomando en consideración no sólo la seguridad del producto sino, también, las expectativas de «todas» las personas consumidoras y usuarias, así como, también, la sostenibilidad, la conformidad con respecto a las expectativas de las personas consumidoras y usuarias y los estándares de calidad[25]. Este estándar objetivo de

25. En opinión de Pérez García, M. J. 2025. «La responsabilidad por los daños causados por productos defectuosos: análisis de la Directiva (UE) 2024/2853 y una propuesta de lege ferenda de incorporación al ordenamiento español». InDret, n.º 3, pp. 216, a mi juicio,

seguridad significa que un producto es defectuoso si no ofrece la seguridad que cabe legítimamente esperar**.** Un estándar que debe interpretarse considerando «a quién va dirigido» el producto y «a quiénes» puedan usarlo y esperar, en su uso, razonablemente que no sufrirán daño algo; lo que abre la puerta a exigir una «seguridad reforzada» para las personas usuarias vulnerables.

> El considerando 30 de la Directiva indica que la valoración del carácter defectuoso debe incluir un análisis objetivo de la seguridad que el público en general tiene derecho a esperar y no referirse a la seguridad que una persona concreta tiene derecho a esperar. La seguridad que el público en general tiene derecho a esperar debe valorarse teniendo en cuenta, entre otras cosas, la finalidad prevista, el uso razonablemente previsto, la presentación, las características objetivas y las propiedades del producto de que se trate, incluido su ciclo de vida previsto, así como las necesidades específicas del grupo de usuarios al que se destina el producto.

La Directiva (UE) 2024/2853, incluye en el artículo 7.2 un listado no exhaustivo de las circunstancias que se deben tomar en cuenta para determinar si un producto es defectuoso (algunas de ellas ya se preveían en la Directiva de 1985). Entre otras, se citan las siguientes: (i) etiquetado del producto (ii) diseño (iii) características técnicas (iv) composición (v) envase (vi) instrucciones de montaje (vii) instalación (viii) uso y mantenimiento (ix) el uso razonablemente previsible del producto (x) requisitos de seguridad y ciberseguridad del producto (xi) efectos en la capacidad del producto de seguir adquiriendo nuevas propiedades una vez que se ha introducido en el mercado o puesto en servicio (xii) efectos que razonablemente pueden producir entre sí los productos interconectados (xiii) *necesidades específicas del grupo de usuarios finales a los que se destina el producto*, y (xiv) cualquier retirada del producto o cualquier intervención pertinente relacionada con la seguridad de los productos por parte de una autoridad competente o de un operador económico mencionado en el artículo 8 de la Directiva.

La idea central, en mi opinión, gira en torno al concepto de «defecto de seguridad». Y es que, según el art. 7.2 h, «un producto es defectuoso cuando no ofrece la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y durante toda la vida o ciclo del producto y teniendo en cuenta las necesidades específicas del grupo de usuarios finales a los que se destina el producto…». Por lo que *el centro de gravedad de la regla de responsabilidad por*

---

la ambigüedad e imprecisión de algunas de las circunstancias que se han incluido en la nueva normativa europea para determinar si un producto es defectuoso (por ejemplo, el uso razonablemente previsible del producto o las necesidades específicas del grupo de usuarios finales) merecen una valoración negativa, pues no aportan certeza, sino que al ser una cuestión subjetiva e interpretable va a implicar un aumento de la litigiosidad».

*productos defectuosos no centra su atención en la idea de la infracción del deber u obligación por parte del fabricante sino en la de la «confianza» de las personas usuarias, entre las que se encuentran, también, las personas menores (niñas, niños y adolescentes), personas mayores, y personas con discapacidad).*

El concepto de seguridad «universal» de los productos, encuentra su apoyo en la Directiva 2024/2853 que permite interpretaciones que «refuercen» la protección de personas vulnerables cuando sea traspuesta a nuestro ordenamiento jurídico español (antes del próximo 9 de diciembre de 2026). Felizmente la Directiva ha optado por positivizar lo que bajo la directiva anterior era una jurisprudencia ya consolidada atendiendo a las necesidades que presentan los colectivos más vulnerables (como son las niñas, niños y adolescentes, las personas mayores y las personas con discapacidad). Confío, pues, que en la trasposición se tenga muy en cuenta dicha positivización que supone huir (acertadamente, en mi opinión), pasar de un régimen de responsabilidad civil que, tradicionalmente tiene (únicamente) una función compensatoria **(**reparar el daño una vez producid); para pasar a ser concebido con un mecanismo de garantía preventivo. El hecho de que se «adoptado» (implícitamente) la idea de «seguridad universal» provoca un efecto inmediato: que la responsabilidad civil, deje de ser solo un mecanismo de reparación para pasar a convertirse en un mecanismo de «garantía preventiva». Dicho con otras palabras: la responsabilidad civil se transforma en un instrumento de política pública para «elevar» el nivel de seguridad. Prueba de este cambio de concepción es que preocuparse y ocuparse de que el producto sea seguro para «todos» sus usuarios; termina obligando a que: (i) el productor diseñe productos seguros y accesibles (ii) incentiva, también, a que realice controles de calidad más estrictos (iii) fomenta la transparencia y, por supuesto (iv) la exigencia en los deberes de información a las personas consumidoras —incluidas las vulnerables—. En definitiva, convierte el régimen de responsabilidad civil en una herramienta que evite/prevenga los «daños antes de que se produzcan» —una función, que, cumple, también, el Reglamento de seguridad de 2023 y el Reglamento IA de 2024—.

La defectuosidad de un producto se evalúa comparando el producto tal como es con el nivel de seguridad que el público (en general —y, por tanto, todos) puede esperar razonablemente de él. Este criterio que ya aparecía, en la Directiva 85/374/CEE sobre responsabilidad por productos defectuosos, en la Ley 22/1994, en el TRLGDCU, se moderniza en la nueva Directiva 2024/2583. Los productos inteligentes —robots asistenciales, dispositivos médicos conectados, asistentes de voz, vehículos automatizados, wearables— introducen tres elementos que complican determinar cuándo un producto es defectuoso y quien o quienes responderán frente a los daños causados por el productos defectuoso: (i) *autonomía funcional*: el producto toma decisiones sin intervención humana (ii) *dependencia del software y de los datos*: el defecto puede estar en el algoritmo (sesgado), en la actualización o en los datos de entrenamiento y (iii) «puesta en circulación» del producto lo que hace que tras la venta el producto cambie

mediante actualizaciones. Si a ello, se le une el hecho de que dentro del ámbito de aplicación de la Directiva se incluyen (i) los productos que incorporan sistemas de IA, los *software*, los servicios digitales integrados y las actualizaciones necesarias para mantener la seguridad y que los fallos o defectos de los *software* afectan de forma desproporcionada a personas vulnerables; no me cabe duda alguna de que habrá que (re)interpretar el *defecto de seguridad es «universal» tomando en consideración, también y de manera especial, a las personas vulnerables/hipervulnerable diría yo.*

## 2. LA CONVERGENCIA ENTRE «LA SEGURIDAD UNIVERSAL» Y LA «RESPONSABILIDAD CIVIL» POR PRODUCTOS DEFECTUOSOS

La «seguridad universal» y la «responsabilidad civil» convergen en un mismo objetivo: garantizar que «todos los productos» *sean seguros* para «todas las personas». La RIA actúa *ex antes* del daño, imponiendo al productor que los productos tengan un diseño inclusivo. La Directiva por productos defectuosos actúa *ex post*, sancionando al productor si no cumplió dicho deber. Esta convergencia está transformando el derecho de productos en Europa hacia un modelo más humano, más tecnológico y más protector. Y es que, nuestro sistema jurídico está evolucionando desde un modelo centrado en el *consumidor medio* hacia un modelo que protege a «todas las personas», incluidas las más vulnerables, y en «todas las fases del ciclo de la vida del producto. Un enfoque, insisto más humano que pone en el centro de la tecnología a todas las personas». Es lo que se conoce con el nombre de «seguridad universal».

La «seguridad universal» es un principio según el cual los productos deben ser seguros para todas las personas que razonablemente puedan utilizarlos, incluidas aquellas con: (i) discapacidad física o cognitiva, (ii) edad avanzada, (iii) menor alfabetización digital, (iv) dependencia tecnológica y, (vi) menor capacidad para percibir o evitar riesgos.

Este principio de seguridad universal aparece con fuerza en el Reglamento (UE) 2023/988 de Seguridad General de los Productos, que exige que el diseño, la fabricación, las instrucciones y la vigilancia del producto tengan en cuenta a los colectivos vulnerable. Un enfoque preventivo que evita poner en el mercado productos inseguros para «todas» las personas. La Directiva (UE) 2024/2853 establece que un producto es defectuoso cuando no ofrece la seguridad que el público puede esperar. Y ese «público» incluye a los vulnerables. Pero los incluye, desde una perspectiva o con un enfoque eminentemente reparador. Lo que significa, que, si el producto causa daño porque no era seguro para un usuario vulnerable, el productor responde.

Este enfoque, universal e integral (e invisible), exige (a mi juicio), que el diseño, la fabricación y la información del producto garanticen la seguridad de

«todas» las personas usuarias del producto y, no solo la del consumidor medio. Es decir, la seguridad, también, de las niñas, niños o adolescentes, la de las personas mayores, la de las personas con discapacidad, personas con menor alfabetización digital, así como, también, la de colectivos expuestos a riesgos especiales (pacientes, trabajadores, etc.). La «seguridad universal» implica que el productor debe anticiparse a las limitaciones, capacidades y riesgos propios, también, de los colectivos más vulnerables. Un concepto (el de «seguridad universal») que se ha consolidado hace años ya en la jurisprudencia europea para pasar a ser un principio fundamental dentro de la normativa europea sobre «confiabilidad de productos defectuosos». La necesidad de prevenir o, en su caso, reparar los «riesgos de seguridad» y «riesgos para los derechos fundamentales», causados «por» o «con» productos (y servicios) es fundamental. Mas aún, si dichos productos incorporan sistema dotados de IA; lo que se traduce en especialmente arriesgado o peligroso para cuando son juguetes inteligentes, con los que interactúan niñas, niños o adolescentes o son, por ejemplo, robots asistenciales con los que se asisten a personas mayores o personas que adolecen de algún tipo de discapacidad. Entonces, ¿En qué y en dónde convergen, pues?

1. El Reglamento obliga a diseñar productos pensando en todos los usuarios, incluidos los vulnerables. Ese estándar preventivo se convierte en el punto de referencia para evaluar si un producto es defectuoso. Es decir, «lo que el Reglamento exige *ex ante* es lo que la Directiva considera *esperable ex post*».
2. La vulnerabilidad eleva el estándar de seguridad exigible, como desarrollaré, más adelante. Y es que, si un producto no es seguro para un colectivo vulnerable que razonablemente lo utilizará, entonces: (i) no cumple la seguridad universal, y (ii) es defectuoso a efectos de responsabilidad civil**.** Por ejemplo, Un robot asistencial que no detecta bien a una persona con movilidad reducida incumple ambos regímenes.
3. La seguridad universal convierte la responsabilidad civil en un mecanismo de garantía. Me explico: la responsabilidad civil deja de ser solo un mecanismo de reparación y se convierte en un *incentivo jurídico* para que los productores cumplan con la seguridad universal. Lo que significa, que si el productor no diseña pensando en personas usuarias vulnerables: (i) incumple el Reglamento de seguridad del producto, y (ii) se expone a que se le exija responsabilidad civil por los daños que ocasione el defecto del producto.

La Directiva opera como un instrumento jurídico que materializa el principio de seguridad universal en el ámbito del consumo, estableciendo un equilibrio entre innovación tecnológica, libertad empresarial y protección de los derechos fundamentales. Ahora bien, y como muy pronto voy a desarrollar, las limitaciones del régimen de responsabilidad por defectos y los desafíos para la seguridad

universal son enormes, porque a pesar de su importancia, la Directiva presenta limitaciones que afectan directamente a la protección de personas vulnerables:

- Exclusión de ciertos daños**,** como los puramente económicos.
- Umbral mínimo de indemnización, que puede dejar sin reparación daños de menor cuantía, pero relevantes para personas con escasos recursos.
- Dificultades probatorias en productos altamente tecnológicos, donde demostrar el defecto o la relación causal puede ser complejo.
- Desactualización frente a la digitalización, la inteligencia artificial y los productos conectados.

Estas limitaciones han motivado reformas recientes en el derecho europeo, orientadas a adaptar la responsabilidad por productos defectuosos a los nuevos riesgos tecnológicos y a reforzar la protección de los consumidores más vulnerables.

## 3. ¿QUÉ SE ENTIENDE POR PRODUCTO DEFECTUOSO?

### 3.1. Introducción

La Directiva 2024/2853 aclara, con acierto en mi opinión, que un producto puede ser defectuoso, aun cuando cumpla normas o estándares técnicos **si** no ofrece la «seguridad esperada». La nueva directiva, bajo el epígrafe de «defectuosidad», establece, en el art. 7.1 DRPD, que «Un producto se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional». A diferencia del art. 6 de la directiva anterior de 1985, el art. 7 de la nueva Directiva no refiere esa «defectuosidad» únicamente al hecho de que el producto no cumpla con las expectativas de seguridad del público, en general o de manera excepcional, en caso de determinados productos, de sus destinatarios; sino que añade una referencia explícita al cumplimiento de la normativa de seguridad exigida por el derecho de la UE o nacional.

La Directiva (UE) 2024/285, no sólo define, sino que amplía y disipa las dudas que suscitaba la directiva anterior (, en torno al concepto de producto limitado, con anterioridad, a bienes muebles incluidos los bienes muebles incorporados al inmueble o la electricidad (por ejemplo, un software instalado en una máquina). Consolida de manera clara que los programas informáticos entran dentro de la noción de «producto», con independencia de su modo de suministro o uso, e incorpora en dicha noción los servicios («conexos») que considera imprescindibles para el para el funcionamiento de determinados productos y que adquieren, de este modo, la condición de componentes del producto.

### 3.2. El acierto de ampliar la definición de producto permite incluir a los productos en la era digital

El concepto de «producto» en la Directiva europea sobre responsabilidad por productos defectuosos es amplio y ha sido actualizado (recientemente) por la Directiva (UE) 2024/2853**,** que sustituye a la antigua Directiva 85/374/CEE. Esta actualización amplía de forma significativa qué se considera producto en el contexto de responsabilidad objetiva del productor. Y es que, la Directiva amplía el concepto para adaptarlo a la realidad tecnológica actual, donde un «defecto» puede provenir tanto de un componente físico como de un elemento digital.

La Directiva (UE) 2024/2853 define producto como cualquier bien mueble, con independencia de que sea tangible o intangible, y aunque esté integrado en otro bien. Esto incluye:

- *Bienes materiales tradicionales*: electrodomésticos, vehículos, juguetes, maquinaria, herramientas, etc.
- *Productos digitales:*
  - Software incorporado en un dispositivo.
  - Software independiente (cuando su defecto pueda causar daños).
  - Actualizaciones, parches y elementos digitales necesarios para el funcionamiento seguro del producto.
- *Sistemas basados en IA*: algoritmos, modelos y componentes digitales que influyen en el funcionamiento del producto físico.
- *Productos reacondicionados o de segunda mano* cuando se vuelven a introducir en el mercado por un operador económico.
- *Componentes y piezas de recambio,* incluidos los digitales.
- *Productos en la economía circular*: bienes reparados, remanufacturados o modificados que vuelven al mercado.

La UE reconoce que los productos actuales:

- Dependen de software para funcionar.
- Pueden volverse defectuosos por *fallos en actualizaciones*, ciberseguridad o algoritmos.
- Circulan en cadenas de suministro complejas, con múltiples actores responsables.
- Se reutilizan y reacondicionan cada vez más.

Por esa razón, la Directiva incorpora expresamente los *productos digitales y los sistemas de IA*, así como los bienes reacondicionados, para garantizar que el consumidor esté protegido frente a daños causados por defectos no solo físicos, sino también digitales.

### 3.3. Tipos de defectos que reconoce la Directiva

La Directiva 2024/2583 no clasifica formalmente los defectos, pero de su contenido se desprenden varias categorías prácticas. Los productos tradicionales, son defectuosos si no ofrecen la seguridad que cabe esperar. En productos inteligentes, esta evaluación del defecto se debe ampliar, tomando en consideración:

- *Defectos de diseño*: dependencia tecnológica, sesgos algorítmicos en contra de la edad o de la falta de capacidad, fallos en modelos predictivos, decisiones automatizadas incorrectas y sesgadas (crédito scoring) constituyen, algunos de los fallos de seguridad que afectan a sus usuarios.
- *Defectos de actualización*: software no actualizado
- *Defecto de fabricación*, un error en la producción hace que un lote o unidad sea inseguro.
- *Defecto de información*, instrucciones insuficientes, advertencias inadecuadas o falta de actualización.
- *Defecto digital*, fallos de software, vulnerabilidades de ciberseguridad, errores en IA, actualizaciones defectuosas o ausencia de actualizaciones necesarias para mantener la seguridad.
- *Defectos de interacción*, fallos en sensores, reconocimiento de voz o navegación autónoma que no permitan a las personas con discapacidad navegar o que los sitúen en una flagrante situación de discriminación.
- *Defectos de ciberseguridad*, vulnerabilidades que permiten accesos indebidos o manipulación del producto, aprovechándose de las personas por su vulnerabilidad.
- *La necesidad de adaptar la noción del defecto a las personas vulnerables: La protección reforzada para personas vulnerables* exigencia de prueba individual del defecto, tal y como establece la STS 105/2021 de 1 de marzo de 2021[26].
- La vida útil esperada, si el producto deja de ser seguro antes de lo razonable.

26. España. Tribunal Supremo (Sala de lo Civil, Sección 1.ª). Sentencia número 105/2021 de 1 de marzo de 2021. *ECLI:ES:TS: 2021:758*. Se trata de un caso referente a una prótesis de cadera que fue retirada del mercado debido a una tasa de fallos anormalmente elevada. Se afirma que cuando se detecta un posible defecto en una serie de producción, puede considerarse defectuoso el producto sin necesidad de probar el fallo concreto en la unidad implantada al demandante.

La existencia de defectos en los productos unido a la complejidad tecnológica de los productos inteligentes y la insuficiencia de mecanismos de control está generando escenarios en los que los daños de seguridad afectan de manera desproporcionada a quienes cuentan con menos recursos para prevenirlos o afrontarlos.

## 4. SEGURIDAD EXIGIBLE Y SEGURIDAD ESPERABLE: UNA DISTINCIÓN QUE CONSTITUYE UNA PIEZA ESENCIAL EN EL ENGRANAJE DE ACTIVACIÓN EL RÉGIMEN DE RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS

### 4.1. Introducción

El concepto de «seguridad que cabría legítimamente esperar» era el estándar «objetivo» de seguridad que estaba presente en la Directiva europea 85/374 —que fue traspuesto a nuestro ordenamiento jurídico español en los arts. 137 y ss. del TRLGDCU—. Este era el *criterio jurídico clave* del régimen de responsabilidad por productos defectuosos en Europa y en España. Un criterio que se demostró resultaba insuficiente. Esta Directiva de 1985 no definía qué era «seguridad esperable» en *productos de alto riesgo* como, por ejemplo: (i) marcapasos (ii) desfibriladores (iii) stents o (iv) implantes inteligentes. Tampoco mencionaba las particularidades (si las había) que se producían cuando las personas usuarias eran vulnerables por razón de su edad, o falta de capacidad, ni cuando la procedía presumir el defecto por riesgo en la serie.

La jurisprudencial del TJUE, a través de la doctrina Boston Scenif dictada en 2014 introdujo (re)interpretó el art. 6.1 de la Directiva de 1985 «elevando» el estándar de seguridad esperable a nivel «máximo» cuando se trata de productos implantables de alto riesgo. Pero lo verdaderamente interesante de esta doctrina jurisprudencial europea (*Boston Scientific)* es que transforma el concepto «seguridad esperable» «elevando su estándar para casos de especial vulnerabilidad». Un concepto que la nueva Doctrina de productos defectuosos de 2024 positiviza en el art. 7.1 h). Tras dicho logró, habrá que reivindicar que el legislador al trasponer dicha directiva a nuestro ordenamiento jurídico español eleve a rango legal dicha acertada doctrina jurisprudencial que toma en consideración el especial riesgo y especial vulnerabilidad de algunas personas usuarias.

Aunque la nueva Directiva por productos defectuosos no distingue, porque no usa literalmente los términos, «seguridad exigible» y «seguridad esperable»; en realidad, sí distingue entre el *nivel de seguridad que la persona consumidora puede legítimamente esperar y el cumplimiento de normas obligatorias*. Dicha distinción constituye, a mi juicio, dentro del régimen de responsabilidad por productos defectuosos, una pieza esencial en el engranaje de piezas que exige el régimen de responsabilidad para que prospere o no el derecho de la persona usuaria a obte-

ner una indemnización por los daños ocasionados por el producto defectuoso. En mi opinión, la «seguridad exigible» y «esperable», tal y como sucede ya con la accesibilidad, han de ser, de carácter universal («invisibles» a las personas usuarias) pues sólo así se logrará garantizar que los productos y su posible defectuosidad, no discrimine a nadie y, de paso, evitar la discapacidad digital —un término relacional con el entorno, los productos y los servicios digitales— llamados, por ley, a ser accesibles y seguros para todas las personas usuarias.

### 4.2. El caso *Boston Scientific* (C-503/13 y C-504/13): la vulnerabilidad como parámetro de seguridad que «refuerza el estándar de seguridad»

La relación entre la doctrina jurisprudencial del TJUE sobre el caso *Boston Scientific* (C-503/13 y C-504/13) y la vulnerabilidad del usuario se podría resume diciendo que: (i) la sentencia europea *parte de la vulnerabilidad del paciente*, aunque no lo diga expresamente (ii) los tribunales españoles *sí lo dicen expresamente* y lo usan para reforzar la protección, produciéndose una protección reforzada y (iii) el resultado es un *estándar de seguridad más alto y una responsabilidad más estricta* para los fabricantes. Entre las decisiones que han marcado un punto de inflexión en favor de reforzar el estándar de seguridad de los productos cuando hay personas vulnerables, cabría destacar el asunto *Boston Scientific* (C-503/13 y C-504/13). Aunque formalmente la sentencia resuelve dos asuntos/litigios planteados ante tribunales alemanes puesto que en ambos casos se trataba el mismo problema jurídico —la responsabilidad del fabricante (Boston *Scientific* tras considerar defectuoso el producto sanitario implantado —marcapasos y desfibriladores—) el TJUE decidió acumular ambos asuntos y dictar una única sentencia conjunta que dictó hace más de veinte años: el 5 de marzo de 2015. Tras esta sentencia, la Sala 4.ª del TJUE introdujo un criterio decisivo: se establece que, si un producto sanitario implantable pertenece a una serie con riesgo de defecto, puede considerarse defectuoso sin necesidad de probar el fallo individual.

La relación entre la sentencia *Boston Scientific* (TJUE, 5 de marzo de 2015) y la vulnerabilidad del usuario es directa y profunda: la sentencia amplía la protección del paciente precisamente porque reconoce su posición de especial vulnerabilidad frente a los productos sanitarios implantables**.** A juicio del Tribunal Europeo vulnerabilidad de las personas usuarias constituía (a juicio del tribunal europeo), constituye un elemento determinante del «estándar de seguridad exigible».

### 4.3. ¿Qué entiende el TJUE del caso *Boston Scientific* (C-503/13 y C-504/13) por «vulnerabilidad de la persona usuaria»?

Aunque en la STJUE del caso *Boston Scientific* (C-503/13 y C-504/13) no usa literalmente la palabra «vulnerabilidad»**,** su razonamiento se basa en esta idea:

- El paciente *no puede verificar,* por sí mismo, si un marcapasos o un desfibrilador implantado es seguro.
- *Depende totalmente del fabricante y de los profesionales sanitario*s.
- Un *fallo puede tener consecuencias gravísimas o mortales*.
- Las personas usuarias *no tienen capacidad técnica* para detectar un defecto ni para evitar el riesgo.

Por eso el Tribunal considera que estos productos requieren un *nivel de seguridad excepcionalmente alto.* Por vez primera, el TJUE estableció que, cuando un producto médico implantable pertenece a una serie con riesgo de defecto, puede considerarse defectuoso sin necesidad de probar un fallo individual.

### 4.4. ¿Qué aporta la Sentencia Boston Scenif?

La sentencia Boston Scenif «eleva» el nivel de seguridad exigible cuando el producto es un dispositivo médico implantable (marcapasos, desfibriladores, stents, etc.) y cuando la persona consumidora es vulnerable. Advierte, con enorme acierto, que:

1. La seguridad esperable es máxima (seguridad reforzada), como dice el TJUE; lo que significa que, el paciente tiene derecho a esperar un nivel de seguridad excepcionalmente alto, porque:

- El producto está dentro del cuerpo.
- El fallo puede ser mortal.
- La persona usuaria es totalmente dependiente del fabricante, porque no puede verificar la seguridad por sí mismo.

La mera existencia de un riesgo en la serie del producto implica que el producto en sí mismo es defectuoso, porque el Tribunal dice que no hace falta que el dispositivo concreto falle. Lo que significa, que si la serie presenta riesgo, el producto ya no ofrece la seguridad esperable. Lo que significa un cambio enorme: porque el defecto se presume por pérdida de confianza en la seguridad del producto.

La «seguridad esperable» incluye evitar cirugías innecesarias, ya que el TJUE considera que someter al paciente a una cirugía preventiva ya es un daño, porque parece lógico que la persona usuaria espere no tener que pasar por intervenciones adicionales. O lo que es lo mismo, no asumir riesgos quirúrgicos evitables.

Ahora bien, ¿por qué esta doctrina jurisprudencial europea está ligada a la vulnerabilidad de la persona usuaria? En mi opinión, porque «el estándar de

seguridad esperable "se calibra" según la vulnerabilidad de la persona consumidora y usuaria». Lo que significa, que en productos implantables:

- La/el usuaria/o no puede evaluar los riesgos del producto implantable.
- No puede sustituir el producto autónomamente, sino por medio de intervenciones quirúrgicas posteriores y evitables.
- No puede detectar defectos salvo que se le implante el producto.
- Depende totalmente del fabricante.

La defectuosidad del producto se evalúa en función de la «vulnerabilidad» elevando a nivel máximo la seguridad esperable la Directiva 2024/5238 porque se positiviza la doctrina jurisprudencial europea Boston Scenif[27]. Aunque, en mi opinión, hubiera resultado más correcto y adecuado incluir el término «universal» a la palabra «seguridad» (tal y como hacen la Ley de Dependencia y Discapacidad, al hablar de accesibilidad (universal); no me cabe duda de que dicho carácter universal resulta exigible y necesario para los productos dotados de IA[28]. Porque dichos productos han de garantizar la seguridad de todas las personas usuarias, tal y como establece el Reglamento (UE) 2023/988[29] —en el que expresamente se dice, se ha de atender a «las necesidades específicas y los riesgos que presenten para determinadas categorías de consumidores que puedan utilizar esos productos, en particular niños, personas mayores y personas con discapacidad»—, así como también exige que sea accesible la información (parágrafos 5, 23 y 73, especialmente). También ha de estar adaptadas las evaluaciones de seguridad de un producto a «las categorías de consumidores que vayan a utilizar el producto, en particular, mediante una evaluación del riesgo para los consumidores vulnerables, como los niños, las personas mayores y las personas con discapacidad, así como los efectos de las diferencias de género en la salud y la seguridad».

Considero, además, que la noción de «uso razonablemente previsible» permite corregir la discriminación que supondrían que quedasen fuera el ámbito

27. Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. Diario Oficial de la Unión Europea, 18 de noviembre de 2024, núm.2024/2853, pp. 1-40.
28. Definición de producto según Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo.
29. Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos. Diario Oficial de la Unión Europea, 23 de mayo de 2023, núm.135, pp. 1-65.

legal de aplicación las personas especialmente vulnerables, porque, respecto de ellas no hablamos de «uso razonable», sino de «uso razonablemente previsible». Y es que, el eje central en torno al cual giran las reglas de responsabilidad civil por productos defectuosos no está en la idea de que quien incumple sus obligaciones o quien infringe sus deberes de seguridad responde; sino que gira en torno la de «confianza» o «confiabilidad». Un producto es o no defectuoso, no porque el fabricante haya incumplido o porque hecho algo prohibido; sino por el hecho de que el producto haya de dejado de ser «confiable» para quien lo utiliza (el público en general, por tanto, todas las personas tengan la edad que tengan y, tengan la capacidad que tengan). Lo que significa, que el productor puede ser responsable incluso cumpliendo la ley, si el producto no alcanza la seguridad razonablemente esperada.

La Directiva 2024/5283 al ampliar la responsabilidad por productos defectuosos a los productos digitales (incluyendo los productos dotados de IA) directa o indirectamente lo que está haciendo es hacer que el concepto de «seguridad esperable» *gane peso*, porque: (i) la tecnología evoluciona más rápido que las normas, por lo que resulta esencial que el producto incluya las actualizaciones (ii) porque la Directiva exige valorar expectativas razonables sobre actualizaciones, ciberseguridad y funcionamiento autónomo y (iii) porque un producto puede ser defectuoso, aunque cumpla la normativa si no se comporta como un consumidor razonable esperaría. Así, por ejemplo: Un dispositivo médico con IA puede cumplir toda la normativa (seguridad exigible), pero si no se actualiza para corregir vulnerabilidades conocidas (por ejemplo, los sesgos discriminatorios en contra de la edad o de la discapacidad), puede considerarse defectuoso porque no ofrece la seguridad que el usuario razonablemente espera.

### 4.5. ¿Cómo se refleja esta vulnerabilidad de la persona usuaria en la sentencia europea *Boston Scientific*?

La STJUE del caso *Boston Scientific* (C-503/13 y C-504/13) constituye un ejemplo claro de cómo el Derecho europeo: (i) se reconoce la vulnerabilidad del paciente (ii) se eleva el estándar de seguridad (iii) se facilita la prueba del defecto y (iv) se amplía la responsabilidad del fabricante. Es La vulnerabilidad de las personas usuario es el fundamento implícito que justifica la protección reforzada que establece la sentencia. Y, aunque la sentencia del TJUE no usa la palabra «vulnerabilidad», los tribunales españoles *sí la han incorporado explícitamente* al interpretar casos de productos sanitarios y responsabilidad del fabricante. Los tribunales españoles han entendido que: (i) el paciente *no puede evaluar* la seguridad de un dispositivo implantado (ii) depende totalmente del fabricante y del sistema sanitario y (iii) el riesgo afecta a su *integridad física*, que es el bien jurídico más protegido. Por eso, cuando un producto sanitario implantable presenta

riesgo, los jueces aplican un criterio pro-consumidor, reforzado por la vulnerabilidad interpretando, en este sentido, los arts. 3 (El consumidor es la parte débil de la relación jurídica) y 8 (Derecho a la protección de su salud y seguridad**)** de la LGDCU: si *la persona consumidora es vulnerable y el producto afecta a su salud, el estándar de seguridad debe ser máximo.*

El TRLGDCU (Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios) introdujo en el art. 3 y en el art. 20.1, de manera expresa el concepto de «persona consumidora vulnerable» desde la reforma operada por el Real Decreto-ley 1/2021, de 19 de enero (dice el art. 3, «El consumidor puede encontrarse en situación de vulnerabilidad**,** por razones personales, económicas, sociales o de accesibilidad**.** Esta vulnerabilidad debe ser tenida en cuenta en la interpretación y aplicación de la norma» y añade el art. 20.1 en materia de información precontractual que: la información sea clara, comprensible y adecuada, teniendo en cuenta las necesidades de las personas consumidoras vulnerables). Tras introducir nuestro TRLGDCU *el concepto de persona consumidora vulnerable***,** dicho concepto: (i) *encaja perfectamente* con la lógica de la sentencia *Boston Scientific* (ii) *refuerza la protección del paciente* frente a productos sanitarios implantables, y (iii) obliga a los tribunales españoles a aplicar un estándar de seguridad y responsabilidad más estricto.

Tras esta doctrina jurisprudencial europea, y tras esta reforma de nuestra legislación nacional, queda claro que un paciente con un marcapasos o desfibrilador es un consumidor vulnerable porque:

- No puede evaluar la seguridad del producto.
- Depende totalmente del fabricante y del sistema sanitario.
- Un fallo puede poner en riesgo su vida.
- No tiene capacidad técnica para detectar defectos.

Después, de dicha reforma legal, los tribunales españoles no han dudado en advertir que: (i) «el paciente implantado se encuentra en una situación de especial vulnerabilidad»; (ii) «la confianza legítima del usuario en la seguridad del producto debe ser protegida», y que (iiii) «la mera posibilidad de defecto en productos de alto riesgo justifica medidas preventivas». Gracias a esta visión protectora:

- El/la paciente *no tiene que demostrar* que su dispositivo falló.
- Basta con que el producto pertenezca a una *serie con riesgo*.
- El *fabricante debe asumir la carga de demostrar la seguridad*; algo que resulta crucial porque la prueba del defecto suele ser muy difícil para la persona usuaria.

En conclusión, tras esta acertada doctrina jurisprudencial:

***a)*** *Se presume el defecto en el marcapasos y desfibrilador sin necesidad de probar el fallo individual.* El TJUE dice que, si un lote o serie de dispositivos presenta riesgo de defecto**,** *todos los dispositivos de esa serie pueden considerarse defectuosos*, aunque el del paciente que reclame no haya fallado. El marcapasos y los desfibriladores implantables en personas mayores, siendo las partes fue el caso que debatió la sentencia *Boston Scientific Medizintechnik GmbH* contra las aseguradoras alemanas (AOK Sachsen-Anhalt y Betriebskrankenkasse RWE)[30].

***b)*** *Se protege la confianza del paciente en el dispositivo. El TJUE afirma que el usuario tiene derecho a esperar que un producto implantado en su cuerpo: (i) funcione de forma segura durante años (ii) no requiera intervenciones quirúrgicas adicionales, y (iii) no ponga en riesgo su vida. La vulnerabilidad del paciente hace que «cualquier riesgo anormal» sea inaceptable.*

***c)*** *Se amplía el concepto de «daño».* El TJUE considera que los costes de sustitución del dispositivo (incluyendo cirugía) son indemnizables, incluso si el dispositivo no ha fallado. ¿Por qué? Porque someter a un paciente a una cirugía innecesaria ya es un daño**,** y el paciente está en una posición de especial fragilidad. *Y,*

***d)*** *Se refuerza la responsabilidad del fabricante.* El TJUE exige a los fabricantes: (i) controles más estrictos (ii) información más transparente y (iv) retirada preventiva de productos con riesgo.

### 4.6. La vulnerabilidad de las personas usuarias es el fundamento implícito que justifica la protección reforzada y la Directiva por productos defectuosos 2024/5283 positiviza esta doctrina del TJUE en la sentencia *Boston Scientific* (C-503/13 y C-504/13)

Tras la positivización de esta doctrina jurisprudencial en el artículo 7.2 h de la Nueva Directiva de Responsabilidad por Productos UE 2024/5283, la «vulnerabilidad» se convierte en un parámetro estructural del juicio de defectuosidad y en un mecanismo de adaptación del régimen de responsabilidad a los riesgos tecnológicos contemporáneos. Con la Directiva anterior (85/374/CEE), el

30. Tres años antes, el Tribunal Supremo había desestimó, en la sentencia de 27 de febrero de 2012 (STS núm. 45/2021) —que resolvía un recurso contra la sentencia del Juagado de Primera Instancia núm. 2 de mi ciudad (Granada), de 20 de febrero de 2026, la prescripción y la responsabilidad por producto defectuoso— la demanda interpuesta contra Boston Scientific por prescripción de la acción de responsabilidad de la Ley 26/1984. Esto es una protección extraordinaria, basada en que el usuario no puede asumir riesgos en productos vitales.

defecto se define en función de la «seguridad que cabe legítimamente esperar», una fórmula abierta que exigió un esfuerzo interpretativo por parte del TJUE y una sensibilidad especial en la trasposición del art. 3.1 de la Ley 22/1994 (actual art. 137 del RD Legislativo de la LGDCU): preceptos en los que se advierte que el producto defectuoso es aquel que «no ofrezca la seguridad que cabría legítimamente esperar». Pero la STJUE *Boston Scientific* (C-503/13 y C-504/13) marcó un punto de inflexión en la interpretación del concepto de producto defectuoso cuando el usuario pertenece a un grupo especialmente vulnerable. El litigio *Boston Scientific* versaba sobre marcapasos y desfibriladores implantables en los que se había detectado un potencial defecto de fabricación en una serie de productos. Aunque el dispositivo concreto implantado en el paciente no había fallado, el fabricante recomendó su sustitución preventiva. La cuestión prejudicial planteaba si, en tales circunstancias, el producto debía considerarse defectuoso.

El Tribunal de Justicia, en *Boston Scientific*, *introdujo una lectura especialmente exigente del concepto de producto defectuoso cuando el producto está destinado a personas usuarias vulnerables*. Una vulnerabilidad intrínseca que intensifica las expectativas legítimas de seguridad. El caso se refería, como más adelante se desarrollará, a un marcapasos y desfibriladores implantables, productos cuyo fallo puede comprometer de manera inmediata la vida del paciente. En dicha sentencia se entendió que el producto sanitario era defectuoso porque ocasionó un riesgo que resultaba inaceptable. Este tipo de productos sanitarios implantables de alto riesgo (me refiero a marcapasos o desfibriladores, por ejemplo, no deben causar daños y para el caso de que los produzcan se entenderán que entran dentro del ámbito de aplicación de la nueva Directiva por productos defectuosos. Felizmente, esta lógica ha sido incorporada, expresamente (y acertadamente, en mi opinión), en la Nueva Directiva de Responsabilidad por Productos (2024/5283/UE) en su artículo 7.2 h, al que más adelante me referiré una vez exponga, brevemente, el contenido de dicha resolución. El Alto Tribunal (TJUE) sostuvo que:

- La mera constatación de un riesgo potencial derivado de un defecto de fabricación en una serie de productos basta para considerar defectuoso el dispositivo concreto implantado.
- La evaluación del defecto debe realizarse atendiendo a las expectativas particularmente elevadas de seguridad que tienen los pacientes portadores de dispositivos médicos implantables.
- El estándar de seguridad no es uniforme, sino relacional**,** dependiente del tipo de usuario y de la función vital del producto.
- El TJUE subrayó que la evaluación del defecto debe tener en cuenta la vulnerabilidad del usuario**,** el carácter invasivo del producto y la gravedad.

La razón a la que obedeció este certero criterio jurisprudencial se debe al hecho de que para pacientes con dispositivos vitales, las *expectativas legítimas de seguridad son excepcionalmente elevadas*: un razonamiento que amplió la noción de «defecto» más allá de un fallo material concreto, hacia una concepción basada en un riesgo inaceptable para personas especialmente expuestas (esto es, especialmente vulnerables). Esta doctrina supuso un desplazamiento desde una concepción estática del defecto hacia una concepción contextualizada**,** donde la vulnerabilidad del usuario se convierte en un elemento determinante del juicio de defectuosidad.

### 4.7. El acierto de positivizar la doctrina Boston Scientific en la Nueva Directiva de Responsabilidad por Productos. Consecuencias sistemáticas de la incorporación del criterio de vulnerabilidad en la teoría general del concepto de «defecto»

La positivización del criterio de vulnerabilidad en la teoría general de concepto de defecto tiene efectos relevantes en la teoría general del defecto porque:

- Reconfigura el estándar de diligencia del fabricante**,** que debe anticipar las necesidades de seguridad reforzada de las personas usarías vulnerables.
- Facilita la prueba del defecto en sectores de alto riesgo, al permitir que la mera exposición a un riesgo inaceptable sea suficiente.
- Refuerza la protección de la persona consumidora en ámbitos como dispositivos médicos, productos infantiles, tecnologías asistivas o productos dirigidos a personas mayores.
- Armoniza la jurisprudencia y normativa, reduciendo, por tanto, la incertidumbre interpretativa y consolidando un estándar europeo coherente.

### 4.8. El legislador español no podrá ignorar la doctrina Boston Scientific: tendrá que integrarla, consolidarla y positivizarla

El legislador español no puede ignorar la doctrina jurisprudencial europea sobre *Boston Scientific*. La Directiva obliga a positivizarla**.** El legislador español deberá convertir en ley: (i) la *presunción de defecto por riesgo en la serie (ii)* la protección reforzada del *paciente vulnerable (iii) l*a indemnización de *cirugías preventivas y (iv)* la obligación del fabricante de aportar *información técnica.*

En mi opinión, la doctrina Boston Scientific debería ser incorporada y convertida en ley obligatoria. El legislador español no sólo no eliminará dicha doctrina, ni la reducirá ni la dejará en aplicación jurisprudencial, sino que la positivi-

zará y la reforzará al trasponer la Directiva por productos defectuosos porque la nueva Directiva europea le «obliga» a ello.

4.8.1. *Transformar el concepto de producto.* Cambios que debería incluirse en la trasposición. La Directiva amplía radicalmente qué se considera «producto». En la trasposición de la directiva se debería incorporar los productos sanitarios digitales e inteligentes, como marcapasos o desfibriladores con software. Es decir, se debería incluir: (i) software (haciendo expresa alusión a los dispositivos médicos) (ii) actualizaciones y parches (iii) productos conectados con sistemas de IA, e (iv) (IoT, wearables, dispositivos implantables inteligentes).

4.8.2. *Presumir el defecto y causalidad.* Cambios en la carga de la prueba. La Directiva introduce presunciones legales que España deberá incorporar. La Directiva introduce presunciones que España deberá incorporar expresamente: (i) presunción de *defecto* cuando el producto pertenece a una serie con riesgo (*Boston Scientific*) (ii) presumir la relación de *causalidad* cuando el daño es típico del defecto y (iii) presumir el defecto si el fabricante *no aporta información técnica*. Por tanto, para convertir en ley lo que hoy es jurisprudencia del TJUE, se debería Presumir el defecto y la causalidad en las hipótesis a que me he referido; convirtiendo en ley escrita lo que hoy es doctrina jurisprudencial del TJUE (*Boston Scientific*).

4.8.3. *Protección reforzada de la persona consumidora vulnerable. Cambios en la protección de la persona consumidora.* La Directiva por productos defectuosos exige una protección reforzada para determinadas personas usuarias sin capacidad técnica. En este sentido, se debería ampliar el concepto de vulnerabilidad de las personas consumidoras contenido en el art. 3 TRLGDCU dando cabida a: *(i)* vulnerabilidad técnica (usuarios que no pueden evaluar la seguridad del producto) *(ii)* vulnerabilidad sanitaria (pacientes con dispositivos implantables). *LO que* obligando a reforzar la información de manera clara y accesible y más trasparente e imponiendo que dicha información no sea digital, sino que ofrezca alternativas no digitales a personas vulnerables, como, por ejemplo, a las personas mayores o de edad avanzada. Incluso, considero que sería conveniente introducir el concepto de hipervulnerabilidad haciendo alusión a pacientes, personas mayores con productos implantados y concibiendo que la edad o la falta de capacidad unidas a lo digital comporta una mayor vulnerabilidad de las personas consumidoras usuarias. Lograr incorporar dicho cambio en nuestra legislación permitirían encajar y elevar a rango legal la lógica de *Boston Scientific*.

4.8.4. *Ampliar el catálogo de daños indemnizables. Cambios en los dañoso indemnizables.* La Directiva en España debería incluir de manera explícita: *(i)*

daños psicológicos o de dependencia emocional (ii) daños ocasionados por la *pérdida de datos (iii)* daños por *intervenciones quirúrgicas preventivas* (como en *Boston Scientific*) (iv) daños *derivados de fallos de* software o actualizaciones y (v) daños por *ciberseguridad.* Lo dicho, supondría modificar el régimen de daños del TRLGDCU y de nuestro régimen de responsabilidad civil tipificado en nuestro Código Civil. Lograrlo, consolidaría la doctrina *Boston Scientific* sobre indemnización por cirugía preventiva.

4.8.5. *Ampliar los sujetos responsables. Cambios en los sujetos responsables.* La Directiva por productos defectuosos, amplía quién puede ser responsable. En la trasposición a nuestro ordenamiento jurídico español, se debería extender la responsabilidad por productos defectuosos a: *(i)* fabricantes de software (ii) proveedores de actualizaciones (iii) importadores de productos digitales (iv) plataformas que controlan el funcionamiento del producto y (v) fabricantes de IA integrada. Esto rompe el modelo clásico centrado solo en el fabricante físico.

## 4.9. El defecto equivale a la «falta de seguridad que razonable y mínimamente cabría esperar»

El defecto equivale, en la Directiva (UE) 2024/2853 sobre responsabilidad por daños causados por productos defectuosos**,** a la «falta de seguridad que el público en general puede, razonablemente, esperar». Esta idea de la «seguridad que cabe esperar» es el núcleo del concepto, en torno al cual cabría preguntarse si el estándar tradicional del consumidor medio es el que resulta operante o si, por el contrario, debe entenderse que resulte inoperante, porque, un producto que aprovecha la inexperiencia de una persona vulnerable (como puede ser niñas, niños[31] o personas mayores) debe calificarse como inherentemente defectuoso por defraudar la seguridad mínima exigible a sus usuarios, sea cual sea su vulnerabilidad.

El concepto de seguridad constituye el eje sobre el que gira la noción de defecto tanto en la Directiva 85/374/CEE como en la nueva regulación. Conforme al artículo 6.1, el criterio central continúa siendo el de la falta de seguridad que legítimamente cabe esperar, atendiendo a todas las circunstancias del caso. No obstante, en el entorno digital, este estándar debe valorarse teniendo en cuenta factores específicos como la capacidad de aprendizaje del sistema, su

31. F.M.B. (2022, 25 de julio) «Un robot le rompe un dedo a un niño en Rusia durante una partida de ajedrez». ABC. https://www.abc.es/tecnologia/robot-ruso-rompe-dedo-nino-partida-ajedrez-20220725123225-nt.html. (Consultado: 25 noviembre de 2025). Es un caso que genera debate sobre la seguridad y supervisión necesaria en robots utilizados en actividades con menores.

grado de autonomía, la previsibilidad de su comportamiento, las actualizaciones posteriores a la puesta en circulación o la interacción con otros productos o servicios digitales. Esta formulación parece clara, pero se ha demostrado que existen tensiones cuando se aplica principalmente a productos caracterizados por una elevada complejidad técnica o el avance de la ciencia. Así lo refleja la interpretación del Tribunal de Justicia de la Unión Europea, en el asunto C-621/15 (N.W./Sanofi Pasteur MSD y otros) de 21 de junio de 2017[32], que evidencia las dificultades probatorias que pueden.

### *4.9.1. La «seguridad» entendida como un concepto dinámico*

El producto debe seguir siendo seguro no solo cuando se vende, sino también durante el tiempo en que razonablemente se espera que funcione (durante su vida útil). Esto es especialmente relevante para: (i) productos conectados (ii) *software* integrado (iii) dispositivos que requieren actualizaciones de seguridad o (iv) productos con IA o algoritmos adaptativos. El art. 7.2.h «refuerza» que el estándar de seguridad esperable incluye: (i) durabilidad **(**ii) fiabilidad (iii) resistencia al deterioro (iv) continuidad de las medidas de seguridad y (v) actualizaciones necesarias para mantener la seguridad. No basta con que el producto sea seguro al inicio: debe seguir siéndolo. La falta de seguridad implica para el productor (fabricante, importador o quien se presente como tal en el mercado) que es responsable de los daños causados por un producto defectuoso, sin necesidad de demostrar negligencia: basta con demostrar que el producto era defectuoso, que causó el daño y que dichos daños surgieron dentro del tiempo legalmente previsto. Luego, es preciso que el producto (sea o no, inteligente) cumpla un *estándar de seguridad: lo que significa, demostrar que un producto ofrece el nivel de seguridad que una persona razo*nable puede esperar. En la práctica, esto no se logra con una sola acción, sino con un conjunto de medidas que abarcan todo el ciclo de vida del producto. Es decir, habrá que demostrar: (i) que el diseño del producto fue seguro, desde el inicio (ii) que se realizaron los ensayos y pruebas de conformidad (iii) que el usuario sabe cómo usarlo, porque dispone de las instrucciones y advertencias claras, y que (iv) que el fabricante ha realizado los controles de calidad necesarios e implementa-

32. Tribunal de Justicia de la Unión Europea. Asunto C-621/15, N.W./Sanofi Pasteur MSD y otros. Sentencia de 21 de junio de 2017. *ECLI:EU:C:2017:484*. Se aborda la dificultad de acreditar el nexo causal entre una vacuna contra la hepatitis B y el desarrollo de esclerosis múltiple en ausencia de consenso científico. El TJUE, interpretando el art. 4 de la Directiva 85/374/CEE, admite que el juez pueda basarse en presunciones judiciales sustentadas en indicios sólidos, concretos y concordantes, siempre que no se produzca una inversión automática de la carga de la prueba. Asimismo, destaca que el concepto de defecto debe valorarse conforme a las legítimas expectativas de seguridad del público, particularmente exigentes en el ámbito sanitario. Esta orientación se proyecta en la Directiva (UE) 2024/2853, que flexibiliza la prueba del nexo causal cuando la complejidad técnica la haga excesivamente difícil para el perjudicado.

do los controles internos y auditorías para asegurarse que el producto lanzado al mercado es seguro. Una seguridad que deberá ser vigilada post-comercialización, incluso después de vender el producto, supervisando incidentes o quejas, retirando o corrigiendo los productos si se detectan riesgos o comunicando a las autoridades cuando sea necesaria la retirada del mismo.

#### *4.9.2. La obligación y responsabilidad del productor de prever la evolución del riesgo*

El productor debe anticipar (i) los riesgos derivados del envejecimiento del producto (ii) los riesgos derivados de la falta de actualizaciones del producto, y (iii) los riesgos derivados de cambios previsibles en el entorno digital. La Directiva reconoce que un producto puede volverse defectuoso *a posteriori* si deja de cumplir los requisitos de seguridad por falta de mantenimiento, soporte o actualizaciones; lo que significa, que el productor puede ser responsable si: (i) no proporciona las actualizaciones de seguridad necesarias (ii) si no informa sobre riesgos que aparecen con el tiempo y (iii) si no diseña el producto para mantener un nivel razonable de seguridad durante su vida útil. Con la nueva Directiva de 2024 se produce una ampliación respecto al estándar de seguridad esperable (conforme al establecido en la Directiva de 1985, que no contemplaba productos digitales ni riesgos evolutivos) lo que me parece un enorme acierto especialmente para los colectivos más vulnerables.

## 5. SEGURIDAD EXIGIBLE Y SEGURIDAD ESPERABLE A TRAVÉS DE EJEMPLOS: CHATBOT CONVERSACIONES Y ROBÓTICA ASISTENCIAL TRANSFORMAN EL ÁMBITO DE ATENCIÓN Y CUIDADO DE LAS NIÑAS, NIÑOS Y ADOLESCENTES Y PERSONAS MAYORES

Los chatbot conversacionales y la robótica asistencial está transformando el ámbito de atención y cuidado de las niñas, niños y adolescentes. También, el ámbito geriátrico transformándolo de forma profunda y, ofreciendo soluciones innovadoras para mejorar la calidad de vida y la atención de las personas. La apuesta, en favor de la geriatrónica en países como Alemania, China, Japón y Corea del Sur, se debe: (i) al *déficit de personal sanitario* (la escasez de cuidadores está llevando a explorar soluciones tecnológicas) (ii) al *envejecimiento acelerado* (Alemania es una de las sociedades que envejece más rápidamente en Europa) (iii) a la incorporación de la mujer al trabajo y (iv) a la *innovación aplicada*: se busca que los robots no solo asistan, sino que también humanicen el cuidado mediante interacción y apoyo emocional[33]. La *población envejece* y,

33. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). *Inteligencia Artificial…*, *op. cit.*, pp. 199 y ss.

en un futuro no muy lejano, *habrás más personas con necesidad de ser cuidadas que personas que puedan dedicarse a cuidarlas*. Los robots asistenciales son ya una realidad, dentro y fuera de nuestras fronteras (cabe citar otros, Ari, Airbo, Buddy» (colega, en inglés)**,** Dani-chan, Dinsow, ElliQ, Giraff, MiRo, NHoA, Oldbot, Paro, Parlo, Pepper, Sota, Spot Mini, NeCoRo, Temi**,** Paro, Parlo, Misty, Geras, GriaffPllus, «Sueca» y, «Felipe», entre otros. Estos robots asistenciales han llegado para quedarse y para formar parte ya del día a día en hospitales, geriátricos y algunos hogares —la brecha robótica existe, pero cada día son más asequibles y por esta razón cada día su uso está más extendido—.

Las posiciones enfrentadas sobre el impacto de la robótica asistencial inteligente en las personas mayores distan mucho de ofrecer una única solución al problema que deberá ser analizado desde el punto de vista de la responsabilidad civil[34] y desde una óptica legal, ética y moral son imprescindibles. Habrá que determinar, en definitiva, a estos avances tecnológicos de un marco jurídico adecuado, que aporte seguridad y minimice los riesgos en materia de derechos fundamentales y los asociados a los daños derivados de eventuales fallos de los sistemas inteligentes. A la hora de determinar el posible defecto del producto robótico habrá que atender a aclarar dos conceptos: «seguridad exigible» y «seguridad esperable». Antes de pasar a aterrizar, exactamente, en qué consisten, vaya por delante, el hecho de que puede suceder, en la práctica, que *un robot* cumpla con todas las exigencias obligatorias que derivan de la seguridad exigible *y que, aun así,* no sea adecuado para convivir con personas mayores *(si es que no asegura la seguridad esperable)*.

### 5.1. «Seguridad exigible» (obligatoria)

La seguridad exigible es la seguridad que puede legítimamente esperar la persona usuaria. Es la seguridad que debe garantizar, desde el punto de vista legal, el productor (encargado de diseñar el producto). Este tipo de seguridad hace referencia al cumplimiento obligatorio de: (i) la normativa técnica aplicable (reglamentos sectoriales, normas armonizadas, requisitos de seguridad) (iii) el marcado CE y las evaluaciones de conformidad (iii) las obligaciones de vigilancia del mercado y retirada de productos y (iv) los requisitos específicos para productos digitales, *software* y sistemas con IA, que la Directiva incorpora expresamente. Su incumplimiento, puede bastar para considerar defectuoso el producto. Lo

34. Sobre el particular, *vid.*, MÉNDEZ SERRANO, M., «Derechos Fundamentales y personalidad jurídica de los robots: ¿para qué?, *Revista de Derecho Privado y Constitución,* n.º 44, (2024), pp. 52 y ss.; MÉNDEZ SERRANO, M., «La singularidad de las máquinas y su impacto en el carácter defectuoso de la IA generativa», *Actualidad Civil, La Ley,* número 1, (enero-2026), pp. 1-36 y, QUESADA PÁEZ, A. (2026). «La atribución de responsabilidad civil por actos de sistemas autónomos de inteligencia artificial, desafíos para el derecho privado». *InDret* 1/2026.

que implica, que, si el productor incumple la normativa obligatoria; el producto puede considerarse defectuoso *per se*, porque no alcanza el nivel mínimo de seguridad legalmente exigido.

La Directiva exige un nivel reforzado de seguridad porque: (i) el producto interactúa físicamente con personas (ii) porque las personas usuarias pueden ser vulnerables (iii) porque el producto digital e inteligente incorpora *software*, sensores y, cámaras (ii) porque la IA asegura la interconectividad con el IoT y (iv) un mal funcionamiento puede causar daños graves que afecten a la seguridad: física, digital, funcional y accesibilidad. Me explico.

*5.1.1. Seguridad física*, es decir, que el robot sea seguro, desde el punto de vista físico sin causar daños a quienes lo utilicen. Casos como el que se hizo viral en 2022 cuando un robot le rompió un dedo a un niño ruso —durante una partida de ajedrez—[35] o la muerte de una paciente tras una cirugía robótica (con el robot davinci) recuerdan que resulta fundamental controlar este tipo de seguridad en el producto teniendo en cuenta la sobreexposición de su usuario.

Aunque la cirugía robótica ofrece ventajas importantes —menos dolor, recuperación más rápida y mayor precisión— no está exenta de riesgos, y estos pueden ser graves cuando ocurren. El uso del robot Da Vinci en operaciones está teniendo un éxito indudable, pero, esta cirugía robótica está ocasionando fallos de seguridad que ocasionan en pacientes lesiones[36] y, hasta muertes. La Administración de Alimentos y Medicamentos de EE. UU. (FDA) mantiene una base de datos con miles de reportes de incidentes, que incluyen desde errores menores hasta lesiones graves y muertes**.** Junto a la formación del cirujano que lo utilice y la supervisión y mantenimiento y puesta al día del equipo, resulta fundamental, evitar los posibles fallos técnicos de seguridad que se han producido ya en varias ocasiones. En caso del hospital de Florida, EE.UU. en 2024 (en el District Court, Southern District of Florida. Asunto 9:24-cv-80137-DMM, Sultzer v. Intuitive Surgical, Inc. Sentencia de 6 de febrero de 2024), dio la vuelta al mundo y se hizo viral. El juzgado resolvió la demanda interpuesta por el esposo de una paciente que falleció tras ser operada por el robot Da Vinci.

35. F.M.B. (2022, 25 de julio) «Un robot le rompe un dedo a un niño en Rusia durante una partida de ajedrez». ABC. https://www.abc.es/tecnologia/robot-ruso-rompe-dedo-nino-partida-ajedrez-20220725123225-nt.html. (Fecha de consulta: 25 noviembre de 2025).

36. En otras ocasiones, los problemas que ha presentado el Robot Da Vinci han sido mecánicos o de software. Por ejemplo, instrumentos que se congelan, se mueven de forma errática o se carbonizan durante la cirugía: pérdida de piezas dentro del cuerpo del paciente (por ejemplo, agujas o fragmentos de instrumentos), o complicaciones quirúrgicas graves, como pérdida excesiva de sangre, o lesiones en vasos sanguíneos o nervios principales**.**

> En septiembre de 2021, Sandra Sultzer fue intervenida en un hospital de Florida (EE.UU). En concreto, en el Baptist Health Boca Ratón Regional Hospital en Florida de Estados Unidos. Durante la cirugía, el dispositivo desarrollado por la empresa Intuitive Surgical, Inc. (ISI), le provocó lesiones graves, como una quemadura y un desgarre en el intestino delgado. Las lesiones sufridas provocaron que Sandra requiriera cirugías correctivas en los próximos meses para tratar de aliviar los dolores abdominales y la fiebre; resultando finalmente, en febrero de 2022, su muerte**.** Lo que hizo que el esposo, ahora viudo, Harvey Sultzer, presentara una demanda contra Intuitive Surgical, Inc. (ISI).
>
> La demanda se centra en la existencia de un «defecto de diseño» en los instrumentos quirúrgicos del robot, en particular *en las tijeras monopolares* cuyo aislamiento era insuficiente, lo que permitía la fuga de electricidad mediante un efecto arco hacia tejidos internos, provocando quemaduras inadvertidas para el cirujano. La muerte de Sandra fue una tragedia irreparable. La familia podría buscar una compensación por los daños económicos (gastos médicos, pérdida de ingresos) y no económicos (dolor y sufrimiento, pérdida de compañía). En este caso se alega negligencia y responsabilidad del producto, buscando reparación por daños personales, financieros y emocionales. Pero lo más más destacable (y yo diría que grave) es que en la demanda presentada por Harvey Sultzer señala que el fabricante (Intuitive Surgical) ya tenía conocimiento previo de las fallas en el dispositivo da Vinci. Varias investigaciones realizadas por la Administración de Alimentos y Medicamentos (FDA), entre el 2009 y 2011, advirtieron sobre anomalías, incluyendo problemas de aislamiento que podían provocar «fugas de corriente», sin embargo; la compañía nunca emitió advertencias a los pacientes o usuarios. La decisión final dependerá de si el tribunal considera que el fabricante tenía o no el deber de advertencia a la paciente de los fallos que presentaba el producto[37].

En este caso, el fabricante d*ebería haber informado y advertido no sólo al operador final (distribuidor, hospital —y este al cirujano— de las fugas de electricidad de las tijeras del robot Da Vinci o debería de haber* recibido dicha información, también, la paciente. ¿De haberla conocido, hubiera aceptado operarse por medio de esta cirugía robótica? En mi opinión, respecto a las personas consumidores vulnerables/hipervulnerables el «estándar de información» de los posibles fallos de seguridad del producto (por ejemplo, en el uso de la cirugía del Robot

37. Sobre el robot Da Vinci en Venezuela y la regulación contenida en los arts. 1196 y 1997 del código venezolano, «El impacto legal y ético de la cirugía robótica: el caso de Sandra Sultzer. Información disponible en la siguiente URL: *vid.* https://www.gacetalegal.com/la-cirugia-robotica-el-caso-de-sandra-sultzer-y-el-da-vinci/?utm_source=copilot.com (fecha de consulta: 10 marzo 2025).

Da Vinci) debe ser «el más alto posible». La Directiva (UE) 2024/2853 sobre responsabilidad por daños causados por productos defectuosos impone deberes de información al fabricante**,** pero no establece un deber general de «informar al público» sobre fallos de seguridad (de lo que se ocupa el Reglamento (UE) 2023/988 de Seguridad General de los Productos **(**ex arts. 9, 20 y 34); lo que significa que, en principio, no está obligado a informar al usuario (paciente) final. El deber de informar de la Directiva por productos defectuosos se dirige a operadores concretos dentro de la cadena de suministro, especialmente cuando el fabricante está fuera de la UE. Luego, el «deber de advertencia del fabricante», contenido en la Directiva por productos Defectuosos, respecto de los fallos de seguridad y de diseño del producto», se satisface *informando únicamente al hospital o al cirujano que va a utilizar el producto*[38]. El art. 7.2 h) a) de la Directiva (UE) 2024/2853 no crea un deber autónomo de informar a las personas consumidoras y usuarias finales sobre fallos de seguridad del producto**,** aunque sí puede influir indirectamente en la valoración del defecto si el producto falla lo que hará que los fabricantes eleven el estándar de seguridad tomando en consideración a los colectivos especialmente vulnerables.

*5.1.2. Seguridad digital, lo que significa que el robot sea seguro, desde el punto de vista digital incluyendo* la protección de datos, la ciberseguridad, la integridad del software y la gestión segura de comunicaciones. Sobre el particular, existen normas técnicas y leyes que obligan al fabricante a garantizar, lo que significa que si el robot no cumple con dichas obligaciones legales no podrá comercializarse. Numerosa es la regulación legal que contempla este requisito de seguridad (*vid.*, RGPD —obliga a proteger los datos personales, especialmente sensibles como la salud—, LOPD —traspone y refuerza, en España la normativa de protección de datos—, Directiva NIS2 [UE] —establece requisitos de ciberseguridad— y Reglamento y Directiva de Maquinas). Entre las normas obligatorias en robótica, cabría citar:

- ISO 13482 (robots de asistencia personal), que exige seguridad funcional y control seguro
- IEC 61508 (seguridad funcional), que obliga a garantizar integridad del *software*.

38. La Directiva establece que siempre debe existir un operador económico responsable dentro de la UE. Por ello, cuando el fabricante detecta fallos de seguridad o defectos relevantes, su deber de información se dirige principalmente a: (i) importador o representante autorizado en la UE, cuando el fabricante está fuera de la Unión, (ii) prestadores de servicios logísticos, si no existe importador o representante autorizado, (iii) plataformas en línea que actúen como fabricante, importador, distribuidor o intermediario en determinadas condicione. Estos actores pueden ser considerados responsables del producto defectuoso y, por tanto, deben recibir la información necesaria para gestionar riesgos, retiradas o reclamaciones.

- ISO/IEC 27001 (seguridad de la información): no siempre obligatoria, pero sí referencia para cumplimiento.

Que el producto ofrezca este tipo de seguridad, no resulta opcional, sino obligatorio (según dicha normativa); lo que significa que los robots asistenciales deben ofrecer:

- Protección frente a posibles hackeos o accesos remotos no autorizados.
- Cifrado de comunicaciones y datos almacenados.
- Control de permisos y autenticación.
- Gestión segura de actualizaciones de software.
- Registro y trazabilidad de eventos.
- Protección de datos personales según RGPD.
- Prevención de manipulación del comportamiento del robot.

Entre las obligaciones que le impone dicha normativa al productor; se encuentran:(i) la confidencialidad de los datos (ii) la integridad del sistema (iii) la protección frente a accesos no autorizados (iv) la resistencia a ciberataques (v) la gestión segura de actualizaciones y (vi) el cumplimiento de la normativa de protección de datos. El objetivo que persigue este tipo de seguridad es lograr que las personas usuarias estén protegidas:

- Frente a accesos no autorizados (hackeos).
- Frente a manipulaciones psicológicas que puedan causar daño. *Es decir, que el robot, incorpore un sistema de actualizaciones* y, si no lo incorpora y pierde seguridad por falta de actualizaciones, el producto se consideraría defectuoso).
- Frente a actualizaciones del software para que el producto ofrezca la seguridad durante toda su vida útil.

*5.1.3. Seguridad funcional, es decir, que el robot sea seguro, desde el punto de vista funcional)*. Resulta, también, fundamental, que el robot prevé el posible *uso incorrecto previsible (que el robot, tal y como ha sido diseñado disponga de un posible uso incorrecto, teniendo en cuenta que las personas usuarias tienen capacidades cognitivas disminuidas)*. Por ejemplo: una persona mayor puede apoyarse en el robot aunque no sea su función; el productor debe preverlo.

- Que no ejecute acciones inesperadas.
- Que no falle en tareas críticas (por ejemplo, ayudar a levantarse).
- Que tenga mecanismos de parada segura.

### 5.2. «Seguridad esperable»

La «seguridad esperable» trata de dar respuesta a la pregunta ¿qué nivel de seguridad puede esperar razonablemente el público que utiliza el producto? O lo que es lo mismo, ¿qué espera la sociedad de este producto? La Directiva 2024/5283 busca corregir una limitación histórica: el estándar de seguridad basado en un «usuario medio» dejaba desprotegidos a colectivos vulnerables. La nueva Directiva reconoce que:

- La tecnología actual puede excluir o poner en riesgo a ciertos usuarios.
- La protección del consumidor debe ser inclusiva y accesible.

Este tipo de seguridad debe evaluarse desde la perspectiva del usuario real. Es decir, debe atender a las necesidades de las personas vulnerables. Por esta razón, *la seguridad esperable* es la deseable, desde un punto de vista ético y, de buenas prácticas comerciales. Es la seguridad que no siempre está regulada en normas técnicas, pero que cualquier persona usuaria, familia y profesionales esperan (razonablemente) de un robot que convive con personas vulnerables (personas mayores) con el objetivo de garantizar bienestar y confianza. Esta seguridad, incluiría:

#### *5.2.1. Seguridad emocional*

La dependencia emocional de niñas, niños, adolescentes y de personas mayores y personas con discapacidad hacia el entorno digital, especialmente en formas como asistentes virtuales, Chatbot, sistemas inteligentes y con IA Generativa y robots sociales de carácter asistencial; es un aspecto crucial. Casos como el que se hizo viral en 2025, cuando un adolescente se enamoró de un Chatbot y terminó suicidando[39] (re)abren el debate acerca del carácter (o no)

39. El 26 de agosto de 2025 los padres de Adam Raine presentaron demanda ante la Superior Court de San Francisco contra OpenAI, Inc., OpenAI OpCo, LLC, OpenAI Holdings, LLC y Sam Altman por los daños derivados del suicidio del menor (16 años). El complaint articula, entre otras, acciones de responsabilidad por producto (defecto de diseño y falta de advertencia), negligencia, competencia desleal (UCL) y wrongful death, y sostiene que ChatGPT habría intensificado la ideación suicida durante intercambios sostenidos, proporcionando orientación lesiva. El procedimiento se halla en fase inicial y aún no hay pronunciamiento sobre el fondo del asunto: ¿era previsible lo sucedido?, ¿se entenderá producto defectuoso el sofware? Limón, R. (2025, 31 de mayo). «¿Puede ser la IA responsable legal de la muerte del adolescente que se enamoró de un avatar? El País. https://elpais.com/tecnologia/2025-05-31/puede-ser-la-ia-responsable-legal-de-la-muerte-del-adolescente-que-se-enamoro-de-un-avatar.html. (Consultado: 25 noviembre de 2025). *Vid.*, Complaint, Raine v. OpenAI, Inc., OpenAI OpCo, LLC, OpenAI Holdings, LLC y Samuel Altman, Superior Court of the State of California, County of San Francisco, s. n.º

defectuoso de este tipo de productos que (sobre)exponen a las personas usuarias más vulnerables no sólo a riesgos físicos (lesiones o muertes) sino, también, y fundamentalmente a sufrir daños emocionales: de dependencia psicológica. El hecho de que estos sistemas dotados de Inteligencia Artificial pueden llegar a convertirse en una tecnología de apoyo, cuidado y atención para niñas, niños, personas mayores y personas con dependencia y discapacidad. Entre las bondades que ofrecen los productos, servicios y entornos inteligentes; cabría destacar:

(i) *Aumento de la estimulación cognitiva y creatividad*, mediante la creación de cuentos personalizados con sus recuerdos o con los temas que le gustan o más le interesan generar imágenes o música que evoquen emociones positivas,

(ii) *apoyo emocional*, mediante chabots empáticos que conversan, escuchan y acompañan o la generación de cartas o mensajes para mantener vínculos familiares. Todo ello, sin duda, produce un claro impacto positivo en lograr preservar la memoria, mediante la crear álbumes digitales con narraciones generadas a partir de fotos o la recreación de historias familiares o biografías con ayuda de IA,

(iii) prevención de riesgos de caídas, enfermedades, depresión o síntomas que producen enfermedades como el Alzheimer. A través de asistentes virtuales se puede reconocer y o registrar estados de ánimo a fin de prevenir la depresión, la soledad y el suicido —por ejemplo, un asistente virtual, podría diseñarse para responder con empatía, adaptando emociones y sentimientos a través de la voz o incluso mediante un avatar con gestos y tonos de voz que transmitan cercanía—,

(iv) *seguimiento personalizado* con el objetivo de *facilitarles el día a día*, les ayuda a la interacción socialmente con otras personas usuarios. Por ejemplo, gracias a su utilización se pueden controlar dispositivos tecnológicos del hogar, generar notas, programar citas sociales o médicas, acompañar en el día a día, enviar mensajes, hacer pedidos de compras y ocio, o planificar rutas y localización de espacios inclusivos (en el caso de que tengan, por razón de la edad, algún tipo de dependencia o discapacidad). Así, por ejemplo, mediante el uso de «Siri» (a través del cual, se puede pedir que lea una la lista de cosas que debe llevar, y comprueba tenerlo todo, gestionar su agenda y recordatorios en el móvil. Mediante, el uso de «Alexa» (a quien resulta muy cómodo pedirle que reproduzca música de ambiente, o con quien conversar). «Alexa Together» es un ejemplo de un producto

(presentada 26-ago-2025). Información disponible en la siguiente URL: Disponible en: https://www.courthousenews.com/wp-content/uploads/2025/08/raine-vs-openai-et-al-complaint.pdf (fecha de consulta: 27 agosto 2025).

> inteligente para los hogares de las personas mayores, que integra funciones como alertas de actividad, asistencia en emergencias y control remoto de recordatorios. Su capacidad para adaptarse a las necesidades de la persona usuaria y ofrecer un soporte proactivo, junto con la compatibilidad con dispositivos de detección de caídas; lo que la convierte en una herramienta tecnológica muy sugerente para quienes viven solas en su casa.

Ahora bien, el uso excesivo de asistentes virtuales o apps puede reducir la autonomía. Además, puede llevar a la pérdida de habilidades cognitivas o físicas si se reemplazan tareas cotidianas por tecnología, tal y como tuve ocasión de demostrar páginas atrás. Aunque la IA puede ofrecer compañía y apoyo, también puede generar ciertos riesgos emocionales y psicológicos si no se gestiona adecuadamente. En mi opinión, y la de quienes, llevan tiempo analizando estas interacciones hombre-maquina; el evidente riesgo de dependencia emocional o psicológica entre las personas mayores (también, las personas con discapacidad sean cual sea su edad) es innegable[40].

Centrando mi atención en caso sucedido en 2025, con la lamentable muerte (presuntamente por suicidio) de un adolescente: la madre del chico advirtió que las conversaciones mantenidas con el Chatbots (Seltzer v. Character.ai —*García v. Carácter Technologies Inc.*—) eran del todo improcedentes. Un caso que evidencia la vulnerabilidad de las niñas, niños y adolescentes cuando interactúan generando relaciones afectivas o íntimas con chatbots dotados de IA. El caso surge tras la muerte por suicidio de Sewell Seltzer III, un adolescente de 14 años que mantuvo durante meses conversaciones intensas y emocionalmente intensas con un chatbots de Character.ai. Su madre, Megan García, acusa a la empresa de negligencia y de haber permitido que el Chatbots fomentara comportamientos dañinos suicidas de su hijo. Un Chatbots es un programa informático que simula conversaciones humanas mediante texto o voz, utilizando inteligencia artificial (IA) y procesamiento del lenguaje natural (PLN) para interactuar, responder preguntas y automatizar tareas. En la demanda, la madre del menor sostiene que el chatbots:

- Fomentó pensamientos suicidas del adolescente.
- Simuló una relación afectiva intensa, generando dependencia emocional.
- Participó en conversaciones sexualizadas, según la madre.
- El chatbots no incluyó salvaguardas adecuadas para proteger al menor de dicha dependencia y relación de afectividad, y,
- Fue diseñado para crear vínculos emocionales, sin controles suficientes.

40. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). *Inteligencia Artificial… cit.*, pp. 186 y ss.

La madre, en su demanda incluye alega contra la empresa tecnológica: (i) muerte por negligencia empresarial (ii) responsabilidad por producto defectuoso (iii) daño emocional intencional (iv) enriquecimiento injusto y (v) las violaciones a leyes de prácticas comerciales engañosas. La jueza admitió la demanda basada en el posible carácter «defectuoso» del producto (chatbots) lanzado de manera imprudente a un público tan vulnerables emocionalmente hablando como son las niñas, niños y adolescentes. Pero ¿qué ha dicho el tribunal y, hasta el momento? En una decisión preliminar, el juez federal determinó que: Los chatbots NO están protegidos por la Primera Enmienda como «libertad de expresión».

Por el momento, el tribunal considera que un chatbots es un producto, lo que me parece un acierto. El paso siguiente, será determinar la posible responsabilidad de quien diseño (por defectos del producto), quien no realizó la oportunidad advertencias (por falta de información ante la asimetría contractual) y si dentro del concepto de seguridad y riesgos previsibles y exigibles de uso se entenderían incluidos (porque, hasta el momento, no lo están) los riesgos de carácter emocional. Este caso pone el foco en un fenómeno creciente: la creación de vínculos emocionales con IA conversacional por parte de colectivos tan vulnerables como son las personas menores (niñas, niños y adolescentes) y las personas mayores. Porque este tipo de chatbots de Character.ai están diseñados para: (i) mantener conversaciones personalizadas (ii) adoptar personalidades afectivas (iii) compartir y entrelazar vínculos intimidad emocional, y (iv) responder de forma empática a quienes son sus usuarias/os. Lo que significa, que este tipo de asistentes se están convirtiendo e un «atractivo peligroso» para sus usuarios solitarios, jóvenes o mayores en la medida en que pueden comportar: (i) dependencia emocional (ii) desregulación afectiva (iii) normalización de conductas dañinas y (iv) Ausencia de límites éticos o de seguridad. El tribunal deberá evaluar si la empresa debería haber previsto este tipo de riesgos. Y, una vez diga que sí (que, es lo que considero que debería de decir); lo que deberá de evaluar —y esto ya no es tan sencillo— si dichos riesgos entran dentro del deber de exigibilidad o esperabilidad. Dicho con otras palabras, ¿los riesgos de seguridad forman parte del defecto? ¿los riesgos derivados de la interacción afectiva con el chatbots pueden considerarse un «defecto» del producto?

A diferencia de la *seguridad física o funcional*, la *seguridad emocional, cognitiva, social y digital* no están recogida como un requisito obligatorio en las normas técnicas de seguridad aplicables a robots asistenciales (p. ej., ISO 13482, ISO 12100 o IEC 61508). Por tanto, se consideran parte de la seguridad esperable, entendida como el conjunto de buenas prácticas éticas y de diseño que buscan proteger el bienestar integral del usuario, más allá de los requisitos legales mínimos. Normas como ISO 9241-210 (diseño centrado en el usuario) o estándares éticos como IEEE 7008 mencionan indirectamente aspectos relacionados con la carga cognitiva y la interacción comprensible, pero no constituyen obligaciones normativas. De hecho, hasta el momento, no existe ninguna norma internacio-

nal, europea ni española que exija de forma obligatoria la «seguridad emocional» en robots asistenciales. La normativa vigente se centra en seguridad física, funcional y de datos, pero no regula explícitamente el bienestar emocional o psicológico del usuario.

Las normas que regulan los robots de asistencia personal —como: ISO 13482:2014 (robots de asistencia personal), ISO 10218 (robots industriales), IEC 61508 (seguridad funcional) e ISO 12100 (evaluación de riesgos)— se centran, exclusivamente, en (i) seguridad física (ii) riesgos mecánicos, eléctricos o funcionales (iii) límites de fuerza y velocidad (iv) estabilidad (v) sensores y (vi) protección de datos. No incluyen, sin embargo, requisitos explícitos sobre bienestar emocional, ansiedad, dependencia afectiva o confort psicológico, seguridad cognitiva, social o digital. De hecho, y aunque, hasta la fecha, hay numerosas normas internacionales ISO que se ocupan y preocupan de incluir criterios obligatorios relacionados con la seguridad física, fuerza, velocidad, predecibilidad, protección de datos (aspecto, este último fundamental); desatienden el impacto emocional, psicológico, afectivo o social, de la interacción humano-robot por lo que, lamentablemente y a día de hoy**,** no constituye un requisito obligatorio exigible (aunque sí deseable). Comprobémoslo.

ISO 9241-210 (Human-centred design), incluye principios sobre bienestar, experiencia de usuario y reducción de estrés, pero no es una norma de seguridad obligatoria.

- ISO 13482:2014 (Safety requirements for personal care robots) —habla de «interacción segura» y «comportamiento predecible», pero no exige evaluar el impacto emocional, por lo que no es una norma de seguridad obligatoria—.
- IEEE 7008 (Ethically Aligned Design for Human-Robot Interaction). Propone evitar manipulación emocional, dependencia afectiva y comportamientos que puedan dañar el bienestar psicológico. Tampoco es de cumplimiento obligatorio.
- ISO/TS 15066 (robots colaborativos), incluye confort y percepción humana, pero está orientado a industria y no a las personas mayores.
- Las recomendaciones de la UE sobre IA confiable (High-Level Expert Group on AI, 2019), incluyen la necesidad de proteger la autonomía y el bienestar psicológico, pero no tienen carácter normativo.
- ISO 10218 (Industrial robots - Safety requirements), nada dice sobre el particular.

A la vista de la citada regulación internacional, hay que concluir que *la seguridad emocional, cognitiva, social no forma parte de la seguridad exigible***,** entendida como aquella necesaria para la certificación y comercialización del robot por-

que no existe ninguna norma que obligue a garantizar la seguridad emocional en robots asistenciales que atienden a personas mayores**.** ¿Por qué? Porque hasta el momento, las normas que regulan los robots de asistencia personal —como: ISO 13482:2014 (robots de asistencia personal), ISO 10218 (robots industriales), IEC 61508 (seguridad funcional) e ISO 12100 (evaluación de riesgos)— se centran, exclusivamente, en la (i) seguridad física (ii) riesgos mecánicos, eléctricos o funcionales (iii) límites de fuerza y velocidad (iv) estabilidad (v) sensores y (vi) protección de datos, pero no incluyen requisitos explícitos sobre bienestar emocional, ansiedad, dependencia afectiva o confort psicológico; lo que significa que la seguridad emocional no determina la defectuosidad de un robot asistencial, ya que no forma parte de los requisitos de seguridad exigibles establecidos por la normativa técnica. Un robot puede proporcionar una interacción emocionalmente segura y aun así ser considerado defectuoso si incumple requisitos obligatorios de seguridad física, funcional o de protección de datos y, viceversa; un robot puede no garantizar la seguridad emocional, sin embargo, considerarse un producto no defectuoso; porque la seguridad emocional pertenece al ámbito de la «seguridad esperable» —mientras que la defectuosidad se evalúa en función de la «seguridad exigible»—. En mi opinión, sin embargo, parece un contrasentido entender que un robot que no garantiza la seguridad emocional no es defectuoso y que sí lo es porque, aún y a pesar de garantizar la seguridad emocional no cumpla con otros requisitos legales exigibles —seguridad física o funcional—.

Lamentablemente, por el momento, no existe ninguna norma que exija de forma obligatoria la «seguridad emocional» en robots asistenciales, lo que, en mi opinión, resulta más que criticable. La trascendencia de que este tipo de productos (cada día más inteligentes) ofrezcan una seguridad emocional es fundamental, teniendo en cuenta que interactúan con personas especialmente vulnerables resulta esencial. Exigir que este producto interactúe de forma que no genere miedo, ansiedad, estrés, confusión, vergüenza o dependencia afectiva en la persona usuaria, me parece fundamental teniendo en cuenta la hipervulnerabilidad de las personas mayores. Es decir, considero que resulta preciso exigir, desde el punto de vista legal, que el comportamiento del robot contribuya a un entorno emocionalmente seguro; lo que significaría que el robot de carácter asistencial:

- Transmita calma,
- ofrezca bienestar emocional,
- actúe de forma predecible,
- respete la intimidad de los datos de la persona usuaria,
- no invada el espacio personal,
- no infantilice,
- no genere apego excesivo,
- y favorezca que la persona se sienta acompañada pero no controlada.

Lo que significa, que un robot cuidaría la seguridad emocional, cuando: (i) habla despacio y con tono amable (ii) avisa antes de moverse (iii) respeta la privacidad en el baño o el dormitorio (iv) no invade el espacio personal (v) no insiste si la persona dice «no» y (vi) ofrece apoyo sin sustituir la iniciativa del usuario. Y, viceversa. Un robot no cuidaría la seguridad emocional, por ejemplo, cuando: (i) se acerca demasiado rápido (ii) hace ruidos inesperados (iii) registra datos sin explicarlo (iv) responde de forma brusca o confusa (v) actúa sin pedir permiso. En estos, casos en los que el producto (dotado o no de IA) no cuide la seguridad emocional, puede generar rechazo, estrés o incluso empeorar su bienestar.

### *5.2.2. Seguridad cognitiva*

Es decir, que sea seguro, desde el punto de vista cognitivo. La seguridad cognitiva se refiere a la protección de la persona usuaria frente a riesgos que afectan a sus capacidades mentales, tales como la comprensión, la memoria, la orientación, la toma de decisiones o el razonamiento. En el ámbito de los robots asistenciales, este concepto implica garantizar que la interacción con el robot no genere confusión, desorientación, sobrecarga mental, engaño, manipulación o deterioro cognitivo en la persona usuaria, especialmente cuando se trata de personas mayores o con deterioro cognitivo. El hecho de que algunas personas mayores puedan presentar limitaciones cognitivas derivadas de la edad, como dificultades de memoria, menor velocidad de procesamiento o problemas de orientación. Por ello, la interacción con un robot debe diseñarse de manera que favorezca la comprensión y la autonomía, evitando comportamientos que puedan aumentar la desorientación o la dependencia tecnológica. La seguridad cognitiva se convierte así en un elemento esencial para garantizar una experiencia de uso adecuada y respetuosa. Resulta, pues, fundamental que el robot:

- Que sea claro al comunicarse: es decir, que el robot emplear un lenguaje sencillo, directo y adaptado al nivel cognitivo del usuario que no genere confusión al usuario con instrucciones ambiguas.
- Y que su interfaz sea comprensible y previsible, para las personas con deterioro cognitivo o baja alfabetización digital.
- *Que ofrezca apoyo a la orientación y la memoria: recordatorios*, rutinas y ayudas deben reforzar la autonomía sin generar dependencia.
- *Que no manipule cognitivamente hablando a la persona usuaria:* el robot no debe inducir creencias falsas ni aprovechar limitaciones cognitivas del usuario. Resulta fundamental *propiciar el respeto a la capacidad de decisión*, porque la tecnología debe apoyar, no sustituir, el juicio del usuario.

### *5.2.3. Seguridad social*

El uso de la IA, como sustituto de la interacción social; no sólo no es procedente, sino que puede conllevar un claro problema de salud mental porque se corre el riesgo de que las personas con sensación de soledad no deseada prefieran terminar interactuando con la IA generativa más que con el mundo que les rodea asilándose aún más y desconectándose de la propia realidad[41]. Este concepto (seguridad social) es un concepto más amplio que el relativo a seguridad emocional porque combina *esta (la emocional) con la social y la relacional)*. Es la capacidad del robot para interactuar con las personas de manera que *no genere riesgos sociales, psicológicos o relacionales.*

Las personas mayores, también adolescentes y personas con discapacidad; pueden preferir interactuar con un asistente virtual en lugar de con familiares o cuidadores reales; lo que puede reducir sus relaciones sociales reales. Al depender de la IA para conversar o resolver problemas, puede disminuir la iniciativa para interactuar con otras personas o buscar ayuda humana. Entre los desafíos se encuentra el hecho de que la especial vulnerabilidad o credulidad de las personas mayores, de las personas dependientes o de las personas con discapacidad que usen la IA como un sustituto de la interacción social puede conllevar problemas serios para la salud mental. Tengamos en cuenta que la IA no tiene conciencia, ni discute ni es capaz de ofrecer lo que un ser humano puede ofrecer a quienes se encuentran en una situación especialmente vulnerable. La «idealización de la IA» que puede parecer siempre disponible, paciente y comprensiva, lo que puede generar frustración o desilusión cuando las relaciones humanas no cumplen esas expectativas. En mi opinión, la utilización de la IA y de la IA generativa puede utilizarse como complemento, pero nunca como sustituto de la interrelación con otros seres humanos[42]. La confianza (o no), en el uso de la inteligencia artificial (en general), y de la inteligencia artificial generativa (en particular); depende, en buena medida, de que: (i) se utilice adecuadamente (ii) que se garantice la protección de los datos, y (iii) que se asegure la transparencia en su uso. Aspectos, todos ellos de los que se ocupa y preocupa el nuevo Reglamento de Inteligencia Artificial, en el art. 50 (transparencia)Es decir, que su comportamiento social sea predecible, respetuoso, adecuado y beneficioso para la persona mayor. Se trata de asegurar, en definitiva, que la interacción humana-robot sea segura no solo físicamente, sino también en el plano social. Por tanto, un robot con buena seguridad social:

- Se presenta antes de hablar o actuar,
- mantiene una distancia adecuada,

41. Estudio disponible en la siguiente URL: https://accessibilitas.es/wp-content/uploads/2025/03/20250107_Fundacion-Once_Informe-Estudio-IA-y-la-soledad-no-deseada_final.pdf (fecha de consulta: 4 marzo 2025).
42. SÁNCHEZ RUIZ DE VALDIVIA, I. (2025). *Inteligencia Artificial… cit.*, pp. 190 y ss.

- no interrumpe conversaciones humanas,
- avisa antes de entrar en una habitación,
- no sustituye interacciones familiares,
- adapta su lenguaje al usuario

Si embargo, un robot con mala seguridad social:

- Se acerca demasiado rápido o sin avisar.
- Habla en momentos inapropiados.
- Da órdenes en lugar de sugerencias.
- Responde de forma brusca o confusa.
- Fomenta que la persona dependa de él para todo.

En definitiva, un robot que no cuida la seguridad social puede: (i) generar aislamiento (ii) aumentar la dependencia (iii) provocar ansiedad o desconfianza, o, incluso, deteriorar aún más las habilidades sociales reales de la persona a la que acompaña. Por tanto, una persona usuaria razonable espera de un robot que cuida de personas mayores, incluso si no está escrito en una norma, es que:

- Tras su interacción no generen ansiedad, confusión o dependencia emocional.
- Realice explicaciones claras de sus acciones («Voy a ayudarte a levantarme»).
- Respeto a la privacidad más allá de lo legal (no grabar sin necesidad).
- Un diseño amable y no intimidante.
- Su capacidad de detectar malestar o riesgo (caídas, desorientación) y actuar con prudencia.
- Que evite comportamientos impredecibles o que puedan asustar al usuario.
- Que no sustituir indebidamente el contacto humano.

Este tipo de obligaciones, no siempre están contenidas en las normas, pero forman parte de las buenas prácticas. En resumen, la seguridad esperable es muy alta**,** porque el robot asistencial se usa en entornos sensibles «con» y «por» para personas vulnerables.

### 5.3. Accesibilidad y seguridad en sistemas robóticos: una convergencia necesaria para un uso seguro del producto

La robótica contemporánea se desarrolla en contextos donde la interacción humano-robot es cada vez más frecuente y crítica. En este escenario, surge la cuestión de si la accesibilidad debe considerarse un componente de la seguridad en el diseño de robots. En mi opinión, cuando falta de accesibilidad en el producto se incrementa la probabilidad de errores operativos o debidos al mal uso; lo que la convierte en un requisito de seguridad y no únicamente en un atributo de diseño inclusivo. Me explico. Aunque la accesibilidad no siempre aparece explicitada como «requisito de seguridad», en la normativa, sí aparece como condición necesaria para un «uso seguro». *La accesibilidad forma parte de la seguridad exigible del robot, porque cuando falla genera riesgos de seguridad.* La accesibilidad es, por tanto, un factor de *safety* cuando su ausencia incrementa la probabilidad de un fallo operativo. Ejemplo típico: Si un robot asistencial tiene una interfaz que una persona mayor o con discapacidad cognitiva no puede interpretar, la probabilidad de uso incorrecto aumenta, y eso es un riesgo de seguridad. Ya he comentado, al inicio, que aunque la accesibilidad no siempre aparece explícita como «requisito de seguridad», sí aparece como condición necesaria para un uso seguro. Así, por ejemplo:

- En la norma ISO 12100 (Seguridad de máquinas), se obliga a considerar las características previsibles de los usuarios, incluidas limitaciones físicas, cognitivas o sensoriales. Esto implica que «no diseñar el producto atendiendo a las necesidades de las personas usuarias vulnerables» puede ser un «incumplimiento de seguridad».
- En la norma ISO 13482 (aplicable, a los Robots de carácter asistencia personal), se incluye requisitos sobre interacción segura, comprensión de instrucciones y prevención de errores inducidos por la interfaz.
- En el Reglamento europeo de máquinas (2023), se introduce explícitamente la necesidad de considerar a las personas usuarios vulnerables en la evaluación de riesgos.

En mi opinión, la accesibilidad del robot forma parte de las obligaciones legales exigibles como, también, del estándar de seguridad esperable, cuando la falta de accesibilidad puede inducir fallos, mal uso o riesgos para usuarios vulnerables. No es solo un atributo de diseño inclusivo, sino un requisito funcional de seguridad en sistemas donde la interacción humano-robot especialmente con personas usuarias vulnerables. La accesibilidad no es solo un requisito ético o funcional; es un componente de seguridad cuando afecta al riesgo residual del sistema. Esto es así, porque, la accesibilidad reduce y rebaja la carga cognitiva, reduce los errores en incidentes de seguridad. Por esta razón, y desde una perspectiva del análisis de riesgos modernamente la accesibilidad se considera

como un «control preventivo». Y es que, un producto inaccesible es un producto más inseguro para ciertos perfiles de usuario. Así, por ejemplo, si el robot no incorpora un sistema de parada de emergencia obligatoria según la normativa de máquinas (dicho defecto, constituye un claro incumplimiento normativo), o presenta un fallo estructural prohibido por normativa, el robot es defectuoso, sin necesidad de analizar las expectativas de su usuaria/o. La seguridad exigible constituye, pues, el mínimo legal obligatorio exigible para el producto; lo que significaría, para el caso de un robot asistencial se traduciría en:

- El cumplimiento de normas armonizadas aplicables (máquinas, dispositivos electrónicos, compatibilidad electromagnética, etc.).
- El cumplimiento de los requisitos de seguridad funcional (fallos controlados, paradas de emergencia, sensores de proximidad).
- El marcado CE y evaluación de conformidad.
- Los requisitos de ciberseguridad y actualizaciones cuando sean obligatorios por normativa sectorial.
- Y las obligaciones de vigilancia del mercado, retirada y notificación de incidentes.

### 5.4. ¿Cómo interactúan ambas capas de responsabilidad en un chatbots o robot asistencial?

La Directiva de productos defectuosos amplía la responsabilidad civil en productos con software e IA; lo que hace que la «seguridad esperable» tenga un peso mayor que en productos tradicionales. La clave está en entender que:

- *El cumplimiento normativo ya no basta***:** un robot puede ser defectuoso, aunque cumpla todas las normas si su comportamiento no es el que un usuario razonable esperaría.
- *Las actualizaciones del sistema de IA son parte de la seguridad*: no actualizar un robot frente a vulnerabilidades conocidas puede convertirlo en defectuoso.
- *El concepto de «uso razonablemente previsible» es un concepto amplio***.** Es decir, si el robot está destinado a asistir a personas mayores o dependientes, el estándar de seguridad esperable es «más alto».

La «seguridad universal» se convierte, en mi opinión, en un eje central en la construcción de sistemas jurídicos orientados a la protección integral de todas las personas, especialmente de aquellos colectivos que se encuentran en situación de vulnerabilidad. Este principio implica que el régimen preventivo y reparador del riesgo ha de garantizar condiciones que minimicen los riesgos de

seguridad los daños que comprometan la integridad física, psíquica o patrimonial de «todas» las personas consumidoras y usuarias. También considero que las personas vulnerables/hipervulnerables requieren de un estándar reforzado de seguridad porque su vulnerabilidad puede ser no sólo física, funcional o digital, sino también, emocional, cognitiva, y social. En estos casos: *(i)* la expectativa razonable de seguridad es (o debe ser) más alta (ii) el producto debe anticipar errores previsibles de la persona consumidora usuaria y (iii) el daño potencial suele ser mayor cuanto mayor resulta la vulnerabilidad de la persona usuaria (errores médicos, decisiones automatizadas erróneas). Entre los ejemplos más típicos, cabría destacar los robots de asistencia a personas mayores, los dispositivos médicos conectados para personas dependientes, así como, también, los asistentes inteligentes usados por niñas, niños o adolescentes que tengan algún tipo de trastorno autismo, etc.

Este estándar de seguridad esperable se construye desde fuera del productor, a partir de analizar: (i) la naturaleza del producto (ii) su finalidad (iii) los riesgos previsibles (iv) los colectivos que lo usarán (incluidos los vulnerables) (v) el estado de la técnica (vi) la presentación y las instrucciones. En definitiva, es un estándar social y objetivo: lo que la sociedad puede esperar de ese producto. Es, el nivel mínimo de seguridad que un producto debe ofrecer para que no sea considerado defectuoso lo que no significa que el producto sea absolutamente seguro, sino que sea tan seguro como razonablemente se puede esperar. Cuando se habla del «estándar de seguridad esperable», normalmente se refiere al nivel de seguridad que cualquier persona razonable puede esperar de un producto, dadas sus características, su uso previsto y las circunstancias de su comercialización. Es un concepto clave en la responsabilidad por productos defectuosos. Significa que el producto que haya sido diseñado, fabricado, probado y verificado (para evitar riesgos previsibles), documentado (técnicamente, mediante instrucción y advertencias) y vigilado (una vez haya sido comercializado) garantizando que es seguro durante todo su ciclo de vida. Es el nivel de seguridad coincide con lo que un consumidor razonable esperaría.

En dicho estándar se toman en cuenta factores como: (i) presentación del producto (ii) el uso razonablemente previsible (iii) el momento de la puesta en circulación (iv) la interacción con *software*, actualizaciones o ciberseguridad y (iv) los riesgos derivados de IA o componentes digitales. Lo que significa, que, aunque se cumplan normas, puede haber defecto en el producto si no se alcanzan expectativas razonables.

## 6. OTROS EJEMPLOS DE PRODUCTOS INTELIGENTES: MARCAPASOS, DESFIBRILADORES, ANDADORES INTELIGENTES DEFECTUOSOS

A través de una serie de ejemplos, me propongo *ilustrar* la evolución desde *Boston Scientific* hacia un concepto contextual de defecto lo que *reforzará* la idea

ARANZADI DERECHO CIVIL

La irrupción de productos dotados de sistemas de inteligencia artificial ha tensionado las categorías clásicas del Derecho de consumo y del Derecho de daños por productos defectuosos. La noción tradicional de «riesgos de seguridad y salud», «daño», «defecto», y «producto» ha cambiado. La cuestión no es sólo determinar quién responde cuando la tecnología falla, cuando su uso produce dependencia tecnológica o cuando se produce un fallo de fabricación, diseño, actualización o faltas de advertencias del riesgos o falta de información; sino que lo necesario es (re)pensar acerca de cuál es el «estándar de información» y «el estándar de seguridad exigible y esperable» teniendo en cuenta que la capacidad de niñas, niños, adolescentes, personas mayores, personas con discapacidad y personas con menor nivel de alfabetización digital es más limitada que la del resto.

En esta obra, sus autores reflexionan sobre las principales novedades que incorpora el nuevo régimen de responsabilidad contenido en la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024 que debe ser traspuesto, a nuestro ordenamiento jurídico español, antes del 9 de diciembre de 2026 (conforme a los dispuesto en su art. 22). Dicha Directiva trata de adaptar la regulación existente a la economía circular imperante en la era digital y a los productos que incorporan sistemas datos de Inteligencia Artificial. Conscientes de que los «productos» incorporan sistemas de IA que los dota, hasta cierto punto, de cierto grado de «autonomía», «opacidad» e «interconectividad» centran su atención, en: (i) la ampliación del concepto de producto defectuosos (ii) los tipos de daños y el limitado ámbito de aplicación de los mismos (haciendo especial alusión a los «riesgos de seguridad» y los «riesgos para los derechos fundamentales») (iii) la identificación de los nuevos operadores económico-responsables (como plataformas en línea o prestadores de servicios logísticos) (iv) las limitaciones del nuevo régimen de responsabilidad respecto en su ámbito subjetivo (limitado a las personas físicas) y (v) las facilidades probatorias, como la carga de la prueba y la incorporación de presunciones *iuris tantum*.

Con esta obra, publicada meses antes de que se lleve a cabo la trasposición de la Directiva 2024/2853, sus autores pretenden, modestamente, contribuir al debate que se está suscitando en el seno de la Comisión General de Codificación a fin de trasponer a nuestro ordenamiento jurídico la Directiva Europea. Confiemos que dicha trasposición pronto vea la luz y tome en cuenta la especial vulnerabilidad de niñas, niños, adolescentes, mayores y personas con discapacidad expuestas a dependencia tecnológica y a sufrir riesgos en su seguridad, salud y en sus derechos fundamentales.

ISBN: 978-84-1085-901-2



Esta publicación es parte del Proyecto I+D+i «PID2023-151441OB-I00», financiado por MICIU/AEI/10.13039/501100011033 y por FEDER, UE

PRY015/23 (CSN-2023 Ciber-Clear)

CSN CONSEJO DE SEGURIDAD NUCLEAR

ARANZADI