Inteligencia Artificial y Responsabilidad Civil: Caso Práctico

Cristina Delgado Salazar

Borrador del 24 de marzo de 2025

CAPÍTULO I. INTRODUCCIÓN Y OBJETIVOS

1. MARCO NORMATIVO
2. OBJETIVO DEL TRABAJO

CAPÍTULO II. CONCEPTO Y CONFIGURACIÓN JURÍDICA

1. CONCEPTO
   1.1. Evolución de la Definición Regulada por la UE
   1.2. Características esenciales
2. CONFIGURACIÓN JURÍDICA

CAPÍTULO III. ANÁLISIS DE SUPUESTOS PRÁCTICOS: RESPONSABILIDAD OBJETIVA POR PRODUCTOS DEFECTUOSOS

1. SUPUESTO DE HECHO
2. RESPONSABILIDAD OBJETIVA DEL PRODUCTOS POR PRODUCTOS DEFECTUOSOS: DIRECTIVA (UE) 2024/2853

   2.1. Concepto de producto: ¿Puede calificarse un sistema de hogar inteligente basado en inteligencia artificial como "producto" a efectos del régimen de responsabilidad objetiva por productos defectuosos del TRLGDCU? ¿Y conforme a la Nueva DRPD?

   2.2. Producto defectuoso I : ¿Existe un defecto de información a efectos del régimen de responsabilidad objetiva por productos defectuosos de la Nueva DRPD?

   a. Uso razonablemente previsible del producto (art. 6.1.b)
   b. Uso razonablemente imprevisible: Capacidad de aprendizaje y evolución autónoma (art. 6.1.c) e interacción con otros productos (art. 6.1.d).
   c. Conservación del control por parte del fabricante tras la comercialización (art. 6.1.e)

   2.3. Producto defectuoso II: ¿Existe un defecto de diseño a efectos del régimen de responsabilidad objetiva de la Nueva DRPD?

2.4. Nexo causal y carga de la prueba: ¿Cómo se acredita la relación entre el defecto y el daño cuando interviene un sistema de IA?

2.5. Régimen de solidaridad de los operadores económicos: ¿Quién responde cuando intervienen múltiples agentes?

3. CONCLUSIÓN

CAPÍTULO IV. ANÁLISIS DE SUPUESTOS PRÁCTICOS: RESPONSABILIDAD SUBJETIVA EXTRACONTRACTUAL

1. SUPUESTO DE HECHO
2. RESPONSABILIDAD SUBJETIVA EXTRACONTRACTUAL: PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO 28.9.2022

2.1. El modelo tradicional: límites del artículo 1902 CC ante sistemas de IA autónomos

2.2. El marco propuesto por la Directiva COM(2022) 496: una transformación procesal del modelo de responsabilidad subjetiva

a. Acceso a la información
b. Presunción iuris tantum de relación de causalidad

3. CONCLUSIÓN

CAPÍTULO V. PROPUESTAS Y CONCLUSIONES

CAPÍTULO I. INTRODUCCIÓN Y OBJETIVOS

La inteligencia artificial (**IA**) se ha insertado vertiginosamente en múltiples ámbitos de la actividad humana, dando lugar a una transformación tecnológica que combina un potencial muy beneficioso con riesgos jurídicos todavía inciertos. En la medicina, por ejemplo, ya se utilizan sistemas de IA para ayudar a los médicos a detectar enfermedades a partir de radiografías o resonancias, e incluso existen robots que asisten en operaciones quirúrgicas con gran precisión. En el mundo de las finanzas, los algoritmos inteligentes pueden gestionar inversiones o alertar sobre posibles fraudes en tiempo real. En la industria y el transporte, la IA controla robots que trabajan en fábricas o permite que los vehículos autónomos circulen sin intervención humana. Y en muchos ámbitos más.

Esta introducción de la IA en contextos donde anteriormente existía un vínculo causal lineal entre un operador humano, un producto y un daño plantea una dificultad estructural para los sistemas jurídicos. La autonomía funcional de los sistemas de IA, su capacidad de autoaprendizaje, su funcionamiento opaco y su dependencia de grandes volúmenes de datos e interconectividad erosionan los presupuestos clásicos de atribución de responsabilidad, basados en la previsibilidad del riesgo, la identificación del sujeto causante y la posibilidad de probar el defecto o la conducta negligente.

1. MARCO NORMATIVO

Ante esta situación, la Unión Europea (**UE**) ha impulsado una estrategia dual anunciada en su Libro Blanco sobre Inteligencia Artificial de 2020[1], que articula normas de seguridad *ex ante,* orientadas a la prevención del daño, con normas de responsabilidad *ex post*, como pilares esenciales de una estrategia jurídica que busca fomentar la innovación responsable.

1.1. Prevención *ex ante*

El principal instrumento preventivo es el 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 IA**)[2], que establece un sistema de riesgos para los sistemas de IA, cuyo objetivo es imponer requisitos reforzados de transparencia,

[1] Comisión Europea. (2020). *Libro Blanco sobre la inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza* (COM(2020) 65 final).
[2] 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.

trazabilidad y supervisión humana para aquellos que se clasifican como de alto riesgo—tales como los sistemas biométricos, los algoritmos utilizados en la toma de decisiones crediticias o los vehículos autónomos—y establecer garantías que reduzcan la probabilidad de que se materialicen riesgos lesivos.

1.2. Responsabilidad *ex post*

Ahora bien, como ha reconocido la propia Comisión, la seguridad y la responsabilidad constituyen las dos caras de una misma moneda[3], de modo que cuando las medidas preventivas resultan insuficientes para evitar la producción del daño, debe activarse un marco de responsabilidad eficaz que permita resarcir a las víctimas, garantizar el derecho fundamental a la tutela judicial efectiva (Art 47 Carta de Derechos Fundamentales de la UE[4] y el artículo 2 de la Constitución Española[5]) y, al mismo tiempo, genere incentivos para el cumplimiento de las obligaciones normativas.

a. Personalidad jurídica del robot y responsabilidad objetiva generalizada o para sistemas de alto riesgo.

El ámbito de la responsabilidad civil ex post ha tenido un gran recorrido de discusión y el Parlamento Europeo fue pionero en identificar la necesidad de adaptar los regímenes existentes. En 2017, con su Resolución del Parlamento Europeo de 16 de febrero de 2017[6], sobre normas de Derecho civil sobre robótica, propuso por primera vez establecer un régimen específico de responsabilidad civil objetiva para estos sistemas, planteando incluso la creación de una personalidad jurídica electrónica para los sistemas de IA más avanzados. Asimismo, recomendaba la implantación de un sistema de seguro obligatorio, complementado con un fondo de compensación que garantizase la reparación de daños en ausencia de seguro, así como la adopción de un código ético para los desarrolladores y fabricantes de sistemas autónomos. En 2020[7], se abandona la idea de la personalidad jurídica del robot, y se matiza la idea de la responsabilidad objetiva, de forma que se plantea un sistema dual: por un lado,

---

[3] Comisión Europea. (2022). *Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial* (COM(2022) 496 final).
[4] Carta de los Derechos Fundamentales de la Unión Europea. (2000). *Artículo 47: Derecho a la tutela judicial efectiva y a un juez imparcial*. Diario Oficial de la Unión Europea, C 364, 18.12.2000, p. 1–22.
[5] Constitución Española. (1978). *Artículo 24: Tutela judicial efectiva*. Boletín Oficial del Estado, núm. 311, de 29 de diciembre de 1978.
[6] Parlamento Europeo. (2017). *Resolución de 16 de febrero de 2017 con recomendaciones a la Comisión sobre normas de Derecho civil sobre robótica* (2015/2103(INL)).
[7] Parlamento Europeo. (2020). *Resolución con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL)).

responsabilidad objetiva para los operadores de sistemas de alto riesgo, con seguro obligatorio y límites máximos de indemnización; por otro, responsabilidad subjetiva para el resto de sistemas, pero con medidas procesales reforzadas para facilitar el acceso a pruebas y la imputación del daño.

Desde un punto de vista doctrinal, muchos autores[8] han defendido la instauración de un régimen de responsabilidad objetiva generalizada para los operadores de IA, con base en la existencia de un riesgo inherente y difícilmente controlable vinculado al uso de sistemas autónomos y opacos, buscando asimilar jurídicamente la inteligencia artificial a otras fuentes de peligro.

Desde la perspectiva del derecho español, la jurisprudencia del Tribunal Supremo ha sostenido de forma constante que la responsabilidad objetiva sólo puede admitirse en supuestos en los que la actividad en cuestión entrañe un riesgo que exceda los niveles de peligrosidad socialmente tolerados (STS 421/2010, de 7 de julio). Bajo esta lógica, la imputación automática de responsabilidad sin necesidad de acreditar culpa solo se justifica en el caso de actividades que, por su propia naturaleza, introducen en el tráfico jurídico una fuente significativa de peligro.

Y es que se me hace difícil plantear una responsabilidad objetiva generalizada para todos los sistemas de IA. En primer lugar, porque no toda aplicación de IA genera un riesgo significativo o desproporcionado. De hecho, muchas de sus aplicaciones han sido diseñadas para reducir la incidencia de errores humanos y aumentar la seguridad operativa, como sucede en la cirugía asistida o en los sistemas de alerta temprana. En segundo lugar, desde una perspectiva de análisis económico del Derecho, la aplicación indiscriminada de un régimen de responsabilidad objetiva podría incrementar significativamente los costes de desarrollo, producción y aseguramiento de estos sistemas, lo cual afectaría de forma desproporcionada a los pequeños operadores y reforzaría la posición dominante de las grandes plataformas tecnológicas, únicas con capacidad para absorber tales costes.

No obstante, tal y como ha señalado la propia Comisión Europea, no se descarta que en el futuro puedan establecerse regímenes específicos de responsabilidad objetiva para aquellos usos de la IA que presenten un perfil de alto riesgo. Queda por ver si esa eventual evolución se producirá mediante la asimilación de estos supuestos a las actividades ya tradicionalmente

[8] Citar

consideradas peligrosas, como el transporte o la energía, o si, por el contrario, se optará por construir una nueva categoría jurídica de "actividades de riesgo por IA", inspirada en la lógica del enfoque basado en el riesgo que articula el Reglamento de IA.

b. Adaptar normativa actual: Normas armonizadas de responsabilidad objetiva por productos defectuosos y norma no armonizadas de responsabilidad extracontractual subjetiva

La Comisión finalmente adopta un enfoque con dos normativas complementarias: la Directiva (UE) 2024/2853 de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuoso (**Nueva DRPD**)[9], que moderniza el régimen de responsabilidad por productos defectuosos, y la Propuesta de Directiva COM(2022) 496[10] (**Propuesta de Directiva de Responsabilidad Civil Extracontractual**), relativa a la responsabilidad civil extracontractual en casos de daño causado por IA.

La Directiva sobre responsabilidad por productos defectuosos (**DRPD Derogada**)[11], transpuesta mediante el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (**TRLGDCU**)[12], establece un régimen de responsabilidad objetiva del productor, que se activa cuando un producto, por falta de la seguridad que razonablemente cabe esperar, causa un daño a personas o bienes. No se exige la prueba de culpa, pero sí la prueba del defecto, del daño y del nexo causal. Este esquema, si bien adecuado para productos tradicionales, resulta insuficiente cuando se aplica a tecnologías basadas en IA. La Comisión reconoce estas limitaciones y señala que la creciente complejidad de los productos, la multiplicidad de agentes económicos en la cadena de valor y la imposibilidad técnica o económica de probar ciertos elementos de la acción de responsabilidad, pueden dar lugar a situaciones en las que las víctimas queden privadas de una compensación justa[13]. Esta

[9] 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, L, 25.10.2024.

[10] Comisión Europea. (2022). *Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial* (COM(2022) 496 final).

[11] Consejo de las Comunidades Europeas. (1985). *Directiva 85/374/CEE, de 25 de julio de 1985, 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*. Diario Oficial de las Comunidades Europeas, L 210, 7 de agosto de 1985, p. 29–33.

[12] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. *Boletín Oficial del Estado*, núm. 287, de 30 de noviembre de 2007.

[13] Comisión Europea. (2020). *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la IA, el internet de las cosas y la robótica* (COM(2020) 64 final).

preocupación motivó la Propuesta de Directiva de 2020[14], y finalmente la adopción de la Nueva DRPD, de 23 de octubre de 2024. Esta norma, que será aplicable a los productos puestos en el mercado a partir del 9 de diciembre de 2026, amplía el ámbito material de aplicación del concepto de producto y del defecto, así como también establece presunciones de causalidad en casos de complejidad técnica y refuerza los derechos de acceso a pruebas en manos del productor. Con estas medidas, la Directiva pretende modernizar el régimen de imputación objetiva para adaptarlo a los supuestos de IA, sin alterar su equilibrio básico entre los intereses de las víctimas y los de los operadores económicos.

Por otra parte, en septiembre de 2022, presentó la Propuesta de Directiva de Responsabilidad Civil Extracontractual. En el preámbulo de esta se comentan las tres opciones políticas evaluadas: 1. Establecimiento de medidas para aliviar la carga de la prueba, 2. Las medidas de la opción 1 y la armonización de normas de responsabilidad objetiva en IA con un riesgo elevado y contando con un seguro obligatorio, y 3. Hacer unas fases progresivas de forma que primero se haga la opción 1 y después la opción 2. Finalmente se opta por la opción 3 de forma que se opta un enfoque, bastante alejado del del Parlamento Europeo, de armonización mínima. Esta propuesta no modificaba los criterios sustantivos de imputación nacionales, pero sí introducía mecanismos para corregir los desequilibrios probatorios generados por la opacidad algorítmica y la complejidad técnica de los sistemas de IA: presunciones de causalidad en determinados supuestos, obligación de los operadores de conservar documentación relevante, y medidas para facilitar el acceso a pruebas en manos del responsable. Cabe mencionar que la falta de acuerdo político entre los Estados miembros provocó la retirada de esta propuesta en marzo de 2025[15], lo que ha sido interpretado por una parte significativa de la doctrina como un retroceso en la protección de las víctimas y un fracaso en la articulación de un marco coherente y eficaz a escala europea.

Con todo ello, las normas de responsabilidad civil del marco actual combinan normas armonizadas en materia de responsabilidad por productos defectuosos (traspuestas en la TRLGDCU) con una pluralidad de regímenes nacionales de responsabilidad civil, ya sean subjetivos o, en determinados sectores, objetivos, y a visitas de ver si se armonizan o no con la retoma de la Propuesta de Directiva de Responsabilidad Civil Extracontractual.

---

[14] Comisión Europea. (2022). *Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos* (COM(2022) 495 final, 2022/0302 (COD)). Bruselas, 28 de septiembre de 2022.

[15] Comisión Europea. (2025). *Annexes to the Commission Work Programme 2025* (COM(2025) 45 final ANNEXES).

En España, los regímenes nacionales no armonizados en materia de responsabilidad civil subjetiva, son la responsabilidad civil subjetiva de los artículos 1902 y siguientes del Código Civil[16]. Este modelo impone a la víctima la carga de demostrar no solo el daño y la relación causal, sino también la conducta culposa del agente responsable.

También se contemplan regímenes de responsabilidad objetiva. Una primera categoría comprende aquellas situaciones en las que el ordenamiento jurídico presume la existencia de un riesgo inherente y significativo derivado del uso de determinados bienes o del ejercicio de actividades consideradas peligrosas en sí mismas. Ejemplo de este tipo de regímenes se observa en el ámbito de la responsabilidad derivada del tráfico automotor o el de la responsabilidad del cazador de la Ley de Caza[17], o el de los daños causados por animales domésticos (art. 1.905 Código Civil[18]). En estos casos, la sola existencia de un daño ocasionado en el marco de dichas actividades genera la obligación de indemnización, sin que resulte necesario acreditar defectos en el bien o negligencia en su uso. Y otra configuración de la responsabilidad objetiva se basa en la existencia de hechos concretos que, por su especial naturaleza, son considerados generadores de responsabilidad sin que resulte necesario determinar la existencia de riesgo inherente en el bien o en la actividad en cuestión. Ejemplo de ello es la responsabilidad derivada de la caída de objetos desde edificios (art. 1.910 Código Civil[19]), o la responsabilidad por inmisiones (art 1.908 Código Civil[20]). En estos casos, no se considera peligroso el objeto en sí —como un árbol o una edificación—, sino ciertos eventos concretos asociados a ellos, como la caída de un objeto o una inmisión perjudicial.

2. OBJETIVO DEL TRABAJO

En definitiva, el marco de responsabilidad civil en el contexto de la IA se encuentra en fase de transformación. El enfoque de la Unión Europea descarta, por el momento, la atribución de personalidad jurídica a los sistemas de IA, cuestión en la que profundizaremos más adelante, y la creación de una categoría autónoma de "responsabilidad por IA", apostando en su lugar por una adaptación evolutiva de los regímenes existentes. Esta adaptación se hace a vistas de garantizar que los avances tecnológicos no impongan obstáculos insalvables al ejercicio efectivo de los derechos de los perjudicados, así como también se trata de preservar la seguridad jurídica para los agentes económicos, fomentar la innovación y evitar la

[16] Código Civil español. (1889). *Artículo 1.905*. Gaceta de Madrid, núm. 206, de 25 de julio de 1889.
[17] Ley 1/1970, de 4 de abril, de caza. Boletín Oficial del Estado, núm. 82, de 6 de abril de 1970.
[18] Código Civil español. (1889). *Artículo 1.905*. Gaceta de Madrid, núm. 206, de 25 de julio de 1889.
[19] Código Civil español. (1889). *Artículo 1.910*. Gaceta de Madrid, núm. 206, de 25 de julio de 1889.
[20] Código Civil español. (1889). *Artículo 1.908*. Gaceta de Madrid, núm. 206, de 25 de julio de 1889.

fragmentación del mercado interior. El equilibrio entre estos intereses constituye el eje vertebrador de la futura regulación europea en esta materia.

El presente trabajo tiene por objeto analizar, a partir de este contexto normativo, la manera en que los distintos regímenes de responsabilidad civil se enfrentan a los retos planteados por la inteligencia artificial. Para ello, se parte de un estudio sistemático de las características técnicas y jurídicas de la IA y de su incardinación normativa en función de su configuración jurídica. A partir de ahí, se desarrollan casos prácticos seleccionados que permiten ilustrar cómo se activa, en cada supuesto, la responsabilidad objetiva por riesgo, la responsabilidad objetiva por producto defectuoso o la responsabilidad subjetiva por culpa, y se examina hasta qué punto las reformas introducidas —o proyectadas— por las instituciones europeas constituyen una respuesta adecuada, coherente y eficaz a los problemas concretos que la IA plantea en materia de imputación jurídica y tutela del perjudicado. En última instancia, el trabajo pretende contribuir a la reflexión sobre la suficiencia del modelo actual, y sobre la necesidad (o no) de avanzar hacia soluciones normativas específicas que garanticen un equilibrio justo entre innovación, seguridad jurídica y protección efectiva de las víctimas.

CAPÍTULO II: Concepto y Configuración jurídica de IA

Para comprender plenamente los desafíos jurídicos que plantea la IA en los regímenes de responsabilidad civil, es imprescindible partir de una base conceptual que permita delimitar qué se entiende por IA, cuáles son sus características distintivas, y que configuración jurídica se le ha dado.

1. CONCEPTO

1.1. Evolución de la Definición Regulada por la UE

La definición de inteligencia artificial ha evolucionado con el tiempo, y la Unión Europea ha ido incorporando en sus regulaciones las distintas capas de complejidad y la propia transformación del concepto.

En 2021, la propuesta europea[21] definía un sistema de IA como *"el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información*

[21] Parlamento Europeo y Consejo (2021). Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial. COM(2021) 206 final.

de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa". Esta definición equipara a un sistema de IA con un software, y bajo un control humano de forma que su funcionamiento se limita a generar resultados controlados en base a parámetros definidos por humanos. Desde esta perspectiva inicial, no parece que la IA introduzca problemas jurídicos significativos, pues su influencia es más predecible y controlada.

El Parlamento Europeo, presentó enmiendas a esta propuesta, redefiniendo en su enmienda 165[22] la IA como *"un sistema basado en máquinas diseñado para funcionar con* ***diversos niveles de autonomía*** *y capaz, para objetivos explícitos o implícitos, de generar información de salida—como predicciones, recomendaciones o decisiones—que influya en entornos reales o virtuales."* Con esta nueva formulación, la IA comienza a caracterizarse por su capacidad para operar con cierto grado de autonomía, lo que plantea interrogantes sobre su consideración jurídica, dado que ya no es un simple "instrumento". Además, se eliminó la lista cerrada del Anexo I, reconociendo que las técnicas y estrategias de IA no pueden ser estáticas, por su constante evolución.

Finalmente, en el Reglamento (UE) 2024/1689[23], la definición consolidada en el artículo 3.1 introduce un elemento adicional: la capacidad de adaptación tras el despliegue de la tecnología. Un sistema de IA se define como *"un sistema basado en una máquina que está diseñado para funcionar con distintos* ***niveles de autonomía*** *y que puede mostrar* ***capacidad de adaptación tras el despliegue****, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales."* Este nuevo concepto no solo mantiene la autonomía como característica esencial, sino que destaca que los sistemas de IA pueden modificar su comportamiento tras su despliegue, adaptándose a los datos y situaciones del entorno.

Esta progresión de la definición del concepto, que ha ido evolucionado a la vez que lo han hecho los propios sistemas de IA, desde un sistema que genera información controlada hasta otro que opera con autonomía y capacidad de adaptación, transforma radicalmente cómo se presenta la IA en el sistema jurídico.

[22] Parlamento Europeo (2022). Enmiendas aprobadas en primera lectura. Enmienda 165 a COM(2021) 206.
[23] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024.

1.2. Características esenciales

Más allá de como se ha definido, resulta indispensable estudiar las siete características distintivas de los sistemas de IA recogidas en el Informe Sobre la Responsabilidad por IA y Otras Tecnologías Digitales Emergentes, elaborado por el Grupo de Expertos en Responsabilidad Civil y Nuevas Tecnologías,[24] para los desafíos que plantea en materia de responsabilidad civil:

a) Complejidad (*Complexity*): Los sistemas de IA combinan componentes físicos y digitales altamente sofisticados. Su funcionamiento no depende de una única entidad, sino de la interacción de múltiples agentes dentro de un ecosistema digital. Esta complejidad complica la identificación de causas directas cuando se produce un daño, dificultando la determinación de los responsables.

b) Opacidad (*Opacity*)*:* La mayoría de los sistemas de IA, especialmente aquellos basados en algoritmos de aprendizaje automático (machine learning), operan como auténticas "cajas negras". Es posible observar sus efectos, pero resulta extremadamente difícil reconstruir o entender los procesos internos que los generan, incluso para sus propios desarrolladores.

c) Apertura (*Openness*)*:* La IA no constituye un sistema cerrado ni finalizado en el momento de su comercialización. Su rendimiento depende de interacciones continuas con el entorno, actualizaciones de software, incorporación de nuevos datos y conexión con otros sistemas, lo cual impide una evaluación ex ante completa de su comportamiento.

d) Autonomía (*Autonomy*)*:* Uno de los rasgos distintivos más problemáticos es su capacidad de operar con escasa o nula intervención humana. Los sistemas autónomos procesan datos del entorno y modifican su conducta en tiempo real, sin requerir instrucciones adicionales. Esta independencia funcional plantea serias dudas sobre la imputación jurídica de las decisiones tomadas por la máquina.

e) Imprevisibilidad (*Predictability*)*:* La combinación de complejidad, opacidad y autonomía produce sistemas cuyos comportamientos no pueden ser previstos por completo ni siquiera por sus diseñadores. En consecuencia, el daño que generan puede

[24] Expert Group on Liability and New Technologies – New Technologies Formation (2019). *Liability for Artificial Intelligence and other emerging digital technologies*. Publications Office of the European Union, pp. 19-21 .

escapar a los estándares tradicionales de previsibilidad sobre los que se construye la responsabilidad civil.

f) Dependencia de los datos (*Data-drivenness*)*:* Los sistemas de IA requieren información externa, recopilada por sensores u obtenida de otras fuentes, para funcionar correctamente. La calidad de sus decisiones depende de la integridad y veracidad de los datos recibidos. Fallos en los sensores, fuentes de datos erróneas o sesgos en los algoritmos pueden comprometer gravemente su funcionamiento y producir daños.

g) Vulnerabilidad (*Vulnerability*)*:* al tener un diseño abierto e interacción constante con fuentes externas, se aumenta el riesgo de que sean manipuladas o alteradas de manera malintencionada, generando resultados no deseados y aumentando el potencial de daño.

Estas siete características no solo operan de forma aislada, sino que se retroalimentan entre sí. La complejidad de estos sistemas complica la identificación precisa de la causa de un daño, y su opacidad refuerza esta incertidumbre al limitar la comprensión de su funcionamiento. Al mismo tiempo, su apertura fomenta un constante flujo de actualizaciones y datos externos, lo que incrementa su imprevisibilidad al generar respuestas no preprogramadas y potenciadas por su autonomía que se escapan del control humano. Su dependencia de datos, introduce vulnerabilidades adicionales, ya que datos defectuosos o ciberataques pueden alterar su funcionamiento y agravar los riesgos. Estas interacciones convierten a las tecnologías emergentes en sistemas dinámicos y desafiantes para los marcos normativos, haciendo que los criterios tradicionales de imputación de responsabilidad civil resulten insuficientes para abordar los daños que puedan causar.

2. CONFIGURACIÓN JURÍDICA

Una vez expuesta la evolución conceptual de la inteligencia artificial en el marco normativo europeo, resulta pertinente abordar de forma breve una de las primeras soluciones que se plantearon ante los desafíos que plantea la IA en materia de responsabilidad civil: la posibilidad de atribuirle personalidad jurídica. Esta propuesta buscaba resolver una pregunta clave que vertebra también el presente trabajo: ¿a quién imputar el daño cuando interviene un sistema autónomo, especialmente en aquellos casos en los que no puede identificarse un sujeto humano responsable directo?

La cuestión fue planteada explícitamente por el Parlamento Europeo en su Resolución de 16 de febrero de 2017, que propuso "*crear a largo plazo una personalidad jurídica específica para los sistemas de IA, de forma que como mínimo los sistemas de IA autónomos más complejos puedan ser considerados personas* electrónicas responsables de reparar los daños que puedan causar"[25].

La doctrina ha abordado esta posibilidad desde dos grandes perspectivas: una visión ontológica, que propone considerar ciertos sistemas de IA como un *tertium genus* entre las personas y las cosas[26], y una visión funcional, que admite su personificación como herramienta jurídica, sin implicar reconocimiento de subjetividad moral o derechos fundamentales.

Pues bien, dado que la equiparación ontológica no ha tenido acogida normativa—equiparación que ha sido, además, criticada por entenderse incompatible con principios jurídicos fundamentales como la dignidad humana y la integridad personal, reconocidos en el Derecho de la Unión Europea[27]—este trabajo no entrará a valorar las implicaciones filosóficas que ha suscitado esta propuesta.

Sí interesa, en cambio, examinar el enfoque funcional de esta propuesta, porque permite identificar con claridad los problemas jurídicos que se pretendían resolver y que, como veremos, siguen estando en el centro de los regímenes actuales de responsabilidad civil aplicables a la inteligencia artificial.

Desde esta perspectiva, la idea es conferir personalidad jurídica a la inteligencia artificial con el objetivo de dotar de un centro de imputación a los daños causados por los sistemas de IA en ciertos escenarios donde ni el fabricante ni el operador incurren en culpa ni puede probarse defecto en el producto, para evitar vacíos de responsabilidad que dejen sin reparación a la víctima.[28]

Sin embargo, esta idea tampoco ha prosperado en los desarrollos normativos posteriores de la Unión Europea, ni ha sido mayoritariamente respaldada por la doctrina.

---

[25] Op. Cit Parlamento Europeo (2017)
[26] Cfr Atienza Navarro, M. L. (2022). Daños causados por IA y responsabilidad civil (p. 106). Atelier.
[27] Nevejans, N., & Chatila, R. (2018). *Open Letter to the European Commission: Artificial Intelligence and Robotics*.
[28]Op. cit. Atienza Navarro, M. L. (2022).Daños causados por IA y responsabilidad civil (p.106)

Uno de los principales motivos de su rechazo fue la percepción de que esta fórmula podría facilitar una exoneración indirecta de los fabricantes. Como sostiene ROGEL VIDE[29], atribuir personalidad jurídica a los sistemas de IA tiene como objetivo encubierto reducir la responsabilidad de los fabricantes ya que se podría trasladar la responsabilidad legal de los fabricantes a las propias máquinas, permitiendo que estos evadan su responsabilidad por los daños causados por sus creaciones[30]. Esta crítica se reforzó con la constatación de que, al carecer de voluntad, los sistemas de IA no pueden ser disuadidos por la amenaza de sanción, y que, por tanto, atribuirles responsabilidad implicaría renunciar al efecto preventivo que caracteriza al Derecho de daños. El Dictamen del Comité Económico y Social Europeo de 31 de mayo de 2017 señaló que *"la legislación en materia de responsabilidad tiene un efecto correctivo y preventivo que podría desaparecer si el riesgo de responsabilidad civil dejase de recaer sobre el autor para transferirse al robot"*[31]. En este sentido, RAMÓN FERNANDEZ[32] sostuvo que este modelo vaciaba de contenido el mecanismo tradicional de responsabilidad, basado en el efecto preventivo, cautelar y correctivo.[33]

Otra de las objeciones más relevantes, es que debemos recordar que en última instancia lo que se busca es que haya un patrimonio al que pueda dirigirse la víctima para obtener la indemnización correspondiente. Si la idea funcional detrás de conferir personalidad jurídica a la IA era asegurar que alguien —o algo— respondiera económicamente por los daños causados, resulta imprescindible preguntarse: ¿dónde está y cuál es ese patrimonio?

---

[29] Rogel Vide, C. (2018). Robots y personas. Revista General de Legislación y Jurisprudencia, 1, 79-90.

[30] En contra de esto, ATIENZA NAVARRO argumenta que atribuir responsabilidad a los sistemas de IA autónomos no pretende exonerar a los fabricantes de manera general, sino aplicarse sólo en aquellas situaciones donde, a pesar de la máxima diligencia, los sistemas de IA causen daños inevitables por su carácter autónomo e imprevisible. También argumenta que esta perspectiva podría generar beneficios económicos y sociales, ya que incentivaría el desarrollo tecnológico, al tener los fabricantes mayor seguridad jurídica. A su vez señala, que se promovería la creación de sistemas más seguros, ya que los fabricantes intentarían demostrar que han implementado todas las medidas necesarias para evitar defectos o riesgos, con el fin de acreditar su diligencia y eludir posibles sanciones.
Op. cit. Atienza Navarro, M. L. (2022).Daños causados por IA y responsabilidad civil (p.99)

[31] Comité Económico y Social Europeo. (2017). *Dictamen del Comité Económico y Social Europeo sobre la inteligencia artificial y la sociedad*. Diario Oficial de la Unión Europea, C 288, 1-8.

[32] Ramón Fernández, F. (2019). Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil? Diario La Ley, (9365), p.7

[33] Algunos autores como BERTOLINI refutan esta postura, estableciendo un paralelismo con el régimen de responsabilidad penal de las personas jurídicas, que también fue inicialmente criticado por su índole práctica o funcional para suplir las dificultades que imposibilitan identificar a los responsables individuales. ATIENZA NAVARRO refuerza la parte refutante señalando que existen precedentes donde objeciones similares fueron superadas con éxito, como el seguro de responsabilidad civil, el cual inicialmente se temía que eliminará el efecto preventivo al proteger a los ciudadanos de sus actos negligentes. Pero la autora establece que en la práctica no se ha probado que dicha medida incrementara las conductas negligentes.
Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Parlamento Europeo, Departamento de Políticas C, Comité de Asuntos Jurídicos. P. 41.
Op. cit. Atienza Navarro, M. L. (2022).Daños causados por IA y responsabilidad civil (p.127)

Como ha subrayado NAVAS NAVARRO[34], los sistemas de inteligencia artificial carecen de patrimonio propio, lo que convierte en ineficaz cualquier intento de configurar un sujeto jurídico sin contenido económico. Para responder a esta carencia estructural, se han propuesto diversas soluciones. Algunas apuntan a vincular al sistema de IA los beneficios que pudiera generar a través de su actividad[35]. Otras sugieren la creación de fondos de responsabilidad sostenidos mediante tributos específicos sobre el uso profesional de sistemas inteligentes. NUÑEZ ZORILLA[36] ha llegado incluso a plantear un impuesto colectivo aplicado a todos los consumidores o usuarios de IA, destinado a alimentar un fondo general que actúe como garantía frente a los daños.

No obstante, estas alternativas no resuelven por completo el problema. Como ha advertido ATIENZA NAVARRO[37], cualquiera de estas fórmulas termina repercutiendo, directa o indirectamente, sobre los propios usuarios o propietarios del sistema, lo que reproduce la carga económica que inicialmente se buscaba desplazar. Además, la creación y gestión de patrimonios artificiales asociados a entes sin existencia real implicaría una complejidad administrativa innecesaria. Frente a ello, la doctrina ha señalado que mecanismos ya existentes en los ordenamientos europeos, como el seguro obligatorio o los fondos públicos de compensación, permiten alcanzar los fines resarcitorios de forma más clara, eficiente y operativa, sin necesidad de recurrir a construcciones jurídicas ineficaces o simbólicas.[38]

En definitiva, la atribución de personalidad jurídica a los sistemas de inteligencia artificial surgió como una de las primeras propuestas para resolver los problemas de imputación y reparación de daños causados por tecnologías autónomas. Por tanto, aunque la cuestión ha generado un debate doctrinal relevante, actualmente no tiene efectos prácticos sobre el tratamiento jurídico de la IA, que continúa enmarcándose como un bien dentro del ordenamiento. En su lugar, la Unión Europea ha optado por adaptar los marcos normativos existentes, articulando soluciones a través de los regímenes de responsabilidad civil, tanto objetiva como subjetiva, que serán analizados en los capítulos siguientes.

---

[34] Navarro Navas, S. (s.f.). Sistemas expertos basados en inteligencia artificial y responsabilidad civil. Diario LA LEY.

[35] Op. cit. Atienza Navarro, M. L. (2022).Daños causados por IA y responsabilidad civil (p.113)

[36] Núñez Zorrilla, M. del C. (2019). *Inteligencia artificial y responsabilidad civil: Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*, p. 33.

[37] Op. cit. Atienza Navarro, M. L. (2022).Daños causados por IA y responsabilidad civil (p.129)

[38]Atienza Navarro, M. L. (2019). *El aseguramiento de los robots. Hacia un seguro obligatorio de responsabilidad civil por los daños que cause la inteligencia artificial*, en Monterroso Casado, E. (Dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (pp. 1135–1173). Valencia: Tirant lo Blanch

CAPÍTULO 3. ANÁLISIS DE SUPUESTOS PRÁCTICOS

Descartada la posibilidad de otorgar personalidad jurídica a los sistemas de inteligencia artificial, el análisis debe centrarse ahora en los mecanismos existentes o propuestos por la UE que permiten atribuir responsabilidad por los daños que puedan ocasionar estos sistemas. Como se explicó en el marco normativo, la UE ha optado por ajustar los regímenes de responsabilidad civil, tanto objetiva como subjetiva, a los desafíos que plantean las nuevas tecnologías, sin modificar las categorías jurídicas fundamentales.

Este capítulo tiene como objetivo analizar, desde una perspectiva práctica, cómo operan estos regímenes cuando interviene un sistema de IA, y hasta qué punto las soluciones normativas actuales son eficaces para garantizar tanto la atribución de responsabilidad como la reparación del daño.

Construiremos y analizaremos, dos casos prácticos donde estén involucrados sistemas de IA, que permitan activar y comparar las diferentes modalidades de imputación jurídica previstas en el ordenamiento jurídico español y europeo. Cada caso estará estructurado en torno a una pregunta jurídica central, derivada de las particularidades que introduce la IA en un determinado contexto. Con cada supuesto se analizarán, de forma ordenada, dos posibles vías de imputación: la responsabilidad objetiva por productos defectuosos conforme a la Nueva DRPD[39], y la responsabilidad subjetiva por culpa conforme a los artículos 1902 y siguientes del código civil español y la Propuesta de Directiva de Responsabilidad Civil Extracontractual[40], que aunque paralizada, refleja las soluciones técnicas que se pretendían dar para abordar el problema. De este modo, se busca no sólo ilustrar cómo se aplican estos marcos normativos, sino también poner de relieve sus límites, contradicciones y potenciales zonas de incertidumbre.

Comenzaremos con el caso de responsabilidad objetiva por productos defectuosos conforme a la Nueva DRPD.

[39] 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, L, 25.10.2024.

[40] Comisión Europea. (2022). *Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial* (COM(2022) 496 final).

1. SUPUESTO DE HECHO

El producto objeto de análisis es un sistema de hogar inteligente compuesto por una unidad central de procesamiento (hardware), sensores conectados y una interfaz de usuario accesible mediante comandos de voz y aplicación móvil. Este sistema ha sido comercializado como una solución integral de domótica doméstica orientada a mejorar el confort, la eficiencia energética y la seguridad del hogar. Está diseñado para interactuar con diversos dispositivos conectados —como luces, persianas, electrodomésticos y sistemas de climatización—, permitiendo su activación, regulación o desactivación.

La utilidad de este sistema radica en su capacidad para ofrecer un entorno doméstico inteligente y personalizado. Además de permitir al usuario programar o ejecutar funciones a distancia, incorpora un módulo de inteligencia artificial que le permite observar y procesar los hábitos de uso del hogar e identificar patrones de comportamiento, y a través de este aprendizaje automático, puede anticiparse a las necesidades del usuario y recomendarle ciertas acciones, como un cambio en los horarios de funcionamiento de los electrodomésticos para reducir el consumo energético en función del estudio de cuánto tiempo pasa en casa, o encender la calefacción media hora antes de la hora a la que suele llegar a casa cuando fuera hace una temperatura muy fría. Incluso puede llegar a operar de forma autónoma si las acciones recomendadas son aceptadas por el usuario en la mayoría de veces.

Con el fin de abordar estas cuestiones de forma ordenada, abordaremos los siguiente puntos para determinar si las variantes de este supuesto que planteamos:

- Son un producto: ¿Puede calificarse un sistema de hogar inteligente basado en inteligencia artificial como "producto" conforme a los artículos 128 y siguientes del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU)? ¿Y conforme a la nueva Directiva 2024/2853?
- Son defectuosos: ¿Existe un defecto de información atendiendo a la nueva Directiva 2024/2853? ¿Existe un defecto de diseño atendiendo a la nueva Directiva 2024/2853?
- Nexo causal y carga de la prueba: ¿cómo se acredita la relación entre el defecto y el daño cuando interviene un sistema de IA?
- Régimen de solidaridad de los operadores económicos: ¿Quién responde cuando intervienen múltiples agentes?

2. RESPONSABILIDAD OBJETIVA DEL PRODUCTOS POR PRODUCTOS DEFECTUOSOS: DIRECTIVA (UE) 2024/2853

2.1. Concepto de producto: ¿Puede calificarse un sistema de hogar inteligente basado en inteligencia artificial como "producto" a efectos del régimen de responsabilidad objetiva por productos defectuosos del TRLGDCU? ¿Y conforme a la Nueva DRPD?

En primer lugar, el sistema de hogar inteligente que sirve de base para el análisis integra distintos elementos: hardware (dispositivos conectados), software (sistema operativo y algoritmos de aprendizaje), este último diseñado para aprender de los hábitos del usuario y adaptar su funcionamiento. De este modo, el sistema infiere recomendaciones, ajustes automáticos y acciones que inciden directamente sobre el entorno físico, como regular la temperatura, activar electrodomésticos o modificar parámetros energéticos. Este tipo de funcionamiento se corresponde con la definición antes expuesta de sistema de IA contenida en el artículo 3.1 del Reglamento de IA.

Una vez calificado como sistema de IA, debemos determinar si este sistema, puede ser calificado como "producto" a efectos del régimen de responsabilidad por productos defectuosos. Esta cuestión resulta clave, ya que la aplicabilidad de este régimen presupone que el daño haya sido causado por un producto.

Bajo el marco normativo tradicional se entiende por producto cualquier bien mueble, incluso si está incorporado o unido a otro bien mueble o inmueble, incluyendo bienes como el gas y la electricidad (art. 136 TRLGDCU). Sin embargo, bajo esta definición no tienen cabida nuestros protagonistas digitales, como el software y los sistemas de IA. Esta omisión daba lugar a una zona de inseguridad jurídica, donde el daño causado por el comportamiento autónomo de sistemas de IA, podía quedar fuera del ámbito de imputación objetiva, a pesar de tener un impacto material relevante sobre personas o bienes.

La Nueva DRPD[41], introduce una redefinición amplia y tecnológica del concepto de producto, con el fin de adaptarlo a la realidad digital. El artículo 4.1 establece expresamente que se considerarán productos, entre otros, el "*software, incluidas las actualizaciones y los sistemas de inteligencia artificial*" ya sea a través de descarga o de prestación como servicio. Con ello, se supera de forma definitiva la exclusión tradicional de los bienes intangibles y se incorpora

[41] 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, L, 25.10.2024.

al ámbito de responsabilidad objetiva toda clase de productos digitales, siempre que su funcionamiento pueda causar un daño.

El caso que nos ocupa, responde plenamente a la nueva definición normativa de producto, en tanto que se trata de un sistema operado y distribuido comercialmente, con capacidad para interactuar con el entorno físico y causar daños a personas o bienes, que incorpora funcionalidades autónomas y aprendizaje continuo, se encuentra expresamente contemplado en el ámbito de aplicación material del nuevo texto legal.

Por tanto, el sistema objeto de análisis puede ser calificado, sin dificultad, como un producto a efectos del régimen de responsabilidad objetiva del productor, de conformidad con la Nueva DRPD y su futura transposición al Derecho interno prevista para diciembre de 2026. Esta calificación permite abrir el análisis hacia la siguiente cuestión relevante: la existencia o no de un defecto imputable al productor, lo que requerirá examinar el tipo de defecto que pudiera estar presente —de información, de diseño o de fabricación— y la carga probatoria que incumbe a la víctima.

2.2. Producto defectuoso I : ¿Existe un defecto de información a efectos del régimen de responsabilidad objetiva por productos defectuosos de la Nueva DRPD?

Una vez calificado el sistema de hogar inteligente como producto a efectos del régimen de responsabilidad objetiva, corresponde examinar si en su funcionamiento puede apreciarse un defecto. En el ámbito del Derecho de la Unión Europea, el término "producto defectuoso" se divide generalmente en tres categorías principales: a) defectos de fabricación; b) defectos relacionados con la falta o insuficiencia de información; y c) defectos de diseño[42]. En este caso concretamente, vamos a asumir que no hay defectos ni de fabricación, ni de diseño, y vamos a estudiar la existencia de un defecto de información, conforme a los parámetros del artículo 137.1 del TRLGDCU y del artículo 6 de la Nueva DRPD.

A diferencia de los defectos de fabricación o de diseño —que inciden en la configuración física o funcional del producto—, el defecto de información se produce cuando el producto, siendo en sí estructuralmente correcto, deviene inseguro por la omisión o insuficiencia en la información facilitada al usuario[43].

[42] CITAR
[43] CITAR

La extensión de este deber de información, se ha acotado tradicionalmente, de acuerdo con el artículo 137.1 del TRLGDCU, a el "uso razonablemente previsible" del producto.

En el ámbito de los sistemas de IA, este entendimiento del deber de información se queda corto, por cuanto la autonomía funcional, el aprendizaje continuo y la capacidad de adaptación del sistema introducen una dimensión de incertidumbre que hace más difícil acotar, de forma anticipada, todos los riesgos derivados del "uso razonablemente previsible", del producto. Es más, la propia naturaleza de los sistemas de IA, hace que lo que se busque sea la evolución creativa e imprevisible del sistema[44].

Pues bien, la Nueva DRPD ha abordado esta ambigüedad incorporando una expansión del deber de información partiendo del tradicional deber de informar del uso "razonablemente previsible" (b), tanto desde el punto de vista material (c,d) como temporal (e). En su artículo 6.1, se establece que, para valorar el carácter defectuoso de un producto, deben tenerse en cuenta todas las circunstancias, incluidas las siguientes:

> ***b)*** *el uso razonablemente previsible del producto;*
>
> ***c)*** *el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado;*
>
> ***d)*** *el efecto razonablemente previsible en el producto de otros productos con los que pueda interconectarse;*
>
> *y* ***e)*** *el momento en que el producto dejó de estar bajo el control del fabricante, en caso de que dicho control se haya mantenido tras su comercialización.*

Pasaremos a definir diferentes variantes del caso para atender a estas soluciones que se proponen ante los riesgos de la incorporación de sistema de IA, en el esquema de responsabilidad civil.

a. Uso razonablemente previsible del producto (art. 6.1.b)

Como hemos establecido, la obligación de informar del uso razonablemente previsible, incluso aquellos indebidos (Considerando 31), se ratifica en esta nueva DRPD. En este caso

[44] Peña López, R. (2023). *Responsabilidad por productos defectuosos y nuevas tecnologías: el caso de la inteligencia artificial*, en J. M. Muñoz Vela (Dir.), *Inteligencia artificial y responsabilidad civil* (p. 29). Madrid: Aranzadi.

parece que no hay nada nuevo, de forma que el fabricante deberá de seguir informando en los casos en los que haya sistemas de IA involucrados, de los usos y riesgo que puede prever.

Por ejemplo, en nuestro caso, si el fabricante ha informado adecuadamente sobre los posibles fallos de reconocimiento de voz o sobre la posibilidad de activación involuntaria del sistema por ruido ambiental o por expresiones similares a comandos, y pese a ello el sistema reconoce erróneamente una frase como una orden válida, no puede hablarse de defecto de información.

Imaginemos que, durante una reunión social en casa, una persona está contando una historia y en algún momento dice la frase "…y entonces dije: enciende el horno", y el sistema, interpretándolo como un comando válido, activa el horno automáticamente. Si ello provoca un incendio porque, por ejemplo, había algo dentro del horno, el riesgo derivado no es atribuible a una falta de información del fabricante, sino a una consecuencia previsible advertida del uso del sistema por control vocal.

El sistema ha funcionado conforme a sus capacidades, el riesgo era conocido, informado y razonablemente previsible, y, por tanto, el régimen objetivo no permite imputar responsabilidad por defecto de información en este caso concreto.

b. Uso razonablemente imprevisible: Capacidad de aprendizaje y evolución autónoma (art. 6.1.c) e interacción con otros productos (art. 6.1.d).

Como venimos estableciendo, la sola referencia al uso razonablemente previsible se muestra insuficiente para fundar un régimen informativo sólido en contextos de aprendizaje automático, y precisamente, la novedad de la Nueva RDPD son las circunstancias adicionales que han de tenerse en cuenta a la hora de evaluar el defecto de productos de IA— capacidad de aprendizaje, evolución autónoma e interacción con otros productos—que son las que pueden precisamente llevar a usos imprevisibles.

Ahora bien, estas circunstancias ¿Cómo han de tenerse en cuenta a la hora de definir el defecto de información de un sistema de IA?

¿Basta con que el fabricante incluya una advertencia general de que el sistema puede evolucionar de forma autónoma e interactuar con productos externos, sin especificar sus consecuencias concretas?[45] Si se interpretase que esta disposición permite al fabricante

[45] Cfr. Ibid.

cumplir su deber de información mediante una declaración genérica, el fabricante cumpliría formalmente su deber informativo sin necesidad de identificar los riesgos concretos que esa autonomía podría generar en el futuro, lo que dejaría sin cobertura al usuario en caso de daño.

Por tanto, tiene sentido que no baste con una advertencia general, porque de lo contrario estas novedosas circunstancias devendrían inútiles. Entonces, parece que el productor debe esforzarse por identificar qué nuevas conductas podría desarrollar el sistema, y advertir al usuario de los riesgos asociados. Ahora bien, esto sigue sin resolver el problema de fondo ya que toda la arquitectura del deber de información sigue descansando sobre el principio de previsibilidad.

Como indica PEÑAS LÓPEZ[46] una inteperetacion conjunta de las tres circunstancias de las letras b), c) y d) del artículo 6 Nueva DRPD deriva que las obligaciones informativas del productor han de extenderse a los siguientes aspectos: a) Información sobre usos que el fabricante ha previsto para el producto, y sus riesgos, b) Información sobre usos que el fabricante no ha previsto para el producto, pero puede preveer que el usuario final pueda hacer uso (incluso si este uso es indebido), c) Información relativa a la capacidad de aprendizaje de la IA y su evolución autonoma, así como de la interacción con otros dispositivos y los riesgos razonablemente previsibles derivados de estas características técnicas.

Entonces en un supuesto práctico, supongamos que el sistema de hogar inteligente ha aprendido, tras varias semanas de uso, que el usuario suele encender la calefacción de Noviembre - Febrero a las 18:00 h. Como el sistema ha sido configurado para automatizar tareas habituales en función de patrones de comportamiento, comienza a encenderla de forma autónoma a esa hora.

Un día, el usuario está de viaje y ha olvidado desactivar el sistema. A las 18:00 h, como de costumbre, la calefacción se activa. Al mantenerse encendida durante varias horas, un radiador cerca provoca un incendio (daños materiales) y un consumo energético anómalo.

Ahora bien, el fabricante había informado previamente al usuario de que:

- El sistema incluye funciones de aprendizaje automático que permiten ejecutar acciones de forma autónoma.

[46]Cfr. Op Cit. Peña López p. 50

- Estas acciones pueden activarse sin intervención directa si se repiten ciertos patrones.
- El usuario puede desactivar o limitar dichas funciones en el panel de configuración.
- Y que, como parte del uso normal del producto, existe el riesgo de que algunos dispositivos se activen sin supervisión directa, especialmente cuando el sistema ha sido autorizado previamente para ejecutar determinadas tareas de forma recurrente.

En este caso, no cabe hablar de defecto de información, ya que según se regula en la Nueva DRPD, se ha anunciado correctamente del funcionamiento autónomo del sistema, y el riesgo derivado de estas características.

Entonces, ¿Qué solución se ha dado realmente al problema? Pues realmente, la responsabilidad objetiva por productos defectuosos, incluso en su versión reformada, sigue descansando sobre un modelo cognoscitivo de imputación, en el que el defecto se define por referencia a los riesgos que el fabricante debía conocer y comunicar. Aunque la Directiva extiende el deber de información a la características especiales de estos sistemas no llega a alterar el núcleo del criterio de previsibilidad, que permanece como barrera dogmática ante supuestos de evolución inesperada de la IA.

Por ello, las actuación imprevisibles del sistema de IA, parece que siguen quedándose fuera del defecto de información: no puede imputarse al fabricante responsabilidad por aquello que no podía razonablemente prever, ni siquiera bajo el nuevo marco de la Nueva DRPD, porque "informar sobre lo que no se puede prever es, por definición, imposible"[47].

c. Conservación del control por parte del fabricante tras la comercialización (art. 6.1.e)

La extensión en el ámbito temporal, en cambio, sí que considero que da en el problema a solucionar. Esta novedad hace que el carácter defectuoso del producto pase de valorarse únicamente en el momento de su puesta en circulación, a valorarse también en momentos posteriores cuando el fabricante conserve el "control" del producto.

Este control será conservado por el fabricante, cuando se realiza bien por él o bien por un tercero*: "i) la integración, interconexión o suministro de un componente, incluidas las actualizaciones o mejoras de los programas informáticos, ii) la modificación del producto, incluidas las modificaciones sustanciales; iii) la capacidad del fabricante de un producto de*

[47] Op Cit. Peña López p.51

suministrar actualizaciones o mejoras de programas informáticos, por sí mismo o a través de un tercero;"

Por ejemplo, en este caso, una vez lanzado el producto, el fabricante lanza una actualización crítica del software destinada a corregir errores de compatibilidad con determinados dispositivos térmicos. Sin embargo, no se envía un mensaje de actualización al usuario. Pues bien, en el caso de que la no instalación de esta actualización, cause un daño como por ejemplo un incendio por sobrecalentamiento se desplegará el régimen de responsabilidad objetiva por productos defectuoso.

Esto se trata de una mejora con respecto del régimen anterior, regulando la ambigua situación de actualización de los sistemas de digitales, obligando al productor a mantener actualizado el deber de información debiendo comunicar los nuevos riesgos que vayan apareciendo como consecuencia de su evolución o integración con otros productos.[48]

Problema	**Regulación DRPD Derogada**	**Novedad Nueva DRPD**	**Consecuencias**	**Caso**	**Defecto de información**
El productor no puede informar sobre riesgos imprevisibles que se derivan de la evolución funcional autónoma del sistema de IA.	Se exigía advertir al consumidor sobre los riesgos previsibles del uso del producto.	Extensión del deber de información: Capacidad de aprendizaje y evolución autónoma (art. 6.1.c) e interacción con otros productos (art. 6.1.d).	Se debe informar sobre estas características y los riesgos previsibles de las mismas.	Funcionamiento imprevisible y autónomo de encender la calefacción que provoca incendio: • Habiendo informado de la capacidad de aprendizaje y autonomía del sistema, pero no habiendo informado de los riesgos concretos.	NO DEFECTO DE INFORMACIÓN
Los sistema de IA, se actualizan y evolucionan con el tiempo por lo que el defecto se debe apreciar no solo en el momento de puesta en el mercado.	La información se valora en el momento de la puesta en el mercado.	Extensión del deber de información: Conservación del control por parte del fabricante tras la comercialización (art. 6.1.e)	Se extiende el deber de información si se mantiene el control, como con las actualizaciones	Incendio por no instalación de una actualización: • Sin haber notificado al usuario de la actualización	DEFECTO DE INFORMACIÓN. Se activa la responsabilidad objetiva.

[48] Ibid.

2.3. Producto defectuoso II: ¿Existe un defecto de diseño a efectos del régimen de responsabilidad objetiva de la Nueva DRPD?

Como se ha expuesto en el apartado anterior, el presente análisis descarta que el daño derivado del funcionamiento imprevisible y autónomo del sistema de hogar inteligente pueda calificarse como un defecto de información cuando el productor ha cumplido su deber de advertencia y ha proporcionado datos relevantes al consumidor sobre la autonomía del sistema, su capacidad de aprendizaje y el riesgo derivado de la activación de dispositivos sin intervención directa, así como los mecanismos para desactivar dichas funciones. AHora nos planteamos, ¿podría esta imprevisibilidad y su materialización dañosa calificarse este diseño como defectuoso en los términos del artículo 6 de la Directiva (UE) 2024/2853?

En el supuesto planteado, el sistema ha aprendido, a través de patrones de uso repetidos, que el usuario activa la calefacción a las 18:00 h durante los meses de invierno. Conforme a su configuración, el sistema automatiza esta tarea y, al detectar el patrón, activa la calefacción de forma autónoma. Un día en que el usuario se encuentra ausente y no ha desactivado la funcionalidad, el sistema la ejecuta como de costumbre. El encendido prolongado de un radiador cercano provoca un sobrecalentamiento que origina un incendio, causando daños materiales. ¿Puede calificarse de defecto de diseño el hecho de que un producto funcione de manera técnicamente correcta, pero de forma potencialmente peligrosa, por carecer de salvaguardas estructurales frente a su autonomía?

El defecto de diseño se produce cuando el producto, aun actuando conforme a la lógica técnica prevista por su fabricante, presenta una configuración estructural que no garantiza un nivel de seguridad adecuado. A diferencia del defecto de fabricación, que implica una desviación puntual respecto del diseño previsto, el defecto de diseño es congénito: el riesgo está presente en todos los ejemplares del producto, porque deriva del modo en que fue concebido. Y se diferencia también del defecto de información en que no se trata de un problema de omisión o insuficiencia de advertencias, sino de una arquitectura técnica que genera peligros evitables.

La DRPD Derogada, establece que un producto se considerará defectuoso cuando no ofrezca la seguridad que cabe legítimamente esperar, atendiendo a todas las circunstancias del caso. Este juicio de imputación se basa en el criterio de las **expectativas legítimas del consumidor** medio razonablemente informado y prudente, que constituye el eje central para determinar si

un producto es seguro. El productor no responde por todo resultado lesivo, sino por aquellos derivados de un diseño que frustra razonablemente esas expectativas.

A esta dimensión subjetiva se suma una valoración objetiva vinculada al estado de la técnica. Según el conocido test de riesgo-utilidad, un diseño será jurídicamente defectuoso si, en el momento de su comercialización, existía una alternativa más segura, técnica y económicamente viable, que habría evitado el daño prevesible sin comprometer la funcionalidad del producto.

Pues en este caso concreto, donde tenemos la presencia de un sistema de IA, tenemos varios desafíos. En primer lugar, el problema de la imprevisibilidad también está presente, dado que no se le puede exigir al productor que tome una serie de medidas en el diseño a vistas de los posibles riesgos que puede generar una IA que actúa de forma imprevisible. En este caso, el daño se produce por una acción que no estaba directamente programada, sino que surge del comportamiento adaptativo del sistema, ¿puede hablarse de riesgo previsible? ¿Dónde está el límite entre la autonomía legítima y el riesgo imputable? La Nueva DRPD no elimina este requisito, pero lo matiza: en su artículo 6.1 establece que debe valorarse, al determinar el carácter defectuoso de un producto, su capacidad para adquirir nuevas funcionalidades tras la comercialización. Con ello, parece reconocer que el productor debe anticipar no solo los riesgos inmediatos, sino también los que deriven razonablemente del comportamiento evolutivo del sistema.

En segundo lugar, mientras que en el modelo tradicional de responsabilidad por defecto de diseño bastaba con valorar si el diseño era seguro conforme al estado de la técnica en el momento de la comercialización, los productos inteligentes, especialmente aquellos con capacidad de aprendizaje, siguen operando, actualizándose e interactuando con nuevos entornos durante años. Esto genera una tensión jurídica evidente: si el estado de la técnica en el momento de lanzamiento del producto era uno, pero al poco tiempo se generalizan soluciones más seguras, ¿puede exigirse al productor que adapte su diseño, o que lo actualice conforme a los nuevos estándares? La Nueva DRPDD introduce aquí un criterio intermedio: si el productor mantiene el control del producto —por ejemplo, mediante actualizaciones, conectividad remota o supervisión continuada—, se le podrá exigir que actúe conforme al estado de la técnica vigente, no solo al del momento de la comercialización. Pero si no tiene control posterior, el juicio se mantendrá en el plano clásico.

Por último, exigir al productor que incorpore todas las salvaguardas posibles o que reaccione ante cada avance técnico puede suponer una carga económica desproporcionada, especialmente si hablamos de sistemas complejos en mercados dinámicos. ¿Dónde se sitúa el equilibrio entre la innovación y la seguridad? ¿Hasta qué punto se puede exigir rediseñar o reconfigurar todo un sistema para cubrir un riesgo que, aunque técnicamente previsible, solo se concreta tras muchas combinaciones contextuales? En este punto, la Directiva no introduce un criterio explícito, pero mantiene implícitamente el tradicional test de riesgo-utilidad: el diseño solo será defectuoso si existía una alternativa más segura, técnicamente viable y económicamente razonable.

Ahora bien, la calificación del diseño como defectuoso en este supuesto práctico planteado requiere un análisis más matizado respecto de la previsibilidad del riesgo y el uso previsible del producto. En efecto, nos encontramos ante un sistema de inteligencia artificial que no ejecuta una orden concreta programada ex ante, sino que actúa en virtud de un patrón de conducta aprendido a partir del comportamiento del usuario. El daño no se produce por un mal uso voluntario, sino por una combinación de factores: la autonomía funcional del sistema, la ausencia del usuario y la prolongación del encendido térmico. Esta situación plantea una dificultad jurídica evidente: ¿puede exigirse al productor que prevea un riesgo que no se deriva de un defecto puntual ni de un uso anómalo, sino del aprendizaje algorítmico del propio sistema?

Aplicando estos criterios al caso del sistema de calefacción autónomo, vemos que atendiendo a criterios de expectativas legítimas del consumidor, para le usuario resulta evidente que el diseño adoptado frustra la expectativa legítima de seguridad del consumidor medio, que aun sin entender del funcionamiento interno del sistema de IA, e incluso habiendo sido informado de que el sistema puede actuar de forma autónoma, el usuario medio puede razonablemente esperar que el sistema se capaz de detectar de algún tipo de forma, que el no esta en casa, o que está habiendo un sobrecalentamiento que puede causar un daño. Estas expectativas son especialmente significativas tratándose de un sistema destinado al hogar, cuyo uso está estrechamente vinculado a la protección de la vida, la integridad física y el patrimonio.

Pasando al criterio riesgo-utilidad, la calificación del diseño como defectuoso en este supuesto requiere matizar con precisión la cuestión de la previsibilidad del riesgo, para no incurrir en contradicción con el análisis del defecto de información. En efecto, como se ha argumentado anteriormente, el productor no podía prever ni advertir con precisión el riesgo concreto que

finalmente se materializa, ya que la conducta del sistema —activar la calefacción en ausencia del usuario— no responde a un comportamiento directamente programado, sino a una lógica adaptativa construida por el propio sistema en función de patrones aprendidos. Por ello, el deber de información del productor se limitaba a advertir que el sistema funcionaba de forma autónoma, que podía ejecutar acciones sin intervención del usuario, y que eso conllevaba ciertos riesgos razonables en el uso ordinario del producto. No se le podía exigir más.

Ahora bien, el juicio de previsibilidad que opera en el análisis del defecto de diseño es de naturaleza distinta: no exige anticipar el resultado concreto, sino valorar si, en el momento de comercialización, el diseño del producto permitía —sin límites ni salvaguardas— que el sistema realizara acciones potencialmente peligrosas en contextos previsibles de uso doméstico. El productor no tenía por qué prever que un radiador específico se sobrecalentaría ese día concreto, pero sí debía contemplar que un sistema que automatiza tareas térmicas, sin verificar presencia humana ni establecer límites temporales, podía llegar a ejecutar una acción de riesgo estructural. Lo que se le imputa, por tanto, no es la imprevisibilidad del resultado puntual, sino la omisión de medidas de protección razonables frente a riesgos típicos de su propia arquitectura funcional autónoma.

Por todo lo anterior, considero que la omisión de estas medidas de seguridad —como sensores de presencia, límites temporales o alertas remotas— no puede justificarse por la imprevisibilidad del resultado concreto. Ahora bien, esta imputación solo es jurídicamente razonable si se demuestra que, en el momento de la comercialización del producto, ya existían soluciones técnicas disponibles y económicamente viables para mitigar ese tipo de riesgo funcional. Es decir, si el estado de la técnica en ese momento ya contemplaba, como prácticas habituales en el sector domótico, sistemas de validación, sensores de presencia o límites programables en tareas de riesgo térmico. Habría que ver en este caso, pero vamos a asumir que estas no se usaban cuando se desplegó el producto por primera vez, sino que se convirtió en un práctica utilizada al año de que el sistema estuviera en el mercado ¿Deberían de haberse introducido, debido a que el fabricante retiene el control? La Nueva DRPD parece indicar que si el productor mantiene el control del producto tras su comercialización, por ejemplo mediante actualizaciones, conectividad remota o canales de supervisión, podrá exigírsele que adapte su producto a los nuevos estándares de seguridad técnica. Esto desplaza el juicio de imputación más allá del instante inicial, y plantea una tensión de fondo entre seguridad jurídica e incentivo a la innovación. Si se exige al productor que esté permanentemente al día con las mejoras técnicas disponibles, corremos el riesgo de desincentivar la evolución

funcional de productos inteligentes. Pero si no se le exige nada tras la comercialización, el sistema normativo puede quedar desbordado ante daños provocados por sistemas autónomos que el productor aún controla, pero no supervisa.

Esta tensión no está resuelta de forma cerrada en la Directiva, pero sugiere un modelo de responsabilidad dinámico: uno que no impone un perfeccionismo retrospectivo, pero que sí refuerza el deber de diligencia técnica cuando el productor conserva capacidad de intervención efectiva sobre el sistema. Así se dibuja el nuevo equilibrio entre protección del consumidor e innovación tecnológica en el régimen europeo de responsabilidad objetiva frente a la inteligencia artificial.

Problema	Regulación DRPD Derogada	Novedad Nueva DRPD	Consecuencias	Caso	Defecto de información
El productor no puede prever todas las situaciones futuras derivadas del aprendizaje autónomo del sistema, el estado de la técnica evoluciona rápidamente y las soluciones más seguras pueden resultar económicamente desproporcionadas.	Se analizaba si el diseño era seguro conforme al estado de la técnica en el momento de la comercialización.	Extensión de las circunstancias a la hroa d tener en cuenta el diseño: Capacidad de aprendizaje y evolución autónoma (art. 6.1.c) e interacción con otros productos (art. 6.1.d), Conservación del control por parte del fabricante tras la comercialización (art. 6.1.e)	El diseño será defectuoso si no incorpora barreras razonables frente a riesgos previsibles, debiendo incorporar estas técnicas mientras se mantenga el control del producto.	Funcionamiento imprevisible y autónomo de encender la calefacción que provoca incendio: • Sin establecer medidas de protección.	DEFECTO DE DISEÑO. Se activa la responsabilidad objetiva.

2.4. Nexo causal y carga de la prueba: ¿Cómo se acredita la relación entre el defecto y el daño cuando interviene un sistema de IA?

La mera calificación de un producto como defectuoso no es suficiente para atribuir responsabilidad al productor; es imprescindible, además, que el perjudicado logre probar la existencia de un nexo causal entre ese defecto y el daño sufrido. Esta exigencia, heredada del régimen tradicional de la derogada Directiva 85/374/CEE, se mantiene en la Nueva DRPD, aunque incorporando mecanismos que suavizan la carga probatoria ante las particularidades tecnológicas de los productos inteligentes. Uno de los principales obstáculos que enfrentan los consumidores en estos supuestos reside en la opacidad y complejidad técnica del sistema, que impide reconstruir el funcionamiento del producto en el momento del daño.

Esta dificultad se hace patente en ambos supuestos analizados. En el primer caso, referido al defecto de información, el sistema sufrió un fallo tras no haberse instalado una actualización crítica que el usuario desconocía por completo, al no haber sido debidamente notificado por el fabricante. En tales condiciones, el consumidor carece tanto de los conocimientos como de los medios técnicos para demostrar que el daño deriva directamente de esa omisión. Sin acceso al historial de versiones, registros de control o trazabilidad del software, la prueba del nexo causal queda fuera de su alcance.

En el segundo caso, el daño proviene del diseño estructural del sistema, cuya capacidad de aprendizaje automático llevó al encendido autónomo de un calefactor en ausencia del usuario, desencadenando un incendio. Aunque el producto funcionó conforme a su lógica interna, carecía de medidas de seguridad básicas —como sensores de presencia, alertas o apagado automático— que habrían evitado un uso peligroso en contextos no supervisados. Sin embargo, para la víctima resulta prácticamente imposible demostrar que ese comportamiento fue consecuencia directa de un defecto de diseño, dado que no puede acceder ni comprender los procesos algorítmicos que guiaron la acción del sistema en ese momento.

La Directiva 2024/2853 aborda esta problemática mediante el artículo 10.4, que permite al órgano jurisdiccional presumir la existencia del defecto y/o del nexo causal cuando el demandante acredite, por un lado, la existencia de una dificultad técnica o científica significativa, y por otro, aporte indicios serios que apunten a dicho defecto o vínculo causal. En ambos escenarios analizados, concurren claramente estos elementos: la alta complejidad del sistema impide reconstruir su conducta, la opacidad algorítmica obstaculiza la identificación de la causa precisa del daño, y la información proporcionada por el productor ha resultado insuficiente o incompleta.

Por tanto, la presunción establecida en el artículo 10.4 permite reequilibrar la posición procesal del consumidor en casos donde el daño proviene de sistemas inteligentes opacos y autónomos, ofreciendo una vía realista para exigir responsabilidad en un entorno técnico en el que la prueba directa se vuelve, en muchos casos, inaccesible.

Esta presunción no es, sin embargo, definitiva. El productor podrá refutarla, pero mientras tanto, el marco probatorio europeo coloca al consumidor en una posición más equilibrada, haciendo recaer sobre el productor —único que controla el comportamiento interno del producto— el deber de aportar una explicación técnica alternativa.

Ahora bien, también se recoge causa de inexoneracion de responsabilidad si el defecto se deriva de la omisión de una actualización crítica, la Directiva prevé expresamente en su artículo 11.2 que el productor no podrá exonerarse de responsabilidad si el defecto se debe a: (i) un servicio conexo, (ii) programas informáticos (incluidas las actualizaciones), (iii) falta de actualizaciones o mejoras de los programas informáticos necesarias para mantener la seguridad o (iv) una modificación sustancial del producto bajo su control.

Este régimen refuerza de manera significativa la responsabilidad del productor frente a productos evolutivos, como los sistemas de IA, que dependen de mantenimientos periódicos, ajustes y mejoras para preservar sus condiciones de seguridad.

En conclusión, el nuevo marco probatorio de la Directiva 2024/2853 permite una mejor adaptación del régimen de responsabilidad por productos defectuosos a los sistemas inteligentes y complejos como el hogar digital. La introducción de presunciones de defecto y de causalidad, bajo condiciones razonables, permite aligerar la carga que tradicionalmente recaía sobre el consumidor, pasándosela al fabricante, sin comprometer los derechos de defensa del fabricante.

Cabe mencionar, que los fabricantes disponen de mayores medios técnicos y acceso a la información necesaria para analizar el funcionamiento interno del sistema, ello no significa que la tarea de identificar la causa concreta del daño sea sencilla. La imprevisibilidad inherente a los sistemas de inteligencia artificial, especialmente aquellos basados en aprendizaje automático, genera comportamientos que ni siquiera sus desarrolladores pueden anticipar plenamente. A esto se suma la opacidad algorítmica, que dificulta la trazabilidad de la decisión o acción que desencadena el daño. Por tanto, aunque el productor sea quien está en mejor posición para reconstruir el fallo, no puede presumirse que esa labor sea directa o mecánica, y menos aún cuando intervienen múltiples variables dinámicas y datos contextuales en tiempo real.

Pero en definitiva, en casos como el aquí analizado, donde concurren dificultades probatorias técnicas y una omisión significativa en el deber de información, la víctima podrá acogerse a este régimen de presunción para revertir la carga de la prueba y exigir una reparación por los daños sufridos, siempre que logre aportar indicios razonables de que el defecto y el daño están conectados.

2.5. Régimen de solidaridad de los operadores económicos: ¿Quién responde cuando intervienen múltiples agentes?

Una última cuestión que resulta especialmente relevante en el contexto de productos complejos como los sistemas de hogar inteligente es la identificación del sujeto responsable. Aun cuando se presuma la existencia de un defecto y su relación causal con el daño, en muchos casos el consumidor no puede determinar con certeza quién fue el operador económico que incurrió en la omisión.

Precisamente por eso, el artículo 12 de la Directiva 2024/2853 establece un régimen de responsabilidad solidaria entre todos los operadores económicos que, conforme al artículo 8, puedan considerarse responsables del defecto:

- el fabricante del producto final, que responde directamente cuando el defecto de diseño reside en el funcionamiento autónomo del sistema bajo su control.
- el fabricante de un componente defectuoso, si dicho componente ha sido integrado o interconectado en el producto y ha causado su defectuosidad.
- En caso de que el fabricante esté establecido fuera de la Unión, la responsabilidad podrá recaer en el importador, en su representante autorizado, o, en su defecto, en el prestador de servicios logísticos.
- Además, cualquier persona que modifique sustancialmente el producto fuera del control del fabricante original y lo comercialice será considerada igualmente responsable como fabricante.
- Solo de forma subsidiaria, y en defecto de identificación de estos operadores económicos, podrá exigirse responsabilidad al distribuidor, e incluso al proveedor de una plataforma en línea.

Esta solidaridad opera con independencia del tipo de defecto, e incluye expresamente el defecto de información, en el que la falta de una advertencia adecuada puede atribuirse a distintos actores de la cadena de suministro o comercialización.

Así, la víctima no necesita probar quién fue exactamente el causante de la omisión, sino que puede dirigirse contra cualquiera de ellos para exigir la reparación del daño. Esta previsión refuerza de forma práctica la protección del consumidor frente a productos complejos, donde los componentes (hardware, software, actualizaciones, integraciones) están en manos de múltiples agentes intervinientes.

3. CONCLUSIÓN

El análisis del supuesto del hogar inteligente demuestra que la Directiva 2024/2853 supone un avance significativo en la protección del consumidor frente a productos defectuosos basados en inteligencia artificial. Su principal aportación radica en adaptar las categorías clásicas del defecto (información y diseño) a las nuevas realidades tecnológicas, así como en reequilibrar las cargas procesales y probatorias que, de otro modo, harían inviable la acción de responsabilidad.

No obstante, este nuevo marco mantiene como fundamento último el principio de previsibilidad del daño. Los actos realmente imprevisibles —es decir, aquellos que el productor no podía anticipar razonablemente ni en términos técnicos ni contextuales— siguen quedando fuera del perímetro de imputación objetiva. En este sentido, la Directiva continúa anclada a un modelo cognoscitivo de responsabilidad, en el que se responde por lo que se conoce, se debe conocer o se puede conocer. Esto deja sin cobertura, todavía, a ciertos riesgos emergentes de la inteligencia artificial.

Pese a ello, los mecanismos presuntivos de causalidad y la responsabilidad solidaria entre operadores introducen mejoras sustanciales que refuerzan el derecho efectivo a la reparación. En definitiva, aunque el régimen sigue siendo perfectible —especialmente ante los límites dogmáticos de la imprevisibilidad—, la Directiva 2024/2853 constituye un paso firme hacia un Derecho de daños europeo más adaptado a la era digital.

CAPÍTULO IV. ANÁLISIS DE SUPUESTOS PRÁCTICOS: RESPONSABILIDAD SUBJETIVA EXTRACONTRACTUAL

1. SUPUESTO DE HECHO

Una empresa multinacional con sede en España utiliza un sistema de inteligencia artificial para realizar una **filtración preliminar de currículums vitae** en sus procesos de selección de personal. El sistema, provisto por un tercero tecnológico, está entrenado para detectar perfiles “ajustados” a los valores y el “historial de éxito” de la empresa, priorizando trayectorias laborales similares a las de sus empleados actuales. El sistema filtra automáticamente los currículums que no superan cierto umbral, que varía según el puesto.

Una candidata, licenciada con expediente brillante, experiencia internacional y recomendación académica de alto nivel, no supera el primer corte. Al pedir explicaciones, se

le comunica que “su perfil no encajaba con el modelo predictivo” y que no podrá acceder a la siguiente fase.

La demandante presenta una acción por daños y perjuicios contra la empresa, alegando discriminación indirecta y negligencia en la supervisión del sistema de IA. La empresa niega responsabilidad, alude a la fiabilidad del proveedor, y se niega a exhibir los criterios técnicos del sistema, invocando secreto empresarial.

2. RESPONSABILIDAD SUBJETIVA EXTRACONTRACTUAL: PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO 28.9.2022

2.1. El modelo tradicional: límites del artículo 1902 CC ante sistemas de IA autónomos

Ante esta situación, el régimen tradicional de responsabilidad civil recogido en el artículo 1902 del Código Civil muestra su insuficiencia estructural. Como es sabido, la aplicación de esta norma exige la concurrencia de un comportamiento humano activo u omisivo, un daño cierto, una relación de causalidad entre ambos y la existencia de culpa o negligencia por parte del agente.

Sin embargo, este modelo presenta importantes limitaciones cuando el daño resulta de una decisión algorítmica no transparente. Aplicando el régimen subjetivo clásico del artículo 1902 del Código Civil, la víctima debería acreditar la concurrencia de una acción u omisión negligente, un daño cierto, y un nexo causal entre ambos. Sin embargo, como señala Peña López, el esquema clásico resulta inviable cuando el funcionamiento del sistema se basa en criterios no observables, no auditables y no justificables conforme a patrones humanos de racionalidad, lo que impide al perjudicado reconstruir la culpa del operador[49].

Además, en estos contextos, la víctima se enfrenta a una asimetría probatoria insalvable: no dispone de acceso al diseño técnico del sistema, a los datos que lo alimentaron, ni a los logs que permitan rastrear la lógica de decisión. Incluso asistida por peritos, carece de los elementos necesarios para probar la infracción del deber de diligencia, que sigue siendo un presupuesto indispensable incluso en los supuestos cubiertos por presunciones de causalidad[50].

[49] CITR
[50] CITR

Así, el régimen de responsabilidad subjetiva tradicional resulta ineficaz ante decisiones donde el componente humano está diluido y el razonamiento causal se aloja en una caja negra algorítmica. Sin conexión verificable entre conducta humana y daño, la noción de culpa pierde operatividad funcional[51].

2.2. El marco propuesto por la Directiva COM(2022) 496: una transformación procesal del modelo de responsabilidad subjetiva

Ante esta situación, el régimen tradicional de responsabilidad civil recogido en el artículo 1902 del Código Civil muestra su insuficiencia estructural. Por lo que analizaremos las propuestas de conciliación con esta situación de la derogada Propuesta de Directiva de Responsabilidad Extracontractual, para evaluar si estaba bien encaminada.

a. Acceso a la información (Art. 3)

El artículo 3 introduce una regla general de exhibición judicial de pruebas técnicas, inspirada en el discovery estadounidense, que obliga al operador, proveedor o usuario a exhibir documentación técnica cuando el perjudicado haya presentado una solicitud razonada y se hayan agotado los intentos proporcionados. Si el demandado incumple esta obligación, se presume que ha infringido un deber de diligencia (art. 3.5), lo que, a su vez, activa la presunción de causalidad del artículo 4.

b. Presunción iuris tantum de relación de causalidad (Art. 4)

Una de las principales dificultades que plantea la exigencia de responsabilidad civil subjetiva en entornos tecnológicos complejos es la reconstrucción del nexo de causalidad entre la conducta negligente del operador y el daño derivado del funcionamiento del sistema. Cuando el daño es provocado o facilitado por un sistema de inteligencia artificial de comportamiento autónomo y razonamiento no interpretable, el requisito probatorio tradicional —que exige al demandante acreditar que la acción u omisión del demandado ha sido causa eficiente del daño— se convierte en una carga imposible. Como ha destacado PEÑA LOPEZ, en estos supuestos, el concepto mismo de "culpa" queda jurídicamente desactivado si no se establece un marco específico de facilitación de la prueba, capaz de traducir el principio de responsabilidad subjetiva a entornos de causalidad tecnológicamente interpuesta y cognitivamente opaca.

[51] CITAR

El artículo 4 de la Propuesta de Directiva sobre responsabilidad civil en materia de inteligencia artificial introduce una presunción refutable de relación de causalidad entre la culpa del operador (profesional) y el daño producido por el sistema de IA, siempre que se cumplan de forma acumulativa una serie de requisitos estrictamente definidos. A diferencia de lo que ocurre con otros modelos de inversión de la carga de la prueba, el artículo 4 no elimina la lógica subjetiva, sino que la adapta a las condiciones reales del entorno probatorio, estableciendo un sistema escalonado que solo se activa si concurren tres elementos.

En primer lugar, el órgano jurisdiccional deberá constatar que el demandado ha incurrido en culpa, entendida como el incumplimiento de un deber de diligencia establecido por el Derecho nacional o de la Unión, dirigido específicamente a proteger frente al tipo de daño sufrido. Esta culpa puede haber sido demostrada directamente por el demandante o puede ser presumida conforme al artículo 3.5 si el operador ha incumplido su deber de exhibir pruebas o registros técnicos. La presunción de causalidad, por tanto, no se activa de forma automática: exige una base normativa previa para considerar que existió una infracción de deber.

En segundo lugar, debe apreciarse que, atendiendo a las circunstancias del caso, es razonablemente probable que el incumplimiento haya influido en el resultado generado (o no generado) por el sistema de IA. El legislador europeo no exige certeza técnica, sino probabilidad razonable, un estándar de valoración judicial que toma en consideración el grado de dependencia de la decisión respecto al sistema, el margen de actuación humana y la naturaleza del riesgo.

Finalmente, el demandante debe acreditar que el output (o su ausencia) del sistema de IA ha sido causa del daño. Esta última exigencia es clave, ya que evita que la presunción se aplique de forma abstracta o genérica: no basta con demostrar que el sistema funcionó mal, sino que debe acreditarse que el resultado técnico ha tenido efectos jurídicos lesivos sobre la posición del demandante.

Este triple filtro normativo responde, a un diseño legislativo orientado a reconfigurar la carga probatoria sin quebrar la matriz de la responsabilidad subjetiva, mediante un modelo de presunción estructurada, progresiva y técnicamente razonable. La Directiva no crea un sistema de imputación objetiva por el mero uso de IA, sino que articula un régimen de responsabilidad gradual, condicionado al incumplimiento verificable de estándares jurídicos de diligencia.

Además, el artículo 4 incorpora un segundo nivel normativo dirigido a los proveedores o sujetos que asumen sus obligaciones conforme al Reglamento de Inteligencia Artificial. En estos casos, el requisito de la letra a) solo se considera cumplido si el demandante acredita que se han vulnerado ciertos preceptos técnicos del Reglamento, como los relativos a la calidad de los datos de entrenamiento (art. 10), la transparencia (art. 13) o la robustez del sistema (art. 15). Se impone así una carga técnica adicional al demandante que dirija su acción contra el diseñador del sistema, reforzando el enfoque centrado en el operador profesional como sujeto primario de imputación.

Por último, el artículo 4 excluye de esta presunción a los usuarios no profesionales, salvo que hayan interferido sustancialmente en el funcionamiento del sistema o hubieran estado en condiciones de determinar sus parámetros de uso. Esta exclusión refuerza el carácter profesional de la responsabilidad prevista por la Directiva, que no pretende extenderse a contextos domésticos o no especializados.

La presunción puede ser refutada por el operador si demuestra que el resultado habría ocurrido igualmente o que el sistema funcionó correctamente conforme a sus parámetros. En este sentido, como concluye Díez Royo, se trata de una presunción racionalizada y técnicamente proporcionada, que no rompe el principio de imputación por culpa, sino que lo hace compatible con el uso de sistemas autónomos en entornos regulados.

c. Aplicación práctica

El sistema utilizado por la empresa para el filtrado de currículums constituye un sistema de IA de alto riesgo, según lo establecido por el artículo 6 del Reglamento de IA, al afectar al acceso al empleo y al ejercicio de derechos fundamentales. En este contexto, el operador profesional —la empresa usuaria— está sujeto a obligaciones jurídicas específicas en virtud del Reglamento, como el deber de transparencia (art. 13), supervisión activa del sistema (art. 28) y documentación de los criterios de decisión.

Tras la negativa de la empresa a exhibir los parámetros técnicos de evaluación utilizados por el sistema, la candidata podría instar al órgano jurisdiccional a declarar la existencia de un incumplimiento del deber de diligencia conforme al artículo 3.5 de la Propuesta, lo que activaría la presunción de culpa exigida por el artículo 4.1 a).

En segundo lugar, la relación entre ese incumplimiento (falta de transparencia, de revisión humana, uso de criterios sesgados) y el resultado producido (exclusión de la candidata) puede razonablemente considerarse probable, especialmente si se constata que la decisión fue íntegramente automatizada y que no existió intervención humana ni posibilidad de revisión interna. Ello satisface el requisito de la letra b).

Por último, si la candidata acredita que la exclusión le impidió acceder a un proceso selectivo objetivo y provocó un daño profesional o moral concreto, se cumplirá también el requisito de la letra c): la relación causal entre el output del sistema y el daño. En tal caso, el tribunal podría activar la presunción de relación causal entre el incumplimiento y el perjuicio, obligando a la empresa a refutarla para eludir su responsabilidad.

Este caso demuestra que el diseño escalonado del artículo 4 es plenamente funcional en escenarios en los que la responsabilidad subjetiva —aunque formalmente conservada— se encuentra en riesgo de quedar vacía de contenido práctico por falta de acceso a elementos probatorios clave.

3. CONCLUSIÓN

A través de estos mecanismos, la Propuesta logra reorientar el análisis jurídico hacia lo verdaderamente decisivo: no el funcionamiento interno del sistema de IA, sino la conducta del operador que lo utiliza. Se preserva así el principio de imputación por culpa, pero se redefine su contenido material. Como ha señalado el Grupo de Expertos sobre Nuevas Tecnologías de la Comisión, quien decide operar con tecnologías opacas asume la responsabilidad de su gobernanza, y no puede escudarse en su complejidad técnica para exonerarse. La clave ya no reside en demostrar cómo funciona el algoritmo, sino en acreditar que se ha cumplido con los deberes de diligencia, supervisión y control que exige su uso ético y jurídicamente responsable.

Desde una perspectiva crítica, la Propuesta representa un avance significativo en el proceso de adaptación del Derecho de daños a los entornos algorítmicos. Su gran virtud reside en que, sin necesidad de abandonar el paradigma de responsabilidad subjetiva, introduce herramientas para equilibrar el acceso a la prueba, rebajar la exigencia de prueba diabólica del nexo causal y desplazar el foco de la responsabilidad hacia el control humano sobre el riesgo tecnológico. Como señala Fernando Peña López, estas reformas permiten que el modelo clásico de culpa sobreviva en escenarios donde, de otro modo, resultaría inoperante[7].

No obstante, la Propuesta presenta lagunas importantes. En primer lugar, no define con precisión cuáles son las obligaciones legales cuya infracción activa la presunción de causalidad. La remisión al Reglamento de IA plantea dificultades de integración normativa, ya que no todas las infracciones técnicas son jurídicamente relevantes para el Derecho de daños. En segundo lugar, la Propuesta no incorpora mecanismos de reparación automática ni impone obligaciones de aseguramiento, lo que deja sin resolver los problemas estructurales de insolvencia o de cobertura en los supuestos de daños masivos. Tampoco se abordan los problemas de imputación en escenarios de múltiples operadores o de responsabilidad en cadena. Finalmente, su paralización en el proceso legislativo europeo, que ha quedado detenida tras la aprobación del Reglamento de IA, evidencia una falta de consenso político sobre el alcance y el momento oportuno de esta reforma.

En este contexto, la respuesta jurídica no puede ser la inacción. La paralización de la Propuesta no elimina los problemas que esta intentaba resolver. Por el contrario, exige una respuesta interpretativa de los tribunales nacionales que, en ausencia de norma armonizada, comiencen a aplicar los principios en ella contenidos por vía de analogía, interpretación integradora o mediante el desarrollo de jurisprudencia pro víctima. Resulta urgente que los Estados miembros articulen, al menos a nivel procesal, reglas de facilitación probatoria, de exhibición de registros técnicos y de presunción razonable de causalidad tecnológica. No hacerlo supone condenar al fracaso cualquier intento de tutela efectiva frente a daños derivados de sistemas cuyo funcionamiento solo conocen quienes los operan o diseñan.

En conclusión, la Propuesta de Directiva COM(2022) 496 ofrecía una solución razonable, jurídicamente viable y técnicamente adaptada a los retos que plantea la inteligencia artificial en el ámbito de la responsabilidad civil. Su aplazamiento supone que bien se replantean otras formas de lidiar con la situación, como la responsabilidad objetiva.

CAPÍTULO IV. PROPUESTAS Y CONCLUSIONES