InDret
4.2025

Vulnerabilidades de ciberseguridad en productos con elementos digitales y su incidencia en la responsabilidad del fabricante

Guillem Izquierdo Grau
Universitat Autònoma de Barcelona

Sumario

El presente trabajo aborda la conexión entre el Reglamento (UE) 2024/2847, sobre ciberseguridad de los productos con elementos digitales (RCR) y la Directiva (UE) 2024/2853, sobre responsabilidad por daños causados por productos defectuosos (DRP). La digitalización e interconexión de los productos con elementos digitales ha propiciado que estos productos sean vulnerables frente ataques malintencionados de terceros que tienen lugar en el ciberespacio. El RCR trata de garantizar, ex ante, la conformidad de los productos con elementos digitales cuando se introducen en el mercado o son puestos en servicio, además de imponer obligaciones, ex post, a los fabricantes de velar por la ciberseguridad del producto durante el periodo de soporte. Por su parte, la DRP regula la responsabilidad de los fabricantes por daños causados por sus productos. Ambas regulaciones presentan algunas interconexiones en materia de vulnerabilidades de ciberseguridad de los productos que son tratadas en este trabajo.

Como conclusiones más relevantes se destaca la desarmonía entre el periodo de soporte de cinco años del art. 13.8 RCR y el plazo de caducidad de las acciones de diez años del art. 17 DRP; la posible aplicación de la excepción de responsabilidad por los riesgos del desarrollo a las vulnerabilidades de ciberseguridad; una lectura en clave de ciberseguridad de la causa de defectuosidad del art. 7.2.d) DRP sobre el efecto razonablemente previsible de la interconexión de productos y la no concurrencia de la causa de defectuosidad del art. 7.2.f) DRP cuando el producto con elementos digitales cumpla los requisitos esenciales de ciberseguridad del anexo I, parte I RCR, a pesar de poder estar afectado de vulnerabilidades no conocidas cuando se introduce en el mercado.

Abstract

This paper explores the interplay between Regulation (EU) 2024/2847 on the cybersecurity of products with digital elements (Cyber Resilience Act, CRA) and Directive (EU) 2024/2853 on liability for defective products (Product Liability Directive, PLD). The digitalisation and interconnection of products with digital elements have made these products increasingly vulnerable to malicious third-party attacks in cyberspace. The CRA aims to ensure, ex ante, the conformity of products with digital elements when they are placed on the market or put into service, while also imposing ex post obligations on manufacturers to maintain the cybersecurity of the product throughout the support period. For its part, the PLD governs the liability of manufacturers for damage caused by their products. Both legal instruments present various interconnections concerning cybersecurity vulnerabilities in products, which are analysed in this paper.

Among the main conclusions, the paper highlights the lack of alignment between the five-year support period under Article 13(8) CRA and the ten-year limitation period for bringing claims under Article 17 PLD; the applicability of the development risk defence to cybersecurity vulnerabilities; a cybersecurity-focused interpretation of the defectiveness criterion under Article 7(2)(d) PLD regarding the reasonably foreseeable effect of product interconnection; and the non-applicability of the defectiveness criterion under Article 7(2)(f) PLD in cases where the product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I to the CRA, even if unknown vulnerabilities are present at the time of placing the product on the market.

Title: *Cybersecurity vulnerabilities in products with digital elements and their impact on the manufacturer's liability*

Palabras clave: Ciberresiliencia, ciberseguridad, vulnerabilidades, productos con elementos digitales, responsabilidad del fabricante, producto defectuoso, riesgos del desarrollo, derecho de daños, hacking.

Keywords*: *Cyber resilience, Cyber security, vulnerabilities, products with digital elements, manufacturer liability, product liability, development risks, Tort Law, hacking.

-

DOI: 10.31009/InDret.2025.i4.03

InDret

4.2025

Recepción
18/06/2025
-
Aceptación
14/08/2025
-

Índice

-

-

1. Introducción[1*]

Los productos con elementos digitales se han convertido en indispensables para los consumidores y en el sector industrial, constituyendo uno de los componentes principales en el llamado *Internet of Things (IoT).*[2] Estos productos no pueden concebirse aisladamente, pues su interconectividad nos mantiene vinculados a red y, asimismo, están preparados para conectarse entre ellos, de forma directa o indirecta, de tal forma que la vida, en la era digital, transcurre a través de estos productos, que captan nuestros datos personales para transferirlos a otros usuarios y productos. La interconexión entre productos es posible gracias a una gran variedad de equipos y programas que procesan y transmiten la información. Actualmente, los productos con elementos digitales han colonizado todos los ámbitos de nuestra vida, desde que nos despertamos con el reloj de pulsera que nos indica la calidad del sueño, los datos recopilados por nuestros vehículos, que nos enseñan a conducir de una forma más sostenible considerando nuestro patrón de conducción, hasta la preparación del sueño mediante un sistema de domótica que nos bajará las persianas automáticamente de nuestro hogar.

Los productos de la era digital tratan nuestros datos personales bajo el pretexto de hacernos nuestra vida más confortable y cómoda, de tal forma que su atracción es irresistible, hasta el punto que se estima que en 2025 existen 75.000 millones de productos con elementos digitales, que nos conectan con los demás y con las cosas que nos rodean.[3] Sin embargo, esta interconexión de productos disfrazada de una aparente comodidad acarrea graves riesgos para nuestra privacidad.[4] Si bien es cierto que estos riesgos se han abordado desde diferentes vertientes,[5] la ciberseguridad de los productos con elementos digitales, la llamada ciberresiliencia, es la última arista que faltaba por tratar para completar un marco jurídico transversal que nos dote de una protección integral, que a pesar de todo no es completamente infranqueable.

Dichos productos pueden constituir un vector de entrada al ciberespacio que puede poner en peligro, de forma exponencial, la seguridad de los usuarios y de las estructuras críticas de los Estados y de la Unión Europea. Es por este motivo que es necesario que estos productos se introduzcan en el mercado de la forma más segura posible, después de haber superado el cumplimiento de unos requisitos estrictos de ciberseguridad cuyo cumplimiento se impone a los fabricantes de dichos productos. No obstante, las obligaciones que se imponen a los fabricantes no solo apuntan al proceso de diseño, fabricación y comercialización de los productos, sino que se extienden en el futuro, mientras el producto siga bajo su ámbito de control, en la medida que podrá ser actualizado para eliminar los riesgos que se pongan de manifiesto con posterioridad a su introducción en el mercado o puesta en servicio. A pesar del cumplimiento de determinados requisitos que garantizan que el producto es seguro (pero no sin riesgos), es imposible garantizar que dichos productos no se revelen defectuosos, en este caso, por algún defecto en su ciberseguridad que los convierte en vulnerables. Por tanto, su posible defectuosidad por defectos de ciberseguridad nos conduce a abordar esta cuestión desde la nueva legislación europea sobre responsabilidad por daños causados por productos defectuosos, el último estadio legislativo aplicable ante

---

[1]* Guillem Izquierdo Grau (guillem.izquierdo@uab.cat). 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.

[2] GREENGARD, Samuel., *The internet of things*, 2ª ed., The Mitt Press, Londres, 2021, pp. 14-21.

[3] FRIEDMAN, Vlad., «On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT», puede consultarse en: https://www.databank.com/resources/blogs/solving-edge-computing-challenges-in-era-of-iot/. Consulta realizada en fecha 11 de junio de 2025.

[4] Por todos, HARARI, Yuval Noah., *21 lliçons per al segle XXI*, La Butxaca, 2021, pp. 81-133.

[5] Basta con citar la legislación europea que se ha adoptado en los últimos diez años en materia de protección de datos personales en general (Reglamento (UE) 2016/679, de datos personales; Reglamento (UE) 2022/868, de gobernanza de datos) y la aplicable en diferentes ámbitos, como el sanitario (Reglamento (UE) 2025/327, de datos de salud) o de la conducción autónoma, además de otros Reglamentos aplicables al ámbito de la ciberseguridad (Reglamento 2019/881, de ciberseguridad y Directiva (UE) 2022/2555).

la producción de un daño por un producto defectuoso que, aun así, ha cumplido toda la legislación de seguridad de los productos.

La legislación de responsabilidad por daños causados por productos defectuosos tiene un ámbito de aplicación general, aplicable, con algunas excepciones, a todos los productos introducidos en el mercado o puestos en servicio después del 6 de diciembre de 2026, entre los que se incluyen los productos con elementos digitales. El problema de la ciberseguridad está contemplado en la nueva Directiva 2024/2853, sobre responsabilidad por daños causados por productos defectuoso (en adelante, DRP),[6] que contiene algunas referencias a la ciberseguridad y a las vulnerabilidades de productos. No obstante, debido al enfoque general adoptado, los defectos por vulnerabilidades que afectan a la ciberseguridad del producto suscitan algunas cuestiones que son abordadas en el presente trabajo, como las circunstancias para apreciar el carácter defectuosos de un producto (art. 7 DRP) o las causas de exoneración de responsabilidad, en lo que puedan referirse a la ciberseguridad.

El presente trabajo se divide en dos partes claramente diferenciadas. En primer lugar, se hace un tratamiento mayoritariamente descriptivo del Derecho regulatorio aplicable a los productos con elementos digitales, el Reglamento de Ciberresiliencia. Sin embargo, no puede pasarse por alto normas transversales de ámbito de aplicación general al ámbito de la ciberseguridad, como el Reglamento (UE) 2019/881, relativo a la ENISA y la Directiva (UE) 2022/2555. Se exponen sucintamente las bases sobre las que se asienta dicha regulación y las principales obligaciones que se imponen a los fabricantes. En segundo lugar, se aborda la nueva DRP, en especial, las implicaciones que tienen para los fabricantes las vulnerabilidades de sus productos y la ciberseguridad en general. Se abren debates y se alcanzan conclusiones relevantes en esta materia que espero que sean de interés para el lector.

2. Reglamento (UE) 2019/881 (Reglamento sobre la ciberseguridad)

Dispone el art. 1.1 del Reglamento (UE) 2019/881, en adelante RC,[7] que el objeto y ámbito de aplicación de la norma es la regulación de la ENISA, la Agencia Europea para la Ciberseguridad, y el establecimiento de unos esquemas europeos de certificación de ciberseguridad. Por lo que se refiere al primer objeto, ENISA es una agencia de la Unión Europea creada para reforzar la ciberseguridad dentro del mercado interior europeo. Su función principal es asistir a los Estados miembros, a las instituciones europeas y al sector privado en la mejora de la seguridad de las redes y sistemas de información. En particular, proporciona orientación técnica a la Comisión Europea y a los Estados miembros sobre políticas y legislación en ciberseguridad; apoya el desarrollo y la coordinación de los CSIRT;[8] promueve campañas de concienciación y formación sobre buenas prácticas en ciberseguridad; publica informes y estudios sobre tendencias, riesgos y vulnerabilidades de ciberseguridad y supervisa y coordina la implantación de sistemas europeos de certificación en ciberseguridad para productos, servicios y procesos TIC, entre otras funciones.

[6] 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. DOUE núm. 2853, de 18 de noviembre de 2024. La legislación sobre daños causados por productos defectuosos se ha reformado para abordar los retos de la digitalización de los productos.

[7] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) núm. 526/2013 («Reglamento sobre la Ciberseguridad»). DOUE núm. 151, de 7 de junio de 2019.

[8] La abreviatura empleada se corresponde con las siglas en inglés de *Computer Security Incident Response Team.*

Respecto del segundo objeto, es decir, el establecimiento de esquemas europeos de certificación de ciberseguridad. A grandes rasgos, el RC obliga a los fabricantes a que sus productos sean seguros en cuanto a su ciberseguridad desde el diseño (*security by design*), es decir, los esquemas europeos de certificación de la ciberseguridad velarán para que los fabricantes diseñen sus productos considerando la ciberseguridad como parámetro para que sean seguros frente a vulnerabilidades aprovechables por terceros malintencionados (art. 51.i) RC). Asimismo, se impone la obligación a los fabricantes de suministrar las actualizaciones de seguridad necesarias para hacer frente a vulnerabilidades que aprovechables una vez el producto ya se haya introducido en el mercado (art. 51.j) RC). Veremos los requisitos y el plazo de tiempo durante el cual deben suministrarse dichas actualizaciones en el tratamiento dispensado al Reglamento (UE) 2024/2847, el Reglamento de Ciberresiliencia.

3. Directiva (UE) 2022/2555 (Directiva SRI 2)

La Directiva (UE) 2022/2555, en adelante, Directiva SRI 2,[9] constituye un actualización de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, que busca establecer un alto nivel común de ciberseguridad en la Unión Europea, mejorando la resiliencia frente a las ciberamenazas y garantizando el funcionamiento continuo de servicios esenciales y críticos, incluso ante incidentes graves o ataques cibernéticos. Para ello se ha ampliado el conjunto de operadores económicos que tienen la consideración de entidades esenciales (art. 3 Directiva SRI 2). De esta directiva cabe destacar la regulación que contiene el art. 12 sobre la base de datos europea de vulnerabilidades, puesto que permite dar publicidad a las vulnerabilidades conocidas que pueden afectar a productos con elementos digitales, de tal manera que los fabricantes tendrán la obligación de comprobar si sus productos están afectados por dichas vulnerabilidades. Veremos posteriormente los efectos de esta publicidad sobre la responsabilidad de los fabricantes por daños causados por sus productos como consecuencia del incumplimiento de esta obligación. Finalmente, la Directiva SRI 2 destaca por su aplicación al software y a los servicios digitales.[10]

4. Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia)

El día 20 de noviembre de 2024 fue publicado en el DOUE el nuevo Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, de Ciberresiliencia, en adelante, RCR.[11] Con carácter general, el RCR será aplicable a partir del 11 de diciembre de 2027, a pesar de que el art. 14 RCR y el capítulo IV (artículos 35 a 51) serán aplicables a partir del 11 de junio de 2026 (art. 71 RCR). El RCR se enmarca dentro de la Estrategia de Ciberseguridad de la Unión Europea.[12]

---

[9] 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 (Directiva SRI 2). DOUE núm. 333, de 27 de diciembre de 2022.

[10] Considerando núm. 33 Directiva SRI 2: *"Los servicios de computación en nube deben abarcar los servicios digitales que permiten la administración bajo demanda y el acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos que se pueden compartir, también cuando esos recursos están distribuidos entre varias ubicaciones. Entre tales recursos se encuentran las redes, los servidores u otras infraestructuras, sistemas operativos, software, almacenamiento, aplicaciones y servicios. Los modelos de servicios de computación en nube incluyen, entre otros, la infraestructura como servicio (IaaS, por sus siglas en inglés), la plataforma como servicio (PaaS, por sus siglas en inglés), el software como servicio (SaaS, por sus siglas en inglés) y la red como servicio (NaaS, por sus siglas en inglés)."*

[11] Reglamento UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia). DOUE núm. 2847, de 20 de noviembre de 2024.

[12] COMISIÓN EUROPEA, Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, Bruselas, 7.2.2013, JOIN(2013) 1 final. En un mundo globalizado donde internet se ha convertido en esencial para sectores clave de la economía y de la sociedad (servicios financieros, santidad, energía, transporte, etc), ha convertido en necesaria la adopción de una estrategia global para hacer frente a los riesgos y amenazas existentes en el ciberespacio. En el marco de la Estrategia de Ciberseguridad de la Unión Europea, se fijan las siguientes prioridades y medidas estratégicas: Lograr la ciberresiliencia, reducir drásticamente la ciberdelincuencia, desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD), desarrollar recursos industriales y tecnológicos de ciberseguridad,

Una primera lectura de los considerandos del RCR pone de manifiesto los problemas detectados en materia de ciberseguridad de los productos y los objetivos que persigue. Por un lado, el RCR pretende mejorar el nivel bajo de ciberseguridad de los productos con elementos digitales y, por otro lado, quiere incrementar la seguridad de dichos productos mediante actualizaciones de seguridad eficaces para combatir las vulnerabilidades detectadas en productos, que puedan afectarles, evitando que estas puedan ser explotadas por un tercero malintencionado. Asimismo, el legislador europeo pretende incentivar a los consumidores a adquirir productos seguros, evitando que la seguridad sea un atributo del producto meramente complementario a la finalidad que sirven (considerandos 1 y 2 RCR).

El ámbito de aplicación material del RCR gira en torno a los denominados "productos con elementos digitales", que aparecen definidos en el art. 3.1) RCR: "producto consistente en programas informáticos o equipos informáticos y sus soluciones de procesamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado". La definición es congruente con la conceptualización del software como producto, una particularidad que se ha consolidado en la nueva legislación europea sobre productos. No obstante lo anterior, el denominado "Software como servicio" queda fuera del ámbito de aplicación del RCR (considerando núm. 12 RCR),[13] por lo que quedarían comprendidos dentro del ámbito de aplicación de la Directiva SRI 2. La principal característica de los productos con elementos digitales es su conexión a internet. Esta propiedad hace que estos productos puedan ser vulnerables frente a ataques perpetrados por terceros aprovechando alguna vulnerabilidad que se materialice en una brecha de ciberseguridad del producto (considerando núm. 9 RCR). Sin embargo, en ocasiones los ciberataques no solo tienen como resultado el control de un producto, sino que los efectos del ataque pueden tener un alcance exponencial si con un primer ataque exitoso un agente puede infiltrarse en el sistema y atacar a otros productos que también presenten vulnerabilidades.[14]

El legislador europeo es consciente de que la legislación europea no daba una respuesta adecuada a los problemas planteados, situación que repercutía en un nivel de ciberseguridad muy bajo de los productos con elementos digitales, haciéndolos vulnerables frente a los ataques y amenazas del ciberespacio. Por tanto, el principal objetivo del RCR es garantizar la conformidad de los productos con elementos digitales en materia de ciberseguridad y, de esta forma, impedir su libre circulación entre los Estados miembros de la UE cuando dichos productos no cumplan los requisitos de conformidad del RCR.[15]

establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE. Dentro del desarrollo tecnológico de ciberseguridad, y en lo tocante a este trabajo, la Comisión Europea pretende crear un mercado único de productos de ciberseguridad. Es en este punto donde los fabricantes de productos con elementos digitales se erigen como una pieza clave para conseguir que la ciberseguridad de sus productos se convierta en una prioridad para los consumidores, en aras de conseguir unos productos más ciberresilientes, infranqueables frente amenazas y ataques de terceros.

[13] Considerando núm. 12 RCR: "Por otra parte, los sitios web que no admiten la funcionalidad de un producto con elementos digitales o los servicios en la nube diseñados y desarrollados fuera de la responsabilidad de un fabricante de un producto con elementos digitales no entran en el ámbito de aplicación del presente Reglamento. La Directiva (UE) 2022/2555 se aplica a los servicios de computación en la nube y a los modelos de servicios en nube, como la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS), el software como servicio (SaaS) y la red como servicio (NaaS)." En este sentido, CHIARA, Pier Giorgio., «The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction», International Cybersecurity Law Review, 3, 2022, pp. 258, 269. BURRI, Mira/ZIHLMANN, Zaira., «The Cyber Resilience Act – An Appraisal and Contextualization», Zeitschrift für Europearecht, 2, 2023, pp. 19.

[14] RAIZ SHAFFIQUE, Mohammed., «Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?», *Computer Law & Security Review*, 54, 2024, pp. 4-5.

[15] AZIZ AL KABIR, Mohammed/ELMEDANY, Wael/SAEED SHARIF, Mhd., «Securing IoT devices against emerging security threats: challenges and mitigation techniques», *Journal of Cyber Security Technology*, 7, 2023, pp. 199-200. El RCR pone especial atención en la etapa previa a la introducción en el mercado o puesta en servicio del producto, a pesar de que también se ocupa de la gestión de los riesgos del producto una vez se ha introducido en el mercado. El legislador europeo se ha percatado de que los fabricantes se centran, fundamentalmente, en mejorar la ciberseguridad de sus productos, relegando su seguridad. Es por ello que mediante la declaración de conformidad se pretende que solo se introduzcan en el mercado productos seguros.

En consecuencia, el ámbito del RCR es transversal, pues tiene la vocación de aplicarse en defecto de legislación sectorial aplicable para cualquier categoría de producto. En este sentido, existen varios productos excluidos del ámbito de aplicación de RCR.[16]

4.1. Vulnerabilidad, vulnerabilidad aprovechable, vulnerabilidad aprovechada activamente y vulnerabilidad conocida

Este trabajo gira en torno al concepto de "vulnerabilidad", en tanto que se trata de una circunstancia que afecta a los productos con elementos digitales que puede comprometer la responsabilidad de los fabricantes. Por este motivo, es necesario abordar este concepto, partiendo de las definiciones contenidas en el RCR y las aportaciones que la doctrina ha hecho al mismo.

A los efectos del RCR, el término vulnerabilidad aparece definido en el art. 3.40 RCR): *"deficiencia, susceptibilidad o fallo de un producto con elementos digitales que puede ser aprovechada por una ciberamenaza".* Los sustantivos "deficiencia, susceptibilidad o fallo" aluden a una brecha en la ciberseguridad del producto, que lo convierten en vulnerable frente a los ataques perpetrados en el ciberespacio por terceros malintencionados. Por tanto, un producto con elementos digitales vulnerable es un producto mermado en cuanto a su ciberseguridad, que lo convierte en potencialmente dañino. La debilidad que entraña un producto vulnerable es una nota común del concepto de vulnerabilidad utilizado en otras normas europeas, como la Directiva SRI 2.[17]

En paralelo al concepto de "vulnerabilidad", entendido como una debilidad que presenta, en general, el producto con elementos digitales en cuanto a su ciberseguridad, el art. 3.41) RCR define el concepto de "vulnerabilidad aprovechable": *"vulnerabilidad que puede ser utilizada de manera efectiva por un agente malintencionado en condiciones operativas prácticas"*. El elemento que permite diferenciar a ambos conceptos es la referencia a las "condiciones operativas prácticas", que conduce a distinguir entre vulnerabilidades que pueden afectar a los productos con elementos digitales, pero que no son inmediatamente aprovechables, sino que lo serán en condiciones operativas prácticas, es decir, en ciertas condiciones reales que efectivamente permitan que la vulnerabilidad que presenta el producto sea aprovechable activamente por un tercero,[18] lo que nos conducirá al concepto de "vulnerabilidad aprovechada activamente". El RCR pone el acento en las vulnerabilidades aprovechables en la fase previa a la comercialización del producto, pues se obliga a los fabricantes a no introducir en el mercado o poner en servicio productos con elementos digitales que presenten vulnerabilidades aprovechables conocidas (Anexo I Parte I RCR), como uno de los elementos que integran los requisitos generales de conformidad. A este respecto, adquiere relevancia la base de datos europea de vulnerabilidades creada por la Directiva SRI 2, cuyo art. 12 regula la divulgación coordinada de vulnerabilidades, de tal manera que las vulnerabilidades aprovechables conocidas gozan de publicidad para los fabricantes, lo que obligará a su consulta a los efectos de certificar que sus productos que están afectados por una vulnerabilidad aprovechable conocida. Veremos, en la siguiente sección, cómo incidirá este elemento de publicidad en la responsabilidad del fabricante.

---

[16] Los productos sanitarios y los productos para el diagnóstico in vitro se regulan, respectivamente, por los Reglamentos 2017/745 y 2017/746. Los vehículos, en tanto que incorporan sistemas y componentes digitales, se rigen por lo dispuesto en el Reglamento (UE) 2019/2144, especialmente en lo que se refiere a los sistemas de gestión de la ciberseguridad certificado y a las actualizaciones de los programas informáticos. Asimismo, en el ámbito de la aviación, para la certificación de los requisitos esenciales de ciberseguridad de la aeronavegabilidad debe tener en cuenta el Reglamento (UE) 2018/1139 (considerando núm. 27 y art. 2 RCR).

[17] Art. 3.15 Directiva SRI 2: *"«vulnerabilidad»: deficiencia, susceptibilidad o fallo de productos de TIC o servicios de TIC que puede ser aprovechado por una ciberamenaza"*.

[18] ROYTMAN, Michael/BELLIS, Ed., *Modern Vulnerability Management. Predictive Cybersecurity*, Artech House, Londres, 2023, pp. 4. Es posible identificar las vulnerabilidades aprovechables con las amenazas de ciberseguridad (*threats*): *"a vulnerability is distinct from a threat, which is the potential for a specific actor to exploit, or take advantage of, a vulnerability. Tens of thousands of vulnerabilities are discovered each year, but only a small fraction become threats. A vulnerability becomes a threat when an exploit (code that compromises a vulnerability) is written."*

Finalmente, una vez el producto ha sido introducido en el mercado o puesto en servicio, adquiere relevancia el concepto de "vulnerabilidad aprovechada activamente" (art. 3.42) RCR), que hace hincapié en el conocimiento fehaciente que el fabricante tiene de que el producto ha sido atacado de forma exitosa, es decir, habiendo aprovechado a un tercero: *"vulnerabilidad respecto de la cual existen pruebas fiables de que un agente malintencionado la ha aprovechado en un sistema sin autorización del propietario del sistema"*.[19] La constatación por el fabricante de que una vulnerabilidad en sus productos ha sido aprovechada activamente se traduce en un deber de notificación al CSIRT designado como coordinador (art. 14.1 RCR). En cuanto a los plazos del deber de notificación el art. 14.2.a) RCR impone una alerta temprana de la vulnerabilidad que deberá realizarse dentro del plazo de veinticuatro horas desde que el fabricante haya tenido conocimiento de ella y otra notificación a realizar dentro del plazo de setenta y dos horas, que incluirá mayores detalles sobre la vulnerabilidad aprovechada activamente: *"que proporcionará la información general disponible sobre el producto con elementos digitales en cuestión, la naturaleza general de la vulnerabilidad en cuestión y el modo en que es aprovechada, así como sobre las medidas correctoras o paliativas adoptadas y las medidas correctoras o paliativas que los usuarios pueden adoptar, y que también indicará, cuando proceda, en qué medida el fabricante considera sensible la información notificada"* (art. 14.2.b) RCR). Por último, dentro del plazo de catorce días a contar desde que el fabricante disponga de una medida correctora de la vulnerabilidad (art. 14.2.c) RCR) el fabricante deberá confeccionar un informe con una información mínima necesaria: *"i) una descripción de la vulnerabilidad, que incluya su gravedad y sus repercusiones, ii) cuando se disponga de ella, información relativa a cualquier agente malintencionado que haya aprovechado o esté aprovechando la vulnerabilidad, iii) detalles sobre la actualización de seguridad u otras medidas correctoras disponibles para subsanar la vulnerabilidad."* El deber de notificación no solo se limita al CSIRT responsable, sino que los fabricantes deberán dirigirse a los usuarios afectados por la vulnerabilidad aprovechada activamente (art. 14.8 RCR).

En definitiva, el uso del concepto de vulnerabilidad, entendido como una debilidad del producto con elementos digitales que afecta a su ciberseguridad, el RCR pone el acento, por un lado, en las vulnerabilidades aprovechables para certificar que el fabricante introduce en el mercado o pone en servicio el producto sin vulnerabilidades conocidas y, por otro lado, en la obligación del fabricante de reportar los incidentes que hayan comportado las explotaciones de vulnerabilidades una vez el producto ya se encuentra en manos de los usuarios.

4.2. Requisitos generales de conformidad

Para que los productos con elementos digitales puedan ser introducidos en el mercado europeo, es necesario que cumplan determinados requisitos de conformidad (considerandos núm. 8 y 10 y arts. 4.1 y 6 RCR), en aras a proteger a los consumidores y a los propios fabricantes. Dichos requisitos generales de conformidad se prevén en el Anexo I Parte I RCR.[20] Sin embargo, los requisitos que figuran en el Anexo I RCR no constituyen una lista cerrada, puesto que los fabricantes deben adoptar medidas para eliminar los riesgos que presente el producto, a pesar de que no consten en el Anexo I RCR (considerando núm. 54).[21]

a. El nivel adecuado de ciberseguridad en consideración a los riesgos existentes

Sin ánimo de comentar los requisitos de conformidad previstos en el Anexo I Parte I RCR, sí que parece oportuno detenerse en alguna consideración general, como es la necesidad de reducir al mínimo el riesgo existente durante toda la cadena de producción del producto. En este sentido, a título de ejemplo puede citarse el art. 13.3 RCR: *"La evaluación de los riesgos de ciberseguridad se documentará y actualizará*

[19] ROYTMAN, Michael/BELLIS, Ed., *Modern Vulnerability Management. Predictive Cybersecurity*, pp. 5. *"An exploitation is the actual event of using an exploit to take advantage of a vulnerability. This is the threat becoming materialized, coming to pass."*

[20] Anexo I Parte I RCR.

[21] ZIRNSTEIN, Yannick/LIN LEE, Yue/GE, Amanda., «Evolving Cybersecurity Landscape – Comparing the Regulatory Approaches in the EU, in China and in Singapore — An Analysis of Legislative Approaches to Key Issues in Tackling a Global Phenomenon», *Computer Law Review Inetrnational*, 6, 2022, pp. 167.

según proceda durante un período de soporte que se determinará de conformidad con el apartado 8 del presente artículo. Dicha evaluación de los riesgos de ciberseguridad incluirá, como mínimo, un análisis de los riesgos de ciberseguridad basado en la finalidad prevista y el uso razonablemente previsible del producto con elementos digitales, así como sus condiciones de uso, tales como el entorno operativo o los activos que deben protegerse, teniendo en cuenta el período de tiempo durante el que se prevé que el producto esté en uso." A mi modo de ver, la correcta ponderación entre un nivel adecuado de ciberseguridad y la base de riesgos existentes obliga al fabricante a reducir al mínimo el riesgo para determinar el nivel de seguridad exigible, atendiendo a algunos parámetros que establece el propio RCR. El art. 13.3 RCR, que versa sobre la evaluación de los riesgos de ciberseguridad, contiene algunos elementos que deben utilizarse para ponderar los riesgos existentes.[22]

En primer lugar, se alude al uso razonablemente previsible del producto. Se trata de un término definido en el art. 3.24) RCR: *"uso que no coincide necesariamente con la finalidad prevista indicada por el fabricante en las instrucciones de uso, los materiales y las declaraciones de promoción y venta y la documentación técnica, pero que puede derivarse de un comportamiento humano o de intervenciones e interacciones técnicas razonablemente previsibles"*. Habida cuenta de la definición transcrita, el uso razonablemente previsible del producto podría equipararse al "uso normal" del producto, atendiendo a dos grandes parámetros. Por un lado, desde un punto de vista subjetivo, las declaraciones provenientes del fabricante, plasmadas en las instrucciones de uso, la documentación técnica y las declaraciones de promoción y venta, elementos que constituyen la finalidad prevista del producto. Por otro lado, desde un punto de vista objetivo, el uso previsible del producto que deriva de un comportamiento humano o de interacciones técnicas razonablemente previsibles, lo que amplía el deber de diligencia del fabricante en el momento de ponderar los posibles riesgos existentes.

En segundo lugar, se hace referencia a las condiciones de uso, como el entorno operativo o los activos que deben protegerse. El entorno operativo de los productos con elementos digitales puede cambiar con mucha celeridad debido a los avances tecnológicos que operan en el ciberespacio, por lo que, en mi opinión, obliga a extremar la diligencia y no solo a contemplar las condiciones de uso en el momento de la introducción en el mercado o puesta en servicio del producto, sino que deben tenerse en cuenta los avances tecnológicos previsibles que puedan producirse durante el periodo de soporte.[23]

De acuerdo con el art. 13.3 RCR, ambos elementos, el uso normalmente previsible y las condiciones de uso deben medirse según el periodo de soporte del producto con elementos digitales determinado, que conforme al art. 13.8 RCR, debe ser determinado principalmente por los fabricantes, considerando factores como las expectativas razonables de los usuarios, la naturaleza del producto y el Derecho vigente. Sin embargo, la Comisión reserva la facultad de determinar el periodo de soporte de determinados productos mediante actos delegados.

En tercer lugar, bajo mi punto de vista, otro elemento a considerar para valorar los riesgos de ciberseguridad es el uso indebido razonablemente previsible. Según el art. 3.25) RCR, se trata de un uso del producto no conforme con su finalidad prevista, pero que es razonablemente previsible según un comportamiento humano o de interacciones con otros sistemas. En la evaluación de los riesgos existentes en el producto, el art. 13.3 RCR no hace hincapié al uso indebido razonablemente previsible, es decir, el uso indebido razonablemente previsible obliga a contemplar aquellos posibles usos del producto no alineados con la finalidad prevista y que entrañan un riesgo existente de ciberseguridad. Pero lo cierto es que si el art. 13.3 RCR busca reducir el riesgo existente a la mínima expresión, debería incluir dicho tipo de uso, en tanto que

[22] Desde mi punto de vista, el correcto entendimiento de "los riesgos existentes" que aparecen en el primer criterio del Anexo I Parte I RCR deben valorarse considerando el uso razonablemente previsible del producto y el uso indebido razonablemente del producto. Este enfoque se sustenta sobre la base de lo prevenido en el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos. La definición de "riesgo grave" del art. 3.5) de dicho reglamento contempla el "uso normal y previsible del producto".

[23] MILLER, Kevin L., «What we talk about when we talk about 'reasonable cybersecurity': a proactive and adaptive approach», *Florida Bar Journal,* 90-8, 2016, pp. 5-6.

puede ser previsible. El Anexo II RCR, entre la información e instrucciones que deben darse al usuario, se hace referencia al deber de indicar al usuario: *"cualquier circunstancia conocida o previsible, asociada al uso del producto con elementos digitales conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos de ciberseguridad significativos"*. Por tanto, en la medida que el uso indebido razonablemente previsible es una circunstancia que debe ser comunicada al usuario, el fabricante tendría que contemplarlo en la evaluación del riesgo, de conformidad con el nivel de riesgo mínimo exigible que defiendo que incorpora el art. 13.3 RCR.

En otro orden de cosa pivota el criterio de la razonabilidad empleado en el art. 6 RCR. Una cosa es que los riesgos existentes del producto no se tengan que considerar sólo sobre la base del uso indicado por el fabricante, sino considerando, también, el uso razonable que pudiera darse al producto y, otra cosa es que el nivel de riesgo exigible al fabricante deba reducirse a la mínima expresión cuando se evalúen los riesgos existentes del producto. En el primer caso, parece que el RCR explícitamente aplica el criterio de la razonabilidad para delimitar los usos de producto que ha de contemplar el fabricante y también lo usa como criterio equivalente a la adecuación para significar que el nivel de seguridad tiene que ser proporcional al nivel de riesgo. En el segundo caso, el art. 13 RCR usa un criterio más estricto que el de la razonabilidad para determinar el nivel de seguridad exigible, porque obliga a minimizar los riesgos y reducir al mínimo sus repercusiones.

b. Protección de datos personales desde el diseño y por defecto

Las vulnerabilidades de ciberseguridad que presentan los productos con elementos digitales pueden tener, como potencial resultado dañoso, la corrupción de datos. Es por este motivo que una parte de los requisitos esenciales de ciberseguridad (d, e, f, g, m) previstos en el Anexo I Parte I RCR tienen por objeto la protección de datos personales de los usuarios de este tipo de productos.[24] Esto implica que, desde el prisma de la ciberseguridad, los productos con elementos digitales también deben ser diseñados, en aras a cumplir los requisitos esenciales de ciberseguridad, para cumplir con las previsiones del Reglamento 2016/679, en adelante, RGPD.[25]

Estamos, por tanto, ante criterios esenciales de ciberseguridad que persiguen la protección de los datos personales de los usuarios y que obliga a los fabricantes, como responsables del tratamiento de los datos, a adoptar, sobre todo, medidas técnicas específicamente diseñadas para salvaguardar los datos personales de los usuarios.[26] Habida cuenta del alto riesgo para los derechos y libertades de los usuarios que implica el tratamiento de datos personales en productos con elementos digitales, los fabricantes, de conformidad con el art. 35 RGPD, deben realizar una evaluación de impacto que determinará qué medidas deben adoptarse desde el diseño y por defecto para la protección de los datos personales de los usuarios.[27] En materia de ciberseguridad, los fabricantes deberán diseñar y producir sus productos evitando que sean vulnerables ante ataques que puedan tener como objetivo la corrupción de datos.

[24] *Vid.* Considerando núm. 32 RCR.

[25] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE núm. 119, de 4 de mayo de 2016.

[26] BYGRAVE, Lee. A., «Article 25. Data protection by design and by default», en KUNER, Christopher/BYGRAVE, Lee. A/DOCKSEY, Christopher/DRECHSLER, Laura (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*., Oxford University Press, Londres, 2020, pp, 571-581.

[27] KOSTA, Eleni., «Article 35. Data protection impact assessment and prior consultation», en KUNER, Christopher/BYGRAVE, Lee. A/DOCKSEY, Christopher/DRECHSLER, Laura (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*., Oxford University Press, Londres, 2020, pp, 665-679. GRUPO DE TRABAJO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017 Revisadas por última vez y adoptadas el 4 de octubre de 2017. 17/ES WP 248 rev.01. Salvo las excepciones que contempla el propio RGPD, será necesario realizar una evaluación de impacto cuando el tratamiento de datos personales "entrañe probablemente un riesgo alto". En este sentido, la posibilidad de que los productos con elementos digitales traten datos sensibles o muy personales (art. 9 RGPD), obliga a realizar una evaluación de impacto. En caso de duda sobre si la operación de tratamiento requiere la evaluación de impacto, el Grupo de Trabajo del Artículo 29 recomienda realizarla.

4.3. Clasificación de los productos basada en el nivel de riesgo

El RCR parte de la premisa de que no todos los productos con elementos digitales presentan el mismo nivel de riesgo de ciberseguridad. Tomando este punto de partida, el RCR clasifica los productos con elementos digitales en cuatro grupos, en función de su funcionalidad relacionada con la ciberseguridad, riesgo significativo de efectos adversos, la naturaleza de los incidentes de ciberseguridad y la dependencia de entidades esenciales (art. 3.1 Directiva 2022/2555), [28] lo que permite sostener que se trata de una clasificación tomando como referencia, principalmente, el riesgo inherente del producto en cuestión:[29]

a) Productos importantes con elementos digitales de la clase I (art. 7 y Anexo III RCR). Esta categoría incluye productos como los gestores de contraseñas, sistemas operativos, asistentes virtuales de propósito general para hogares inteligentes, etc.

b) Productos importantes con elementos digitales de la clase II (art. 7 y Anexo III RCR). Se incluye productos como cortafuegos y sistemas de detección y prevención de intrusiones.

c) Productos críticos con elementos digitales (art. 8 y Anexo IV RCR). Forman parte de este grupo productos críticos como dispositivos de equipos informáticos con cajas de seguridad y tarjetas inteligentes. La lista de productos críticos contenida en el Anexo IV RCR no es una lista cerrada, habida cuenta que la Comisión Europea se reserva la facultad de, mediante actos delegados, incluir nuevos productos en esta categoría, sobre todo por el rápido avance de la tecnología y evitar, así, que quede desfasada (considerando núm. 48 y art. 8 RCR).

d) Otros productos con elementos digitales no incluidos en los grupos anteriores. Este grupo incluiría productos como software de edición de fotos, auriculares inteligentes, videojuegos, editores de texto, etc. Se trata de productos cuyas brechas de ciberseguridad no acarrean un riesgo grave.[30]

El art. 6 RCR establece la prohibición de comercializar productos con elementos digitales que no satisfagan los requisitos esenciales de ciberseguridad del Anexo I RCR, después de examinar la conformidad de dichos requisitos esenciales a través de los procedimientos que establece el propio RCR (art. 32 RCR). Considerando la naturaleza del producto con elementos digitales en cuestión, el RCR prevé un determinado procedimiento para valorar la conformidad con los requisitos esenciales de conformidad del Anexo I.[31]

---

[28] Considerando núm. 46 RCR: *"Las categorías de productos críticos con elementos digitales establecidas en el presente Reglamento tienen una funcionalidad relacionada con la ciberseguridad y desempeñan una función que conlleva un riesgo significativo de efectos adversos en términos de intensidad y capacidad para perturbar, controlar o dañar un gran número de otros productos con elementos digitales mediante manipulación directa."* SCHMITTNER, Christoph/VELEDAR, Omar/FASCHANG, Thomas/MACHER, Georg/BRENNER, Eugen., «Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act», en YLMAZ, Murat/CLARKE, Paul/RILE, Andreas/MESSNARZ, Richard/GREINER, Christian/PEISL, Thomas (eds.), *Systems, Software and Services Process Improvement*, Springer Nature Switzerland AG, 2024, pp. 398.

[29] BURRI, Mira/ZIHLMANN, Zaira., *Zeitschrift für Europearecht*, 2, 2023, pp. 25-27.

[30] COMISIÓN EUROPEA., «Cyber Resilience Act. New EU cybersecurity rules ensure more secure hardware and software products», 2022, puede consultarse en: https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products. Consulta realizada el día 30 de mayo de 2025. La Comisión Europea estima que el 90% de los productos con elementos digitales formarán parte de esta categoría. Sin embargo, puede que existan productos que, sin considerar el entorno donde despliegan su funcionalidad, no sean incluidos en las tres primeras categorías, pero que considerando el entorno operativo, una brecha en su ciberseguridad podría afectar instalaciones o procesos críticos. BURRI, Mira/ZIHLMANN, Zaira., *Zeitschrift für Europearecht*, 2, 2023, pp. 28. *"For instance, smart LED bulbs would likely be classified as non-critical products. However, if a smart LED light bulb is compromised, it can serve as a gateway into the network it is connected to and the threat can spread to an entire network. If a smart LED bulb is used in a private home network, the ramifications of its compromise may be less problematic. However, if such a light bulb is in use in a factory and can thus be exploited as an entry point into the factory's network and for example be used to shut down the factory's production, the consequences could be much more widespread."*

[31] Esta obra ofrece una explicación clara del procedimiento de conformidad a seguir a los efectos de la certificación de los requisitos esenciales de seguridad en función de la clasificación de los productos con elementos digitales. MUECK, Marcus/ROBERTS, Taylor/DU BOISPÉAN, Stéphane/GAIE, Christophe., «E 4. Introduction to the European Cyber Resilience Act», en MUECK, Marcus/GAIE, Christophe (eds.), *European Digital Regulations*, Springer Nature, 2025, pp. 98-103.

4.4. Requisitos de gestión de las vulnerabilidades

Habida cuenta de lo dispuesto en el Anexo I RCR, los requisitos de gestión de vulnerabilidades operan en dos grandes momentos. Por un lado, antes de que el producto con elementos digitales se introduzca en el mercado y, por otro lado, una vez el producto ya se haya comercializado.

a. Prohibición de comercialización de productos con vulnerabilidades conocidas

La letra a) del Anexo I Parte I obliga a los fabricantes a comercializar sus productos sin que presenten vulnerabilidades conocidas, en atención a los resultados que arroje la evaluación de riesgos de ciberseguridad. La referencia que hace el requisito a que sean "vulnerabilidades conocidas" nos conduce a hacer referencia, de nuevo, a la base de datos europea de vulnerabilidades, que se regula en el art. 12 Directiva SRI 2. Dicha base se alimenta de las vulnerabilidades que reporten los usuarios, fabricantes y proveedores de TIC que afecten a productos con elementos digitales, de tal manera que los demás fabricantes estarán obligados a comprobar, antes de introducir en el mercado sus productos, que no están afectados por las vulnerabilidades publicadas en la base de datos europea de vulnerabilidades (considerando núm. 62 Directiva SRI 2).

Sin embargo, la doctrina ha alertado que los productos con elementos digitales suelen introducirse en el mercado con vulnerabilidades que aún son desconocidas por los fabricantes. Además, si los productos no deben introducirse en el mercado con vulnerabilidades conocidas que resulten de la evaluación de riesgos de ciberseguridad que realice el fabricante, esto conlleva que la ciberseguridad del producto se haya probado en un ambiente simulado, lejos de los riesgos del ciberespacio.[32] Veremos qué responsabilidad acarrea para el fabricante que su producto se introduzca en el mercado sin vulnerabilidades conocidas, pero pudiendo estar afectado por vulnerabilidades no conocidas en los siguientes epígrafes.

b. Etapa posterior a la comercialización del producto

La Parte II del Anexo I contiene propiamente los requisitos de gestión de las vulnerabilidades una vez el producto haya sido introducido en el mercado, que igualmente son de obligado cumplimiento (art. 6.b) RCR). La gestión de las vulnerabilidades en esta fase se extiende a lo largo de todo el periodo de soporte (art. 13.8 RCR). En línea de principio, el periodo de soporte debe determinarse por los fabricantes teniendo en cuenta el periodo de uso de sus productos, considerando, en particular, *"las expectativas razonables de los usuarios, la naturaleza del producto —incluida su finalidad prevista— y el Derecho pertinente de la Unión que fija la vida útil del producto con elementos digitales. A la hora de determinar el periodo de soporte, los fabricantes también podrán tener en cuenta los periodos de soporte de productos con elementos digitales que ofrezcan una funcionalidad similar introducidos en el mercado por otros fabricantes, la disponibilidad del entorno operativo y los periodos de soporte de los componentes integrados que proporcionan las funciones principales y se obtienen de terceros, así como las orientaciones pertinentes facilitadas por el Grupo de Cooperación Administrativa (ADCO) específico establecido en virtud del artículo 52, apartado 15, y por la Comisión."*

Se parte, por tanto, de la premisa de determinar el periodo de soporte para cada producto en particular, considerando las circunstancias que establece el propio artículo, lo que conduce a una falta de seguridad jurídica. No obstante, con el fin de objetivar la duración del periodo de soporte, el tercer párrafo del art. 13.8 RCR establece una duración determinada de cinco años. Quizá este plazo de cinco años sea suficiente para los productos con elementos digitales de uso corriente de los consumidores, que quedan desfasados rápidamente por los avances tecnológicos, pero en caso de productos industriales el plazo puede ser mucho más extendido en el tiempo.[33] A mi modo de ver, los fabricantes deben fijar un periodo de soporte acorde

[32] ELLUL, Joshua/PAECE, Gordon. J/REVOLIDIS, Ioannis/SCHNEIDER, Gerardo., «When is good enough good enough? On software assurances», *ERA Forum*, 23, 2023, pp. 345-346.

[33] Considerando núm. 60 RCR. Este considerando apunta a esta idea. No obstante, no se justifica la duración del periodo de soporte de cinco años. Algún autor defendió la opción de introducir un periodo de soporte de diez años, una opción que no se

con el tiempo de uso previsible, considerando los factores del primer párrafo del art. 13.8 RCR, operando el plazo de cinco años con carácter supletorio y de mínimos, con la salvedad de aquellos productos que se prevea que tengan un periodo de vida útil inferior a los cinco años, en cuyo caso deberá estarse a este periodo más breve (tercer párrafo art. 13.8 RCR). A pesar del esfuerzo el legislador europeo por tratar de individualizar y concretar el periodo de soporte de cada tipo de producto, considero que por la Comisión Europea deberían adoptarse tablas para determinar el periodo de vida útil de los productos y bienes, pues esta es una cuestión que también afecta, por ejemplo, a la responsabilidad contractual del vendedor por falta de conformidad en las compraventas de bienes. El art. 7.1.d) Directiva (UE) 2019/771, en adelante DCC, se refiere a la durabilidad de los bienes como criterio objetivo de la conformidad.[34]

La forma de gestionar las vulnerabilidades después de haber introducido el producto en el mercado es mediante el suministro de actualizaciones de seguridad, que se proporcionarán durante el periodo de soporte y que deberán permanecer disponibles tras su publicación durante un período mínimo de diez años o durante el resto del período de soporte si este plazo fuera más largo (art. 13.9 RCR). En consecuencia, una vez finalizado el periodo de soporte, los fabricantes pueden dejar de suministrar actualizaciones de seguridad, lo que va a comprometer la ciberseguridad de sus productos, haciéndolos vulnerables frente ataques de terceros, si bien las actualizaciones de seguridad suministradas durante el periodo de soporte tendrán que estar disponibles durante un plazo de 10 años. A mi modo de ver, la publicidad de las actualizaciones de seguridad recibidas durante el periodo de soporte no extiende el plazo durante el cual los fabricantes velen por la gestión efectiva de las vulnerabilidades más allá del periodo de soporte, sino que, mediante su publicación, puede plantear la duda de si se traslada la responsabilidad al usuario final de velar por la ciberseguridad de su producto una vez finalizado el periodo de soporte. El punto 7 del Anexo II RCR obliga a especificar *"el tipo de apoyo técnico en materia de seguridad ofrecido por el fabricante y la fecha de finalización del período de soporte durante el que está previsto que se gestionen las vulnerabilidades y que los usuarios puedan recibir actualizaciones de seguridad"* y, en este sentido, el considerando núm. 61 RCR prevé que, una vez finalizado el periodo de soporte, los fabricantes deben *"considerar la posibilidad de divulgar el código fuente de dichos productos con elementos digitales a otras empresas que se comprometan a ampliar la prestación de servicios de gestión de vulnerabilidades o al público"*. La referencia expresa a la divulgación del código fuente al público en general para la gestión de vulnerabilidades permite deducir que los usuarios finales deberán velar por la ciberseguridad de su producto una vez finalizado el periodo de soporte, algo que ante los riesgos potenciales que asumirán los usuarios finales induce a renovar el producto con elementos digitales, lo que no se alinea con los objetivos de desarrollo sostenible que se ha fijado la Unión Europea.

5. Directiva 2024/2853 (Directiva de responsabilidad por daños causados por productos defectuosos

La Directiva 85/374/CEE[35] quedará derogada con efectos al próximo 9 de diciembre de 2026. Desde su adopción hasta entonces habrá regulado, durante más de 40 años, la responsabilidad de los operadores económicos por los daños causados por productos defectuosos. El pasado 13 de diciembre de 2024 el DOUE publicaba la nueva Directiva 2024/2853, sobre responsabilidad por daños causados por productos defectuosos, que actualmente se encuentra vigente, pero que será aplicable a partir del 9 de diciembre de 2026, la fecha máxima de su transposición (art. 21 DRP).

Una lectura de la DRP permite constatar que sigue, en general, y salvo algunas particularidades, las mismas directrices que la Directiva 85/374/CEE. Aspectos como la responsabilidad en cascada de los operadores económicos que integran la cadena de suministro del producto, la previsión de un régimen objetivo de

adoptó en el texto aprobado del RCR. BERTUZZI, Luca., «EU Council moves to adjust product lifecycle, reporting in new cybersecurity law», 2023. Puede consultarse en: https://www.euractiv.com/section/tech/news/eu-council-moves-to-adjust-product-lifecycle-reporting-in-new-cybersecurity-law/. Consulta realizada el día 31 de mayo de 2025.

[34] Directiva (UE) 2019/771 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modifican el Reglamento (CE) núm. 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE. DOUE núm. 136, de 22 de mayo de 2019.

[35] 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. 210, de 7 de agosto de 1985.

responsabilidad, el plazo para el ejercicio de acciones contra los operadores económicos y el plazo de caducidad de la acción son pilares sobre los que se asentaba la regulación de la Directiva 85/374/CEE y que siguen presentes en la DRP. La principal causa que ha propiciado la adopción de una nueva directiva en esta materia ha sido la digitalización de los productos, la irrupción de la inteligencia artificial y la economía circular.[36]

Por lo que se refiere al objeto de este trabajo, la DRP no dedica especial atención en su articulado a las vulnerabilidades que pueden afectar a los productos, tan solo en el art. 7.2.f) DRP se refiere genéricamente a los requisitos de ciberseguridad como una circunstancia para apreciar el carácter defectuoso de un producto. Sin embargo, en algunos de sus considerandos se hace referencia a las vulnerabilidades de productos como una causa de defectuosidad que afecta a la responsabilidad de los operadores económicos.

Antes de entrar a examinar las diferentes circunstancias que permiten apreciar el carácter defectuoso de un producto que pueden afectar a su ciberseguridad, debo hacer una prevé referencia a la novedad que presenta el art. 7.1 DRP en relación con el art. 6 Directiva /85/374/CEE, al referirse al Derecho de la Unión Europea o al Derecho nacional como un segundo estándar de referencia. ¿Este segundo estándar de referencia completa y es el mismo que las expectativas razonables del público en general o es un segundo estándar alternativo? El art. 7.1 DRP utiliza la conjunción "asimismo", mientras que la versión en inglés, francés, italiano y alemán se emplea la conjunción "o". El considerando núm. 30 DRP nos conduce a interpretar el art. 7.1 DRP como dos estándares de referencia alternativos porque se emplea la conjunción "o". Por tanto, un producto será defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y cuando no cumpla las normas aplicables en materia de seguridad.[37] habida cuenta del carácter alternativo de los estándares de diligencia, un producto será defectuoso si, a pesar del cumplimiento normativo de las normas de seguridad que sean aplicables, en nuestro caso de ciberseguridad, no ofrece la seguridad que el público puede esperar.[38]

5.1. Defectuosidad del producto por vulnerabilidades de seguridad

La DRP ha ampliado las circunstancias para apreciar el carácter defectuoso de un producto, sobre todo, en aras a prever aquellas circunstancias propias de los productos con elementos digitales. En este sentido, se contempla el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio (art. 7.2.c) DRP); el efecto razonablemente previsible en el producto de otros productos de los que se pueda esperar que se utilicen junto con el producto, también mediante interconexión (art. 7.2.d) DRP); los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad pertinentes para la seguridad (art. 7.2.f) DRP), entre otros.

A pesar del incremento de las circunstancias para apreciar el carácter defectuoso de un producto, se mantiene, como característica indispensable e ineludible de un producto defectuoso, la necesidad de que se produzca un daño. En caso contrario, no obstante encontrarnos ante un producto peligroso o inseguro, si el

[36] Para una introducción general a la nueva DRP, *vid.* WAGNER, Gerhard., «Liability Rules for the Digital Age - Aiming for the Brussels Effect», *Journal of European Tort Law*, 3, 2022, pp. 191-243. VELDT, Gitta., «The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up? An Analysis of the Draft Product Liability Directive», *European Journal of Consumer and Market Law*, 1, 2023, pp. 24-31. ATIENZA NAVARRO, María Luisa., «¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)»., *Indret*, 2, 2023, pp. 1-53. MARTÍN-CASALS, Miquel., «Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial», *Indret*, 3, 2023, pp. 75-93. PÉREZ GARCÍA, Máximo Juan., «La responsabilidad por los daños causados por productos defectuosos: análisis de la Directiva (UE) 2024/2853 y una propuesta de *lege ferenda* de incorporación al Ordenamiento español», *Indret*, 3, 2025, p. 206-239. CARRASCO PERERA, Ángel., «Análisis de la nueva Directiva de responsabilidad por daños causados por productos defectuosos», *CESCO*, 2024, p. 1-7.

[37] PAZOS CASTRO, Ricardo., «El carácter defectuoso del producto en la nueva Directiva europea 2024/2853», *Revista de Internet, Derecho y Política*, 43, 2025, pp. 3-4.

[38] LI, Shu/FAURE, Michael., «The Revised Product Liability Directive: A Law and Economics Analysis», *Journal of European Tort Law*, 2, 2024, p. 149. *"From a law and economics perspective, if a manufacturer is not held liable on the basis that they have met all essential safety requirements provided by law, producers will have no further incentives to delve into the potential product risks that have not yet been reflected in the mandatory requirements but can contribute to harmful consequences."*

producto no causa un daño es irrelevante para la responsabilidad de los operadores económicos, manteniendo la existencia de un daño como el presupuesto básico para estar ante un producto defectuoso (art. 5 DRP).[39] Esto no significa que, a pesar de que el producto no haya provocado un daño, las autoridades competentes no deban reaccionar adoptando las medidas restrictivas adecuadas para reducir o anular el riesgo de que el producto provoque un daño. En el ámbito que nos toca, el RCR obliga a las autoridades de vigilancia del mercado nacionales a realizar una evaluación del producto cuando presente un riesgo de ciberseguridad significativo. En caso de confirmarse dicho riesgo, la autoridad de vigilancia deberá dirigirse contra el operador económico a fin de que adopte las medidas correctoras oportunas (art. 54.1 RCR).

a. Defectuosidad por incumplimiento de los requisitos de ciberseguridad (art. 7.2.f) DRP)

Texto del cuerpo en PT Serif 10. El art. 7.2.f) DRP dispone lo siguiente: *"2. Al valorar el carácter defectuoso de un producto, se tendrán en cuenta todas las circunstancias, incluso: f) los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad pertinentes para la seguridad"*. Por tanto, la DRP determina que una de las circunstancias a valorar para apreciar el carácter defectuoso de un producto es el cumplimiento de los requisitos de ciberseguridad pertinentes. En este sentido, tendrán que considerarse los requisitos esenciales de ciberseguridad del Anexo I RCR.

En mi opinión, el art. 7.2.f) DRP utiliza un concepto amplio de cumplimiento de los requisitos de ciberseguridad (considerando núm. 32 *in fine* DRP), toda vez que la verificación del cumplimiento de los requisitos esenciales de seguridad del Anexo I RCR, a través del procedimiento correspondiente según la categoría de producto con elementos digitales en cuestión y la correspondiente expedición de la declaración UE de conformidad, dará lugar a la presunción de conformidad (art. 27.8 RCR) y que el producto pueda ser introducido en el mercado o puesto en servicio. Adoptando el criterio normativo (art. 7.1 *in fine* DRP), basado en el cumplimiento de los requisitos esenciales de ciberseguridad en relación con el Anexo I RCR, implica que se consideraran "ciberseguros" productos que en realidad no lo son, por ejemplo, por el hecho de estar afectados por vulnerabilidades desconocidas que puedan comprometer la ciberseguridad del producto una vez introducido en el mercado. Con todo, el cumplimiento de los requisitos esenciales de ciberseguridad del Anexo I RCR, permitirá considerar que el producto con elementos digitales ha alcanzado un nivel de ciberseguridad óptimo y que, por tanto, pueda ser introducido en el mercado, lo que viene justificado por la imposibilidad de los fabricantes de poder garantizar que su producto es infranqueable por cualquier riesgo de ciberseguridad, como las vulnerabilidades desconocidas. Por tanto, es en este punto donde puede verse el carácter alternativo de los dos estándares de referencia del art. 7.1 DRP. A pesar de que el producto con elementos digitales cumpla los requisitos de ciberseguridad fijados por el Derecho de la Unión o el Derecho nacional, ello no es un impedimento para declararlo defectuoso cuando no ofrece la seguridad que el público en general puede esperar si, a pesar del cumplimiento normativo, los usuarios pueden experimentar un daño derivado de una vulnerabilidad.

El legislador europeo es conocedor de esta circunstancia, como se desprende de lo dispuesto en el considerando núm. 111 RCR: *"En determinados casos, un producto con elementos digitales que cumpla lo dispuesto en el presente Reglamento puede, no obstante, presentar un riesgo de ciberseguridad significativo o plantear un riesgo para la salud o la seguridad de las personas […]. Es por tanto necesario establecer normas que garanticen la reducción de estos riesgos. En consecuencia, las autoridades de vigilancia del mercado deben adoptar medidas para exigir al operador económico que se asegure de que el producto ya no presenta dicho riesgo, que lo retire del mercado o que lo recupere, dependiendo del riesgo que presente."* Por tanto, las autoridades de vigilancia del mercado juegan un papel de control de los riesgos de ciberseguridad del producto en el momento de su introducción en el mercado o puesta en servicio y una monitorización de los riesgos del producto después de su comercialización, que en caso de apreciarse un riesgo significativo obligará a adoptar las medidas correctoras necesarias, que pueden conllevar, incluso, la retirada del producto del mercado.

[39] Para diferenciar los conceptos de "producto seguro" "producto inseguro" y "producto defectuoso", *vid*. RUÍZ GARCÍA, Carlos Alberto/MARÍN GARCÍA, Ignacio., «Producto inseguro y producto defectuoso», *Indret*, 4, 2006, pp. 1-20.

b. Retirada o recuperación del producto del mercado (art. 7.2.g) DRP)

El art. 7.2.g) DRP se refiere a la retirada del producto del mercado o de impedir su comercialización a lo largo de toda la cadena de suministro (art. 3.23 Reglamento (UE) 2019/1020)[40]: *"cualquier retirada del producto o cualquier intervención pertinente relacionada con la seguridad de los productos por parte de una autoridad competente o de un operador económico contemplado en el artículo 8"*.[41] El considerando núm. 34 DRP aporta algo de luz para interpretar dicha causa de defectuosidad, aduciendo que por sí sola estas intervenciones no deben dar lugar a presumir el carácter defectuoso de un producto. La aclaración es bienvenida, pero se alcanza fácilmente esta conclusión a tenor del articulado del RCR. En este sentido, la retirada del producto con elementos digitales del mercado es una medida a adoptar cuando el producto presente un riesgo significativo en materia de ciberseguridad (arts. 56 y 57 RCR), aunque no se haya materializado en un daño.[42]

El precepto alude a la retirada o a "cualquier intervención pertinente". La DRP no se refiere a cuáles pueden ser dichas intervenciones pertinentes, pero lo cierto es que el RCR también se refiere a la recuperación de productos, concepto que se define en el art. 3.23 Reglamento (UE) 2019/1020: *"toda medida destinada a recobrar un producto ya puesto a disposición del usuario final"*. La diferencia radica en el punto de haber llegado el producto en posesión del usuario final, en cuyo caso procederá la recuperación, mientras que si los operadores económicos se percatan de un riesgo significativo cuando el producto se encuentra en la cadena de comercialización procederá su retirada.[43] En este punto cabría añadir que la recuperación tiene por finalidad la reparación, sustitución o reembolso adecuado del valor del producto y, en último caso, el reembolso del producto (art. 37.2 RSGP), por lo que una vez realizadas las tres primeras intervenciones el producto tendrá que volver a ponerse a disposición del usuario final, mientras que en el caso de la retirada el producto, que no ha llegado en manos del usuario final, podrá comercializarse de nuevo sin adolecer, en nuestro caso, de las vulnerabilidades que lo convertían en potencialmente dañoso.

En cuanto a quienes compete adoptar estas medidas, entre las autoridades competentes pueden incluirse las autoridades de vigilancia del mercado, a quienes el Reglamento (UE) 2019/1020 y el RCR (art. 54.9 RCR) dedican una posición preminente, los Estados miembros (art. 55.2 RCR) y la propia Comisión (art 56.5 y 57.9 RCR). A continuación, se alude a los operadores económicos contemplados en el art. 8 DRP. A mi modo de ver, en este punto se trata de integrar en la DRP la obligación impuesta por el RSGP a los fabricantes (art. 9.8 RSGP), importadores (art.11.8 RSGP) o distribuidores (art.12.4 RSGP) de velar para impedir la comercialización de productos peligrosos una vez introducidos en el mercado, basándose en la información que obre en su poder.

c. El efecto razonablemente previsible en el producto de otros productos (art. 7.2.d) DRP)

En el nuevo paradigma digital, los productos con elementos digitales se caracterizan, entre otras cosas, por su capacidad de interconectarse con otros productos, respecto de los cuales realizan algunas de sus funciones conjuntamente. Este efecto razonablemente previsible de unos productos respecto de otros, como causa de defectuosidad, se encuentra previsto en el art. 7.2.d) DRP. Veamos que implicaciones tiene esta

[40] Reglamento (UE) 2019/1020 del Parlamento europeo y del Consejo de 20 de junio de 2019 relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) núm. 765/2008 y (UE) núm. 305/2011. DUE núm. 169, de 25 de junio de 2019.

[41] Se trata de una causa para tener en cuenta el carácter defectuoso de un producto que no aparecía en la Directiva 85/374/CEE y que obedece a la necesidad de introducir en la DRP el rol de supervisión del mercado que se reserva a las autoridades de vigilancia del mercado y a la Comisión.

[42] Art. 9.8.a) Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) núm. 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (en adelante, RSGP).

[43] MARÍN LÓPEZ, Manuel Jesús., «Productos peligrosos (no seguros) y medidas de protección del consumidor: el artículo 37 del Reglamento 2023/988, de seguridad general de los productos», *CESCO*, 46, 2023, pp. 91.

interconexión de productos en cuanto a las vulnerabilidades que puedan presentar productos que pueden usarse conjuntamente.

Como cuestión preliminar, considero que, para el correcto análisis del art. 7.2.d) DRP debe prescindirse de la existencia de una relación de accesoriedad entre ambos productos, de suerte que alguno de ellos actúe como un componente respecto del otro.[44] En el ámbito que nos ocupa, en el art. 7.2.d) DRP no subyace la idea de una integración de una parte (componente) respecto del todo (producto), sino que ambos productos, que se encuentran interconectados, no se encuentran subordinados uno respecto del otro. El ejemplo del sistema doméstico inteligente que aparece en el considerando núm. 32 DRP me parece clarificador. Un sistema doméstico inteligente es un ecosistema de productos con elementos digitales interconectados que persigue la seguridad del hogar y de sus habitantes.

Partiendo de la premisa anterior, me planteo que implicaciones tendría una vulnerabilidad de ciberseguridad de un producto respecto de otro. Un ejemplo clarificador podría ser la interconexión existente entre un vehículo y un teléfono inteligente durante la conducción. ¿Una vulnerabilidad del vehículo que diera lugar a la corrupción de datos del teléfono inteligente entraría dentro del art. 7.2.d) DRP? Para dar respuesta a esta cuestión considero que el primer elemento que debe analizarse es qué se entiende por "efecto razonablemente previsible" del art. 7.2.d) DRP, un concepto respecto del cual la DRP no aporta ningún dato interpretativo más allá de la breve referencia en el considerando núm. 32 DRP. No obstante, existe un elemento que sí que está claro según el articulado y los considerandos de la DRP: el "efecto razonablemente previsible" es un concepto diferente del de "uso razonablemente previsible". Este último aparece presidido claramente por la funcionalidad del producto.[45] En este sentido, el "uso razonablemente previsible" del producto se encuentra reconocido como una circunstancia autónoma para apreciar el carácter defectuoso de un producto (art. 7.2.b) DRP). Considerando el efecto razonablemente previsible como todo aquello que sigue por virtud de la interconexión de productos, no debería haber inconvenientes para admitir una noción amplia de dicho concepto para comprender los efectos negativos de la interconexión relativos a la ciberseguridad.

Si la interpretación que se propone se traslada del "efecto razonablemente previsible" al ámbito de la ciberseguridad, hay que destacar otro concepto utilizado en el RCR: la conexión directa o indirecta entre sistemas electrónicos (art.3.9) y 10) RCR). A esta circunstancia alude, el considerando núm. 9 *in fine* RCR. Por tanto, la conexión que puede existir entre dos productos con elementos digitales como la del ejemplo propuesto también debe tenerse en cuenta por los fabricantes en cuanto al "efecto razonablemente previsible". Es decir, los fabricantes del vehículo y del teléfono inteligente deberán prever, considerando la conexión que puede establecerse entre ellos, que pueden conectarse para el cumplimiento de su finalidad y que, durante la conexión, las vulnerabilidades que presenten los productos conectados pueden afectarles recíprocamente. Tratando de orientar una posible solución al caso propuesto, podría defenderse que, si ambos productos interconectados presentan vulnerabilidades y, como consecuencia de ello, se ha producido la corrupción de datos, el art. 12 DRP determina responsabilidad solidaria de los operadores económicos

[44] Art. 4.4) DRP: *"«componente»: cualquier artículo, ya sea tangible o intangible, materia prima o servicio conexo, que está integrado en un producto o interconectado con él"*. A mayor abundamiento sobre el concepto de componente de la DRP, *vid*. HERBOSA MARTÍNEZ, Inmaculada., «Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos. Análisis de la legislación vigente con la vista puesta en la Propuesta de Directiva del Parlamento europeo y del Consejo de 28 de septiembre de 2022 (COM/2022/495)», *Indret*, 3, 2024, pp. 52-98.

[45] Considerando núm. 31 DRP: *"Al determinar el carácter defectuoso de un producto, el uso razonablemente previsible incluye también el uso indebido pero razonable en las circunstancias, como por ejemplo el comportamiento previsible de un usuario de maquinaria derivado de una falta de concentración o el comportamiento previsible de determinados grupos de usuarios, como los niños."*

Considerando núm. 46 DRP: *"El uso razonablemente previsible comprende el uso al que está destinado un producto de conformidad con la información facilitada por el fabricante o el operador económico que lo introduzca en el mercado, el uso ordinario determinado por el diseño y la construcción del producto, y el uso que pueda preverse razonablemente cuando dicho uso pueda derivarse de un comportamiento humano lícito y fácilmente previsible."*

responsables. En caso contrario, si el defecto sólo es imputable a uno de los dos fabricantes implicados, el segundo no debería responder.[46]

5.2. Exoneración y reducción de la responsabilidad

El régimen de responsabilidad objetiva que consagra la DRP obviamente prescinde de la culpa como criterio de imputación de responsabilidad. No obstante, tampoco se configura como un régimen de responsabilidad objetivo puro, porque se reconocen ciertes causas de exoneración de responsabilidad que permiten a los operadores económicos eximirse de su responsabilidad.

Repasando el articulado de la DRP, ninguna de las causas de exoneración de responsabilidad se refiere específicamente a las vulnerabilidades de los productos con elementos digitales. Sin embargo, ello no es óbice para hacer una lectura de las mismas en clave de ciberseguridad.

a. Inexistencia de la vulnerabilidad en el momento de la introducción en el mercado o puesta en servicio del producto (art. 11.1.c) DRP). Riesgos del desarrollo (art. 11.1.e) DRP), vulnerabilidades y actualizaciones de seguridad (art. 11.3 DRP)

El art. 11.1.c) DRP dispone lo siguiente: *"1. Los operadores económicos a que se refiere el artículo 8 no serán responsables de los daños causados por un producto defectuoso si demuestran que: c) que es probable que el carácter defectuoso que haya causado el daño no existiera en el momento en que el producto fue introducido en el mercado, puesto en servicio o, en el caso de un distribuidor, comercializado, o que ese carácter defectuoso se originase después de ese momento"*.[47] El art. 11.2 DRP, al que se dedica el considerando núm. 50 DRP para su interpretación, aporta algunos elementos para interpretar dicha causa de exoneración de responsabilidad, aludiendo expresamente a los programas informáticos o servicios conexos que estén bajo el control del fabricante. Es decir, teniendo en cuenta que las propiedades de los productos con elementos digitales pueden cambiar sustancialmente desde el momento en que fueron introducidos en el mercado debido a las actualizaciones o algoritmos de aprendizaje automático que pueden llevar incorporados, la DRP exonera de responsabilidad a los fabricantes si prueban que el defecto que ha causado el daño no existía en el momento en que el producto fue introducido en el mercado o puesto en servicio.[48] No obstante, considero que la interpretación del art. 11.1.c) DRP mira hacia el futuro, una vez el producto ha sido introducido en el mercado, en lugar de remontarse a las circunstancias existentes en el momento en que el producto se introdujo en el mercado.[49]

---

[46] Una conclusión parecida alcanza este autor. HERRERA DE LAS HERAS, Ramón., *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022, pp. 94.

[47] Dicha causa de exoneración de responsabilidad ya estaba reconocida en el art. 7.b) Directiva 85/374/CEE: *"o que, teniendo en cuenta las circunstancias, sea probable que el defecto que causó el daño no existiera en el momento en que él puso el producto en circulación o que este defecto apareciera más tarde"*. Esta causa de exoneración de responsabilidad ha sido muy criticada por la doctrina cuando estamos ante productos con elementos digitales que se actualizan mientras están bajo el control del fabricante. No obstante, se ha mantenido en la DRP y no se ha excluido su aplicación en el caso de la inteligencia artificial o de les vulnerabilidades. EUROPEAN LAW INSTITUTE, «Response of the European Law Institute (ELI) to the European Commission's Public Consultation on Civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence», 2022. Puede consultarse en: https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf.

[48] ATIENZA NAVARRO, María Luisa., *Indret*, 2, 2023, pp. 42.

[49] Nótese que el art. 11.1.c) DRP no alude a las circunstancias existentes, como hacía el art. 7.b) Directiva 85/374/CEE. No obstante, a mi juicio las circunstancias existentes en el momento de la comercialización del producto siguen siendo relevantes para valorar la procedibilidad de la causa de exoneración aquí estudiada. RAMOS GONZÁLEZ, Sonia/RUBÍ PUIG, Antoni., «Causas de exoneración de responsabilidad», en SALVADOR CODERCH, Pablo/GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 533-536. FAIRGRIEVE, Duncan/HOWELLS, Geraint., *et. ali*., «Product Liability Directive» en MACHNIKOWSKI, Piotr (ed.), *European product liability (European Group on Tort Law) European product liability: an analysis of the state of the art in the era of new technologies*, Intersentia, Cambridge, 2016, pp. 76. Como bien indican estos autores, el alcance de esta causa de exoneración de responsabilidad es una presunción de inexistencia del defecto cuando el producto se introdujo en el mercado.

Si nos planteamos la admisibilidad de esta causa de exoneración de responsabilidad en el ámbito de la ciberseguridad, me planteo la siguiente cuestión: ¿Puede una vulnerabilidad no conocida,[50] pero que existía en el momento de la introducción en el mercado del producto, amparar el recurso a esta causa de exoneración de responsabilidad? El problema de las vulnerabilidades no conocidas en el momento de la introducción en el mercado del producto conduce a la excepción de responsabilidad por los riesgos del desarrollo, prevista en el art. 11.1.e) DRP, ante los riesgos desconocidos (*unknown risks*)[51] según en estado de la ciencia y de la técnica.[52] El considerando núm. 52 DRP aborda esta cuestión: *"En aras de un reparto equitativo de los riesgos, los operadores económicos 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 operador económico en cuestión, durante el periodo en que el producto estaba bajo el control del fabricante, era tal que no podía detectarse su carácter defectuoso."* Repárese que la referencia al "nivel más avanzado de conocimiento objetivo accesible"[53] permite abogar por una imputación de la responsabilidad al fabricante ante vulnerabilidades conocidas, que son las que se reportan y publican en la base de datos europea de vulnerabilidades, lo que permite que el conocimiento sea compartido entre todos los operadores económicos, en especial los fabricantes. A mi modo de ver, el elemento fundamental para apreciar la concurrencia de los riesgos del desarrollo es que el defecto, en nuestro caso la vulnerabilidad, no pudiera detectarse cuando el producto fue introducido en el mercado según el estado más avanzado del conocimiento. Por consiguiente habría la posibilidad de que los fabricantes excusaran su responsabilidad si el defecto no podía ser detectado ni subsanado mediante actualizaciones de seguridad y, en este caso, la responsabilidad debería imputarse al tercero que ha causado el daño aprovechando la vulnerabilidad.[54] En caso contrario, si la vulnerabilidad era desconocida cuando el producto se introdujo en el mercado, pero se detectó, como una vulnerabilidad aprovechable durante el periodo de soporte, el fabricante estará obligado a reportarla a la base de datos europeo de vulnerabilidades y a repararla de forma inmediata mediante una actualización de seguridad, sin que pueda excusarse su responsabilidad (art. 11.2 DRP), y sin perjuicio de

[50] Las vulnerabilidades no conocidas podrían ser aquellas que afectan el producto, pero que aún no han sido detectadas por los operadores económicos en el momento de la introducción en el mercado del producto, habida cuenta de las pruebas realizadas durante la fase de prueba (art. 33.2 RCR), o bien aquellas vulnerabilidades que afectan a los productos después de operar alguna modificación, por ejemplo, a través de una actualización del software, o que se materializan después de que el producto haya sido atacado.

[51] BYRNE, Richard E., «Strict Liability and the Scientifically Unknowable Risk», *Marquette Law Review*, 4, 1974, pp. 660-675. FAURE, Michael/VISSCHER, Louis/WEBER, Franziska., «Liability for Unknown Risks – A Law and Economics Perspective», *European Journal of Tort Law*, 2, 2016, pp. 209-211.

[52] Los riesgos del desarrollo constituyen una causa de exoneración de responsabilidad arraigada en el Derecho europeo de daños, estudiada profusamente por la doctrina más autorizada. SALVADOR CODERCH, Pablo/RUBÍ PUIG, Antonio., «Causas de exoneración de la responsabilidad. Excepción por riesgos de desarrollo», en SALVADOR CODERCH, Pablo/GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 585-646. SALVADOR CODERCH, Pablo/SOLÉ FELIU, Josep, *Brujos y aprendices: los riesgos de desarrollo en la responsabilidad de producto*, Marcial Pons, Madrid, 1999. PARRA LUCÁN, Mª Ángeles., *La protección del consumidor frente a los daños. Responsabilidad civil del fabricante y del prestador de servicios*, Reus, Madrid, 2011, 180-185.

[53] La referencia fue introducida como consecuencia de la Sentencia de 29 de mayo de 1997, C-300/95, con motivo de la transposición de la Directiva 85/374/CEE al Derecho inglés, que objetivó los riesgos del desarrollo, prescindiendo del elemento de culpa del fabricante, circunstancia que también aparece en el considerando núm. 52 DRP: "*y no al conocimiento efectivo del operador económico en cuestión".* FAIRGRIEVE, Duncan., GOLDBERG, Richard., *Product Liability*, 3ª ed., Oxford University Press, 2020, pp. 508. La referencia al nivel más avanzado de conocimiento accesible suscita la duda de si comprende meras hipótesis no constatadas científicamente. Estos autores abogan por un conocimiento basado en el método científico.

[54] En este sentido, NIKOLINAKOS, Nikos Th., *Adapting the EU Civil Liability Regime to the Digital Age: Artifcial Intelligence, Robotics, and Other Emerging Technologies*, Springer, 2024, pp. 114.*"It is reminded that the Product Liability Directive exempts the producer from liabilities if he can prove that the defect did not exist when the product was put into circulation or that the state of technical knowledge at the time of putting the product on the market made it impossible to discover the defect. This exemption could be triggered by the manufacturer in a cyber-attack context in order to demonstrate that, at the time of putting the product into circulation, no software vulnerability was discovered."* GÓMEZ LIGÜERRE, Carlos., «La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos», *Indret*, 4, 2022, pp. 6. BORGHETTI, Jean-Sébastien., «Taking EU Product Liability Law seriously: How can the Product Liability Directive effectively contribute to consumer protection?», *French Journal of Legal Policy*, 1, 2023, pp. 38-39. *"As a result, even if the defect could not be discovered when the product was put into circulation, the producer may still be liable based on fault if it failed to adequately monitor the product between that moment and the moment when the product was used or consumed by the victim."*

que la responsabilidad recaiga en la propia víctima si evita la instalación de las actualizaciones de seguridad (considerando núm. 51 DRP).

No obstante, existen serios obstáculos para aplicar dicha causa de exoneración a las vulnerabilidades de seguridad: por una parte, la publicidad que brinda la base de datos europea de vulnerabilidades constituye un instrumento de publicidad al alcance de los fabricantes que les permite comprobar y actualizar sus productos digitales de conformidad con las vulnerabilidades reportadas por otros fabricantes. Por otro lado, el considerando núm. 55 DRP parece reconducir este supuesto a un problema de concurrencia de responsabilidades del fabricante y del tercero que explota la vulnerabilidad. Una interpretación en aras a salvaguardar la responsabilidad del fabricante se basaría en admitir la concurrencia de los riesgos del desarrollo ante vulnerabilidades no conocidas y, por tanto, no reportadas a la base de datos europea de vulnerabilidades.

b. Intervención de tercero y explotación de vulnerabilidades

En aras a la protección de la víctima cuando varios operadores económicos puedan haber intervenido en la provocación del daño, el art. 12 DRP prevé la responsabilidad solidaria de los operadores económicos, un principio que ya estaba presente en la Directiva 85/374/CEE. Con la responsabilidad solidaria se evita que la víctima haya de determinar a cuál de los operadores que ha intervenido en la cadena de fabricación y distribución del producto deba imputarse la responsabilidad del daño. En caso contrario, la víctima se vería abocada a asumir cuantiosos gastos para preparar la prueba y determinar, asumiendo el riesgo de costas en juicio, cuál de los operadores debe responder. La responsabilidad solidaria asegura que, probando la implicación del responsable en el daño, la demanda de reclamación de responsabilidad esté correctamente interpuesta, sin perjuicio del derecho de repetición que el art. 12 DRP deja en manos del Derecho interno.[55]

En el ámbito de la explotación de vulnerabilidades en productos, adquiere especial relevancia la previsión contenida en el art. 13.1 DRP: *"Sin perjuicio del Derecho nacional en materia de derechos de división de la responsabilidad o de repetición, los Estados miembros garantizarán que la responsabilidad de un operador económico no se reduzca o anule cuando los daños sean causados tanto por el carácter defectuoso de un producto como por un acto u omisión de un tercero."* El considerando núm. 55 DRP alude al problema de las vulnerabilidades en productos en materia de reducción de responsabilidad de los operadores económicos. La solución adoptada es tajante y deja sin margen de maniobra a los operadores económicos para reducir su responsabilidad: no podrá reducirse cuando el producto sea defectuoso, por ejemplo, por alguna vulnerabilidad que debilita su ciberseguridad, salvo que el producto haya sido atacado por culpa de la propia víctima, que no ha instalado las actualizaciones de seguridad pertinentes (art. 13.2 DRP).

Técnicamente, considero que el legislador está pensando en las vulnerabilidades aprovechables, es decir, aquellas que en condiciones operativas prácticas pueden ser explotadas por terceros malintencionados (art. 3.41) RCR).[56] En este escenario, si el agente externo ha sido más eficaz que el propio fabricante, quien no ha detectado la vulnerabilidad aprovechable o, habiéndola detectado, no ha suministrado la actualización de seguridad pertinente para subsanarla, es lógico que el operador económico no pueda reducirse su responsabilidad porque el incumplimiento es doble: la no detección de la vulnerabilidad y la falta de reacción tempestiva. En consecuencia, en estos casos de explotación de vulnerabilidades, la víctima

[55] El legislador europeo ha querido proteger la innovación que llevan a cabo las pequeñas empresas, previendo en el art. 12.2 DRP que las microempresas que fabriquen componentes consistentes en programas informáticos defectuosos no responderán en ejercicio del derecho de repetición.

[56] GÓMEZ LIGÜERRE, Carlos/PIÑEIRO SALGUERO, José., «Responsabilidad solidaria, intervención de tercero y culpa del perjudicado», en SALVADOR CODERCH, Pablo/GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 297-299, 314. La concurrencia de un tercero malintencionado, juntamente con el defecto del producto, significa la actuación de un tercero ajeno al círculo del fabricante. La hipótesis que apunta del considerando núm. 55 DRP, en referencia a las vulnerabilidades, no se trataría propiamente de una intervención "conjunta" sobre la que se asienta el precepto, pues el producto puede ser introducido en el mercado sin vulnerabilidades conocidas que posteriormente son explotadas, lo que constituye, propiamente, una actuación sucesiva.

accionará correctamente dirigiéndose contra el operador económico responsable, no habiendo de demandar al tercero, en muchas ocasiones desconocido, que haya triunfado en su intento de explotar la vulnerabilidad del producto.

5.3. Periodo de soporte (art. 13.8 RCR) y plazo de caducidad (art. 17 DRP). Algunas consideraciones sobre el art. 13.2 DRP

La DRP sigue estableciendo un plazo de caducidad de las acciones contra los operadores económicos de 10 años, a contar desde que el producto fue introducido en el mercado o puesto en servicio, salvo que sobre el producto se haya realizado una modificación sustancial, lo que conllevará el reinicio del plazo de caducidad a partir de este momento (art. 17 DRP). Se trata de un elemento que no es novedoso, pues la Directiva 85/374/CEE preveía el mismo plazo de caducidad. La finalidad de dicho plazo no es otra que, en aras a la seguridad jurídica, los operadores económicos no queden expuestos indefinidamente a responsabilidad por los daños causados por sus productos.

El plazo de caducidad de 10 años del art. 17 DRP no es equiparable al plazo de duración del periodo de soporte que el art. 13.8 RCR fija en cinco años, salvo que considerando el producto con elementos digitales en cuestión requiera un plazo de soporte más largo, teniendo en cuenta, fundamentalmente, el periodo que se prevea que el producto va a ser utilizado, las expectativas razonables de los usuarios, la naturaleza del producto y el Derecho de la Unión. Podría darse el caso, por ejemplo, de la fijación de un periodo de soporte con una duración de cinco años para un ordenador y que, pasado este plazo de tiempo, el fabricante dejará de suministrar actualizaciones de seguridad. ¿Qué ocurrirá si aparece una vulnerabilidad en el producto después de transcurrir el periodo de soporte y antes de que finalice el plazo de caducidad del art. 17 DRP y como consecuencia de ello se produce un daño? Es un problema que podría plantearse dada la desarmonía de los plazos de ambas regulaciones, pues el fabricante se vería obligado a seguir respondiendo por los daños causados como consecuencia de las vulnerabilidades de ciberseguridad de sus productos, a pesar de no tener la obligación de subsanarlas mediante actualizaciones de seguridad, lo que no aporta seguridad jurídica. Un plazo del periodo de soporte fijado en cinco años podría ser adecuado para la mayor parte de productos con elementos digitales que utilizan los consumidores, que quedan rápidamente desfasados por las actualizaciones del software. No obstante, los productos con elementos digitales empleados en el sector industrial sí que podrían tener un periodo de soporte más largo, que podría coincidir con el plazo de caducidad del art. 17 DRP.

Con todo, la desarmonía de los plazos justificaría la crítica al art. 13.8 RCR por razones de falta de seguridad jurídica y de coherencia con la DRP, y por razones de sostenibilidad, dado que la falta de suministro de actualizaciones de seguridad puede incentivar a los particulares a renovar prematuramente los productos con elementos digitales.

La falta de armonía de ambos plazos plantea una ulterior reflexión: ¿debe el usuario, suficientemente informado sobre la duración del plazo de soporte, asumir los daños causados por los defectos de ciberseguridad que se produzcan una vez finalizado el periodo de soporte en virtud del art. 13.2 DRP?[57] Esta es una cuestión que tiene un cierto paralelismo con la responsabilidad contractual del vendedor por falta de conformidad. El art. 7.4 DCC dispone lo siguiente: *"4. En caso de que el consumidor no instale en un plazo razonable las actualizaciones proporcionadas de conformidad con el apartado 3, el vendedor no será responsable de ninguna falta de conformidad causada únicamente por la ausencia de la correspondiente actualización, siempre que: a) el vendedor hubiese informado al consumidor acerca de la disponibilidad de la actualización y de las consecuencias en caso de que el consumidor no la instalase, y b) el hecho de que el consumidor no instalase la actualización o no lo hiciese correctamente no se debiera*

[57] CADENAS OSUNA, Davinia., «Artículo 145. Culpa del perjudicado", en CAÑIZARES LASO, Ana (Dir.), *Comentario al Texto Refundido de la Ley de consumidores y Usuarios*, t. 2, Tirant lo Blanch, Valencia, 2022, pp. 2152-2156.

a deficiencias en las instrucciones de instalación facilitadas al consumidor."[58] La solución es la correcta, dado que entre el consumidor y el vendedor subyace su interés exclusivamente privado y sus efectos repercuten únicamente a las partes afectadas: la conformidad o no del bien. En nuestro ámbito, el punto 7 del Anexo II RCR también prevé la obligación del fabricante de informar sobre el periodo de soporte al usuario final, transcurrido el cual parece que deba ser el usuario el que debe velar por la ciberseguridad de su producto, pero considero que en materia de ciberseguridad subyace un interés público, que no es otro que el correcto funcionamiento de los sistemas democráticos, la salud y la seguridad de todos los usuarios (considerando núm. 1 RCR). Por tanto, la posibilidad de trasladar al usuario final, todo o en parte, la responsabilidad de velar por la ciberseguridad de su producto digital más allá del periodo de soporte en virtud del art. 13.2 DRP no me parece que sea una solución que deba extrapolarse en los mismos términos que el art. 7.4 DCC por las razones aducidas: en el periodo de soporte subyace una cuestión de interés pública inexistente en el régimen de la falta de conformidad de los bienes. Esto pone de manifiesto, a mi modo de ver, de fijar un periodo de soporte mínimo de 5 años, pues más allá de este plazo un producto digital obsoleto que no está sujeto a un periodo de soporte más largo podría constituir un dispositivo fácilmente franqueable para poner en riesgo bienes esenciales como la democracia, la salud y la seguridad.[59] Además, si esta fuera la interpretación del art. 13.2 DRP en relación con el punto 7 del Anexo II RCR, se desincentivaría a los consumidores de adquirir productos complejos como los productos con elementos digitales vulnerables en términos de ciberseguridad, o bien se incentivaría a los consumidores y usuarios a renovar sus productos con elementos digitales una vez finalizado el periodo de soporte y también se podría desincentivar a los fabricantes de seguir investigando sobre los riesgos de sus productos.[60]

5.4. El daño indemnizable. Especial referencia a la corrupción de datos (art. 6.1.c) DRP)

Como se ha apuntado anteriormente, no cabe duda que una de las finalidades que puede perseguir un ciberataque es la destrucción, corrupción o fuga de datos de las personas físicas o de una organización. La incorporación, como daño indemnizable, de la corrupción de datos (art. 6.1.c) DRP), es una de las novedades más destacables de la DRP y va en la línea del reconocimiento del daño que puede acarrear un ataque a este tipo de bienes. Sin embargo, lo que realmente incluye la corrupción de datos y que es realmente indemnizable es la pérdida material de la destrucción, corrupción o fuga de datos, no los datos en sí mismo considerados, como aclara el considerando núm. 20 DRP.[61]

Una vez sentado este principio, es necesario detenerse en la naturaleza de los datos a los efectos de determinar cuál es el ámbito del daño indemnizable por la corrupción de datos de la DRP. En primer lugar, el considerando núm. 20 DRP dice que indemnización resultante de la infracción de datos personales no se ve afectada por la DRP (art. 2.a) DRP) y, por consiguiente, la indemnización resultante se dirime por lo dispuesto en el art. 82 RGPD,[62] el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo,

---

[58] BUENO BIOT, Álvaro., «La conformidad objetiva de los contenidos y servicios digitales», *Revista de Derecho civil*, 1, 2024, p. 223-224. SÁNCHEZ LERÍA, Reyes., «Mercado digital y protección del consumidor: a propósito de la Directiva 770/2019 y su transposición al ordenamiento jurídico español», *Indret*, 4, 2021, p. 61. KALAMEES, Piia., «Goods With Digital Elements and The Seller's Updating Obligation», *JIPITEC*, 2, 2021, p. 137.

[59] BLYTHE, John M., SOMBARUANG, Nissy/JOHNSON, Shane D., «What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?», *Journal of cybersecurity*, 0, 2019, p. 3. Según el estudio llevado a cabo por estos autores solo el 52% de los consumidores actualiza sus productos a la última versión. Estos datos ponen de manifiesto la despreocupación de los consumidores en mantener actualizados sus productos, lo que con más razón justifica un mayor paternalismo del legislador y la necesidad de ampliar el periodo de soporte de los productos con elementos digitales. En mi opinión, la salud y la seguridad no pueden descansar en manos de los usuarios de mantener sus productos actualizados.

[60] LI, Shu/FAURE, Michael., *Journal of European Tort Law*, 2, 2024, p. 164.

[61] Considerando núm. 20 DRP: *"En consecuencia, la protección de las personas físicas exige una indemnización por las pérdidas materiales derivadas no solo de la muerte o las lesiones corporales, como los gastos funerarios o médicos o la pérdida de ingresos, y de los daños materiales, sino también de la destrucción o corrupción de datos."* ATIENZA NAVARRO, María Luisa., *Indret*, 2, 2023, pp. 40. GÓMEZ LIGÜERRE, Carlos., *Indret*, 4, 2022, pp. 4.

[62] RUBÍ PUIG, Antoni., «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, 4, 2018, p. 53-87. DE MIGUEL ASENSIO, Pedro Alberto., «Derecho a

o de la Directiva 2002/58/CE o la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. En estos casos en la mayoría de casos se dará lugar a una indemnización por daños morales. Piénsese en casos de fotografías privadas de índole familiar. En estos casos, no se producirá un daño material por su corrupción, sino un daño moral debidamente indemnizable (considerando núm. 23 *in fine* DRP).[63] En segundo lugar, el art. 6.2.c) DRP deja fuera de su ámbito de aplicación los datos utilizados con fines profesionales. Esta exclusión ha sido criticada por la doctrina[64] ha criticado porque reduce considerablemente el ámbito de aplicación de los daños derivados de la corrupción de datos, que son los que, precisamente, pueden tener un valor económico más elevado. Esta exclusión trae como consecuencia que los daños materiales derivados de la corrupción de datos con fines profesionales deban reclamarse y valorarse según el Derecho interno de los Estados miembros en materia de responsabilidad civil extracontractual.[65] En tercer lugar, y como conclusión, si la indemnización por la corrupción de datos personales de las personas físicas discurre por los cauces de la legislación sectorial aplicable, fundamentalmente el RGPD, y se excluyen los datos con fines profesionales, los daños por corrupción de datos cubiertos por la DRP se limitan a los datos no personales, lo que reduce sustancialmente el ámbito de este tipo de daños cubierto por la DRP.

Las fórmulas para determinar la indemnización por la pérdida material de los datos se dejan en manos de los Estados miembros (considerando núm. 23 DRP), los cuales deben prever una indemnización completa y adecuada para la corrupción de datos. En este sentido, debe tenerse en cuenta la posibilidad de que los datos sean recuperables, por disponer de una copia de seguridad o por la posibilidad de ser restaurados por el operador económico que los custodia.[66]

6. Conclusiones

Primera: En cuanto a la circunstancia para apreciar el carácter defectuoso del art. 7.2.f) DRP, se constata que se asienta sobre un cumplimiento formal de los requisitos de seguridad y, en nuestro caso, de ciberseguridad. El cumplimiento de los requisitos esenciales de ciberseguridad del Anexo I Parte I RCR no garantiza que el producto con elementos digitales no esté afectado por ninguna vulnerabilidad en el momento de ser introducido en el mercado o puesto en servicio, toda vez que pueden existir vulnerabilidades no conocidas que se pongan de manifiesto en el futuro, con las consecuencias que esto conlleva para los fabricantes de subsanarlas mediante actualizaciones de seguridad.

Segunda: Respecto del "efecto razonablemente previsible" del producto sobre otros productos (art. 7.2.d) DRP), se aboga por una interpretación amplia que incluya los efectos que la ciberseguridad puede acarrear para los productos con los que se conecte el producto. La expresa referencia a la "interconexión" de productos que refiere este artículo y las diferencias existentes entre este concepto y el "uso razonablemente previsible" abogan por un efecto razonablemente previsible no limitado a la funcionalidad del producto y que, por tanto, debe abarcar todos los posibles efectos de la conexión de productos, incluida la ciberseguridad.

Tercera: Se defiende la posible aplicabilidad de la excepción de responsabilidad de los riesgos del desarrollo a los daños causados por vulnerabilidades no conocidas en el momento en que el producto es

indemnización en materia de datos personales: aspectos internacionales», *Cuadernos de Derecho Transnacional,* 2, 2024, p. 487-500.

[63] RUBÍ PUIG, Antoni., «Inteligencia artificial y daños indemnizables», en ÁLVAREZ LATA, Natalia, (coord.), *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Asociación de Profesoras y Profesores de Derecho Civil, Aranzadi, Las Rozas (Madrid), 2024, p. 643.

[64] WAGNER, Gerhard., *Journal of European Tort Law*, 3, 2022, pp. 211. MARTÍN-CASALS, Miquel., *Indret,* 3, 2023, pp. 88.

[65] A este respecto, existen algunos métodos para valorar el daño asociado a un defecto de ciberseguridad, tomando como base del cálculo el daño potencial del ciberataque y la efectividad de las medidas preventivas. F. FRANCO, Muriel/KÜNZLER, Fabian/VON DER ASSEN, Jan/FENG, Chao/STILLER, Burkhard., «RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports», *Computers & Security*, 139, 2024, p. 1-13. ROMANOSKY, Sasha., «Examining the costs and causes of cyber incidents», *Journal of Cybsersecurity*, 2, 2016, p. 121-135.

[66] WHITTAM, Sadie., «Mind the compensation gap: towards a new European regime addressing civil liability in the age of AI», *International Journal of Law and Information Technology*, 30, 2022, pp. 258.

introducido en el mercado o puesto en servicio. El fabricante del producto con elementos digitales ha de tener la posibilidad de probar que con la mejor tecnología disponible no era posible conocer y gestionar la vulnerabilidad ni en el momento de poner el producto en el mercado ni con posterioridad. Y si consigue probarlo, el fabricante no responderá del defecto y el único responsable será el tercero que manipula el producto. La admisibilidad de los riesgos del desarrollo sería admisible en el caso de vulnerabilidades no conocidas, puesto que sí son conocidas y reportadas a la base de datos europea de vulnerabilidades no es excusable la responsabilidad del fabricante por la responsabilidad brindada por dicho registro.

Cuarta: La previsión de un periodo de soporte con carácter subsidiario de cinco años (art. 13.8 RCR) y de un plazo de caducidad de diez años (art. 17 DRP) conduce al sinsentido de que la monitorización del producto por el fabricante pueda ser inferior al plazo de responsabilidad del fabricante. La previsión de un periodo de soporte subsidiario más largo, habría conducido a mejorar la seguridad jurídica de los operadores económicos y la sostenibilidad de los productos. Si bien es cierto que el art. 13.8 RCR parte de la premisa de fijar un periodo de soporte singular para cada producto con elementos digitales, no es menos cierto que la subsidiariedad del plazo de cinco años puede conducir a rebajar las expectativas de ciberseguridad de los productos.

Quinta: La previsión en el art. 13.8 RCR de un periodo de soporte mínimo de 5 años, plantea la duda de si, transcurrido este periodo de tiempo, el usuario final debe velar por la ciberseguridad de su producto con elementos digitales y, si no lo hace, pueda imputarse la responsabilidad por los daños propiciados por una vulnerabilidad en el sentido del art. 13.2 DRP. En el ámbito de la ciberseguridad subyace una cuestión de interés público (considerando núm. 1 RCR) que impide que pueda adoptarse la misma solución prevista en el art. 7.4 DCC, es decir, que el consumidor es responsable de las faltas de conformidad que adolece su bien si no lo actualiza. En el régimen de la falta de conformidad subyacen exclusivamente los intereses del vendedor y el consumidor, por lo que es correcto que el consumidor no pueda reclamar una falta de conformidad si no instala las actualizaciones que suministra el vendedor. A mi juicio, es inoportuno que los bienes esenciales como la democracia, la salud y la seguridad dependan de si el consumidor decide velar por la ciberseguridad de su producto, lo que exige, con mayor razón, un periodo de soporte, con carácter de mínimos, más largo que el de cinco años del art. 13.8 RCR.

Sexta: La no afectación de la DRP a los daños causados por la corrupción de datos personales de las personas físicas (art. 2.4 DRP), cuya indemnización será exigible al amparo del art. 82 RGPD y la exclusión de los daños causados a datos con fines económicos (art. 6.2.c) DRP) conduce a la conclusión que los daños cubiertos por la DRP se refieren a los datos no personales. Por tanto, el ámbito de aplicación del art. 6.2.c) DRP es muy restrictivo y se reducen los daños que pueden acogerse a este supuesto.

7. Bibliografía

ATIENZA NAVARRO, María Luisa., «¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)», *Indret*, 2, 2023, pp. 1 ss.

AZIZ AL KABIR, Mohammed/ELMEDANY, Wael/SAEED SHARIF, Mhd., «Securing IoT devices against emerging security threats: challenges and mitigation techniques», *Journal of Cyber Security Technology*, 7, 2023, pp. 199 ss.

BERTUZZI, Luca., «EU Council moves to adjust product lifecycle, reporting in new cybersecurity law», 2023. Puede consultarse en: https://www.euractiv.com/section/tech/news/eu-council-moves-to-adjust-product-lifecycle-reporting-in-new-cybersecurity-law/. Consulta realizada el día 31 de mayo de 2025.

BORGHETTI, Jean-Sébastien., «Taking EU Product Liability Law seriously: How can the Product Liability Directive effectively contribute to consumer protection?», *French Journal of Legal Policy*, 1, 2023, pp. 1 ss.

BLYTHE, John M/SOMBARUANG, Nissy/JOHNSON, Shane D., «What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?», *Journal of cybersecurity*, 0, 2019, p. 1-10.

BUENO BIOT, Álvaro., «La conformidad objetiva de los contenidos y servicios digitales», *Revista de Derecho civil*, 1, 2024, p. 185-237.

BURRI, Mira/ZIHLMANN, Zaira., «The Cyber Resilience Act – An Appraisal and Contextualization», Zeitschrift für Europearecht, 2, 2023, pp. 1 ss.

BYGRAVE, Lee. A., «Article 25. Data protection by design and by default», en KUNER, Christopher/BYGRAVE, Lee. A/DOCKSEY, Christopher/DRECHSLER, Laura (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*., Oxford University Press, Londres, 2020, pp, 571 ss.

BYRNE, Richard E., «Strict Liability and the Scientifically Unknowable Risk», *Marquette Law Review*, 4, 1974, pp. 660 ss.

CARRASCO PERERA, Ángel., «Análisis de la nueva Directiva de responsabilidad por daños causados por productos defectuosos», *CESCO*, 2024, p. 1-7.

CADENAS OSUNA, Davinia., «Artículo 145. Culpa del perjudicado", en CAÑIZARES LASO, Ana (Dir.), *Comentario al Texto Refundido de la Ley de consumidores y Usuarios*, t. 2, Tirant lo Blanch, Valencia, 2022, pp. 2151-2161.

CHIARA, Pier Giorgio., «The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction», International Cybersecurity Law Review, 3, 2022, pp. 255 ss.

COMISIÓN EUROPEA, Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, Bruselas, 7.2.2013, JOIN(2013) 1 final.

COMISIÓN EUROPEA., «Cyber Resilience Act. New EU cybersecurity rules ensure more secure hardware and software products», 2022, puede consultarse en: https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products. Consulta realizada el día 30 de mayo de 2025.

DE MIGUEL ASENSIO, Pedro Alberto., «Derecho a indemnización en materia de datos personales: aspectos internacionales», *Cuadernos de Derecho Transnacional*, 2, 2024, p. 487-500.

ELLUL, Joshua/PAECE, Gordon. J/REVOLIDIS, Ioannis/SCHNEIDER, Gerardo., «When is good enough good enough? On software assurances», *ERA Forum*, 23, 2023, pp. 337.

EUROPEAN LAW INSTITUTE, «Response of the European Law Institute (ELI) to the European Commission's Public Consultation on Civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence», 2022. Puede consultarse en: https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf.

FAIRGRIEVE, Duncan/GOLDBERG, Richard., *Product Liability*, 3ª ed., Oxford University Press, 2020.

FAIRGRIEVE, Duncan/HOWELLS, Geraint., *et. ali*., «Product Liability Directive» en MACHNIKOWSKI, Piotr (ed.), *European product liability (European Group on Tort Law) European product liability: an analysis of the state of the art in the era of new technologies*, Intersentia, Cambridge, 2016, pp. 17 ss.

FAURE, Michael/VISSCHER, Louis/WEBER, Franziska., «Liability for Unknown Risks – A Law and Economics Perspective», *European Journal of Tort Law*, 2, 2016, pp. 198.

F. FRANCO, Muriel/KÜNZLER, Fabian/VON DER ASSEN, Jan/FENG, Chao/STILLER, Burkhard., «RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports», *Computers & Security*, 139, 2024, p. 1-13.

FRIEDMAN, Vlad., «On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT», puede consultarse en: https://www.databank.com/resources/blogs/solving-edge-computing-challenges-in-era-of-iot/. Consulta realizada en fecha 11 de junio de 2025.

GÓMEZ LIGÜERRE, Carlos., «La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos», *Indret*, 4, 2022, pp. 1 ss.

GÓMEZ LIGÜERRE, Carlos/PIÑEIRO SALGUERO, José., «Responsabilidad solidaria, intervención de tercero y culpa del perjudicado», en SALVADOR CODERCH, Pablo., GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 249-414.

GREENGARD, Samuel., *The internet of things*, 2ª ed., The Mitt Press, Londres, 2021.

GRUPO DE TRABAJO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017 Revisadas por última vez y adoptadas el 4 de octubre de 2017. 17/ES WP 248 rev.01.
HARARI, Yuval Noah., *21 lliçons per al segle XXI*, La Butxaca, 2021.

HARARI, Yuval Noah., *21 lliçons per al segle XXI*, La Butxaca, 2021.

HERBOSA MARTÍNEZ, Inmaculada., «Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos. Análisis de la legislación vigente con la vista puesta en la Propuesta de Directiva del Parlamento europeo y del Consejo de 28 de septiembre de 2022 (COM/2022/495)», *Indret*, 3, 2024, pp. 52 ss.

HERRERA DE LAS HERAS, Ramón., *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022.

KALAMEES, Piia., «Goods With Digital Elements and The Seller's Updating Obligation», *JIPITEC*, 2, 2021, p. 131-147.

KOSTA, Eleni., «Article 35. Data protection impact assessment and prior consultation», en KUNER, Christopher/BYGRAVE, Lee. A/DOCKSEY, Christopher/DRECHSLER, Laura (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*., Oxford University Press, Londres, 2020, pp, 665.

LI, Shu/FAURE, Michael., «The Revised Product Liability Directive: A Law and Economics Analysis», *Journal of European Tort Law*, 2, 2024, p. 140-171.

MARÍN LÓPEZ, Manuel Jesús., «Productos peligrosos (no seguros) y medidas de protección del consumidor: el artículo 37 del Reglamento 2023/988, de seguridad general de los productos», *CESCO*, 46, 2023, pp. 87 ss.

MILLER, Kevin L., «What we talk about when we talk about 'reasonable cybersecurity': a proactive and adaptive approach», *Florida Bar Journal*, 90-8, 2016, pp. 1 ss.

MARTÍN-CASALS, Miquel., «Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial», *Indret*, 3, 2023, pp. 55 ss.

MUECK, Marcus/ROBERTS, Taylor/DU BOISPÉAN, Stéphane/GAIE, Christophe., «E 4. Introduction to the European Cyber Resilience Act», en MUECK, Marcus/GAIE, Christophe (eds.), *European Digital Regulations*, Springer Nature, 2025, pp. 91 ss.

NIKOLINAKOS, Nikos Th., *Adapting the EU Civil Liability Regime to the Digital Age: Artifcial Intelligence, Robotics, and Other Emerging Technologies*, Springer, 2024.

PARRA LUCÁN, Mª Ángeles., *La protección del consumidor frente a los daños. Responsabilidad civil del fabricante y del prestador de servicios*, Reus, Madrid, 2011.

PAZOS CASTRO, Ricardo., «El carácter defectuoso del producto en la nueva Directiva europea 2024/2853», *Revista de Internet, Derecho y Política*, 43, 2025, pp. 1 ss.

PÉREZ GARCÍA, Máximo Juan., «La responsabilidad por los daños causados por productos defectuosos: análisis de la Directiva (UE) 2024/2853 y una propuesta de lege ferenda de incorporación al Ordenamiento español», *Indret*, 3, 2025, p. 206-239.

RAIZ SHAFFIQUE, Mohammed., «Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?», *Computer Law & Security Review*, 54, 2024, pp. 1 ss.

RAMOS GONZÁLEZ, Sonia/RUBÍ PUIG, Antoni., «Causas de exoneración de responsabilidad», en SALVADOR CODERCH, Pablo/GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 533-551.

ROMANOSKY, Sasha., «Examining the costs and causes of cyber incidents», *Journal of Cybsersecurity*, 2, 2016, p. 121-135.

ROYTMAN, Michael/BELLIS, Ed., *Modern Vulnerability Management. Predictive Cybersecurity*, Artech House, Londres, 2023.

RUBÍ PUIG, Antoni., «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, 4, 2018, p. 53-87.

«Inteligencia artificial y daños indemnizables», en ÁLVAREZ LATA, Natalia, (coord.), *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Asociación de Profesoras y Profesores de Derecho Civil, Aranzadi, Las Rozas (Madrid), 2024, p. 621 ss.

RUÍZ GARCÍA, Carlos Alberto/MARÍN GARCÍA, Ignacio., «Producto inseguro y producto defectuoso», *Indret*, 4, 2006, pp. 1-20.

SALVADOR CODERCH, Pablo/SOLÉ FELIU, Josep, *Brujos y aprendices: los riesgos de desarrollo en la responsabilidad de producto*, Marcial Pons, Madrid, 1999.

SALVADOR CODERCH, Pablo/RUBÍ PUIG, Antonio., «Causas de exoneración de la responsabilidad. Excepción por riesgos de desarrollo», en SALVADOR CODERCH, Pablo/GÓMEZ POMAR, Fernando (dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008, pp. 585-646.

SÁNCHEZ LERÍA, Reyes., «Mercado digital y protección del consumidor: a propósito de la Directiva 770/2019 y su transposición al ordenamiento jurídico español», *Indret*, 4, 2021, p. 33-87.

SCHMITTNER, Christoph/VELEDAR, Omar/FASCHANG, Thomas/MACHER, Georg/BRENNER, Eugen., «Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act», en YLMAZ, Murat/CLARKE, Paul/RILE, Andreas/MESSNARZ, Richard/GREINER, Christian/PEISL, Thomas (eds.), *Systems, Software and Services Process Improvement*, Springer Nature Switzerland AG, 2024, pp. 390 ss.

VELDT, Gitta., «The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up? An Analysis of the Draft Product Liability Directive», *European Journal of Consumer and Market Law*, 1, 2023, pp. 24 ss.

WAGNER, Gerhard., «Liability Rules for the Digital Age - Aiming for the Brussels Effect», *Journal of European Tort Law*, 3, 2022, pp. 191 ss.

WHITTAM, Sadie., «Mind the compensation gap: towards a new European regime addressing civil liability in the age of AI», *International Journal of Law and Information Technology*, 30, 2022, pp. 249 ss.

ZIRNSTEIN, Yannick/LIN LEE, Yue/GE, Amanda., «Evolving Cybersecurity Landscape – Comparing the Regulatory Approaches in the EU, in China and in Singapore — An Analysis of Legislative Approaches to Key Issues in Tackling a Global Phenomenon», *Computer Law Review Inetrnational*, 6, 2022, pp. 165 ss.