CONDUCCIÓN AUTÓNOMA Y SEGURIDAD JURÍDICA DEL TRANSPORTE DESDE LA PERSPECTIVA EUROPEA E INTERNACIONAL

Eliseo Sierra Noguero
Director

tirant lo blanch
Monografías Maior

CONDUCCIÓN AUTÓNOMA Y SEGURIDAD JURÍDICA DEL TRANSPORTE DESDE LA PERSPECTIVA EUROPEA E INTERNACIONAL

CONDUCCIÓN AUTÓNOMA Y SEGURIDAD JURÍDICA DEL TRANSPORTE DESDE LA PERSPECTIVA EUROPEA E INTERNACIONAL

Director:
Eliseo Sierra Noguero

tirant lo blanch
Valencia, 2025

© TIRANT LO BLANCH
EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email: tlb@tirant.com
www.tirant.com
Librería virtual: www.tirant.es
DEPÓSITO LEGAL: V-1238-2025
ISBN: 978-84-1095-453-3

Si tiene alguna queja o sugerencia, envíenos un mail a: *atencioncliente@tirant.com*. En caso de no ser atendida su sugerencia, por favor, lea en *www.tirant.net/index.php/empresa/politicas-de-empresa* nuestro procedimiento de quejas.

Responsabilidad Social Corporativa: *http://www.tirant.net/Docs/RSCTirant.pdf*

Autores

Joaquín Alarcón Fidalgo

Manuel Alba Fernández

Joan Amenós Álamo

Félix Benito Osma

Kristiaan Bernauw

Marina Cabeza Trujillo

Mª José Castellanos Ruiz

Teresa Freixes

Albano Gilabert Gascón

Guillem Izquierdo Grau

Lela Janashvili

Roser Martínez Quirante

Josefa Muñoz Ruiz

Jose Navarro Hernández

Mónica Navarro-Michel

David Noguéro

Mª Carmen Núñez Zorrilla

Hila Oren

Jorge Ortega Soriano

Manel Pascual Sánchez

Luis Pedrayes Gullón

José Antonio Pejovés Macedo

Mónica Perna Hernández

Alfonso Perona Gómez

José Carlos Remotti

Paola Rodas Paredes

Juan Pablo Rodríguez Delgado

Eliseo Sierra Noguero

Pablo Valerio

Esta obra ha sido financiada por el Proyecto de Investigación “Conducción Autónoma y Seguridad Jurídica del Transporte”, en el marco de la Convocatoria de Proyectos de Generación de Conocimiento 2021 del Ministerio de Ciencia e Innovación. Modalidad: Investigación No Orientada Tipo B. PID2021-123070NB-I00. Investigador Principal: Eliseo Sierra Noguero

Índice

PARTE QUINTA

AERONAVES NO TRIPULADAS Y MOVILIDAD AÉREA URBANA. RESPONSABILIDAD CIVIL Y SEGURO. DRONES MILITARES AUTÓNOMOS

PARTE SEXTA

BUQUES AUTÓNOMOS Y OPERADOS POR CONTROL REMOTO: REGULACIÓN, ACCIDENTES, RESPONSABILIDAD Y SEGUROS. CIBERSEGURIDAD. TERMINALES PORTUARIAS

Responsabilidad del fabricante por el aprendizaje continuado del producto

GUILLEM IZQUIERDO GRAU
Profesor Agregado
Departamento de Derecho Privado. Universidad Autónoma de Barcelona
Instituto de Derecho y Tecnología (IDT)

I. INTRODUCCIÓN

Los productos con elementos digitales que incorporan sistemas de inteligencia artificial han irrumpido en el mercado y se han convertido en el objeto de deseo de los consumidores que, mediante este tipo de productos, quieren aumentar la efectividad de determinadas acciones o tareas. La evolución de la tecnología aplicable a los productos ha comportado que la actualmente vigente Directiva 85/374/CEE haya quedado desfasada por las nuevas tecnologías y la inteligencia artificial generativa. En este sentido, el DOUE del día 18 de noviembre de 2024 publicaba la 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 (PLD),

habida cuenta que, en el ámbito de que nos ocupa[1], que incorpora las enmiendas del Consejo, la experiencia también está demostrando que el aumento de la complejidad técnica de los productos repercute en mayores dificultades para obtener una indemnización por los daños causados por los productos defectuosos, especialmente por las dificultades de reunir pruebas a los efectos de responsabilizar al fabricante por los daños causados por sus productos.

Los posibles efectos adversos de la inteligencia artificial aplicada a los productos y que conviertan al producto en defectuoso tiene especial reconocimiento en el art. 7.2.c) DRP, que se refiere al *"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"*. La DRP dedica poca atención a esta circunstancia para apreciar el carácter defectuoso de un producto, a pesar de tratarse de uno de los aspectos más novedosos que incorpora.. Esta circunstancia obliga a hacer referencia a otras normas que, en el momento de la redacción de este trabajo, acaban de ser adoptadas y que completan las obligaciones impuestas a los fabricantes en relación con la seguridad y la gestión de la inteligencia artificial que integran sus productos. Me estoy refiriendo, fundamentalmente, al Reglamento sobre Ciberresiliencia, en adelante RCR[2] y al Reglamento de Inteligencia Artificial, en adelante RIA, este último publicado en el DOUE del día 12 de julio de 2024.[3]

---

1 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 de 18 de noviembre de 2024).

2 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 (DOUE de 20 de noviembre de 2024).

3 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), de 12 de julio de 2024.

El objetivo que persigue este trabajo es, por tanto, analizar qué repercusiones tiene en torno a la responsabilidad civil del fabricante el aprendizaje continuado de sus productos una vez introducidos en el mercado o puestos en servicio, qué manifestaciones tiene el aprendizaje continuado de los productos y cuál es el alcance de las medidas que debe adoptar el fabricante para reducir o eliminar los riesgos de los sistemas de inteligencia artificial que integran sus productos.

II. HARDWARE, SOFTWARE E INTELIGENCIA ARTIFICIAL: ¿QUÉ CARACTERIZA A UN PRODUCTO QUE INCORPORA INTELIGENCIA ARTIFICIAL?

1. Una nueva concepción del producto

El principal motivo por el cual es necesario adoptar una nueva directiva en la materia que nos ocupa es la necesidad de adaptar la nueva regulación a la complejidad de los productos que han irrumpido en el mercado: los llamados bienes con elementos digitales que pueden incorporar sistemas de inteligencia artificial. La particularidad de este tipo de bienes es que, por un lado, podemos distinguir el bien mueble tangible (hardware) y, por otro lado, los elementos (contenidos y servicios) digitales. Además, en la era digital no todos los productos son tangibles, sino que se han introducido en el mercado los productos o servicios digitales (sistemas operativos, programas de ordenador, aplicaciones o sistemas de inteligencia artificial) que no necesariamente se encuentran incorporados en un bien mueble tangible y que se pueden descargar e incorporar posteriormente en productos, fuera del ámbito de control del productor (considerando núm. 13 DRP).

Son conocidos los problemas de encaje de este tipo de bienes dentro de la definición de producto de la Directiva 85/374/CEE. Es por ello que la DRP pretende cerrar el debate doctrinal existente e incluir dentro del ámbito de aplicación de la futura norma el software y los servicios y contenidos digitales, independientemente de la forma de suministro. En este sentido, el art. 4.1) DRP define el concepto de producto de la siguiente forma: *"cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; incluye la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos"*.

La definición de producto que incorpora la DRP está inspirada en la definición contenida en la Directiva 85/374/CEE[4]. El elemento nuclear de la nueva definición de producto es su carácter mueble, que puede estar incorporado en otro bien mueble o en un bien inmueble. Hasta aquí nada aporta de nuevo la definición de la DRP. Seguidamente la definición incorpora dos nuevos conceptos inexistentes en la definición de producto de la Directiva 85/374/CEE, además de la electricidad: los archivos o copias de fabricación digital (considerandos núm. 16 y 17 DRP) y el software.

El considerando núm. 16 DRP da algunas pautas para interpretar qué debe entenderse por "archivos de fabricación digital", haciéndolo en contraposición a los "archivos digitales". Los primeros contienen "*información funcional necesaria para producir un elemento tangible permitiendo el control automatizado de máquinas o herramientas, como taladros, tornos, molinos e impresoras 3D, deben considerarse productos a fin de garantizar la protección de las personas físicas en los casos en que esos archivos sean defectuosos*". Se trata, por tanto, de archivos digitales que tienen contienen la información necesaria para producir nuevos productos. Por su parte, los archivos digitales, según el considerando núm. 16 DRP no entran dentro del concepto de producto. Se trataría por tanto, de archivos digitales que no contienen información codificada para producir nuevos productos, como las fotografías y los archivos de vídeo o de audio (considerando núm. 13 DRP *in fine*). La DRP hubiera podido referirse a este tipo de archivos digitales como meros contenidos digitales, concepto que utiliza el art. 2.1) Directiva (UE) 2019/770 (DCDS) para referirse a este tipo de archivos y, de esta forma, dotar de coherencia interna la legislación europea de responsabilidad contractual y extracontractual.

Por su parte, el considerando núm. 17 DRP se refiere a los servicios digitales. El art. 4 DRP no contiene una definición del concepto de servicios digitales, por lo que las pautas que establece el considerando núm. 17 DRP adquieren mayor relevancia a los efectos de aproximarnos correctamente a este concepto. No obstante, si que se trata de un concepto definido en el art. 2.2) DCDS:

> "a) un servicio que permite al consumidor crear, tratar, almacenar o consultar datos en formato digital, o

---

4 REPORT FROM THE EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES., Liability for Artificial Intelligence and Other Emerging Digital Technologies, Luxemburgo, 2019, p. 28.

b) un servicio que permite compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos".

A tenor de lo dispuesto en el considerando núm. 17 DRP para el caso de los servicios digitales el criterio de la incorporación o interconexión en productos tangibles es fundamental para aplicar a este tipo de productos las previsiones de la DRP. A pesar de que el considerando núm. 17 DRP declare que no debe aplicarse a los servicios digitales como tales, sí que es necesario extender sus efectos a los servicios digitales cuando estos estén incorporados o interconectados con productos, de tal forma que a falta de aquellos el producto no podría realizar sus funciones. Por tanto, a mi juicio el criterio de la incorporación o interconexión del software y los servicios digitales en productos resulta determinante para que la DRP sea aplicable a los daños causados por productos intangibles.

Una vez conceptualizado el producto según la definición de este concepto contenida en la DRP, debemos detenernos en las características de los productos con elementos digitales que incorporan sistemas de inteligencia artificial para comprender sus riesgos.

2. Inteligencia artificial aplicada a productos

Los productos, tal y como se concebían en el momento de adoptar la Directiva 85/374/CEE, estaban sujetos al poder del individuo, que los usaba para satisfacer sus necesidades según el uso razonable que pudiera esperarse del producto (art. 6.1.b) Directiva 85/374/CEE), o aun estando equipados con un software, este, aunque estaba incorporado en el producto está preprogramado y ejecuta sus funciones según las órdenes del individuo. En el contexto actual, el software de los productos ha adquirido nuevas funcionalidades, hasta el punto de que es capaz de tomar sus propias decisiones sin la necesidad de que su actuación obedezca a un patrón rígido, preprogramado y unidirecciona. En atención a las circunstancias en las que se encuentra el producto y de estímulos exteriores, el producto es capaz de adoptar sus propias decisiones.[5] Esta circunstancia conlleva que un producto que incorpora inteligencia artificial pueda producir daños a terceros por su comportamiento imprevisible y que sea necesario determinar quién

---

[5] WAGNER, Gerhard, "Liability Rules for the Digital Age", *Journal of European Tort Law*, vol. 13, no. 3, p. 193. ABBOTT, Ryan., *The Reasonable Robot*, Cambridge University Press, Londres, 2020, pp. 32-35.

debe responder por ello, lo que la PLD resuelve siguiendo un sistema de responsabilidad de los operadores económicos en cascada, apuntando en primer lugar al productor si el sistema de inteligencia artificial está bajo el control del fabricante del producto (considerando núm. 36 y 37 y art. 8 PDL).[6]

Asimismo, otra característica común de los productos que incorporan elementos digitales e inteligencia artificial es su capacidad de conectarse con otros productos o estructuras, de tal forma que esta característica puede convertirlos en vulnerables frente ataques (*hacking*) de terceros malintencionados. Por tanto, los defectos en la ciberseguridad de un producto (art. 7.2.f) DRP) han adquirido mucha relevancia en el entorno digital, hasta el punto de obligar al legislador europeo a dotarse de una legislación en este campo.[7]

III. ESTATUTO JURÍDICO DEL FABRICANTE: BREVE REFERENCIA AL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

El pasado 14 de mayo de 2024 el Consejo aprobó el Reglamento sobre Inteligencia Artificial, después que lo hiciera el Parlamento Europeo el día 13 de marzo de 2024. Finalmente, el procedimiento legislativo ordinario se culminó con la publicación del Reglamento de Inteligencia Artificial en el DOUE del día 12 de julio de 2024. Una de las principales novedades que

---

6 BECKERS, Anna, y TEUBNER, Gunther, *Three Liability Regimes for Artificial Intelligence*, Hart, London, 2021, pp. 71-84. Estos autores defienden la responsabilidad civil vicaria para los daños causados por productos defectuosos que incorporan sistemas de inteligencia artificial.

7 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 (DOUE de 20 de noviembre de 2024). *"En determinadas condiciones, todos los productos con elementos digitales integrados en un sistema electrónico de información más amplio o conectados a este pueden servir de vector de ataque para agentes malintencionados. En consecuencia, incluso los equipos y programas informáticos considerados menos críticos pueden facilitar que un dispositivo o red se vea comprometido en una fase inicial, lo que permite a los agentes malintencionados obtener un acceso privilegiado a un sistema o moverse lateralmente entre sistemas. Por consiguiente, los fabricantes deben garantizar que todos los productos con elementos digitales se diseñen y desarrollen de conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento."*

trae el futuro reglamento es que, con la finalidad de proteger a los usuarios y consumidores, el RIA se aplicará a: *"los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca"* (art. 2.1.e) RIA). El deseo del legislador europeo es obligar a los fabricantes de productos que incorporan inteligencia artificial al cumplimiento de las obligaciones del RIA, cuando el sistema de inteligencia artificial se encuentre incorporado o instalado en el producto.

Sin embargo, en atención a lo dispuesto en el considerando núm. 87 RIA, parece que el RIA diferencia entre la función que cumple el sistema de inteligencia artificial una vez integrado en el producto, pudiéndose distinguir entre su función como un "componente de seguridad" y cuando no cumple dicha función. El considerando núm. 87 RIA hace especial hincapié a la función del sistema de inteligencia artificial como componente de seguridad: *"Además, cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto que entre dentro del ámbito de aplicación de un acto legislativo de armonización de la Unión basado en el nuevo marco legislativo no se introduzca en el mercado ni se ponga en servicio de forma independiente del producto, el fabricante del producto, tal como se define en el acto legislativo pertinente, debe cumplir las obligaciones que el presente Reglamento impone al proveedor y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumpla los requisitos del presente Reglamento."* El concepto de "componente de seguridad" aparece definido en el art. 3.14) RIA del siguiente modo: *"un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, o cuyo fallo o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes"*. Habida cuenta de las anteriores consideraciones, el sistema de inteligencia artificial que actúa como un componente de seguridad respecto de un producto asume una función de control de dicho producto, evitando que con su funcionamiento se ponga en peligro la salud y la seguridad de las personas y, por tanto, es el elemento de la seguridad el que es tenido en cuenta por el RIA a los efectos de incluir el sistema de inteligencia artificial incorporado en un producto dentro del ámbito de aplicación del RIA.

El art. 25.3 RIA se ocupa de esta cuestión y dispone que cuando el sistema de inteligencia artificial de alto riesgo funcione como un componente de seguridad de un producto de los referenciados en la sección A del Anexo I del RIA, el fabricante actuará como un proveedor de un sistema de inteligencia artificial y estará sujeto a las obligaciones que impone el art. 16 RIA. Si observamos los actos legislativos armonizados que aparecen en la sección A del Anexo I RIA vemos que se refieren a productos cuyos defectos de funcionamiento son especialmente críticos para la seguridad y la

salud de las personas, como por ejemplo las máquinas, los juguetes, las embarcaciones de recreo, los ascensores y los componentes de seguridad, etc.

Lo anterior no permite afirmar que el RIA solo contempla los sistemas de seguridad que son un complemento de seguridad de productos que entran dentro del ámbito de aplicación de los actos legislativos armonizados de la sección A del anexo I RIA, sino que un sistema de inteligencia artificial puede ser catalogado de alto riesgo según los criterios del RIA, pero que se integre en productos referenciados en la sección B del anexo I RIA. En este caso, el art. 2.2 RIA relaja las obligaciones de los fabricantes cuyos productos que incorporan sistemas de inteligencia artificial aparecen referenciados en la sección A del anexo I. Es el caso de los fabricantes de vehículos de motor, que pueden incorporar sistemas de inteligencia artificial que actúan como un componente de seguridad.

En consecuencia, se constata que el RIA se centra fundamentalmente en la función de seguridad que cumplen los sistemas de inteligencia artificial incorporados en productos. Cuando estos sean catalogados de alto riesgo y se inserten en los productos referenciados en el Anexo A, los fabricantes deberán cumplir con los requisitos de los sistemas de inteligencia artificial de alto riesgo previstos en el RIA. En caso contrario, si los sistemas de inteligencia artificial son catalogados de alto riesgo, pero se insertan en productos referenciados en el Anexo B, solo serán aplicables las obligaciones previstas en los arts. 6 (1), 102-109, y 112 RIA (art. 2.2 RIA).

IV. EL APRENDIZAJE CONTINUADO DEL PRODUCTO DESPUÉS DE SU INTRODUCCIÓN EN EL MERCADO O PUESTA EN SERVICIO

El aprendizaje continuado de un producto después de ser introducido en el mercado o puesto en servicio es una característica propia de los productos con elementos digitales que integran sistemas de inteligencia artificial. El art. 7.2.c) DRP se refiere a este requisito para apreciar el carácter defectuoso de un producto: *"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."* A pesar de la transcendencia que puede tener la capacidad de autoaprendizaje continuado en lo que concierne a la responsabilidad del fabricante, no se contienen más referencias sobre este aspecto en la DRP. Tan solo el considerando núm. 32 DRP aporta algo de luz:

> *"Con el fin de reflejar la creciente prevalencia de productos interconectados, la valoración de la seguridad de un producto también debe tener en*

> *cuenta los efectos razonablemente previsibles de otros productos en el producto en cuestión, como por ejemplo en un sistema doméstico inteligente. También debe tenerse en cuenta el efecto en la seguridad de un producto de toda capacidad de aprendizaje o de adquisición de nuevas características tras su introducción en el mercado o su puesta en servicio, a fin de reflejar la expectativa legítima de que el programa informático de un producto y los algoritmos subyacentes estén diseñados de manera que se evite un comportamiento peligroso del producto. Por consiguiente, un fabricante que diseñe un producto con la capacidad de desarrollar un comportamiento inesperado debe seguir siendo responsable de todo comportamiento que cause daños. Para reflejar el hecho de que, en la era digital, muchos productos permanecen bajo el control del fabricante tras su introducción en el mercado, el momento en que un producto deja de estar bajo el control del fabricante también debe tenerse en cuenta en la valoración de su seguridad. Un producto también puede considerarse defectuoso debido a su vulnerabilidad en materia de ciberseguridad, por ejemplo cuando el producto no cumpla los requisitos de ciberseguridad pertinentes."*

El considerando transcrito aporta algunos elementos para valorar el posible carácter defectuoso de un producto como consecuencia del aprendizaje continuado después de la introducción en el mercado o la puesta en servicio: la adquisición de nuevas propiedades y la capacidad del sistema de inteligencia artificial de evitar comportamientos peligrosos del producto. Estos elementos y cómo afectan al producto serán analizados en las páginas siguientes. Además, el hecho que el producto adopte un comportamiento imprevisible no será una circunstancia que exonere de responsabilidad al fabricante. Por tanto, se descarta que una decisión adoptada autónomamente por el producto pueda anular o reducir la responsabilidad del fabricante, en tanto que el producto sigue bajo su ámbito de control y debe seguir respondiendo por cualquier comportamiento o decisión que adopte el producto de forma autónoma.

Considerando, por tanto, lo dispuesto en el texto de la DRP, se parte de las siguientes premisas que conducirán al desarrollo posterior de esta cuestión:

1) La capacidad de aprendizaje continuado del producto es una circunstancia para apreciar su carácter defectuoso, que puede manifestarse en múltiples facetas del producto.

2) En general, el momento relevante para evaluar el carácter defectuoso de un producto por su capacidad de aprendizaje continuado es cuando se introduce en el mercado o se pone en servicio. Sin embargo, las particularidades de los productos con elementos digitales que pueden actualizarse porque siguen bajo el control del fabricante

obligan a tomar en consideración el momento en que el producto deja de estar sujeto al control del fabricante.

3) Debe partirse de la expectativa legítima de los consumidores o usuarios para valorar la capacidad de autoaprendizaje del producto, tendente a evitar un comportamiento peligroso del producto y a la adquisición de nuevas propiedades o cumplimiento de nuevas funciones.

4) Un producto puede ser defectuoso por una vulnerabilidad que comprometa su ciberseguridad. Nos preguntamos, por tanto, si la capacidad del producto de reaccionar frente a la vulnerabilidad es una circunstancia que deba comprender la capacidad de aprendizaje automático.

1. Algunos aspectos de carácter general

1.1. El producto que es capaz de aprender continuamente está sujeto al control del fabricante

En el contexto actual, donde predominan los productos con elementos digitales, debemos partir de un concepto dinámico de producto, es decir, el producto que por ser defectuoso causa un daño a un tercero puede que no tenga las mismas propiedades que cuando fue introducido en el mercado o puesto en servicio, sino que sus características hayan variado por el hecho que el fabricante sigue teniendo el producto bajo su ámbito de control y lo actualice para que sea más seguro o pueda cumplir nuevas funciones. Por tanto, el concepto de "control del fabricante" es sumamente relevante para valorar la responsabilidad del fabricante.

Se trata de un concepto que aparece definido en el art. 4.5) DRP y que ha sufrido cambios significativos a razón de las enmiendas propuestas por el Consejo.

> *"a) la acción del fabricante de un producto mediante la que realiza o, con respecto a las acciones de un tercero, autoriza o consiente en:*
>
> i) la integración, interconexión o suministro de un componente, incluidas las actualizaciones o mejoras de los programas informáticos, o
>
> ii) la modificación del producto, incluidas las modificaciones sustanciales;
>
> *b) la capacidad del fabricante de un producto de suministrar actualizaciones o mejoras de programas informáticos, por sí mismo o a través de un tercero".*

Vemos, pues, que el fabricante mantiene el producto bajo su ámbito de control tanto si el mismo interviene en el producto por medio de una actualización del software, como si el cambio producido en el producto es obra de un tercero que actúa con su autorización. En el primer caso, el fabricante o bien un tercero autorizado actuando por su cuenta integran, interconectan o suministra un componente en el producto o llevan a cabo una modificación en el producto. En el segundo caso, el fabricante o tercero autorizado suministran actuaciones del producto, de tal modo que en ambos casos el producto cambia sus propiedades permaneciendo bajo el ámbito de control del fabricante una vez introducido en el mercado y es por ello que la DRP le imputa la responsabilidad derivada del daño.

Además, nótese que en el supuesto de que el daño se produzca después de la intervención del tercero, este puede intentar exonerarse de su responsabilidad si logra probar que el daño no está relacionado con su intervención (art. 11.1.f) DRP, o bien se debe a las instrucciones dadas por el fabricante. Esta posible causa de exoneración de responsabilidad solo es alegable para el tercero que actúa dentro del ámbito del control del fabricante (art. 8.1.b) DRP. En el caso que el tercero actúa fuera del ámbito de control del fabricante, este tercero tendrá igualmente la consideración de fabricante (art. 8.4 DRP), a los efectos de imputarle el daño que resulte de su intervención en el producto.

1.2. Aprendizaje continuado y valoración del carácter defectuoso del producto

Por lo que se refiere al momento de apreciación del carácter defectuoso del producto, el concepto de control del fabricante es sumamente relevante a los efectos de determinar la responsabilidad del fabricante. En atención a la evolución continua del producto con elementos digitales, el carácter defectuoso no puede valorarse según su estado en el momento de su primera introducción en el mercado o puesta en servicio. El art. 7.2.e) DRP dice que, en estos supuestos, el carácter defectuoso del producto deberá valorarse en el momento en que el producto dejó el control del fabricante. Por tanto, los cambios producidos en el software del producto con elementos digitales que pueden convertir el producto en defectuoso no deberán valorarse según su estado en el momento de la introducción en el mercado o puesta en servicio, entre otras cosas,

porque han cambiado las propiedades del producto.[8] En estos casos, el momento relevante es la independencia del producto respecto del control del fabricante.

Cuando el aprendizaje continuado del producto sea consecuencia del sistema de inteligencia artificial de alto riesgo que lleva incorporado, el art. 8.2 RIA impone al proveedor del sistema el cumplimiento de los requisitos generales que se imponen a los sistemas de inteligencia de alto riesgo (art. 8.1 RIA). En el desarrollo de estos requisitos, los arts. 9.2 y 15.1 RIA establecen, respectivamente, que el proveedor de inteligencia artificial debe gestionar los riesgos de la IA durante toda la vida útil del producto y velar por la precisión, solidez y la ciberseguridad del sistema de inteligencia artificial durante todo el periodo de vida útil. En consecuencia, incorporada la inteligencia artificial de alto riesgo en el producto que permite el aprendizaje continuado, si el proveedor debe seguir gestionando el sistema de inteligencia artificial que incorpora el producto, el fabricante que haya equipado sus productos con dicho sistema de inteligencia artificial será el responsable de controlar sus riesgos (considerando núm. 87 RIA), pero si el producto sale de su ámbito de control, por ejemplo, por una modificación sustancial operada por un tercero ajeno a su círculo o que actúa sin su autorización, entonces parece razonable afirmar que el fabricante original pueda exonerarse de responsabilidad si la modificación sustancial ha afectado el sistema de inteligencia artificial. En caso contrario, si la modificación sustancial no ha alterado el sistema de inteligencia artificial, parece claro que en virtud de los arts. 9.2 y 15.1 RIA el fabricante original seguirá respondiendo (considerando núm. 84 RIA).

La realización de una modificación sustancial del producto, mediante un proceso de reacondicionamiento o remanufacturación fuera del ámbito de control del fabricante original y actuando sin su autorización determina que el tercero adquiera la condición de fabricante (art. 8.2 DRP). Atendiendo a lo dispuesto en el considerando núm. 84 RIA, el operador económico que haya realizado la modificación sustancial estará obligado al cumplimiento de las obligaciones impuestas en el RIA, en tanto que también tendrá la consideración de fabricante.

---

8 WAGNER, Gerhard, "Liability Rules for the Digital Age…", *op. cit.*, p. 206. Este autor afirma que el momento de la emancipación del producto del control del fabricante a los efectos de valorar su carácter defectuoso solamente es aplicable al software y, en particular, sus propiedades en materia de seguridad, y no respecto del hardware, cuyo carácter defectuoso deberá valorarse según el estado que presente en el momento de la introducción en el mercado o puesta en servicio.

1.3. El límite de 10 años de la responsabilidad del fabricante. ¿Cómo debe aplicarse en el caso de daños atribuibles al aprendizaje continuado del producto?

Esta "concepción dinámica" del producto con elementos digitales que incorpora inteligencia artificial, que puede aprender, mejorar y actualizarse durante el transcurso del tiempo mientras se encuentra bajo el ámbito de control del fabricante, tiene un "límite estático" en el tiempo, en cuanto a la responsabilidad del fabricante (art. 17 DRP) derivada de los daños causados por el producto defectuoso: el fabricante no será responsable de los daños ocasionados por el producto más allá de los diez años desde su introducción en el mercado o puesta en servicio, salvo que se produzca una modificación sustancial en el producto, hecho que es considerado una nueva introducción en el mercado y, por tanto, que se reinicie el plazo de responsabilidad del fabricante (art. 17.1.b) DRP).

La previsible continuada evolución del producto debido a las actualizaciones del software y al aprendizaje continuado después de la introducción en el mercado o la puesta en servicio del producto no encaja bien con la fijación de un límite estático para extinguir la responsabilidad del fabricante, máxime cuando los arts. 9.2 y 15.1 RIA obligan al productor a gestionar los riesgos del sistema de inteligencia artificial durante todo el ciclo de vida útil del producto.

El art. 17.2 DRP se refiere a la posibilidad de extender el plazo de responsabilidad del fabricante hasta los 25 años: *"Como excepción a lo dispuesto en el apartado 1, cuando una persona perjudicada no haya podido interponer una acción en un plazo de diez años a partir de las fechas a que se refiere el apartado 1, debido a la latencia de una lesión corporal, la persona perjudicada dejará de tener derecho a indemnización en virtud de la presente Directiva al vencimiento de un plazo de veinticinco años, a menos que esa persona perjudicada haya interpuesto, entre tanto, una acción contra un operador económico que pueda ser considerado responsable con arreglo al artículo 8."* A tenor de lo dispuesto en el considerando núm. 57 DRP, parece que el legislador europeo está pensando en daños causados por productos médicos, cuyos daños pueden manifestarse al transcurso de un período de tiempo más largo de 10 años a contar desde la introducción en el mercado del producto. Por tanto, aduciendo a las obligaciones de seguridad que el RIA impone a los proveedores de sistemas de inteligencia artificial durante toda la vida útil del producto, se deduce de la última parte del considerando núm. 57 DRP *-el plazo de caducidad debe ampliarse a veinticinco años en los casos en que los síntomas de una lesión corporal sean, según pruebas médicas, de aparición lenta-* que el plazo de

25 años es difícilmente aplicable a los daños causados por la inteligencia artificial y el aprendizaje continuado del producto.

1.4. Defectuosidad del producto y expectativas de los consumidores

El carácter defectuoso de un producto debe valorarse según las legítimas expectativas de seguridad que cabe esperar de un producto un criterio que ya fue adoptado por la Directiva 85/374/CEE y que ahora se mantiene vigente con la regulación de la DRP.

El art. 6.1 Directiva 85/374/CEE se refiere a *"la seguridad a la que una persona tiene legítimamente derecho"*, adoptando una apreciación subjetiva del carácter defectuoso del producto, a pesar de que el considerando que se dedica a esta cuestión se adopta un enfoque objetivo, refiriéndose a *"las condiciones de seguridad a que tiene derecho el gran público"*. La DRP adopta el mismo criterio (art. 7.1 DRP): "Un producto se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional." A pesar de este enfoque subjetivo, el considerando núm. 30 DRP objetiviza las expectativas de una persona en concreto en cuanto a la seguridad del producto: *"La valoración del carácter defectuoso debe incluir un análisis objetivo de la seguridad que el público en general tiene derecho a esperar y no referirse a la seguridad que una persona concreta tiene derecho a esperar. La seguridad que el público en general tiene derecho a esperar debe valorarse teniendo en cuenta, entre otras cosas, la finalidad prevista, el uso razonablemente previsto, la presentación, las características objetivas y las propiedades del producto de que se trate, incluido su ciclo de vida previsto, así como las necesidades específicas del grupo de usuarios al que se destina el producto."* En todo caso, independientemente del enfoque que se adopte, el criterio de las legítimas expectativas de los consumidores debe valorarse objetivamente, desvinculado el juicio sobre la defectuosidad de un producto de los sesgos y prejuicios de un consumidor en particular.[9]

El legislador europeo es conocedor de que las expectativas del público en general en torno a los productos que funcionan con inteligencia artificial pueden ser más elevadas, especialmente en aquellos productos que entrañan un riesgo vital: *"Algunos productos, como los productos sanitarios de*

---

9 STAPLETON, Jane, *Product Liability,* Butterworths, 1994, p. 234. BORGHETTI, Jean-Sébastien, "Taking EU Product Liability Law Seriously: How Can Product Liability Directive Effectively Contribute to Consumer Protection", *French Journal of Legal Policy,* núm. 1, 2023, p. 33.

soporte vital, conllevan un riesgo especialmente elevado de daños para las personas y, por lo tanto, generan unas expectativas de seguridad especialmente elevadas." (considerando núm. 30 DRP). Esta posible graduación de las expectativas de los consumidores parece ser acorde con las directrices del Reglamento sobre inteligencia artificial, que diferencia entre sistemas de inteligencia artificial de alto riesgo y sistemas de inteligencia artificial que no son de alto riesgo. Por tanto, las expectativas de los consumidores sobre la inteligencia artificial que incorpora el producto deberán valorarse objetivamente y de acuerdo con los riesgos que entrañen los productos que incorporen inteligencia artificial y sus características.

2. Manifestaciones del carácter defectuoso de un producto por el efecto del aprendizaje continuado

2.1. Corrección de errores y ejecución de funciones

Los productos, tal y como se concebían en el momento de adoptar la Directiva 85/374/CEE, estaban sujetos al poder del individuo, que los usaba para satisfacer sus necesidades según el uso razonable que pudiera esperarse del producto (art. 6.1.b) Directiva 85/374/CEE), o si estaban equipados con un software, este, aunque estaba incorporado en el producto estaba preprogramado y ejecutaba sus funciones según las órdenes del individuo. En el contexto actual, el software de los productos ha adquirido nuevas funcionalidades, hasta el punto de que es capaz de tomar sus propias decisiones sin la necesidad de que su actuación obedezca a un patrón rígido, preprogramado y unidireccional.[10] Esto es posible gracias al *machine learning* o, lo que es lo mismo, la capacidad de aprender del producto una vez ha sido introducido en el mercado o puesto en servicio y a la inteligencia artificial.

El *machine learning* es el proceso mediante el cual un producto puede realizar nuevas funciones o cumplir nuevas tareas mediante la exposición continuada a una gran cantidad de datos.[11] A medida que el producto

---

[10] WAGNER, Gerhard, "Liability Rules for the Digital Age", *op. cit.*, p. 193. ABBOTT, Ryan, *The Reasonable Robot…, op.cit.*, pp. 32-35.

[11] HUBERMAN, Pinchas, "Tort Law, Corrective Justice and the Problem of Autonomous-machine-Caused Harm", *Canadian Journal of Law & Jurisprudence*, núm. 1, 2021, p. 109.

entra en contacto con más datos y se entrena, el algoritmo que incorpora es capaz de mejorar su rendimiento para optimizar el cumplimiento de sus funciones.[12] La capacidad de aprendizaje de los productos que incorporan inteligencia artificial permite que los productos funcionen con una independencia parcial respecto de las instrucciones predeterminadas por sus programadores. La creciente autonomía de los productos se debe, por tanto, a la capacidad del algoritmo de detectar patrones estadísticos que subyacen en los datos analizados y que conforman modelos automáticamente construidos sin una programación manual.[13] A pesar de la creciente autonomía del producto, indudablemente el software debe ser inicialmente programado e introducido en el mercado o puesto en servicio para cumplir sus funciones y, gracias a su capacidad de aprendizaje, será capaz de adoptar nuevas soluciones. No obstante, los datos, las decisiones que adopte el producto y las funciones que progresivamente pueda adquirir como consecuencia de su capacidad de aprendizaje determinarán su posible carácter defectuoso. A este respecto, la doctrina ha realizado diversas aportaciones que se refieren al defectuoso aprendizaje continuado del *machine learning*:[14]

a) Incorrección de los datos que constituyen el *machine learning* sobre los cuales el algoritmo adopta la decisión. En este caso, el sistema de aprendizaje continuado no se ha nutrido de datos actualizados y, por tanto, la decisión que ha adoptado sobre datos o parámetros desfasados es incorrecta.

b) Error del algoritmo por la decisión adoptada, es decir, pudiendo cumplir su función optando por diversos procedimientos, el algoritmo se equivoca de acuerdo con las instrucciones dadas por el usuario del producto. Pongamos por caso el ejemplo de un sistema de navegación GPS donde el usuario selecciona la ruta más rápida posible. Si el producto obvia la situación del tráfico actual, quizá la ruta escogida no será la más rápida, habiendo otras alternativas.

---

12 VALLOR, Shannon y BEKEY, George A., "Artificial Intelligence and the Ethics of Self-Learning Robots", LIN, Patrick, ABNEY, Keith y JENKINS, Ryan (eds.), *Robot Ethics 2.0: From Autonomous Cars to Artificial intelligence,* Oxford University Press, p. 340.

13 SURDEN, Harry, "Machine Learning and Law", *Washington Law Review,* núm. 89, 2014, pp. 89-95.

14 CORMEN, Thomas H., *Algorithms Unlocked,* MIT Press, Londres, 2013, pp. 2-4.

c) Defectuosa ejecución de nuevas funciones. La idea de que los productos que incorporan inteligencia artificial están completamente codificados para cumplir sus funciones debe descartarse. Estos productos son, o deberían ser capaces, de cumplir nuevas funciones que, en el momento de la introducción en el mercado o puesta en servicio del producto aún son desconocidas, o bien adoptar decisiones de acuerdo a un patrón de datos no programado. En este caso, el producto no está preparado de inicio para realizar sus funciones, pero puede aprender a realizarlas si el algoritmo y el aprendizaje continuado lo permiten mediante su entrenamiento.[15] Es decir, el producto debe aprender continuamente a realizar nuevas funciones analizando los datos de que dispone y elaborando nuevos patrones. En este supuesto, el proceso de aprendizaje continuado es controlado según los datos y métodos del desarrollador del software, por lo que la actuación del producto no es completamente autónoma.

Los supuestos que se agrupan en los grupos anteriores permiten, aunque sea esquemáticamente, esbozar los defectos que puede adolecer un producto que afectan a su capacidad de aprendizaje continuado. En todos ellos el fabricante o desarrollador del software pueden ejercer un control, en el sentido de corregir los errores existentes en los datos del sistema, mejorar el proceso de decisión del algoritmo o bien preparando el producto para que pueda cumplir nuevas funciones. Por tanto, la premisa de la cual parte de la DRP de concentrar la responsabilidad en el fabricante que deriva de daños causados por productos defectuosos es adecuada. Asimismo, la responsabilidad conjunta y solidaria de los operadores económicos que consagra el art. 12 DRP tiene el usuario como principal beneficiario, puesto que, presentándose el producto como un todo, incluyendo el hardware y el software, no tendrá que probar a cuál de los operadores económicos es imputable el daño.

2.2. Aprendizaje continuado y explotación de vulnerabilidades

El punto de partida de la DRP es que si el producto, una vez se produce su primera introducción en el mercado o puesta en servicio, sigue estando bajo el ámbito de control del fabricante, por lo que su carácter defectuoso no debe valorarse desde aquel momento, sino desde el momento en que

---

[15] DESAI, Deven R., y KROLL, Joshua A., "Trust but Verify: A Guide to Algorithms and the Law", *Harward Journal of Law & Technology,* núm. 31, 2017, pp. 26-27.

el fabricante deja de ejercitar un control sobre él. Durante este plazo de tiempo, y mientras se ejerce el control sobre el producto, el fabricante lo podrá actualizar, para mejorar su seguridad o sus prestaciones.

El suministro de actualizaciones ha sido abordado en el ámbito de la responsabilidad contractual derivada de una falta de conformidad subjetiva y objetiva del producto, concretamente en la Directiva (UE) 2019/771, en adelante DCCB.[16] Las actualizaciones constituyen un elemento fundamental para que los bienes con elementos digitales no queden obsoletos y sigan satisfaciendo las expectativas del consumidor y, en consecuencia, la falta de suministro de actualizaciones o el suministro de actualizaciones incompletas o defectuosas son un supuesto de falta de conformidad de los bienes (considerando núm. 28 DCCB).

En el ámbito de la responsabilidad del fabricante, nos preguntamos cómo pueden materializarse los ataques en el sistema de inteligencia artificial y, consiguientemente, en la capacidad de aprendizaje automático del producto. En general, pueden distinguirse tres formas de ataques que afectan a los sistemas de aprendizaje continuado: el envenenamiento de datos, el envenenamiento de modelos y la evasión de modelos (art. 15.5 RIA).[17] En los ataques por evasión de datos, el tercero que ataca un producto aprovecha una vulnerabilidad en su seguridad para insertar nuevos datos a los datos originales que tiene el producto para conducir a un resultado erróneo.[18] En los ataques por contaminación de datos, el atacante

---

16 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. L 136, de 22 de mayo de 2019.

17 GOODFELLOW, Ian J., SHLENS, Jonathon y SZEGEDY, Christian, "Explaining and Harnessing Adversarial Examples", *Proceedings of International Conference on Learning Representations*, San Diego, 2015, pp. 1-11. KURAKIN, Alexey, GOODFELLOW, Ian J. y BENGIO, Samy, *Proceedings of International Conference on Learning Representations*, Toulon 2017, p. 1-14. GOODFELLOW, Ian J., McDaniel, Patrick y PAPERNOT, Nicolas, "Making Machine Learning Robust Against Adversarial Inputs", en *Communications of the AC,* vol. 61, núm. 7, 2018, pp. 56-68.

18 BAMSHAD, Mobasher, BURKE, Robin y BHAUMIK, Runa, "Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness", *ACM Transactions on Internet Technology,* vol. 7, núm. 4, pp. 23 y ss. Un ejemplo de este tipo de ataques es el que consiste en la infiltración de perfiles falsos en los algoritmos que tienen una función de asignación de una publicidad determinada a un perfil de usuarios.

altera los datos originales del producto, con lo que se contaminan y también conduce al resultado de una predicción errónea. Finalmente, en los ataques a modelos entrenados, el atacante se apropia del modelo y de los datos originales del producto.[19]

En el ámbito de la responsabilidad por daños causados por productos defectuosos, pueden hacerse diversas observaciones sobre el efecto de las actualizaciones en un producto, según el estado de esta cuestión en la DRP. En primer lugar, la DRP. se refiere exclusivamente a las actualizaciones de seguridad del producto y lo hace como una reacción frente a las vulnerabilidades de ciberseguridad del producto (considerandos núm. 38 y 41 Propuesta de Directiva) y para dejar claro que un defecto consistente en una vulnerabilidad de la seguridad del producto puede convertirlo en defectuoso (considerando núm. 51 DRP). En segundo lugar, el hecho que el producto reciba una actualización no debe conducir a la conclusión que el producto es defectuoso (art. 7.3 DRP). Y, finalmente, el fabricante no podrá exonerarse de su responsabilidad si, mientras el producto se encuentra bajo su ámbito de control, el defecto se deba a programas informáticos, incluidas las actualizaciones o mejoras de programas informáticos o la falta de actualizaciones o mejoras de los programas informáticos necesarias para mantener la seguridad (art. 11.2 DRP).

Por tanto, el punto de partida en esta materia es que los defectos de ciberseguridad, que se materializan en vulnerabilidades del producto, deben subsanarse mediante actualizaciones de seguridad. La Unión Europea recientemente ha adoptado el Reglamento sobre Ciberresiliencia (RCR),[20] que regula las obligaciones de los fabricantes de productos con elementos digitales en aquello relativo a la ciberseguridad de los productos. El texto impone un conjunto de obligaciones a los fabricantes y al resto de operadores económicos que intervienen en la cadena de producción de un producto con elementos digitales. Entre estas obligaciones destaca la declaración (UE) de conformidad y la presunción de conformidad de aquel tipo de productos. A través de la declaración de conformidad, el legislador europeo pretende que cuando los productos

---

19 FUWEI, Li, LIFENG, Lai, y SHUGUANG, Cui, *Machine Learning Algorithms Adversarial Robustness in Signal Processing*, Springer, 2022, pp. 1-2.

20 Para una introducción general, *vid.* CHIARA, Pier Giorgio, "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements," *International Cybersecurity Law Review*, No. 3, 2022, p. 255-272.

con elementos digitales sean introducidos en el mercado se presuma su conformidad si cumplen los requisitos de ciberseguridad del Anexo I de RCR.

Según el art. 1 RCR, el ámbito de aplicación del futuro reglamento sobre ciberresiliencia gira en torno a los productos con elementos digitales y su ciberseguridad. A este respecto, el RCR establece: a) normas para la introducción en el mercado de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos; b) requisitos esenciales para el diseño, el desarrollo y la fabricación de productos con elementos digitales y las obligaciones de los operadores económicos en relación con dichos productos, en lo que respecta a la ciberseguridad; c) requisitos esenciales para los procesos de gestión de la vulnerabilidad establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales a lo largo de todo el ciclo de vida, y las obligaciones de los operadores económicos en relación con dichos procesos; y d) normas relativas a la vigilancia del mercado y a la aplicación de los requisitos y las normas antes mencionados. El RCR, por tanto, prevé unos requisitos horizontales en materia de ciberseguridad aplicables a todos los productos con elementos digitales.

El RCR impone a los fabricantes que las vulnerabilidades[21] que presenta el producto deben subsanarse mediante actualizaciones de seguridad (Anexo I, parte I, 2.c) RCR) y que difundan sin demora y de forma gratuita parches o actualizaciones de seguridad para hacer frente a los problemas de seguridad detectados (Anexo I, parte II 2.8) RCR). Por tanto, a tenor de lo dispuesto en el RCR no parece que el aprendizaje continuado del producto una vez introducido en el mercado o puesto en servicio requiera que el propio producto sea capaz de detectar, corregir, y prevenir las vulnerabilidades que le pudieran hacer vulnerables frente ataques malintencionados de terceros. Por tanto, la obligación del fabricante de velar requiere un atento examen del producto y una evaluación periódica de los riesgos existentes y una reacción rápida ante los riesgos o vulnerabilidades desconocidos.

---

[21] SCHMITZ, Sandra y SCHIFFNER, Stefan, "Responsible Vulnerability Disclosure under the NIS 2.0 Proposal," disponible en https://www.jipitec.eu/issues/jipitec-12-5-2021/5495/schmitz_schiffner_pdf.pdf (consulta realizada en fecha 15 de marzo de 2024). *"A vulnerability is a set of conditions that allows the violation of a security (or privacy) policy. Such conditions might be created by software flaws, configuration mistakes and other human errors of operators, or unexpected conditions of the environment a system runs in."*

Vemos que, según el enfoque adoptado por el RCR, la gestión de las vulnerabilidades del producto se canaliza a través de la obligación de suministrar actualizaciones de seguridad del fabricante y no en la capacidad del sistema de autoprotegerse ante un ataque, aprovechando su capacidad de aprendizaje continuado, en este caso, después de ser objeto de un ataque de un tercero ajeno al fabricante.

Considerando los posibles ataques que pueden afectar a los sistemas de aprendizaje automático, ¿es exigible que estos sistemas de inteligencia artificial lleven integrados sistemas de defensa para aprender, también, de dichos ataques y prevenirlos en el futuro? El aprendizaje automático en materia de seguridad no es algo que se imponga expresamente a los fabricantes de productos con elementos digitales, pero que puede deducirse implícitamente de la obligación de gestionar de forma eficaz las vulnerabilidades de sus productos (art. 11.6 RCR) o, al menos, se desprende de una interpretación extensiva de dicha obligación en aras a garantizar la protección eficaz de los consumidores. En este sentido, la doctrina ha puesto de relieve diversas estrategias para afrontar con éxito los ataques dirigidos a los productos, por lo que el estado de la técnica en esta materia se encuentra sumamente avanzado y, por tanto, si estos sistemas de defensa están al alcance de los fabricantes, deben interpretarse en un sentido amplio las obligaciones que les impone el RCR en esta materia para proteger adecuadamente a los usuarios de sus productos.[22]

El RIA también ha adoptado alguna previsión relativa a la gestión de vulnerabilidades de los sistemas de inteligencia artificial. El considerando núm. 76 RIA hace referencia a los riesgos en materia de ciberseguridad que se materializan en vulnerabilidades de los sistemas y aboga por imponer a los proveedores de sistemas de inteligencia artificial de alto riesgo la obligación de adoptar medidas adecuadas, como controles de seguridad, para alcanzar un nivel de seguridad adecuado. Posteriormente, es el art. 15.4 y 5 RIA el que concreta las directrices del considerando núm. 76 RIA en esta materia e impone a los proveedores de sistemas de inteligencia artificial de alto riesgo el deber de valar para que los sistemas de inteligencia artificial sean resistentes frente a ataques de terceros mediante la explotación de vulnerabilidades.

---

[22] BARRENO, Marco, NELSON, Blaine y JOSEPH, Anthony. D., "The security of machine learning", *Mach Learn,* núm. 81, 2010, pp. 121-148.

2.3. Sesgo de datos

El sistema de inteligencia artificial que incorpora el producto se alimenta de los datos que tiene almacenados para la toma de decisiones. Los datos que constituyen el *machine learning* van evolucionando a través de las sucesivas actualizaciones del producto y, también, de la experiencia del usuario. El aprendizaje continuado del producto a través de la experiencia del usuario es un aspecto que ha merecido la atención del RIA. La versión del RIA aprobada por el Consejo el día 14 de mayo del 2024 hace referencia, en el art. 15.4 RIA, a la necesidad de que los sistemas de inteligencia artificial que continúan aprendiendo después de su introducción en el mercado o puesta en servicio eliminen o reduzcan los posibles riesgos implícitos en los datos sesgados introducidos en el sistema como consecuencia de su entrenamiento, validación y de la experiencia adquirida por el producto (considerando núm. 67 RIA). En este sentido, deben adoptarse medidas eficaces para mitigar este riesgo (bucle de retroalimentación o *feedback loops*).

La experiencia americana ha demostrado que la aplicación de la inteligencia artificial en ámbitos determinados, como por ejemplo la evaluación de la solvencia, ha dado lugar a que determinadas comunidades, como los negros o latinos, obtengan unos peores resultados en los procesos de evaluación de la solvencia, como consecuencia de la discriminación que han sufrido estos grupos en algunas políticas públicas. A la práctica, esto se ha traducido en la denegación del acceso al crédito o a la imposición de peores condiciones financieras, como tipos de intereses moratorios más elevados.[23] Por tanto, el tratamiento de grandes cantidades de datos permite a

---

[23] RICE, Lisa, y SWESNIK, Deidre, "Discriminatory Effects of Credit Scoring on Communities of Color", *Suffolk University Law Review*, núm. 935, 2013, p. 940-943. NOEL, Nick, PINDER, Duwain, STEWART, Shelley y WRIGHT, Jason, "The economic impact of closing the racial wealth gap", puede consultarse en: *https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20economic%20impact%20of%20closing%20the%20racial%20wealth%20gap/the-economic-impact-of-closing-the-racial-wealth-gap-final.pdf*.

los responsables del tratamiento elaborar perfiles[24] que pueden reproducir sesgos discriminatorios, incrementando la discriminación algorítmica.[25]

La reducción o eliminación del sesgo existente en los datos que constituyen la base del aprendizaje continuado del producto es otra manifestación de esta causa para determinar el carácter defectuoso del producto.

V. CONCLUSIONES

El aprendizaje continuado de un producto y cómo esta circunstancia afecta a su carácter defectuoso es una de las principales novedades que trae la nueva regulación europea sobre responsabilidad por daños causados por productos defectuosos.

Una de las características de los productos con elementos digitales que incorporan inteligencia artificial es que cuando son introducidos en el mercado o puestos en servicio el fabricante sigue ejerciendo un control sobre el producto, que se actualizará periódicamente para corregir errores de su software, para cumplir nuevas funciones o para mejorar su seguridad. El concepto de control del fabricante es fundamental para entender su responsabilidad derivada del aprendizaje continuado del producto. Considerando, por tanto, que el producto sigue en el ámbito de control del fabricante, el carácter defectuoso del producto con elementos digitales que integra inteligencia artificial deberá valorarse cuando el producto se emancipe de dicho control del fabricante.

---

24 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 (DOUE núm. L 119/1, de 4 de mayo de 2016). Art. 4.4): "*«elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

25 PRABHAKAR, Tarunima, "A new Era for Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending", puede consultarse en: *https://cltc.berkeley.edu/wp-content/uploads/2020/06/A_New_Era_for_Credit_Scoring.pdf*. El uso de datos alternativos a los tradicionales para evaluar la solvencia ha supuesto el incremento del tipo de interés para los colectivos discriminados.

El aprendizaje continuado del producto también es una circunstancia que afecta al período de responsabilidad del fabricante. El art. 17.1 DRP dice que la responsabilidad del fabricante se extiende por un período a contar desde los diez años de la introducción en el mercado o puesta en servicio del producto. El inicio del *dies a quo* del plazo de responsabilidad del fabricante que prevé el art. 17.1 DRP casa mal con los productos con elementos digitales que funcionan con inteligencia artificial, que siguen bajo el ámbito de control del fabricante después de su primera introducción en el mercado o puesta en servicio, que se actualizan periódicamente y que son capaces de aprender después del despliegue. Por este motivo, se propone una interpretación del art. 17.1 DRP en relación con el art. 7.2.e) DRP, para que el plazo de responsabilidad del fabricante comience cuando el producto sale del ámbito de control del fabricante. En caso contrario, a pesar de que el RIA imponga al proveedor la supervisión del sistema de inteligencia artificial durante toda la vida útil del sistema, la responsabilidad del fabricante por los daños causados por el producto que incorpora inteligencia artificial quedaría limitada a los diez años desde la introducción en el mercado o la puesta en servicio del producto, prescindiendo del hecho que el producto puede ser defectuoso como consecuencia del aprendizaje continuado más allá del plazo de diez años.

El aprendizaje continuado del producto y, por consiguiente, la defectuosidad del producto por esta causa puede tener distintas manifestaciones. En primer lugar, el aprendizaje continuado debe servir para corregir errores del producto o para que este adquiera nuevas propiedades o que cumpla nuevas funciones. En segundo lugar, el aprendizaje continuado también puede desplegar sus efectos en la seguridad del producto, ofreciendo una mayor resistencia del producto frente a ataques malintencionados de terceros y, en tercer lugar, el aprendizaje continuado también debe servir para corregir los sesgos existentes en los datos almacenados en el producto que constituyen la base para la toma de sus decisiones. Habida cuenta de la incidencia de la inteligencia artificial en el funcionamiento de los productos con elementos digitales y la capacidad dañina de estos productos, se aboga por una interpretación extensiva de la causa de defectuosidad del aprendizaje continuado, para que comprenda las múltiples vertientes susceptibles de manifestarse sus efectos.

VI. BIBLIOGRAFÍA

ABBOTT, Ryan, *The Reasonable Robot*, Cambridge University Press, 2020, Londres.

BECKERS, Anna, y TEUBNER, Gunther., *Three Liability Regimes for Artificial Intelligence,* Hart, London, 2021, pp. 71-84.

BAMSHAD, Mobasher, BURKE, Robin y BHAUMIK, Runa, "Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness", *ACM Transactions on Internet Technology*, vol. 7, núm. 4, pp. 23-38.

BARRENO, Marco, NELSON, Blaine y JOSEPH, Anthony. D., "The security of machine learning", *Mach Learn*, núm. 81, 2010, pp. 121-148.

BORGHETTI, Jean-Sébastien, "Taking EU Product Liability Law Seriously: How Can Product Liability Directive Effectively Contribute to Consumer Protection", *French Journal of Legal Policy*, núm. 1, 2023, pp. 1-41.

CHAGAL-FEDERKORN, Karni A, "Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers", en *Stanford Law & Policy Review*, vol. 30, núm. 61, 2019, pp. 61-114.

CHIARA, Pier Giorgio, "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements," *International Cybersecurity Law Review*, No. 3, 2022, pp. 255-272.

COMISIÓN EUROPEA, Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, 28.9.2022. CM(2022) 495 final. 2022/0302(COD).

CONSEJO DE LA UNIÓN EUROPEA, Proposal for a Directive of the European Parliament and of the Council on liability for defective products–Letter sent to the European Parliament, Bruselas, 24 de enero de 2024.

CORMEN, Thomas H., *Algorithms Unlocked*, MIT Press, Londres, 2013.

DESAI, Deven R., y KROLL, Joshua A., "Trust but Verify: A Guide to Algorithms and the Law", *Harward Journal of Law & Technology*, núm. 31, 2017, pp. 1-64.

FUWEI, Li, LIFENG, Lai y SHUGUANG, Cui, *Machine Learning Algorithms Adversarial Robustness in Signal Processing*, Springer, 2022.

GOODFELLOW, Ian J., SHLENS, Jonathon y SZEGEDY, Christian, "Explaining and Harnessing Adversarial Examples", en *Proceedings of International Conference on Learning Representations*, San Diego, 2015, pp. 1-11.

GOODFELLOW, Ian J., McDaniel, Patrick y PAPERNOT, Nicolas, "Making Machine Learning Robust Against Adversarial Inputs", en *Communications of the AC*, vol. 61, núm. 7, 2018, pp. 56-68.

HUBERMAN, Pinchas, "Tort Law, Corrective Justice and the Problem of Autonomous-machine-Caused Harm", *Canadian Journal of Law & Jurisprudence*, núm. 1, 2021, pp. 105-147.

KURAKIN, Alexey, GOODFELLOW, Ian J., y BENGIO, Samy, *Proceedings of International Conference on Learning Representations*, Toulon 2017, pp. 1-14.

NOEL, Nick, PINDER, Duwain, STEWART, Shelley y WRIGHT, Jason, "The economic impact of closing the racial wealth gap", puede consultarse en: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20economic%20impact%20of%20closing%20the%20racial%20wealth%20gap/the-economic-impact-of-closing-the-racial-wealth-gap-final.pdf.

PRABHAKAR, Tarunima, "A new Era for Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending", puede consultarse en: https://cltc.berkeley.edu/wp-content/uploads/2020/06/A_New_Era_for_Credit_Scoring.pdf.

PARLAMENTO EUROPEO, European Parliament legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).

PARLAMENTO EUROPEO, European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)).

REPORT FROM THE EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, Liability for Artificial Intelligence and Other Emerging Digital Technologies, Luxemburgo, 2019, pp. 1-70.

RICE, Lisa, y SWESNIK, Deidre, "Discriminatory Effects of Credit Scoring on Communities of Color", *Suffolk University Law Review*, núm. 935, 2013, pp. 936-966.

SCHMITZ, Sandra y SCHIFFNER, Stefan, "Responsible Vulnerability Disclosure under the NIS 2.0 Proposal," disponible en https://www.jipitec.eu/issues/jipitec-12-5-2021/5495/schmitz_schiffner_pdf.pdf (consulta realizada en fecha 15 de marzo de 2024).

STAPLETON, Jane, *Product Liability*, Butterworths, 1994.

SURDEN, Harry, "Machine Learning and Law", *Washington Law Review*, núm. 89, 2014, p. 87-115.

VALLOR, Shannon y BEKEY, George A., "Artificial Intelligence and the Ethics of Self-Learning Robots", LIN, Patrick., ABNEY, Keith y JENKINS, Ryan (eds.), *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, Oxford University Press, 2017, pp. 338-353.

WAGNER, Gerhard, "Liability Rules for the Digital Age", *Journal of European Tort Law*, vol. 13, no. 3, 2022, pp. 191-243.

WANDEHORST, Christiane, "Safety and Liability Related Aspects of Software", European Comission, Luxemburgo, 2021, pp. 1-99.