La causa de exoneración de los riesgos por desarrollo en el nuevo paradigma digital*

The development risks in the digital era

Guillem Izquierdo Grau
Universidad Autónoma de Barcelona
ORCID ID: 0000-0002-8755-4596

Recibido: 11.05.2023 / Aceptado: 31.05.2023
DOI: 10.20318/cdt.2023.8072

Resumen: Uno de los pilares sobre los cuales se asentó la legislación sobre responsabilidad por productos es la exoneración de responsabilidad del productor por los riesgos del desarrollo. En virtud de tal causa de exoneración de responsabilidad, el productor no responde de los daños causados al perjudicado si en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto. La Propuesta de Directiva elaborada por la Comisión Europea, que fue publicada el día 28 de septiembre de 2022, sigue previendo en su artículo 10.1.e) la causa de exoneración por responsabilidad de los riesgos por desarrollo. A este particular, la Propuesta de Directiva dedica el considerando núm. 39 que introduce algunos requisitos para la apreciación de tal causa de exoneración de responsabilidad.

No obstante, a pesar de este reconocimiento, ¿tiene encaje esta causa de exoneración de responsabilidad del productor en el paradigma digital? ¿cómo puede aplicarse a los daños provocados por defectos en productos con elementos digitales que incorporan inteligencia artificial?

Palabras clave: riesgos por desarrollo, responsabilidad del productor, ciberseguridad, ciberresiliencia, vulnerabilidades, inteligencia artificial, bienes con elementos digitales.

Abstract: One of the pillars on which product liability law is based is the exemption of the producer from liability for development risks. According to this exemption from liability, the producer is not liable for the damage caused to the injured party if, at the time the product was put into circulation, the state of scientific and technical knowledge did not allow the existence of the defect to be discovered. The Proposal for a Directive drafted by the European Commission and published on 28 September 2022 continues to provide in article 10.1.e) for exoneration from liability for development risks. The Proposal for a Directive refers recital no. 39 to this particular issue, which introduces some requirements for the assessment of such a cause for exoneration from liability.

However, despite this recognition, does this cause of exoneration from producer liability fit into the digital paradigm, and how can it be applied to damage caused by defects in products with digital elements that incorporate artificial intelligence?

Keywords: State of the Art Defense, producer liability, cybersecurity, cybserresilience, vulnerabilities, artificial intelligence, goods with digital elements.

* El presente artículo se publica dentro del marco de las actividades del Proyecto I+D+i Conducción autónoma y seguridad jurídica del transporte / Autonomous Driving and legal certainty of transport. IP. Eliseo Sierra Noguero y resulta de la comunicación "Protección de los consumidores y responsabilidad del productor: la casa de exoneración de responsabilidad d ellos riesgos por desarrollo", presentada en el III congreso internacional. La tutela de los derechos en el entorno digital: hacia una transición basada en los derechos de la persona, celebrado en Valencia, los días 4 y 5 de mayo de 2023, cuyo director fue el Dr. José Juan Castelló Pastor.

I. Introducción

1. El Derecho privado se está adaptando al nuevo paradigma digital. Por ello, la Comisión europea ha iniciado la revisión de una de las Directivas más longevas: la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, sobre responsabilidad por daños causados por productos defectuosos[1]. Habida cuenta de la irrupción de los bienes con elementos digitales y los sistemas de inteligencia artificial en el mercado, se han puesto de manifiesto la necesidad de adaptar, si eso fuera posible, los principios de la legislación europea sobre responsabilidad por daños causados por productos defectuosos a la nueva realidad del paradigma digital.

2. Uno de los aspectos más problemáticos que plantea la transición hacia el nuevo paradigma digital es la causa de exoneración de responsabilidad del productor por los riesgos del desarrollo, en virtud de la cual el productor puede eximirse de responsabilidad si prueba que el estado de los conocimientos científicos y técnicos en el momento en que introdujo el producto en el mercado no permitían detectar el defecto. Dicha causa de exoneración de responsabilidad fue la reacción legislativa al caso de la talidomida, un tipo de medicamento que produjo graves malformaciones fetales a mujeres que lo injirieron cuando estaban embarazadas. Pensados para el contexto del paradigma analógico de hace cuarenta años, los riesgos por desarrollo deben seguir aplicándose en el momento actual, donde los bienes con elementos digitales y la inteligencia artificial van ganando cotas en el mercado.

3. La Propuesta de Directiva[2] que se hizo pública el día 28 de septiembre de 2022 se limita a incorporar la doctrina que sentó el Tribunal de Justicia de las Comunidades Europeas en torno a esta cuestión. Sin embargo, ello no aclara cuál será el ámbito de aplicación de los riesgos por desarrollo en el contexto actual. Por tanto, en este trabajo abordaremos la regulación de los riesgos por desarrollo tal y como se prevé en la Propuesta de Directiva y nos plantearemos cuál pueden operar antes los riesgos de la digitalización.

II. Ámbito de aplicación de la Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos

1. Concepto de producto. La consideración de la inteligencia artificial y el software como productos

4. El principal motivo por el cual es necesario adoptar una nueva directiva en la materia que nos ocupa es la necesidad de adaptar la nueva regulación a la complejidad de los productos que han irrumpido en el mercado: los llamados bienes con elementos digitales que pueden incorporar sistemas de inteligencia artificial. La particularidad de este tipo de bienes es que, por un lado, podemos distinguir el

[1] Directiva 85/374/CEE del Consejo, 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, DOCE núm. L 210, de 7 de agosto de 1985.

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

bien mueble tangible (*hardware*) y, por otro lado, los elementos (contenidos y servicios) digitales[3]. Además, en la era digital no todos los productos son tangibles, sino que se han introducido en el mercado los productos o servicios digitales (sistemas operativos, programas de ordenador, aplicaciones o sistemas de inteligencia artificial) que no necesariamente se encuentran incorporados en un bien mueble tangible y que se pueden descargar e incorporar posteriormente en productos, fuera del ámbito de control del productor (considerando n.º 12 Propuesta de Directiva).

5. Son conocidos los problemas de encaje de este tipo de bienes dentro de la definición de producto de la aún vigente Directiva 85/374/CEE[4]. Es por ello que la Propuesta de Directiva pretende cerrar el debate doctrinal existente e incluir dentro del ámbito de aplicación de la futura norma el *software* y los servicios y contenidos digitales. En este sentido, el art. 4.1) de la Propuesta de Directiva define el concepto de producto de la siguiente forma: *"cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble; por «producto» se entiende también la electricidad, los archivos de fabricación digital y los programas informáticos"*.

6. La definición de producto que incorpora la Propuesta de Directiva está inspirada en la definición contenida en la Directiva 85/374/CEE. El elemento nuclear de la nueva definición de producto es su carácter mueble, que puede estar incorporado en otro bien mueble o en un bien inmueble. Hasta aquí nada aporta de nuevo la definición de la Propuesta de Directiva. A continuación, la definición incorpora dos nuevos conceptos inexistentes en la definición de producto de la Directiva 85/374/CEE, además de la electricidad: los archivos o copias de fabricación digital (considerando n.º 14 Propuesta de Directiva) y el *software*.

7. A mi entender, la definición de producto que incorpora la Propuesta de Directiva es confusa porque juntamente con los bienes muebles, la definición incorpora determinados tipos de bienes que son intangibles. Hubiera sido deseable que la definición incluyera, por un lado, los bienes muebles, independientemente que incorporen elementos digitales o no y, por otro lado, los elementos digitales propiamente dichos (contenidos y servicios digitales), destacando la necesidad de que estos se encuentren incorporados o interconectados con bienes muebles tangibles, de tal forma que sin ellos el producto no podría realizar sus funciones. Además, para construir un sistema coherente y en armonía con las Directivas sobre falta de conformidad de los bienes y de los contenidos o servicios digitales, es decir, las Directivas (UE) 2019/770 y 2019/771 (*twin directives*), considero que sería deseable que en lugar de referirse al *software* se hiciera referencia a los servicios digitales y que estos se definieran por remisión a lo dispuesto en la Directiva (UE) 2019/770. De esta forma, el uso de los mismos conceptos dotaría de coherencia la legislación europea en materia de responsabilidad civil contractual y extracontractual[5].

8. Del tenor literal del considerando n.º 12 de la Propuesta de Directiva también resulta que el sistema de inteligencia artificial o algoritmo tiene la consideración de programa informático (*software*) y, consecuentemente, de producto. Por tanto, el legislador europeo cierra uno de los debates[6] más importantes que existía en torno a la Directiva 85/374/CEE, que no hacía referencia alguna a esta cuestión, por lo que la reforma es bienvenida. Se desprende del considerando n.º 12 Propuesta de Directiva que la Comisión Europea está pensando en programas informáticos que inicialmente pueden presentarse incorporados en productos, o bien en programas informáticos que son autónomos y se integran posteriormente en el producto. Es decir, lo que a tenor del considerando n.º 12 Propuesta de Directiva determina

[3] *Vid*. Art. 2.1) y 2) Directiva (UE) 2019/770 del Parlamento europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (en adelante, DCSD).

[4] Report from the Expert Group on Liability and new Technologies, Liability for Artificial Intelligence and Other Emerging Digital Technologies, Luxemburgo, 2019, p. 28.

[5] En el mismo sentido, *vid*. C. Wandehorst, "Safety and Liability Related Aspects of Software", European Comission, Luxemburgo, 2021, pp. 19-21.

[6] Por todos, *vid.* K. A. Chagal-Federkorn, «Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers», *Stanford Law & Policy Review*, vol. 30, núm. 61, 2019, pp. 61-114.

la inclusión de los programas informáticos y de los sistemas de inteligencia artificial dentro del ámbito de aplicación de la Propuesta de Directiva es su incorporación o interconexión en productos.

9. Por su parte, el considerando n.º 15 Propuesta de Directiva se refiere a los servicios digitales. Ya hemos dicho que la Propuesta de Directiva no prevé una definición de servicio digital y nos hemos posicionado en el sentido que la futura directiva debería referirse tanto a los contenidos o servicios digitales por remisión a lo dispuesto en el art. 2 DCSD. A tenor de lo dispuesto en el considerando n.º 15 Propuesta de Directiva para el caso de los servicios digitales, el criterio de la incorporación o interconexión en productos tangibles es fundamental para aplicar a este tipo de productos las previsiones de la Propuesta de Directiva. A pesar de que el considerando n.º 15 Propuesta de Directiva declare que no debe aplicarse a los servicios digitales como tales, sí que es necesario extender sus efectos a los servicios digitales cuando estos estén incorporados o interconectados con productos, de tal forma que a falta de aquellos el producto no podría realizar sus funciones. Por tanto, a mi juicio, el criterio de la incorporación o interconexión del software y los servicios digitales en productos resulta determinante para que la Propuesta de Directiva sea aplicable a los daños causados por productos intangibles.

III. ¿La causa de exoneración de responsabilidad por riesgos del desarrollo es aplicable a los daños causados por productos que incorporan inteligencia artificial?

1. La causa de exoneración de responsabilidad por riesgos del desarrollo

11. Cuando hablamos de riesgos por desarrollo, hacemos referencia a los riesgos que entraña un defecto de producto que en el momento en que es puesto en circulación la ciencia y la tecnología no son capaces de detectar[7].

12. El art. 7.e) Directiva 85/374/CEE prevé la causa de exoneración de responsabilidad del productor por los riesgos del desarrollo. Para comprender el alcance y el ámbito de dicha causa de exoneración de responsabilidad tenemos que remontarnos al origen de la institución para comprobar que fue una reacción legislativa para limitar la responsabilidad de los fabricantes de productos farmacéuticos que producían daños corporales o a la salud de las personas[8].

13. Previamente a la adopción de la Directiva 85/374/CEE se publicaron dos propuestas de directiva que trataron de forma distinta esta cuestión, hecho que refleja el debate que existió entre los Estados miembros. El proyecto de directiva de 9 de septiembre de 1976 responsabilizaba al fabricante por los daños causados, a pesar de que en el momento en el momento de la comercialización del producto, la ciencia y la técnica existentes en aquel momento no podían detectar el defecto[9]. Tres años más tarde, el Parlamento Europeo propuso introducir una excepción para limitar la regla anterior, en el sentido de exonerar de responsabilidad al fabricante si podía demostrar que el defecto no era detectable en el momento de la comercialización del producto según el estado de la ciencia y de la técnica[10]. El cambio ope-

[7] Por todos, *vid*. P. Salvador Coderch / J. Solé Feliu, *Brujos y aprendices: los riesgos por desarrollo en la responsabilidad de producto,* Marcial Pons, Madrid, 1999, p. 29. P. Salvador Coderch / A. Rubí Puig, «Riesgos de desarrollo y evaluación judicial del carácter científico de dictámenes periciales», *Indret*, núm. 1, 2008, p. 5.

[8] P. Salvador Coderch / A. Rubí Puig, «Riesgos de desarrollo y evaluación judicial»..., *op.cit.,* p. 6-8. Son conocidos los efectos que tuvo el fármaco talidomida en Alemania. En este país nacieron 4.000 personas afectadas por embriopatías relacionadas con la ingestión de aquel fármaco por mujeres embarazadas. La reacción legislativa fue la aprobación de la Ley del Medicamento de 1976, que preveía por primera vez la responsabilidad por riesgos del desarrollo.

[9] DOCE núm. 241, de 14 de octubre de 1976. "*Le fabricant est également responsable, mème si la chose en fonction du développment scientifique et technologique prévalant au moment ou il l'a mise en circulation n'a pu être considérée comme defectueuse."*

[10] DOCE núm. 127, de 21 de mayo de 1979. "*Le fabricant n'est pas responsable s'il apporte la preuve que la chose ne peut être considérée comme defectueuse en fonction du l'état de développment scientifique et de la technologie prévalant au moment de sa mise en circulation."*

rado en el texto del proyecto de directiva produjo tensiones entre los Estados miembros y, finalmente, la versión definitiva del proyecto recuperaba la propuesta original de no limitar la responsabilidad de los fabricantes por los riesgos del desarrollo. Fruto, por tanto, de las tensiones existentes entre los Estados miembros, el texto final de los arts. 7.e) y 15.1.b) de la Directiva 85/374/CE adopta una solución que permita satisfacer los intereses de los Estados miembros:

14. Art. 7.e) Directiva 85/374/CEE: *"En aplicación de la presente Directiva, el productor no será responsable si prueba:*

> *[...]*
> *e) o que, en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto;"*
> *Art. 15.1.b) Directiva 85/374/CEE: "no obstante lo previsto en la letra e) del artículo 7, mantener o, sin perjuicio del procedimiento definido en el apartado 2 del presente artículo, disponer en su legislación que el productor sea responsable incluso si demostrara que, en el momento en que él puso el producto en circulación, el estado de los conocimientos técnicos y científicos no permitía detectar la existencia del defecto."*

16. Vemos, pues, que la causa de exoneración de responsabilidad por riesgos del desarrollo ha sido desde su origen muy controvertida y que fue una reacción ante los daños causados a la salud por medicamentos que en el momento en que fueron puestos en circulación la ciencia y la tecnología no fueron capaces de detectar y prevenir el daño.

2. Tratamiento de la cuestión en la Propuesta de Directiva

17. Como he apuntado anteriormente, el día 28 de septiembre de 2022 la Comisión Europea publicó una propuesta de directiva que constituye la base del debate que tendrá lugar en el procedimiento legislativo ordinario y que culminará con la adopción de una nueva directiva que derogará la aún vigente Directiva 85/374/CEE. El documento explica que durante el proceso previo de consulta pública la mayor parte de partes interesadas mostró su oposición a la supresión de la causa de exoneración de responsabilidad de los riesgos por desarrollo[11]. Ello me parece comprensible, habida cuenta que la futura directiva se aplicará tanto a los daños provocados por un bien mueble tangible defectuoso y la electricidad, que son propiamente los productos que entran dentro del ámbito de aplicación de la Directiva 85/374/CEE, o bien un software o sistema de inteligencia artificial y los contenidos digitales, que tienen la consideración de producto en la Propuesta de Directiva.

18. Entrando en el análisis de la Propuesta de Directiva, la atención que dedica a los riesgos por desarrollo es más bien escasa y encontramos una primera referencia en el considerando núm. 39: *"En aras de un reparto equitativo de los riesgos, los fabricantes también deben quedar exentos de responsabilidad si demuestran que el estado de los conocimientos científicos y técnicos, determinado con referencia al nivel más avanzado de conocimiento objetivo accesible y no al conocimiento efectivo del fabricante en cuestión, mientras que el producto estaba bajo su control, era tal que no podía descubrirse la existencia de un defecto."* El considerando comentado, por tanto, incorpora la doctrina que dictó el TJCE en el caso C-300/95, de 29 de mayo de 1997, que declaró que el estado de los conocimientos científicos y técnicos del art. 7.e) de la Directiva 85/374/CEE debía valorarse objetivamente, prescindiendo de las características del productor[12]. Además, el conocimiento científico y tecnológico debe ser accesible para la comunidad científica.

[11] El proceso de consulta pública puede consultarse en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Directiva-sobre-responsabilidad-por-los-danos-causados-por-productos-defectuosos-Adaptacion-de-las-normas-de-responsabilidad-a-la-era-digital-la-economia-circular-y-las-cadenas-de-valor-mundiales_es (consulta realizada el día 12 de abril de 2023).

[12] STJUE C-300/95, de 29 de mayo de 1997. *"(29) De todo lo anterior se deduce que, para poder exonerarse de su responsabilidad, con arreglo a la letra e) del artículo 7 de la Directiva, el fabricante de un producto defectuoso debe acreditar que el estado objetivo de los conocimientos científicos y técnicos, incluido su nivel más avanzado, en el momento de ponerse en circulación el producto de que se trata, no permitía descubrir el defecto de éste."*

19. Posteriormente, la Propuesta de Directiva dedica su art. 10 a la regulación de las causas de exoneración de responsabilidad y prevé la de los riesgos del desarrollo en el art. 10.e): *"en el caso de un fabricante, que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o en el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso"*. Como puede verse, el precepto incorpora las ideas que se expresan en el considerando núm. 39 de la Propuesta de Directiva.

20. La principal novedad que debe destacarse es que desaparece la posibilidad que tenían los Estados miembros, en virtud de lo dispuesto en el art. 15.1.b) Directiva 85/374/CEE de eliminar la posibilidad de que los fabricantes se excusaran su responsabilidad alegando los riesgos del desarrollo, algo que hizo España con los defectos en los medicamentos, alimentos o productos alimentarios destinados al consumo humano (art. 140.3 TRLGDCU). Es decir, habida cuenta del carácter de armonización máxima de la Propuesta de Directiva, no habrá determinados defectos de producto que impidan excusar la responsabilidad alegando los riesgos por desarrollo y, por tanto, los fabricantes podrán acogerse a esta causa de exoneración si se cumplen los presupuestos de su exigibilidad.

3. ¿Realmente tiene sentido hablar de riesgos del desarrollo en productos que incorporan inteligencia artificial?

21. Con anterioridad a la publicación de la Propuesta de Directiva el pasado 28 de septiembre de 2022, la Comisión Europea y la doctrina se plantearon la conveniencia de mantener o suprimir la causa de exoneración de responsabilidad de los riesgos por desarrollo en los defectos de producto[13]. Finalmente, la Propuesta de Directiva reconoce dicha causa de exoneración de responsabilidad en el art. 10.e), pero ¿realmente el productor debe poder alegar esta causa de exoneración de responsabilidad ante los riesgos de la digitalización? Hasta el momento ha habido aportaciones de algunos autores en el sentido de reclamar que los riesgos por desarrollo se interpreten a la luz de la nueva realidad, es decir, teniendo en cuenta la mayor facilidad que existe actualmente para acceder a los conocimientos científicos y técnicos más avanzados (considerando núm. 39 de la Propuesta de Directiva)[14]. No obstante, a pesar de tales aportaciones, pocos se han pronunciado sobre la aplicación de la causa de exoneración de los riesgos por los riesgos de la digitalización.

22. En el ámbito de la conducción autónoma, algún autor ha defendido que los riesgos por desarrollo son clave en los daños causados por la inteligencia artificial: *"Since AV are technological advanced products, the state-of-the-art defence [Art. 7(e)] is expected to play a key role, despite the very high requirements for its establishment. This will have special importance in the case of learning algorithms, which might prove to be inadequate and lead to avoidable accidents. A cost-benefit analysis should be undertaken in which various factors are taken into account, such as the seriousness and the probability of risks, the*

[13] Según la exposición de motivos de la Propuesta de Directiva, la mayoría de organizaciones de consumidores y de empresarios se opusieron a la supresión de la causa de exoneración. No obstante, entre la doctrina hubo más división. En este sentido, *vid*. M. Navarro-Michel, «Vehículos automatizados y responsabilidad por producto defectuoso», *Revista de Derecho civil,* núm. 5, 2020, p. 215. P. Álvarez Olalla, "Responsabilidad civil en la circulación de vehículos autónomos", en E. Monterrosso Casado (Dir.), y A. Muñoz Villarreal (Coord.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, Tirant lo Blanch, Valencia, 2019, p. 160. R. De Bruin, «Autonomous Intelligent Cars on the European Intersection of Liability and Privacy Regulatory Challenges and the Road Ahead», *European Journal of Risk Regulation,* vol. 7, núm. 3, 2016, p. 491. M. F. Lohmann, «Liability Issues Concerning Self-Driving Vehicles», *European Journal of Risk Regulation*, vol. 7, núm. 2, 2016, p. 339.

[14] B. A. Koch, J-S. Borghetti, P. Machnikowski, P. Pichonnaz, T. Rodríguez de las Heras Ballell, C. Twigg-Flesner y C. Wandehorst, "Response of the European Law Institute. European Commission's Public Consultation on Civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence", Viena, European Law Institute, 2022, p. 20. Disponible en: https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf. M. Martín-Casals, «An approach to some EU initiatives on the regulation of Liability for damage caused by AI-systems», *Revista Ius et Praxis,* núm. 2, 2022, p. 18.

expected benefits from the use of the product, the cost and feasibility of constructing a safer product; however, regarding personal injuries the risks have to be minimal."[15] A mi modo de ver, el párrafo transcrito demuestra las dificultades que existen en aras a establecer la diferencia entre las causas de exoneración de responsabilidad, en nuestro caso los riesgos por desarrollo, y el carácter defectuoso del algoritmo. Los autores vinculan los riesgos por desarrollo con los daños que causen los algoritmos como consecuencia de su incapacidad para evitar accidentes, es decir, cuando ejecutan órdenes incorrectamente que deriven en un accidente, la probabilidad del riesgo inherente al producto, etc. Pasamos, por tanto, a examinar las circunstancias que determinan que un producto sea defectuoso a la luz de la Propuesta de Directiva.

A) La defectuosidad del producto

23. Para que un productor pueda eximirse de su responsabilidad, previamente debe haber introducido en el mercado un producto y que este se revele defectuoso según las circunstancias del art. 6 de la Propuesta de Directiva. Es decir, la defectuosidad del producto y consiguientemente la producción del daño es una condición previa para que el producto pueda eximirse su responsabilidad si concurre alguna de las causas previstas a tal efecto.

24. Para valorar el carácter defectuoso del producto, la Propuesta de Directiva adopta el criterio de las expectativas del público general (*Consumer Expectation Test*) referidas a la seguridad del producto que tiene derecho a esperar. Para interpretar dicho artículo, el considerando n.º 22 Propuesta de Directiva establece algunas pautas: 1) Las expectativas de los consumidores se refieren a la seguridad del producto que se espera por el público general; 2) La seguridad que se espera de un producto por el público general debe medirse objetivamente y, 3) La seguridad deberá enjuiciarse teniendo en cuenta la finalidad y las propiedades del producto, sus características objetivas y las necesidades específicas del grupo de usuarios. A continuación, el considerando n.º 22 Propuesta de Directiva contiene una previsión que considero sumamente relevante y que nos sirve para introducir el epígrafe que sigue: *"Algunos productos, como los productos sanitarios de soporte vital, conllevan un riesgo especialmente elevado de daños para las personas y, por lo tanto, generan unas expectativas de seguridad especialmente elevadas."* A tenor de tal previsión, nos podemos plantear si a más riesgo que lleva implícito el producto las expectativas del público en general son más elevadas, hasta el punto de no admitir el error del algoritmo o sistema de inteligencia artificial (nivel experto). De esta forma, si el riesgo implícito en el producto fuera menor, las expectativas del público general no deberían ser tan elevadas (nivel medio).

25. A mi juicio, en el ámbito de los productos con elementos digitales y de los sistemas de inteligencia artificial las expectativas de seguridad del público en general son especialmente elevadas, habida cuenta de los riesgos que entrañan para la seguridad y la vida en general. Por tanto, el criterio adoptado por la Propuesta de Directiva no es nuevo y, en el estado actual de las cosas, hay quien sugiere la adopción del test "riesgo-utilidad (*risk/utility-test*)" para determinar el carácter defectuoso del diseño de un sistema de inteligencia artificial, en lugar del *Consumer Expectation Test* que acoge la Propuesta de Directiva. Según este criterio existe un defecto en un producto cuando se podría haber reducido o evitado el daño con un diseño alternativo con un coste razonable, prescindiendo, por tanto, de las expectativas razonables de los usuarios que pueden ser ilusorias cuando se trata de sistemas de inteligencia artificial. Aplicando este criterio a un sistema de inteligencia artificial como el que incorpora un vehículo autónomo, existirá un defecto en el sistema si existe en el mercado un sistema inteligente alternativo capaz de reducir o evitar el daño a un menor coste[16].

[15] M. Chatzipanagiotis / G. leloudas, «Automated vehicles and third-party liability: A European perspective», *University of Illinois Journal of Law, Technology & Policy* 2020, p. 127.

[16] G. Wagner, "Robot Liability", en H. Eidenmüller / G. Wagner, *Law by Algorithm*, Mohr Siebeck, Tübingen, 2021, p. 86-88. G. Veldt, «The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up? An Analysis of the Draft Product Liability Directive», *Journal of European Consumer and market Law*, núm. 1, 2023, p. 26.

26. Si analizamos el art. 6 de la Propuesta de Directiva veremos que existen nuevas circunstancias para valorar la defectuosidad de un producto que se refieren, fundamentalmente, a productos con elementos digitales que incorporan algoritmos o sistemas de inteligencia artificial.

a) La capacidad de autoaprendizaje o *self-learning*

27. En primer lugar, el art. 6.c) de la Propuesta de Directiva se refiere al *"efecto en el producto de la posibilidad de seguir aprendiendo después del despliegue"*. Centrándonos, por tanto, en la circunstancia del art. 6.c) de la Propuesta de Directiva, la primera conclusión a la que llegamos es que el legislador europeo ha previsto, como circunstancia reveladora del carácter defectuoso de un producto el efecto del aprendizaje o *self-learning* del sistema de inteligencia artificial.

28. Para la mejor comprensión de cómo funciona la capacidad de autoaprendizaje de los productos continuaré explicándolo tomando como referencia los vehículos autónomos. Estos están formados por dos grandes elementos: por un lado, el bien mueble propiamente dicho y tangible y, por otro lado, el *software*, conformado, a su vez, por la tecnología de inteligencia artificial (*machine learning*) y la programación para la ejecución de reglas, tareas y reconocimiento de símbolos. Asimismo, el sistema de inteligencia artificial que incorpora un vehículo autónomo es capaz de realizar cuatro grandes funciones. En primer lugar, observa y analiza sus propios datos que constituyen el *machine learning*. En segundo lugar, como consecuencia del análisis previo de datos, estos bienes son capaces de orientar al usuario sobre la mejor alternativa posible. En tercer lugar, el mismo sistema puede decidir entre todas las alternativas posibles y, finalmente, es capaz de ejecutarla. Por tanto, el vehículo autónomo es un bien dotado con una inteligencia artificial limitada. El vehículo deberá adoptar una decisión basada en el *machine learning* que incorpora y que va evolucionando con la experiencia del propio vehículo y de los demás vehículos autónomos del parque automovilístico (art. 6.1.c) Propuesta de Directiva.

29. El hecho que el sistema de inteligencia artificial del vehículo autónomo esté conformado por datos que van generándose durante la conducción del vehículo y de los demás que se han generado por otros vehículos que se encuentran en el parque automovilístico con quienes está en contacto, dificulta que un productor pueda alegar la causa de exoneración de responsabilidad de los riesgos por desarrollo. Ante una situación nueva y crítica, el vehículo autónomo tomará la decisión que sea más razonable de acuerdo con la experiencia de todos los vehículos autónomos. Por tanto, en tanto que la decisión del vehículo autónomo se fundamenta de un sistema de almacenamiento de datos, la previsibilidad de la decisión del vehículo autónomo aumenta, por lo que no queda justificada la exoneración de la responsabilidad del productor de vehículos autónomos[17]. En consecuencia, la inteligencia artificial del vehículo autónomo deja poco margen para la imprevisibilidad y, en todo caso, la imprevisibilidad estará limitada por la experiencia de usuario. Ello hace que sea más difícil para el productor de vehículos autónomos tratar de eximirse de responsabilidad alegando el carácter defectuoso de la decisión tomada por el vehículo autónomo y que, por tanto, siga respondiendo por los daños causados.

30. Otro aspecto que tenemos que tener en cuenta es que la Propuesta de Directiva sigue previendo que no cabe considerar un producto como defectuoso si se actualiza o mejora después de haber sido introducido en el mercado. Los considerandos núm. 37 y 38 de la Propuesta de Directiva hacen referencia a esta cuestión que también se recoge en el art. 6.2 de la Propuesta de Directiva. Por tanto, si el software del vehículo autónomo se actualiza una vez ya ha sido introducido en el mercado y es capaz

[17] S. Van UytselVAN UYTSEL, "Different Liability Regimes for Autonomous Vehicles: One Preferable Above the Other?", en S. Van Uytsel / D. Vasconcellos Vargas (eds.), *Autonomous Vehicles. Business, Technology and Law,* Springer, Singapore, 2021, p. 77. H. Yeefen Lim, *Autonomous Vehicles and the Law,* Edward Elgar Publishing, Singapore, pp. 92-98. J-S. Borghetti *et al*, «Relevance of Risk-benefit for Assessing Defectiveness of a Product: A Comparative Study of Thirteen European Legal Systems», *European Review of private Law,* núm. 1, 2021, pp. 91-132.

de mejorar sus funciones, el vehículo no será defectuoso. Con esto quiero decir que es previsible y deseable que la tecnología siga evolucionando en el futuro, por lo que, en mi opinión, es extremadamente complicado que el productor pueda excusarse en los riesgos del desarrollo.

31. Asimismo, la razonabilidad[18] de la decisión tomada por el vehículo autónomo basada en el algoritmo y el *machine learning* de evitar un comportamiento peligroso no debe ser, tampoco, una causa que permita acudir a la protección que dispensan los riesgos por desarrollo. La causa de exoneración de responsabilidad por riesgos de desarrollo se fundamenta en la imposibilidad de reconocer un defecto en un producto por el estado de los conocimientos científicos y técnicos (*state of art)* en un momento determinado, pero no en la razonabilidad de la decisión tomada por un producto con inteligencia artificial porque, como se ha expuesto, su decisión es predecible, aunque no necesariamente razonable.

b) La seguridad

32. Para determinar el carácter defectuoso de un producto en cuanto al cumplimiento de las condiciones de seguridad, el considerando núm. 22 adopta el criterio de las expectativas razonables del público en general *consumer expectations test*. En virtud de dicho criterio, cuando un consumidor adquiere un producto, espera que cumpla ciertas funciones, características o propiedades y, asimismo, también espera que el producto adquirido no conlleve otras circunstancias impropias o no deseadas. Este análisis debe realizarse objetivamente y teniendo en cuenta el público en general, prescindiendo, por tanto, de las legítimas expectativas de un consumidor. Esto no es una novedad, toda vez que es el criterio que adopta el art. 6 de la Directiva 85/374/CEE para determinar el carácter defectuoso de un producto.

33. La novedad radica en lo prevenido en el considerando núm. 24 de la Propuesta de Directiva que obliga a tener en cuenta los requisitos de seguridad y de ciberseguridad de los productos en el análisis del carácter defectuoso del producto, una circunstancia que no aparece recogida expresamente en el art. 6 Directiva 85/374/CE. Esta circunstancia para determinar el carácter defectuoso del producto aparece en el art. 6.1.f) de la Propuesta de Directiva. De acuerdo con dicho precepto, el cumplimiento de los requisitos de seguridad y ciberseguridad del producto influyen en su consideración de producto defectuoso.

34. Procedemos a realizar el análisis de esta circunstancia para determinar un producto como defectuoso, diferenciando la legislación aplicable en función de si el producto incorpora inteligencia artificial o no, habida cuenta de las diferentes políticas de la Unión en el ámbito de la seguridad de los productos.

a) Productos que no incorporan sistemas de inteligencia artificial

35. En el estado actual de las cosas, debemos hacer referencia a la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos, en adelante DSGP[19]. El art. 2.b) DSGP contiene la definición de producto seguro: "producto seguro":

[18] Sobre la razonabilidad de la decisión tomada por un algoritmo, *vid*. K. A. Chagal-Federkorn, «How Can I Tell If My Algorithm Was Reasonable?», *Michigan Technology Law Review,* núm. 213, 2021, pp. 256-258. La autora propone un método para valorar la razonabilidad de la decisión tomada por un algoritmo. En primer lugar, debemos comparar la decisión tomada por el algoritmo ante unas circunstancias determinadas con la decisión que habría tomado una persona actuando con un canon de diligencia medio (art. 1094 CC). Un resultado positivo en el primer examen no es suficiente para valorar positivamente la razonabilidad de la decisión tomada por el algoritmo. Posteriormente, debe confrontarse la decisión del algoritmo con la decisión que habría tomado el programador o el fabricante del producto con inteligencia artificial. Solo si el resultado es positivo en los dos exámenes, la decisión del algoritmo es racional. Por tanto, a pesar de que el vehículo autónomo haya causado un daño después de haber observado las circunstancias, decidir la mejor alternativa y de ejecutar la decisión, la decisión no tiene que ser necesariamente irrazonable.

[19] Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos, DOCE núm. 11, de 15 de enero de 2002.

> *"cualquier producto que, en condiciones de utilización normales o razonablemente previsibles, incluidas las condiciones de duración y, si procede, de puesta en servicio, instalación y de mantenimiento, no presente riesgo alguno o únicamente riesgos mínimos, compatibles con el uso del producto y considerados admisibles dentro del respeto de un nivel elevado de protección de la salud y de la seguridad de las personas, habida cuenta, en particular, de los siguientes elementos:*
>
> *i) características del producto, entre ellas su composición, envase, instrucciones de montaje y, si procede, instalación y mantenimiento,*
> *ii) efecto sobre otros productos cuando razonablemente se pueda prever la utilización del primero junto con los segundos,*
> *iii) presentación del producto, etiquetado, posibles avisos e instrucciones de uso y eliminación, así como cualquier otra indicación o información relativa al producto,*
> *iv) categorías de consumidores que estén en condiciones de riesgo en la utilización del producto, en particular los niños y las personas mayores."*

36. A la vista de esta definición, existen dos conceptos para determinar que un producto es seguro. Por un lado, el concepto estricto de producto seguro se refiere a que el producto no presenta riesgos o únicamente riesgos mínimos. La DSGP contiene una definición de "riesgo grave" que no aclara qué debemos entender por riesgo: *"todo riesgo grave, incluidos aquellos cuyos efectos no son inmediatos, que exija una intervención rápida de las autoridades públicas"*. No obstante, actualmente se encuentra siguiendo los trámites del procedimiento legislativo ordinario la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, en adelante, RSGP[20], que sí que contiene nuevas definiciones de los conceptos de "producto seguro"; "riesgo" y de "riesgo grave":

> *"2. «producto seguro»: todo producto que, en condiciones de utilización normales o razonablemente previsibles, incluidas las condiciones de duración y, si procede, de puesta en servicio, instalación y mantenimiento, no presente riesgo alguno o únicamente riesgos mínimos, compatibles con el uso del producto y considerados admisibles dentro del respeto de un nivel elevado de protección de la salud y de la seguridad de las personas*
>
> *4. «riesgo»: la combinación de la probabilidad de que exista un peligro que cause un daño o perjuicio y la gravedad de ese daño o perjuicio;*
>
> *5. «riesgo grave»: un riesgo para el que, sobre la base de una evaluación del riesgo y teniendo en cuenta el uso normal y previsible del producto, se considere que la combinación de la probabilidad de que se produzca un peligro que cause un daño o perjuicio y su gravedad requiera una rápida intervención de las autoridades de vigilancia del mercado, incluidos los casos en que el riesgo no tenga efectos inmediatos;"*

37. La nueva definición de producto seguro del RSGP no aporta grandes novedades respecto de la definición sobre este mismo concepto contenida en la DSGP. Sin embargo, las principales novedades se encuentran en las definiciones de "riesgo" y de "riesgo grave". Ambos conceptos pivotan sobre la combinación de probabilidad de que exista o de que se produzca un peligro como consecuencia del uso normal y previsible del producto. Por tanto, tanto la DSGP como la propuesta RSGP reconocen que el riesgo inexistente en un producto es prácticamente imposible de conseguir, por esto admiten que la seguridad pasa por tolerar los riesgos mínimos.

38. Por otro lado, el concepto amplio de producto seguro alude al cumplimiento de los requisitos mínimos de protección de salud y de seguridad. Los requisitos mínimos de protección de la salud y de la seguridad tienen un carácter generalista y de mínimos, en el sentido que todos los productos que se introduzcan el mercado deberán cumplirlos. Por tanto, si un producto supera los requisitos mínimos de

[20] Comisión Europea, "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo", Bruselas, COM(2021) 346 final.

protección de la salud y la seguridad, podrá ser introducido en el mercado y ponerse al alcance de los particulares y los consumidores.

39. De todo lo anterior podemos extraer la conclusión que no por el hecho de que un producto sea seguro implica que no pueda ser defectuoso, bien sea porque el producto no tenga asociado ningún riesgo -supuesto prácticamente imposible-, o bien porque aun presentando riesgos, estos son mínimos y no impiden que el producto no supere los requisitos mínimos de protección de la salud y la seguridad y una vez en el mercado se revele defectuoso[21].

b) Productos que incorporan sistemas de inteligencia artificial

40. El legislador europeo es consciente de la importancia que han adquirido los productos que integran sistemas de inteligencia artificial y de cómo dichos sistemas afectan a la seguridad de los productos en general. Es por ello que debemos detenernos en el análisis de la propuesta de RSGP en lo que se refiere a su posible afectación a otras normas y políticas de la Unión. En este sentido, podemos leer en la exposición de motivos que: *"La propuesta legislativa sobre inteligencia artificial (IA) establece normas armonizadas para la introducción en el mercado, la puesta en servicio y el uso de sistemas de inteligencia artificial en la UE. Las normas deben garantizar un nivel elevado de protección de los intereses públicos, especialmente en materia de salud y seguridad, y de los derechos y libertades fundamentales de las personas. Establece requisitos específicos que deben cumplir los sistemas de IA de alto riesgo e impone obligaciones a los proveedores y usuarios de dichos sistemas.*

La presente propuesta tiene en cuenta estas disposiciones y proporciona una red de seguridad para los productos y los riesgos para la salud y la seguridad de los consumidores que no entran en el ámbito de aplicación de la propuesta sobre la IA.[22]"

41. Por tanto, el legislador europeo quiere regular la seguridad de los productos que incorporan sistemas de inteligencia artificial de forma unitaria, por lo que la legislación europea sobre inteligencia artificial funcionará como legislación sectorial, estableciendo los requisitos de seguridad aplicables a la inteligencia artificial y, por consiguiente, de adoptarse la propuesta de RSGP en los términos actuales, el futuro RSGP tendrá un alcance general y resultará aplicable a los productos no cubiertos por otra legislación sectorial de la UE. En consecuencia, debemos hacer referencia, también, a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos de la Unión[23].

42. De acuerdo con la definición de "sistema de inteligencia artificial" que incorpora la Ley de Inteligencia Artificial, este puede definirse como *"el software que se desarrolla empleando una o varias de las técnicas y estrategias [...] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa."* La inteligencia artificial puede generar un amplio conjunto de beneficios económicos y sociales, pero también puede generar riesgos y lesionar determinados intereses públicos (considerandos núm. 3 y 4 Ley de Inteligencia Artificial). No obstante, no aparece una definición de "riesgo" en la Ley de Inteligencia Artificial, pero puede deducirse que se

[21] C. A., Ruiz Garcia / I. Marín Garcia, «Producto inseguro y producto defectuoso. Conceptos de producto peligroso, producto seguro y producto defectuoso en la Directiva 2001/95, el Real Decreto 1801/2003 y la Ley 22/1994», *Indret,* núm. 4, 2006, p. 1-20.

[22] Comisión Europea, "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo", Bruselas, COM(2021) 346 final.

[23] Comisión Europea, "Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos de la Unión", Bruselas, COM(2021) 206 final. 2021/0106(COD).

trata de los riesgos propios o implícitos de dicha tecnología. En ningún momento se hace referencia a los riesgos por desarrollo aplicables a la inteligencia artificial.

43. La Ley de Inteligencia Artificial se pone énfasis en los sistemas de inteligencia artificial de alto riesgo, que son aquellos que tienen tal consideración según el anexo II que incorpora la Ley de Inteligencia Artificial y, para estos sistemas, se implantará un sistema de gestión de riesgos que consistirá en un proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de inteligencia artificial de alto riesgo y que identificará "los riesgos conocidos y previsibles" vinculados a un sistema de inteligencia artificial de alto riesgo, estimará y evaluará los riesgos que podrían seguir cuando el sistema de inteligencia artificial de alto riesgo se utilice conforme a su finalidad prevista y cuando de le dé un uso indebido razonablemente previsible y se evaluarán otros riesgos que puedan seguir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización.

44. Por tanto, la Ley de Inteligencia Artificial mide los riesgos de los sistemas de inteligencia artificial en el presente (riesgos conocidos) y en el futuro (riesgos previsibles y riesgos que puedan seguir). Esto encaja mal con el concepto propio de los riesgos por desarrollo, que atiende al estado futuro de la ciencia y la tecnología para valorar si cuando se introdujo un producto en el mercado, el estado de los conocimientos científicos y técnicos existentes en aquel momento permitían detectar el defecto del producto. Lo mismo podemos decir respecto de la concepción del riesgo en la DSGP y la propuesta de RSGP.

C) La ciberseguridad

45. De acuerdo con el art. 6.1.f) de la Propuesta de Directiva, el carácter defectuoso de un producto también debe valorarse conforme al cumplimiento de los requisitos mínimos de ciberseguridad (considerando núm. 23 de la Propuesta de Directiva). A este respecto, hay que destacar la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales[24], la llamada Propuesta Reglamento de ciberresiliencia[25]. Los considerandos de esta propuesta de reglamento aluden a la necesidad de mejorar el funcionamiento del mercado interior mediante el establecimiento de unos requisitos esenciales de ciberseguridad para la introducción en el mercado de productos con elementos digitales, de tal forma que estos productos sean puestos en circulación con menos vulnerabilidades y, por lo tanto, aumentando su seguridad (considerandos núm. 1 y 2 Propuesta de Reglamento sobre ciberresiliencia). Asimismo, los requisitos mínimos de ciberseguridad de los productos con elementos digitales que fija la Propuesta de Reglamento constituyen un marco regulador horizontal, aplicable a todos los productos con elementos digitales (considerandos núm. 4 y 6 Propuesta de Reglamento sobre ciberresiliencia). Por tanto, la Propuesta de Reglamento sobre ciberresiliencia tiene un ámbito de aplicación general, por lo que deberá tenerse en cuenta la legislación sectorial aplicable para completar el marco regulatorio horizontal que prevé[26]. De

[24] Comisión Europea, "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020", Bruselas, COM/2022/454 final.

[25] Para una aproximación general a la propuesta de Reglamento sobre ciberresiliencia, *vid.* P. G. Chiara, «The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements», *International Cybersecurity Law Review,* núm. 3, 2022, p. 255-272.

[26] En este sentido, en el ámbito del sector de la automoción cabe citar el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) núm. 78/2009, (CE) núm. 79/2009 y (CE) núm. 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) núm. 631/2009, (UE) núm. 406/2010, (UE) núm. 672/2010, (UE) núm. 1003/2010, (UE) núm. 1005/2010, (UE) núm. 1008/2010, (UE) núm. 1009/2010, (UE) núm. 19/2011, (UE) núm. 109/2011, (UE) núm. 458/2011, (UE) núm. 65/2012, (UE) núm. 130/2012, (UE) núm. 347/2012, (UE) núm. 351/2012, (UE) núm. 1230/2012 y (UE) 2015/166 de la Comisión [DOUE L 325/1 de 16 de diciembre de 2019]. El considerando núm. 26 del Reglamento alude a la posibilidad de que se produzca un

hecho, el art. 3 de la Propuesta de Reglamento sobre ciberresiliencia prevé que no se aplicará a los productos con elementos digitales de determinados ámbitos, entre los cuales se encuentran los vehículos.

45. Por lo que atañe a los riesgos en materia de ciberseguridad de los productos con elementos digitales, el art. 3.36) de la Propuesta de Reglamento sobre ciberresiliencia contiene la definición de "riesgo de ciberseguridad significativo": *"un riesgo de ciberseguridad debido al cual, sobre la base de sus características técnicas, se puede considerar que existe una alta probabilidad de que se produzca un incidente capaz de acarrear consecuencias negativas graves, en particular causando pérdidas o perturbaciones materiales o inmateriales considerables".* Nuevamente, el elemento nuclear de la definición pivota sobre la probabilidad más o menos alta de que el producto con elementos digitales sufra un accidente que conlleve daños materiales o inmateriales.

46. La comercialización de los productos con elementos digitales se autorizará cuando estos productos cumplan los requisitos esenciales establecidos en el Anexo I de la Propuesta de Reglamento, entre los cuales se prevé que los productos con elementos digitales se diseñarán, desarrollarán y producirán para garantizar un nivel adecuado ciberseguridad en función de los riesgos; se entregarán sin vulnerabilidades conocidas de las cuales pueda aprovecharse un tercero malintencionado, se suministrarán con una configuración segura por defecto; garantizarán la protección contra el acceso no autorizado mediante mecanismos de control adecuados y protegerán la confidencialidad de los datos personales u otros datos procesados mediante los mecanismos más avanzados.

47. Por lo que se refiere a los sistemas de inteligencia artificial que son calificados de alto riesgo conforme a la Propuesta de Reglamento sobre inteligencia artificial, el art. 8 de la Propuesta de Reglamento sobre ciberresiliencia declara aplicables los requisitos esenciales que prevé en el anexo I a aquellos sistemas y, por tanto, su cumplimiento determinará que sean conformes con los requisitos relativos a la ciberseguridad establecidos en el art. 15 de la propuesta de Reglamento sobre inteligencia artificial.

48. Como decía anteriormente, es el anexo I de la Propuesta de Reglamento sobre ciberresiliencia el que fija los requisitos esenciales en materia de ciberseguridad de los productos con elementos digitales. Sin ánimo de realizar un examen exhaustivo de dichos requisitos esenciales, destaca la previsión contenida en el apartado segundo, según la cual: *"Los productos con elementos digitales se entregarán sin ninguna vulnerabilidad conocida que pueda aprovecharse"*. La Propuesta de Reglamento sobre ciberresiliencia no define qué debemos entender por "vulnerabilidad conocida", por lo que sería deseable que el futuro reglamento que regule esta materia previera una definición de tal concepto[27]. Sin embargo, sí que encontramos una definición de "vulnerabilidad" en el art. 3.38) que se remite a la definición de "vulnerabilidad" del art. 6.15) de la llamada Directiva SRI 2: *"deficiencia, susceptibilidad o fallo de productos de TIC o servicios de TIC que puede ser aprovechado por una ciberamenaza"*[28]. Vemos, pues, que el concepto de vulnerabilidad incluye el concepto de deficiencia. No obstante, en la versión

acceso remoto no autorizado en el vehículo y que se modifique el software por vía inalámbrica. Por este motivo, se expresa la necesidad de incorporar las normas de las Naciones Unidas en materia de ciberseguridad.

[27] Comisión Europea, "Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715. Final Study Report", Bruselas, 2021, p. 99. El estudio clasifica las vulnerabilidades conocidas en cuatro grupos: 1) la cibercriminalidad; 2) los ataques de hackers externos; 3) los ciberataques patrocinados por Estados y 4) los ataques causados por agentes internos. Entre los objetivos que se encuentran en estas vulnerabilidades destacan los daños materiales que resulten de la muerte o las lesiones corporales de terceros y la pérdida o corrupción de datos.

[28] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148, DOUE núm. 333, de 27 de diciembre de 2022. S. Schmitz / S. Schiffner, "Responsible Vulnerability Disclosure under the NIS 2.0 Proposal", disponible en https://www.jipitec.eu/issues/jipitec-12-5-2021/5495/schmitz_schiffner_pdf.pdf (consulta realizada el día 25 de abril de 2023). *"A vulnerability is a set of conditions that allows the violation of a security (or privacy) policy. Such conditions might be created by software flaws, configuration mistakes and other human errors of operators, or unexpected conditions of the environment a system runs in."*

en inglés de la SRI la definición de vulnerabilidad incluye el concepto de *weakness.* De acuerdo con el Diccionario de la Real Academia Española, el concepto de "deficiencia" se refiere al de defecto (imperfección), mientras que, a mi juicio, el concepto de *weakness* debería equipararse al de "debilidad", que se refiere a la falta de propiedades que hacen que la cosa sea vulnerable ante intromisiones de terceros. En conclusión, un producto cumplirá los requisitos esenciales de ciberseguridad si se entrega sin ninguna vulnerabilidad conocida que pueda aprovecharse. De lo contrario, el producto será defectuoso por no cumplir los requisitos esenciales de ciberseguridad.

49. Y llegados a este punto, la pregunta que me planteo es la siguiente: ¿Puede una vulnerabilidad o un defecto en la ciberseguridad del producto descubierto posteriormente a su introducción en el mercado y, en consecuencia, la producción de un daño asociado a esta vulnerabilidad, amparar que el productor vea exonerada su responsabilidad por los riesgos del desarrollo? Las anteriores consideraciones que hicimos con la seguridad general de los productos pueden extrapolarse al ámbito de la ciberseguridad para afirmar que, aunque el producto con elementos digitales cumpla los requisitos esenciales en materia de ciberseguridad, esto no impide que pueda tener la consideración de defectuoso si después de haberlo introducido en el mercado provoca un daño a terceros. Por tanto, un producto puede manifestarse defectuoso después de su introducción en el mercado a causa de una vulnerabilidad desconocida o aprovechada activamente en cuanto a su falta de ciberseguridad, a pesar de que en aquel momento su ciberseguridad estaba certificada porque cumplía los requisitos esenciales de ciberseguridad. No obstante, habida cuenta de las vulnerabilidades conocidas de los productos con elementos digitales, resulta difícil pensar en una vulnerabilidad que no haya podido detectarse o preverse.

50. Además, por lo que respecta a las vulnerabilidades, la Directiva SRI 2 encarga a la Agencia de la Unión Europea para la ciberseguridad (ENISA) el desarrollo y mantenimiento de una base europea de vulnerabilidades. Esta base de datos debe ser tenida en el ámbito de la ciberresiliencia de los productos, al efecto de que los fabricantes determinen los riesgos esenciales relacionados con las propiedades de los productos con elementos digitales en el momento de su introducción en el mercado y con posterioridad (considerando núm. 32 Propuesta de Reglamento sobre ciberresiliencia). Es decir, los fabricantes deben velar por el cumplimiento de los requisitos esenciales de ciberseguridad de sus productos durante todo su ciclo de vida útil[29]. Por tanto, en la medida que el producto, a pesar de haber sido introducido en el mercado, sigue bajo el ámbito de control del productor y que los productores tendrán a su disposición la base de datos europea elaborada por la EINSA, también resulta muy complicado que los productores puedan exonerar su responsabilidad alegando los riesgos del desarrollo, en este caso, por las vulnerabilidades no conocidas en el momento que introdujeron el producto en el mercado y que se han detectado con posterioridad.

IV. Conclusión

51. Entendemos por riesgos de desarrollo *"los causados por un defecto de un producto que no era reconocible a la luz del estado de los conocimientos científicos y técnicos existentes en el momento*

[29] Dictamen del Comité Económico y Social Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de la ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020. [COM(2022) 454 final — 2022/0272 (COD)] (2023/C 100/15). En el marco del procedimiento legislativo ordinario el Comité Económico y Social Europeo ha propuesto que los fabricantes tengan que proporcionar rápidamente soluciones gratuitas en caso de nuevas vulnerabilidades, deben verificar periódicamente la "solidez" de los productos con elementos digitales que comercializan y deben eliminar las vulnerabilidades detectadas mediante actualizaciones periódicas del software. En el mismo sentido, *vid*. Digitaleurope, "Building blocks for a scalable cyber resilience act", disponible en *https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf* (consulta realizada el día 25 de abril de 202).

Asimismo, el art. 11 de la Propuesta de Reglamento sobre ciberresiliencia prevé la obligación de los fabricantes de informar a la ENISA sobre las vulnerabilidades que estén siendo aprovechadas activamente por terceros sin demora indebida y, en todo caso, dentro de un plazo de veinticuatro horas.

de la comercialización del producto"[30]. Los riesgos por desarrollo entrañan una responsabilidad para el productor, cuando el defecto que no era reconocible en el momento en que introdujo el producto en el mercado provoca un daño a terceros. Por tanto, los riesgos por desarrollo implican un juicio realizado *ex post,* en virtud del cual el fabricante logrará exonerar su responsabilidad si prueba que el estado de los conocimientos científicos y técnicos impedía apreciar la existencia del defecto.

52. La opción de la Directiva 85/374/CEE y que mantiene la Propuesta de Directiva que pretende derogarla es imputar los daños causados por los riesgos del desarrollo al fabricante, pero reconociéndole la posibilidad de que pueda exonerar su responsabilidad alegando los riesgos por desarrollo (art. 7.e) Directiva 85/374/CEE y art. 10.1.e) de la Propuesta de Directiva), a pesar de que se prevé que se reconoce la posibilidad a los Estados miembros de que los productores puedan impedir la exoneración de responsabilidad por esta causa (art. 15.1.b) Directiva 85/374/CEE). La opción del legislador español ha sido reconocer la causa de exoneración de responsabilidad de los riesgos por desarrollo en general (art. 140.1.e) TRLGDCU), pero ha impedido alegarla cuando los daños sean provocados por defectos existentes en medicamentos y alimentos o productos alimentarios destinados al consumo humano.

53. Tradicionalmente, el ámbito de aplicación de los riesgos por desarrollo se ha limitado a los medicamentos y a los productos farmacéuticos. Casos como el fármaco de la talidomida plantearon la necesidad de limitar la responsabilidad de los productores por los riesgos por desarrollo. Pero esta causa de exoneración de responsabilidad estaba pensada para este supuesto de casos y, a pesar de que la Propuesta de Directiva la sigue reconociendo, nos hemos planteado si tiene encaje en la era digital, donde han irrumpido los bienes con elementos digitales. Partíamos de la base que tal causa de exoneración casa mal con los daños provocados por los productos con elementos digitales que incorporan sistemas de inteligencia artificial. Hemos visto que estos bienes son vulnerables a las intromisiones malintencionadas de terceros y que, por tanto, la seguridad y ciberseguridad de estos productos se revela como uno de los elementos clave para valorar su carácter defectuoso. No obstante, a pesar de que por el cumplimiento de los requisitos esenciales de seguridad y ciberseguridad un producto tenga la consideración de seguro, sea certificado como tal y se introduzca en el mercado, ello no es óbice para que posteriormente se manifieste defectuoso.

54. Considero que, si finalmente la directiva que se adopte sobre la responsabilidad por productos defectuosos incorpora dicha causa de exoneración de responsabilidad, deberá reinterpretarse en el nuevo contexto de la era digital, donde que los productos con elementos digitales y sistemas de inteligencia artificial entrañan riesgos como todos los productos, pero además son vulnerables. La Propuesta de Reglamento sobre ciberresiliencia permite certificar la ciberseguridad de un producto si no presenta ninguna vulnerabilidad conocida que pueda ser aprovechada por intrusos malintencionados. ¿Pero una vulnerabilidad en el momento de la puesta en circulación del producto que es detectada posteriormente con el avance de la tecnología y de la técnica y que ha causado un daño a terceros, es idónea para que el fabricante exonere su responsabilidad, alegando los riesgos por desarrollo? Pienso que es la pregunta clave que nos debemos plantear cuando hablamos de riesgos por desarrollo en la era digital. A mi modo de ver, las vulnerabilidades conocidas a las que alude la Propuesta de Reglamento sobre ciberresiliencia pueden servir para reinterpretar los riesgos por desarrollo en el nuevo paradigma digital. Sin embargo, la previsión de una base europea de vulnerabilidades y la posibilidad de que los productores puedan actualizar sus productos una vez haya sido puestos en circulación dificulta, y mucho, la posibilidad de alegar dicha causa de exoneración de responsabilidad.

[30] P. Salvador Coderch / J. Solé Feliu, *Brujos brujos y aprendices…, op.cit.,* p. 29.