EL MARCO DE SEGURIDAD EUROPEO Y LA RESPONSABILIDAD CIVIL POR PRODUCTOS DIGITALES

CIVIL LIABILITY FOR DIGITAL PRODUCTS: THE ROL OF THE EUROPEAN SECURITY FRAMEWORK

José Carlos Hernández-Zuluaga[*]

RESUMEN: Cada vez más productos incorporan tecnologías digitales. La mayoría de las veces ello aumenta su seguridad, eficacia y funcionalidades. El problema es que la fusión entre productos tradicionales y sistemas de información tiene consecuencias jurídicas derivadas de los aspectos técnicos involucrados en su uso y desarrollo. El *software*, las redes de información y los dispositivos informáticos requeridos para recibir, almacenar, recuperar y analizar los datos con los que estos bienes funcionan, crean riesgos adicionales y afectan la capacidad de las víctimas para reclamar una indemnización. Las nuevas circunstancias han motivado la adecuación de las normas europeas sobre responsabilidad civil a las necesidades de la era digital. Esta adaptación se ha llevado a cabo considerando la estrecha relación que existe entre aquellas y las normas de seguridad aplicable a los productos. La Unión Europea cuenta con un robusto marco de seguridad que es consecuencia de una tradición proteccionista de los derechos y el mercado, el cual establece exigentes estándares que los actores económicos deben cumplir antes y después de la comercialización de sus mercancías. La nueva Directiva de Responsabilidad por Productos Defectuosos reconoce de manera expresa el papel que cumplen estos estándares de seguridad para la atribución de responsabilidad, dictando algunas consecuencias que están asociadas con su incumplimiento. En otros casos estas consecuencias no figuran de forma expresa, pero es posible identificar como la interacción entre ambos grupos de normas contribuye a superar algunos de los desafíos propuestos por las características de los productos digitales para la adecuada atribución de los perjuicios.

[*] Investigador. Instituto de Derecho Privado Europeo y Comparado. Universidad de Girona. Correo electrónico: josecarlos.hernandez@udg.edu

Palabras clave: responsabilidad por productos, normas de seguridad, responsabilidad civil, IA, defecto.

Abstract: The integration of digital technologies into products is becoming increasingly prevalent. In most cases, this enhances their safety, effectiveness, and functionalities. However, the fusion between traditional products and information systems has legal consequences stemming from the technical aspects involved in their use and development. The software, information networks, and computing devices required to receive, store, retrieve, and analyze the data with which these goods operate create additional risks and affect the ability of victims to claim compensation. In light of the evolving landscape, there has been a call for the adaptation of European civil liability regulations to align with the demands of the digital era. This adaptation process has considered the intertwined nature between these regulations and product safety standards. The European Union (EU) has a robust safety framework that has developed over time through a combination of protective traditions, including a strong rights-based tradition and a market-driven approach to regulation. This framework sets high standards that economic actors must meet before and after the marketing of their goods. The new Product Liability Directive explicitly recognizes the role that these safety standards play in attributing liability, dictating some consequences associated with non-compliance. In other cases, these consequences are not explicitly stated, but it is possible to identify how the interaction between both sets of norms helps to overcome some of the challenges posed by the characteristics of digital products for the proper attribution of damages.

Keywords: products liability, safety legislation, torts liability, AI, defectiveness.

Introducción

Los sistemas digitales han modificado los productos del mercado. El empleo de información para su funcionamiento los ha dotado de un nuevo carácter que se expresa con mejoras sustanciales en el desempeño de las tareas que con ellos se ejecutan. Automatización, autonomía y eficiencia energética son algunas de las cualidades que se evidencian al analizar esta nueva generación de dispositivos.

En los últimos años esta evolución ha trascendido de la esfera industrial a la jurídica. Así se confirma con una lectura superficial de la definición de producto que plantea la directiva 85/374/EC sobre responsabilidad por productos

defectuosos[1] (la anterior directiva de productos) y la que trae la nueva Directiva sobre Responsabilidad por Productos Defectuosos (DRPD)[2]. La primera lo define como un bien mueble (art. 2): sus referencias a productos agrarios u objetos tangibles descubren su perfil más primitivo de una época industrial y mecánica. Por su parte, la DRPD toma esta base y le suma los elementos que han dado lugar a la revolución digital: *software*, archivos de fabricación digital y componentes intangibles como la información y los datos adecúan la norma a la realidad social y económica.

Un enfoque de este tipo amplía de forma considerable la responsabilidad del fabricante. Ahora, este es responsable por las conexiones automáticas o los cálculos abstractos que el dispositivo puede hacer sin haber sido determinado para ello. Los productos ya no funcionan como objetos aislados ni responden solo a órdenes humanas. El fabricante hoy responde por las condiciones del entorno donde se utiliza su producto y por los servicios que este requiere para funcionar. En síntesis, la responsabilidad por defecto adquiere una nueva dimensión cuando se le suman otros elementos que dotan a los dispositivos de inteligencia o autonomía.

Puesto en esta situación, el fabricante espera contar con normas que orienten sus esfuerzos hacia la prevención de los daños. Guías de este tipo repercuten no solo en el proceso de fabricación sino en la seguridad del usuario, quien espera contar con instrucciones apropiadas. Con la formulación de reglas de juego claras para el diseño, producción y uso de los productos digitales, las autoridades ejercen un mejor control y se aumenta la percepción general de seguridad en beneficio de la confianza en el mercado. En este sentido, las normas de seguridad constituyen un valioso instrumento para favorecer el desarrollo tecnológico, proteger los derechos y optimizar las actuaciones públicas.

A pesar de todo, el análisis de la responsabilidad civil por productos defectuosos puede pasar por alto el impacto que allí tienen las normas de seguridad. El objetivo de este artículo es presentar los vínculos entre ambos grupos normativos en el ámbito de los *productos digitales*, *i.e.*, aquellos que utilizan sistemas de información para su funcionamiento. En un entorno de creciente complejidad como el digital, la responsabilidad se apoya en las normas de seguridad, generando múltiples efectos por el incumplimiento de sus disposiciones.

Para desarrollar esta idea estimo conveniente comenzar por las nuevas normas de responsabilidad civil europeas, *i.e.*, la Propuesta de Directiva sobre

[1] Consejo Europeo (1985).

[2] A la fecha de presentación de este escrito, el Parlamento Europeo había aprobado, en sesión del 12 de marzo de 2024, el texto de la Propuesta de Directiva sobre Responsabilidad por Productos Defectuosos. Aquí se tiene en cuenta el texto de la propuesta aprobada que está pendiente de trámite legislativo. Comisión Europea (2022a).

Responsabilidad en Materia de Inteligencia Artificial (PD-RCIA)[3] y la nueva DRPD, así como las remisiones que estas hacen al marco europeo de seguridad. Allí queda en evidencia la relevancia del marco de seguridad de los productos para la responsabilidad por los daños que estos causan. Un ejemplo de ello son las presunciones *iuris tantum* que surgen por el incumplimiento de normas de seguridad tendientes a proteger contra el daño que se ha causado.

Establecido lo anterior, presentaré una panorámica del marco legislativo de seguridad europeo: sus antecedentes, política y elementos que permiten controlar la seguridad de los productos. La idea es que, al comprender su compleja arquitectura, se facilita el examen de los efectos en la responsabilidad por el incumplimiento de las normas de seguridad. Esta presentación incluye la transición desde el "antiguo" al "nuevo enfoque"; el Nuevo Marco Legislativo de Seguridad (NML) y algunas de sus principales instituciones *e.g.* la vigilancia del mercado, los operadores económicos o los organismos europeos de normalización.

En la tercera parte describiré los desafíos que ha enfrentado el legislador europeo para adecuar el marco de seguridad a las circunstancias digitales. Esta nueva generación de productos incorpora componentes y posee funcionalidades que el marco de seguridad no habría podido prever. La descripción tendrá en cuenta los tres elementos que componen un producto digital: programa informático, equipo informático y procesos de información. Cada uno de ellos posee características técnicas que pueden afectar el nivel de riesgo o la capacidad de los perjudicados para obtener compensación.

Para finalizar presentaré algunas conclusiones del análisis efectuado.

I. Las relaciones entre las disposiciones sobre responsabilidad civil y las normas de seguridad

1. Aspectos generales de las normas de responsabilidad

La PD-RCIA y la nueva DRPD son la respuesta de la Unión Europea (UE) a las demandas de actualización legislativa por la irrupción tecnológica.

A. PD-RCIA

La PD-RCIA armoniza las reglas probatorias cuando un sistema de inteligencia artificial (IA) de *alto riesgo* causa daño (art. 1). La armonización consiste, por

[3] Comisión Europea (2022b).

un lado, en desarrollar flexibilizaciones probatorias dirigidas a la exhibición de información de parte del demandado y, por el otro, a la aplicación de presunciones *iuris tantum* sobre la culpa del demandado y la relación causal de su negligencia con el hecho de la máquina que causó el daño. Estas flexibilizaciones se justifican en las dificultades que afronta la víctima de IA para demostrar que el demandado le causó daño por su negligencia, en comparación con las víctimas en otros casos. En esencia, la propuesta se propone superar los obstáculos que proponen algunas características de la IA como: la opacidad, la autonomía o la complejidad del sistema, todas las cuales empañan el vínculo entre la conducta del demandado y el hecho de la máquina.

Según veremos, por tratarse de una directiva de mínima armonización, el objetivo de la PD-RCIA es que, por lo menos, cuando de IA de alto riesgo se trate, los países acojan los auxilios probatorios allí descritos. Lo anterior no quiere decir, ni que los países no apliquen tales remedios, ni que se les prohíba adoptar mejores garantías para las víctimas. De acuerdo con el texto, se trata de alcanzar una base común europea para promover las garantías mínimas pretendidas.

B. La DRPD

Por su parte, la DRPD es un régimen mucho más amplio, que armoniza la responsabilidad por *todo tipo de productos* –incluida IA– cuando ciertos intereses protegidos, reclamados por *personas físicas* (art. 1), resulten afectados a consecuencia de un defecto del producto.

Sobre la eficacia de la anterior directiva se ha discutido mucho. La posición oficial es que ha sido un instrumento que ha favorecido la armonización de las normas y la protección del consumidor[4]. Por el contrario, algún sector de la doctrina ha señalado su inutilidad práctica; pidiendo, incluso, su erradicación del ordenamiento europeo[5]. Lo cierto es que han transcurrido casi cuarenta años desde su emisión y durante este tiempo se ha publicado una gran cantidad de artículos doctrinales, cuyo número contrasta con un escaso desarrollo jurisprudencial. Debido a la amplitud de su objeto y la tendencia hacia la automatización de las actividades humanas, parece que la nueva DRPD le podría dar un nuevo aire a este régimen.

2. La PD-RCIA y su relación con las normas de seguridad

Al analizar su objetivo y alcance es posible concluir que lo pretendido con la PD-RCIA es permear los sistemas jurídicos de todos los países de la UE. Su

[4] Comisión Europea (2018).

[5] Borghetti (2023) pp. 136-181.

finalidad es nada menos que la culpa, que es el régimen de fondo de cualquier sistema jurídico de tradición europea. Así, la propuesta llenaría el vacío que dejan otros regímenes de responsabilidad, en especial la DRPD, en ámbitos como el tipo de víctima o el daño causado. Contrario a esta, que insiste en proteger solo a las personas naturales y se cierra ante la protección de algunos intereses protegidos, la PD-RCIA permite que personas jurídicas, no consumidores y los daños patrimoniales puros puedan ser exigidos por la vía de la negligencia.

En ese esfuerzo, la PD-RCIA se plantea reglas probatorias sin inmiscuirse en las concepciones nacionales de la culpa. Se trata de una norma con efectos prácticos que evade las discusiones que suscitaría una decisión legislativa sobre el significado de la culpa en Europa[6].

A. La definición del deber de diligencia

Para entrar en materia, debe decirse que, a pesar de no tomar partido por un concepto de culpa, la norma sí define en qué consiste el *deber de diligencia* que ha de cumplir el demandado. Según el texto, la diligencia se relaciona con: "aquella norma de conducta establecida por el Derecho nacional o de la Unión con el fin de evitar daños [...]". De entrada, parece que esta definición adscribe la culpa al incumplimiento de un deber que puede estar contenido en una norma de seguridad, al señalar como estándar una norma de protección. Se debe advertir que con ello no le señala al tribunal nacional que tal incumplimiento es *per se* culpa; puede ser que la concepción nacional requiera un juicio adicional, por ejemplo, de la condición del infractor.

B. El deber de exhibición y su relación con la Ley de IA

Pasando al aspecto central de la norma, la PD-RCIA señala dos tipos de flexibilizaciones probatorias cuando la IA de *alto riesgo* causa daño[7]:

i) los deberes de exhibición de información (art. 3)[8] y
ii) las presunciones, *iuris tantum*, de culpa o causalidad.

[6] Para un importante análisis de las diferencias conceptuales de la culpa en distintos países de Europa y Estados Unidos, véase Institute for European Tort Law, Winiger, Karner & Olphant (2018).

[7] Como excepción, el art. 4-5 de la PD-RCIA deja abierta la posibilidad de aplicar la *presunción de causalidad* en sistemas de IA de riesgo no elevado cuando: "el órgano jurisdiccional considere excesivamente difícil para el demandante demostrar el nexo causal mencionado en el apartado 1". Sin embargo, la ventaja no se extiende a la exhibición de información del art. 3.

[8] Este artículo señala el deber condicionado de exhibición, cuyo incumplimiento desemboca en una presunción de culpa: "Los Estados miembros velarán por que los órganos jurisdiccionales nacionales estén facultados, ya sea a petición de un demandante potencial que haya solicitado

Sobre el deber de exhibición, considerado en algunos países como un derecho al acceso y conservación de la prueba, la PD-RCIA señala que a ello están obligados los usuarios y quienes de acuerdo con la Ley de IA[9] deban cumplir *deberes del proveedor*[10] en los sistemas de IA de alto riesgo[11] (art. 3-1). Es decir, no es necesario hacer profundas reflexiones para notar que la PD-RCIA depende, en gran medida, de normas de seguridad, en especial de la Ley de IA. Así se advierte de la remisión que a ella hace para descubrir quién es el sujeto obligado a los deberes del proveedor y cuáles son los tipos de IA de alto riesgo. Todo esto conduce a revisar en una acción de responsabilidad, por ejemplo, si la Comisión ha modificado el listado[12] de la IA considerada como de alto riesgo[13].

previamente a un proveedor [...], o a un usuario, que exhiba las pruebas pertinentes que obran en su poder sobre un determinado sistema de IA de alto riesgo que se sospeche que ha causado daños [...]".

[9] El 12 de junio de 2024 el documento final del Reglamento de Inteligencia Artificial había sido aprobado y firmado por los presidentes del Parlamento Europeo y del Consejo. Al momento de la aceptación de este artículo el texto final del reglamento estaba pendiente de publicación en el *Diario Oficial*. Comisión Europea. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados Actos Legislativos de la Unión. 2021/0106 (COD)., Pub. L. No. COM (2021) 206 final (2021). En adelante Ley de IA.

[10] El art. 25 de la Ley de IA dispone que también: "cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de alto riesgo a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor [...]" bajo ciertas condiciones. Con intención enunciativa es posible citar tres condiciones: i. si pone su nombre o marca; ii. si modifica sustancialmente un sistema de IA de alto riesgo o iii. si modifica la finalidad prevista.

[11] El art. 3 de la PD-RCIA señala en todo caso que el potencial demandante deberá presentar hechos y pruebas suficientes para sustentar la viabilidad de una demanda de indemnización. Por tanto, debe existir una causa probable en favor del demandante para proteger a los obligados de asumir el costo de peticiones abusivas.

[12] Nótese que de acuerdo con el art. 7 de la Ley de IA, la categoría de sistemas de alto riesgo está abierta a ajustes. En otros casos se establecen remisiones, por ejemplo, en el art. 10 sobre la gobernanza y gestión de los datos utilizados por IA que implica el estudio de normas como el Reglamento (UE) 2016/679 sobre Protección de Datos Personales (RGPD). Lo anterior sugiere un deber de evaluación permanente de las normas de seguridad a efectos de una demanda de responsabilidad.

[13] La versión final (16 de junio de 2024) de la Ley de IA la define como: "un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales" (art. 3-1). Por su parte, el art. 6 plantea dos grupos de sistemas de IA que se pueden clasificar como de alto riesgo: i. la IA utilizada como componente de seguridad de un

Una vez definido el obligado, es preciso advertir que la finalidad de la exhibición es disminuir la asimetría de los involucrados en el acceso a la información. La norma parte del hecho de que la víctima está a merced del profesional, quien sí está sometido a expectativas normativas. La PD-RCIA, incluso, especifica que el sentido de la exhibición es verificar que el demandado ha cumplido las normas de seguridad a su cargo, en cuestiones como la documentación, información y registro de la información (C. 16)[14]. Lo anterior ha permitido sugerir que la relación entre normas de seguridad y responsabilidad civil puede incentivar el cumplimiento de los deberes legales[15]. Visto desde otra perspectiva, la exhibición también le permitiría a la víctima determinar si el demandado cumplió con su deber y, por tanto, con la norma dirigida a proteger el interés jurídico que reclama. La prueba del incumplimiento, en el contexto de la PD-RCIA, constituye el primer escalón para configurar su responsabilidad. De allí que el conocimiento, cumplimiento y documentación de las medidas de seguridad sean un aspecto crucial en la actividad del fabricante o usuario de IA de alto riesgo[16].

C. Las presunciones *iuris tantum* y los deberes de diligencia

El segundo bloque de flexibilizaciones probatorias está compuesto por presunciones *iuris tantum* de culpa y causalidad. La primera presunción emerge cuando el demandando desatiende la orden judicial de exhibición de las pruebas (art. 3-5). Sin embargo, la presunción no llega hasta la culpa; lo que ordena presumir la PD-RCIA es el incumplimiento de un "deber de diligencia pertinente" (art. 3-5), que, a su vez, puede constituir culpa según la concepción que sobre esta tenga el tribunal correspondiente. Si, por el contrario, se da cumplimiento a la orden, el demandante retiene la carga de la prueba.

La presunción de causalidad, por su parte, opera en la relación culpa del demandado y hecho de la IA. Es decir, no procede la presunción de causalidad entre el hecho de la IA y el daño; la prueba de que la IA lesionó a la víctima si-

producto regulado por las normas descritas en el Anexo I y ii. el sistema incluido en el anexo III por considerarse un riesgo para la salud, la seguridad o los derechos fundamentales de las personas físicas.

[14] Art. 11 y ss. de la Ley de IA.

[15] Martin-Casals (2023) p. 72.

[16] El art. 4-3 de la PD-RCIA señala: "En caso de demandas por daños y perjuicios contra usuarios de sistemas de IA de alto riesgo sujetos a los requisitos establecidos en los capítulos 2 y 3 del título III de la Ley de IA, la condición del apartado 1, letra a) [se debe demostrar una culpa del demandado, el incumplimiento de un deber de diligencia] se cumplirá cuando el demandante demuestre que el usuario [...]" no cumplió con los deberes impuestos por la Ley de IA (a), o expuso el sistema a datos de entrada bajo su control.

gue a cargo del demandante. Si este pretende beneficiarse de la antedicha presunción, el primer requisito que le exige la propuesta es que demuestre que el demandado incurrió en negligencia. Pero no cualquier culpa, una que se justifique en la infracción de un deber de diligencia que tenía por finalidad *directa* prevenir el daño que la IA ha causado (art. 4-1 a). Según esto, el interesado debe constatar la infracción del deber calificado como condición necesaria para configurar la culpa[17]. Como resultado, la propuesta vincula el desarrollo legislativo en seguridad a la configuración de las presunciones[18].

Más específico resulta el numeral 2 del art. 4 sobre sistemas de alto riesgo. Allí, la presunción de causalidad requiere que la culpa verse sobre una infracción a las prescripciones de la Ley de IA[19]. A pesar de la remisión casi taxativa, un análisis desde el marco de seguridad señalará un universo normativo paralelo a cuestiones como la gobernanza de los datos, la documentación o la ciberseguridad. Sin lugar a duda, en la presunción de causalidad de los sistemas de alto riesgo se aprecia mejor la relación entre marco de seguridad y la responsabilidad civil.

3. *La Propuesta de Directiva de Responsabilidad por Productos Defectuosos*

A. Las definiciones adoptadas: el caso de los operadores económicos

La relación de la DRPD con las disposiciones de seguridad es igual o más estrecha que la anterior. De entrada, la norma señala que su objetivo es plantear normas comunes sobre la responsabilidad de los *operadores económicos,* por los daños sufridos por personas físicas y causados con productos defectuosos (art. 1). Allí, la norma no se refiere al *productor,* como lo hacía en la anterior directiva

[17] Esta técnica regulatoria se aproxima al concepto de *Schutzgesetz* del derecho alemán. Así, Ulrich Magnus, en una explicación del § 823-2 del *Código Civil* alemán (*BGB*), indica que allí la atribución: "no requiere de la vulneración de un derecho subjetivo absoluto de la víctima, sino de la violación de un interés estatutario diseñado para proteger a la víctima de los daños que ocurrieron (Schutznorm o Schutzgesetz)" Danneman & Schulze (2020) vol. I p. 1609.

[18] De ello no se infiere que la única forma de probar la infracción del deber es demostrar la vulneración de una norma de seguridad. La intención es señalar que, con la vinculación de este marco, muchas de ellas servirán para establecer el vínculo entre incumplimiento y culpa. Perspectiva que apuntaría a disminuir la discrecionalidad judicial en países con cláusula general de responsabilidad.

[19] La norma señala que la culpa, que es condición necesaria para presumir la causalidad (art. 4-1), *solo se cumplirá*, si el demandante demuestra la infracción de cualquiera de los requisitos listados en el art. 4-2. Este "solo se cumplirá" parece determinante para señalar el incumplimiento relevante a efectos del daño causado.

(art. 3), sino a los *operadores económicos*; concepto que se originó en la decisión n.° 768/2008/CE (anexo I, art. R1-7), que es uno de los pilares del NML. En el concepto de operadores económicos está agrupado: el *fabricante*[20], el importador, el representante autorizado, el distribuidor y el proveedor de servicios logísticos –llamado por la DRPD prestador de servicios de tramitación de pedidos a distancia– (art. 4-15).

De la participación de estos sujetos en la responsabilidad por productos se resalta el nuevo papel del prestador de servicios de tramitación de pedidos a distancia (art. 4-13), que es quien ejecuta algunas actividades comerciales como el embalaje, el almacenamiento o el envío de los productos al consumidor. La DRPD lo hace responsable en ausencia de fabricante, importador o representante autorizado en la Unión (art. 8-1c). En la práctica, esta figura se asocia con plataformas virtuales que, aunque presta tales servicios, al mismo tiempo puede ser el fabricante o distribuidor del producto; todo depende del modelo económico que adopte.

B. La defectuosidad y las normas de seguridad

La DRPD también se vincula con las normas de seguridad al enunciar que la defectuosidad del producto equivale a la *falta de seguridad* que una persona tiene derecho a esperar y "que se *exige asimismo en virtud del Derecho de la Unión o nacional*" (art. 7-1). Una novedad de este tipo para definir la defectuosidad, más que una simple aclaración, sugiere la decisión política de poner al servicio de la responsabilidad la maquinaria administrativa empleada para la seguridad de los productos. Estos esfuerzos legislativos, en principio encaminados a la prevención de los daños, se convierten en estándares de seguridad que ayudan a definir la defectuosidad de los productos.

Las nuevas referencias al marco de seguridad van más allá. A diferencia de su antecesora[21], la DRPD especifica que al evaluar el carácter defectuoso de un producto también se deben constatar los *requisitos de seguridad pertinentes* (art. 7f), entendidos estos como las exigencias impuestas por el marco de seguridad. Incluso, ordena valorar *cualquier intervención pertinente* de una autoridad o de algún otro operador económico. Esto, según se verá, señala a las actuaciones oficiales que derivan de las competencias otorgadas por el reglamento 2008/768/CE en materia de vigilancia del mercado.

[20] Nótese que el *productor* de la DRPD es llamado ahora *fabricante*.

[21] En el art. 6 la anterior directiva señalaba: 1. Un producto es defectuoso cuando no ofrece la seguridad a la que una persona tiene legítimamente Derecho, teniendo en cuenta todas las circunstancias, incluso: a) la presentación del producto; b) el uso que razonablemente pudiera esperarse del producto; c) el momento en que el producto se puso en circulación.

C. Las remisiones normativas: la modificación sustancial del producto

Una situación que ilustra como las normas de seguridad definen responsabilidades en el campo de los productos es el de su modificación sustancial. De acuerdo con la DRPD, una vez puesto en circulación no se podrá alterar el diseño del producto; quien así lo haga, con el objetivo de comercializarlo o ponerlo en funcionamiento, responderá como si se tratara del fabricante (art. 8-2). Conocer cuándo ha ocurrido un cambio de este tipo exige conocer la legislación aplicable al producto correspondiente, la DRPD señala:

> "El carácter sustancial de una modificación debe determinarse de acuerdo con los criterios establecidos en la legislación pertinente de la Unión y nacional en materia de seguridad de los productos" (C. 39).

D. Las flexibilizaciones probatorias y las normas de seguridad

En lo referente a las pruebas, la DRPD incorpora un deber de exhibición en doble vía, que también compromete al usuario-víctima cuando incumpla normas de seguridad a su cargo. Al igual que se explicó para la PD-RCIA, la petición de información obliga al *demandado* a divulgar, aquí sí de forma *accesible* y *comprensible*, las pruebas pertinentes de que disponga (art. 9). Sin embargo, a diferencia de aquella, la exhibición opera, también, en contra del demandante-víctima, quien deberá hacer lo propio. Pues bien, si se trata de un usuario sometido a expectativas legales, por ejemplo, quien utiliza un producto que informe la necesidad de contar con algún nivel de formación para operarlo, la infracción de esta expectativa posibilitaría que el *demandado* refute las presunciones a su cargo (art. 10-5) o que demuestre la culpa exclusiva de la víctima. Como resultado, el conocimiento y cumplimiento de las normas de seguridad, tanto de parte del operador económico como del usuario, resultan fundamentales para atender a los efectos de las presunciones.

La DRPD consagra, también, una *presunción de defectuosidad* que opera cuando el demandante demuestre que el producto:

> "no cumple los requisitos obligatorios de seguridad del producto establecidos por el Derecho de la Unión o en el Derecho nacional que tienen por objeto proteger contra el riesgo del daño sufrido por la persona perjudicada" (art. 10-2).

Esta disposición, de similar contenido a la analizada en la PD-RCIA, permite al tribunal "basar la existencia de un defecto o de un nexo causal en la presencia de otro hecho probado" (C. 46). Como se advierte, también en el ámbito de la presunción de defectuosidad, el marco de seguridad cumple un papel fundamental.

Finalmente, el texto de la DRPD señala que el tribunal puede presumir la defectuosidad y el nexo causal cuando: "[…] considere que el demandante se enfrenta a dificultades excesivas, debido a una complejidad técnica o científica […]". La naturaleza de tales "dificultades" se pueden identificar apelando al contenido de ciertas normas de seguridad. Es el caso de la Ley de IA, que explica muchas de las características de estos sistemas, su nivel de riesgo o los métodos que emplean. Así, también se verifica, por ejemplo, de la base europea de productos sanitarios "Eudamed" creada por el reglamento (UE) 2016/745 sobre productos sanitarios (art. 33), cuyo contenido debe relacionar cuestiones como las investigaciones clínicas o el registro de los dispositivos.

4. Conclusiones preliminares

De todo lo anterior se concluye que existe una íntima relación entre normas de seguridad y las disposiciones que rigen la responsabilidad civil por los productos. Así lo evidencia el análisis de la PD-RCIA y la DRPD, que entre otras cosas plantea:

> "Se han adoptado numerosos requisitos de seguridad obligatorios para proteger […] [y que tienen] el fin de reforzar la estrecha relación existente entre las normas de seguridad de los productos y las normas de responsabilidad […]" (C. 46).

Relación que, por lo antes sostenido, exige el análisis de las normas de seguridad en varios niveles. Así se evidencia de la relación entre deberes de exhibición y normas de seguridad y de los requisitos con que se configuran las presunciones. En síntesis, tanto la DRPD como la PD-RCIA son normas que comparten muchos criterios, uno de los principales: su interés por vincular el marco de seguridad a la responsabilidad civil.

Establecida la relación entre ambos grupos de normas, describiré la naturaleza de las normas de seguridad, los antecedentes de la estrategia europea con la transición del antiguo al nuevo enfoque y, por último, el NML.

II. El concepto de norma de seguridad y los modelos regulatorios de mercado

1. Concepto y características de las normas de seguridad sobre productos

Como cualquier otra norma jurídica, las de seguridad prescriben comportamientos y sanciones y se relacionan con otras normas para establecer parámetros de

conducta[22]. Con todo, las normas de seguridad en el contexto europeo tienen ciertas particularidades que definen su carácter y determinan sus especiales efectos.

A. Son normas formuladas en interés general:
persiguen la protección de la salud,
vida y seguridad de las personas

Las normas de seguridad protegen intereses de carácter general, o lo que es lo mismo, no están diseñadas con fines particulares. Tal interés público las relaciona con políticas de mercado de igual naturaleza que, para el caso de los productos, definen estándares de protección para intereses supremos como la vida o la salud. Por esto, es preciso descartar la idea de que las normas de seguridad pueden o deben intervenir en la protección de la mayor cantidad de derechos posibles. Dado que, por lo general, contemplan mandatos o prohibiciones dirigidos a la industria, deben atender a un diseño cuidadoso para no generar restricciones, burocracia y cargas excesivas que desincentivan la inversión y la innovación.

En el caso europeo, el legislador ha optado por buscar un equilibrio entre la protección de intereses jurídicos de especial relevancia y las restricciones injustificadas al libre comercio. La idea es promover altas expectativas en el cuidado de los intereses individuales y públicos *escogidos*, al tiempo que se otorgan libertades en los demás campos. En específico, los países miembros están comprometidos a proteger la vida, la salud y el ambiente de los ciudadanos, entre otros intereses[23], debiéndose abstener de intervenir en otros ámbitos con el potencial para afectar libertades de mercado. Así, un país no puede denegar la importación de mercancías bajo el pretexto de la protección de la industria local.

Cuando la idea de los intereses protegidos se traslada al ámbito de la responsabilidad, por ejemplo, para sustentar la aplicación de presunciones por infracciones normativas, se advierte como estos *deberes de diligencia* consagrados en normas nacionales o de la Unión deben tener por finalidad la protección de intereses como la vida, integridad y propiedad de las personas físicas. Otros intereses más difusos, *e.g.* los derechos fundamentales a la dignidad o a los datos personales, exigirán un mayor grado de especificación legal para concluir que su incumplimiento generó el daño que se reclama.

El interés público implícito en estas normas es el que faculta a las autoridades competentes para perseguir su infracción. Por ende, las autoridades

[22] Von Bar (1998) p. 26.

[23] La jurisprudencia del TJUE ha dejado abierto el listado de intereses protegidos. Al respecto véase la sentencia Cassis de Dijon explicada en el numeral 3.1(A). Tribunal de Justicia de las Comunidades Europeas (1979).

actúan a petición de cualquier interesado, pero también de oficio. Esto es posible cuando obtienen los medios económicos e institucionales que les permitan ser eficaces. En los últimos años la UE ha promovido la creación de agencias de control en varios ámbitos relacionados con los productos. Muestra de ello son el Comité Europeo de Protección de Datos, la Agencia para la Ciberseguridad (ENISA) y la Oficina Europea de IA.

B. La eficacia del control depende del proceso administrativo sancionador

Las normas de seguridad tienen una finalidad preventiva, que es tan efectiva como el control que sus autoridades ejercen. La promoción de la seguridad exige la aplicación de sanciones disuasorias y en tiempos razonables: los infractores deben percibir la amenaza que deriva del incumplimiento de sus deberes. Esta eficacia, en sociedades democráticas, depende de garantías fundamentales que validen las sanciones. El proceso administrativo sancionador, como vehículo para la eficacia de las normas de seguridad, debe garantizar mínimos fundamentales a los disciplinables.

Estas garantías operan en varios niveles. En un primer nivel, la sanción se debe proyectar sobre el principio de legalidad. Este principio supone la existencia previa de una norma válida y pertinente a la infracción que se imputa. Se trata de una garantía básica que en parte se justifica en la función disuasiva que debe acompañar las normas de seguridad: el infractor debe tener la posibilidad de ajustar su conducta a la expectativa legal. Por consiguiente, la existencia, claridad y correspondencia de la conducta reprochada y la norma son requisitos fundamentales de cualquier control administrativo. La falta de alguno de estos elementos es fuente de conflictos e incertidumbre para los operadores económicos y las autoridades de control. Ello justifica e ilustra algunas razones que motivan los esfuerzos emprendidos por la UE para ir construyendo un marco de seguridad detallado y complejo alrededor de la regulación de los productos. En un segundo nivel, el proceso sancionador debe ser rápido, pero sin lesionar garantías como la presunción de inocencia o la aplicación de sanciones bajo criterios de proporcionalidad, efectividad y equidad. Así, por ejemplo, cuando en 2001 la Directiva General de Seguridad de Productos[24] (DGSP) dispuso por primera vez como sanción el retiro provisional de las mercancías, surgió una controversia alrededor de los derechos que los actores económicos tenían si no se verificaban las infracciones[25]. En tal sentido, la aplicación de sanciones debe ponderar la conveniencia entre protección de *intereses legítimos* y

[24] Parlamento Europeo y el Consejo (2001).

[25] Fairgrieve & Howells (2006) pp. 59-69.

libertades de mercado. Por último, la responsabilidad sancionatoria es personal, lo cual incluye, por supuesto, el hecho de terceros por cuya conducta se responde. Tal responsabilidad individual se relaciona con el principio de legalidad, en el sentido de que la norma debe asignar el titular de la infracción investigada. Tal asignación resulta bastante útil a efectos de la responsabilidad civil, gracias a que la descripción detallada del deber de conducta facilita la atribución del daño. De allí que los estatutos de seguridad permitan construir presunciones a partir del indicio que señala a quien le correspondería, por ley, prevenir el daño que se ha causado. Sin embargo, contrario al ámbito sancionatorio, la responsabilidad civil no exige una conducta personal del demandado. De allí que la responsabilidad por productos canalice al fabricante los efectos del daño, aun si existen dudas sobre el origen del defecto[26].

2. Las opciones regulatorias: extremos de los modelos de mercado y la búsqueda del equilibrio

El planteamiento de la estrategia europea de mercado demanda un breve análisis de las alternativas disponibles. Para ello es posible partir de los modelos tradicionales, que aquí denomino "extremos", los cuales permitirán concluir que cualquier estrategia moderna implica la utilización de elementos de uno y otro. Estos extremos serían: el modelo de corte liberal y el intervencionista[27].

A. Modelo de mercado de corte liberal

El primero es un modelo regulatorio de mercado que protege las libertades individuales y confía en que sus dinámicas, sumadas a puntuales interferencias artificiales, generen un equilibrio entre seguridad y desarrollo científico y tecnológico. Se caracteriza por la confianza que el Estado deposita en los operadores económicos como fuentes de seguridad y bienestar. Esta confianza tiene origen en la creencia de que el interés egoísta de los particulares redunda en provecho de la innovación y el desarrollo social.

El modelo se justifica, en gran parte, en los incentivos económicos que generan las libertades. Por un lado, los actores económicos perciben que la in-

[26] En la anterior directiva, art. 8: "1. Sin perjuicio de las disposiciones de Derecho interno relativas al Derecho a repetir, la responsabilidad del productor no disminuirá cuando el daño haya sido causado conjuntamente por un defecto del producto y por la intervención de un tercero".

[27] Intervencionismo entendido como "sistema intermedio entre el individualismo y el colectivismo, que confía a la acción del Estado el dirigir y suplir la iniciativa privada", véase TRIVIUM (1998) p. 369.

versión en seguridad puede ser fuente de ventaja competitiva en el mercado y llega a ser indispensable para mantener la reputación empresarial. Por el otro, anticipa que la falta de seguridad tiene efectos directos sobre el patrimonio a través de costos de aseguranza, indemnizaciones y multas.

Un paradigma de este modelo es el sistema estadounidense. Allí, las normas federales de seguridad y las intervenciones oficiales son la excepción. Cuando se manifiestan lo hacen en sectores de alto riesgo como los vehículos a motor, los alimentos o los productos farmacéuticos[28]. Por lo demás, las medidas preventivas son voluntarias o provienen de sectores privados especializados; como el Instituto Nacional Estadounidense de Estándares[29]; una entidad privada fundada en 1918, sin ánimo de lucro y cuya principal misión es identificar y desarrollar estándares de calidad y seguridad[30]. Los estándares del ANSI son aplicados por la industria, pero también pueden ser reconocidos por los tribunales en procesos de responsabilidad[31].

La toma de medidas voluntarias en seguridad bajo el modelo estadounidense se explica también en los incentivos que produce la amenaza de costosas indemnizaciones: daños punitivos, carencia de sistemas de seguridad social, altos costos sanitarios y cuantiosos reconocimientos por perjuicios extrapatrimoniales[32]. De allí que se pueda criticar su trasposición a entornos económicos o culturales que no cuenten con las mismas condiciones. Estos incentivos económicos se complementan con altos niveles de competitividad empresarial,

[28] Shapo (2007) pp. 329-353.

[29] Véase www.ansi.org/about/introduction [fecha de consulta: 2 de julio de 2024].

[30] Es importante tener en cuenta que el reglamento (UE) 1025/2012 sobre normalización europea traduce la palabra '*standard*' como 'norma'. Por consiguiente, en el ámbito de la regulación en seguridad de los productos, una norma –*standard*–: "es una especificación técnica adoptada por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria" (art. 2-1). En la misma línea, un *organismo de normalización* –Organization for Standardization– es una entidad privada o agremiación que a petición de la Comisión presenta *especificaciones técnicas* para productos, *i.e.*, las características o métodos de producción aplicables para garantizar la calidad o seguridad de un producto. Cumplido un trámite legal que el reglamento dispone, el estándar se puede convertir en *norma armonizada*. Para evitar la confusión terminológica utilizaré el término "estándar o estándares" de seguridad.

[31] Así lo explican Marc Franklin *et al.* en el asunto Robinson contra G.G.C., Inc., 808 P.2d 522 (Nev. 1991) donde una máquina trituradora lesionó un trabajador. La máquina tenía un dispositivo para evitar este tipo de accidentes, uno que, sin embargo, podía ser removido. ANSI recomendaba que en estos casos se incorporara un bloqueo; cosa que no ocurrió y que sirvió para que el tribunal fallara en favor del lesionado. Franklin (2016) p. 603.

[32] "En algunas jurisdicciones como en EE.UU o Nueva Zelanda, las normas de responsabilidad juegan un rol mayor para complementar las normas de seguridad de carácter público y privado [...]En China, las licencias públicas (llámense certificaciones, licencias, registros o permisos individuales) se requieren para muchos productos o grupos de productos antes de ser introducidos en el mercado". Véase Comisión Europea (2021) p. 7. Amending Regulation (EU).

disponibilidad de servicios jurídicos y sistemas judiciales eficientes[33] que motivan la toma de medidas privadas.

B. Modelo de mercado de corte intervencionista

El otro extremo lo ocupan modelos de corte intervencionista. Sus características son altos niveles de actividad burocrática y sanciones oficiales como incentivo para la seguridad del mercado. El intervencionismo, contrario al modelo liberal, desconfía de la iniciativa privada y se enfoca en la capacidad oficial para controlar la seguridad del mercado. Esta desconfianza genera barreras y produce tensiones con la industria; no obstante, y según las circunstancias, el intervencionismo puede también constituir un buen instrumento de control frente a los excesos de los particulares.

Un modelo de corte intervencionista plantea varios desafíos. En primer lugar, se encuentran los costos asociados a la actividad legislativa y el control oficial. La protección pública demanda grandes cantidades de recursos que se invierten en legisladores especializados, autoridades de control preparadas y medios técnicos.

Por otro lado, la intervención oficial que no es calibrada de forma adecuada puede incidir de forma negativa en las dinámicas del mercado y el ritmo del progreso tecnológico. Es lógico pensar que, a mayores requisitos, autorizaciones y, en general, intervenciones en la actividad privada, menores serán los riesgos que asuman los particulares.

Por último, hay que tener en cuenta que un Estado interventor requiere de un flujo constante de medidas legislativas que reflejen los niveles de control deseados. Además de los recursos económicos que dicha actualización demanda, las dinámicas tecnológicas y del mercado impactan la eficacia normativa, haciendo las leyes obsoletas en poco tiempo. Dado que es imposible anticiparse a los efectos que tendrá el progreso tecnológico, el costo de las actualizaciones normativas se traslada al consumidor en forma de impuestos y costos de producción que encarecen el producto y afectan la oferta y en general el mercado[34].

En suma, el modelo intervencionista es costoso, requiere de una sólida base institucional y supone la permanente actualización y capacitación del legislador y las autoridades de control.

De este breve análisis se concluye que el diseño de una estrategia de seguridad equilibrada constituye un serio desafío social, administrativo, políti-

[33] Howells (1999; 2000) pp. 305-46.

[34] Corones & Clarke (1997).

co y económico. El nivel de intervención oficial escogido impacta el desarrollo tecnológico y los intereses jurídicos que se pretenden proteger. Lo ideal es encontrar un equilibrio entre protección y libertades económicas. Un equilibrio que evite abusos particulares, pero que genere las condiciones para la innovación.

Este ideal supone, entonces, ciertas renuncias. En parte, las correspondientes elecciones se pueden centrar en definir cuáles intereses jurídicos se pretenden proteger con mayor ahínco, así como en la intensidad con que se realizarán las actividades de control. Estas elecciones, se insiste, deben ponderar la influencia positiva del desarrollo tecnológico[35]: en ocasiones estos emprendimientos son socialmente deseables, en especial, porque su finalidad puede contribuir a la protección de los intereses jurídicos que con la intervención se pretenden proteger.

Como se verá a continuación, la UE ha encontrado su propio modelo y ahora se lo está mostrando al mundo.

III. La estrategia europea de seguridad para los productos: antecedentes y características

1. Antecedentes del marco legislativo de seguridad: del antiguo al nuevo enfoque

El actual marco legislativo de seguridad de la UE es producto de la experiencia y el aprendizaje de varias décadas. Un buen punto de referencia para ilustrar tal evolución es el cambio que en la década de 1980 se dio desde el antiguo hacia el nuevo enfoque.

La UE nació y evolucionó sobre el eje de la integración económica. Primero, con la Comunidad Europea del Carbón y del Acero (CECA); luego, con el compromiso político y económico del *mercado común*[36] y la Comunidad Económica Europea (CEE) descrito en el Tratado de Roma (1957). Después, con la introducción, en 1992, de la unión económica y monetaria que

[35] Faure, Goodwin & Weber (2014) pp. 283-364.

[36] Se advierte una transición terminológica asociada al grado de integración del mercado. Desde la eliminación de las barreras arancelarias, hasta el tratamiento del mercado europeo como uno solo. De allí que el término "mercado común" consagrado en el Tratado de Roma (1958) se haya modificado después por el de "mercado interior" o "mercado Único". Este cambio se hizo oficial, primero, con el Acta Única Europea y, luego, con el Tratado de Lisboa (2009) donde ya se eliminaron las referencias al mercado común. Véase Caravaca y Carrascosa (2003) y Weatherill (2017).

originó el euro con el Tratado de Maastricht y, últimamente, mediante la estrategia de mercado único digital europeo (2015). La UE es una empresa en constante evolución.

Aunque los primeros tratados demostraron el potencial de la integración económica, en la década de 1970 se perdió el impulso. Diferencias políticas, ideológicas y económicas entre los países; medidas proteccionistas, y recesión económica derivada de la crisis del petróleo fueron algunos factores que afectaron las dinámicas originales. La integración económica requeriría un nuevo impulso que se apoyaría en medidas legislativas para dinamizar el mercado y sus libertades.

A. El antiguo enfoque legislativo en la seguridad de los productos

En la década de 1960, la integración económica del mercado europeo pasaba por su mejor momento. La unificación de la aduana europea, la eliminación de requisitos aduaneros y la reducción de formalidades en el tráfico transfronterizo favorecieron el nacimiento del mercado común europeo[37]. Sin embargo, con el paso de los años algunas circunstancias políticas y económicas fueron generando fricción entre los países. Se cita, por ejemplo, la influencia que en ello tuvieron dos recesiones económicas, la lentitud legislativa para reaccionar frente al proteccionismo estatal, la unanimidad requerida para las decisiones del Consejo y la proliferación de normas técnicas y requisitos nacionales que frenaban el intercambio de mercancías y creaban desconfianza entre los países[38]. Esto último habría generado un ambiente de litigiosidad entre actores económicos y agentes estatales que se debatían por la legitimidad de las normas. Esto no solo suponía disputas interpretativas, sino que incrementaba los costos de producción, desincentivaba las exportaciones y disminuía los beneficios de las economías de escala de la industria[39].

Tales conflictos derivaban del Tratado de Roma que, si bien impedía las restricciones injustificadas al intercambio de mercancías (art. 30), dotaba de autonomía a los países para regular la protección de intereses legítimos. Esto daba lugar a interpretaciones sobre la validez de las normas emitidas cuando confluían sujetos de distintos países. En este escenario, los actores económicos debían cumplir las normas europeas, pero también las nacionales. En este último caso, tanto las de su país de origen como las del país receptor de las mercancías. Este modelo sería conocido como "el viejo enfoque".

[37] Gormley (2006) p. 17.
[38] *Op. cit*.
[39] Farr (1992).

El viejo enfoque estuvo vigente durante algunos años, pero ya se advertía la necesidad de su abandono como vehículo para la integración económica. Tal cambio se empezó a materializar a fines de la década de 1970. El asunto Rewe-Zentral AG contra Bundesmonopolverwaltung[40] evidenció cómo se vivían estas dificultades en la práctica y cuáles debían ser las soluciones. Allí, el Tribunal de Justicia de las Comunidades Europeas (TJCE) analizó la legitimidad de una norma exigida para la importación en Alemania de la bebida francesa Cassis de Dijon. Según la norma, Cassis no podía ser comercializada porque su baja graduación alcohólica impedía su comercialización como licor. Esta *restricción* se justificaba por las autoridades en la protección de los consumidores.

Al analizar el conflicto, el TJCE concluyó que la norma era ilegítima a la luz del Tratado de Roma. El fallo tuvo en cuenta que la norma constituía una restricción cuantitativa o una medida con efecto equivalente[41], *i.e.* una ley que no tenía por finalidad la protección de un interés legítimo. En su argumentación, el TJCE invocó el principio de reconocimiento mutuo según el cual los países deben aceptar las condiciones legales en que producen los fabricantes comunitarios. El principio tiene en cuenta que, si todos los países persiguen la protección de los mismos intereses, no deben coexistir diferentes niveles de protección.

Cassis de Dijon hizo explícitos algunos intereses legítimos: "la supervisión fiscal, la protección de la salud pública, la justicia en las transacciones comerciales o la defensa del consumidor" (C. 8). Para evitar leyes restrictivas, la CEE debía adquirir el compromiso de armonizar las normas que los Estados miembros exigirían. Estos requisitos se deberían limitar a los esenciales para la protección de *intereses legítimos*, prohibiendo la emisión de normas adicionales. Tal iniciativa demandaba "una obra constructiva"[42] de la legislación armonizada y una comunicación interestatal eficiente[43]. Esta estructura luego se conocería como el "nuevo enfoque" legislativo en seguridad.

---

[40] Tribunal de Justicia de la Comunidad Europea (1979).

[41] Las restricciones cuantitativas son medidas proteccionistas para controlar la cantidad de bienes que se importan. En la práctica son cuotas que se establecen para ciertos productos. Las medidas de efecto equivalente, por su parte, señalan cualquier otra disposición cuya finalidad sea restringir el libre tráfico.

[42] Gasòliba (1989) p. 55.

[43] La directiva 83/189/CEE sobre procedimientos de información dispuso: "Las reglamentaciones técnicas relativas a los productos sólo pueden admitirse si son necesarios para satisfacer exigencias imperativas y persiguen un fin de interés general" (C. 2). Para estar al tanto de las medidas emitidas por cada Estado miembro, esta directiva estableció su derecho a "estar informados de las reglamentaciones técnicas previstas por uno de ellos" (C. 4). Ello, con el fin de plantear objeciones o modificaciones que evitaran restricciones injustificadas. Consejo de las Comunidades Europea (1983) pp. 8-12.

B. El nuevo enfoque legislativo en seguridad de los productos

La resolución del Consejo Europeo del 7 de mayo de 1985 relativa a una nueva aproximación en materia de armonización y normalización[44] planteó los principios del "nuevo enfoque", los cuales se pueden resumir así:

- la aplicación del principio de reconocimiento mutuo en las normas de seguridad,
- armonización europea de las normas de seguridad de los productos,
- autorización para que los Estados miembros regulen la seguridad en ausencia de norma armonizada y
- en caso de conflicto entre normas nacionales, las autoridades solo pueden exigir aquellas que protejan *intereses legítimos*, por tanto,
- los países miembros deben garantizar que sus normas sean adecuadas, necesarias y proporcionadas para cumplir el fin de protección sin restringir injustificadamente el mercado interior.

Los principios descritos descubrían varias líneas de acción. Era necesario acelerar el proceso de armonización legislativa en el ámbito europeo y complementar este marco superior con normas ágiles que se adaptaran a las dinámicas del desarrollo tecnológico. La fórmula que el "nuevo enfoque" propuso consistió en completar las directivas armonizadas con estándares técnicos emanados de organismos de normalización.

C. La armonización y los organismos de normalización (estandarización)

La resolución del Consejo del 7 de mayo dispuso que los instrumentos legislativos comunitarios solo se ocuparían de los *requisitos esenciales* de los productos; es decir, las normas encargadas de proteger los intereses legítimos[45]. Las especificidades técnicas, *i.e.*, las condiciones particulares de seguridad aplicables en cada caso, debían emitirse por *organismos de normalización* (C. 2)[46]. Esta perspectiva conduciría a que los requisitos se armonizaran con normas más flexibles para luego desarrollar las particularidades técnicas.

El anterior proceso se denomina *normalización* y consiste en una política de delegación reglamentaria a organismos de normalización, para que emitan

[44] Consejo de las Comunidades Europeas (1985).

[45] El anexo II lo plantea así: "la armonización legislativa se limitará a la adopción, mediante directivas basadas en el artículo 100 del Tratado CEE, de las exigencias esenciales de seguridad (o de otras exigencias de interés colectivo) [...]".

[46] "a los organismos competentes en materia de normalización industrial se confiará la tarea, teniendo en cuenta el estado de la tecnología, de elaborar las especificaciones técnicas que necesitan los profesionales para producir y poner en el mercado".

estándares o normas armonizadas que son aceptadas como soluciones expertas en determinados campos[47]. En Europa existen tres organismos de normalización que están habilitados para realizar este proceso; cada uno con una especialidad[48]. Si la Comisión se los solicita y se cumple un procedimiento de socialización, los estándares publicados se aceptan como medio para atender los requisitos de seguridad.

La normalización es un aspecto central de la estrategia de seguridad europea. Por una parte, porque pretende eliminar los desacuerdos interpretativos y técnicos alrededor de las medidas necesarias para cumplir con las normas de seguridad. Por el otro, porque es una importante fuente de ventaja competitiva para las empresas europeas al:

i) disminuir los costos de producción al uniformizar los procesos de producción;
ii) ser fuente de seguridad jurídica;
iii) profesionalizar la industria y
iv) si los estándares se afianzan, se convierten en referentes globales que atraen inversión y beneficios colectivos.

De allí que la armonización y la normalización constituyan pilares regulatorios para la UE en su búsqueda de equilibrio entre protección y libertades.

D. La conformidad de los productos y su declaración por el operador económico

Otro principio estructural del nuevo enfoque es la *declaración de conformidad*, *i.e.* la manifestación del fabricante de que el producto cumple con la seguridad jurídicamente esperada[49]. Los instrumentos legislativos desarrollan los parámetros de seguridad, su cumplimiento corresponde a los operadores económicos. Por regla general estos no requieren de autorización alguna para producir y comercializar sus productos. El control que impone la ley consiste en que los operadores económicos declaren que este es conforme con los requisitos esenciales regulados en la norma armonizada o nacional.

La declaración de conformidad surge luego del análisis de los riesgos que el fabricante hace de su producto. Es su responsabilidad identificar y tomar medidas para evitar que dichos riesgos vulneren intereses protegidos. Por los

[47] Véase nota al pie n.° 30.

[48] Incluidos en el anexo I del reglamento (UE) 1025/2012; Comité Europeo de Normalización (CEN); Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI).

[49] En otras palabras, que es compatible a las exigencias que las normas le imponen al producto. En ocasiones, la declaración de conformidad requiere una certificación proveniente de un organismo independiente.

altos estándares que promueve la Unión, en algunos productos de especial peligro, la tolerancia a los riesgos es cercana a cero[50]. Esta declaración es una referencia pública tanto de los riesgos analizados como de las medidas de seguridad adoptadas al momento de su fabricación.

El momento en que se debe declarar la conformidad del producto es importante porque refleja las medidas de seguridad disponibles al tiempo de su comercialización. Cualquier sanción basada en la infracción de una norma debe analizar estas condiciones. Esta misma idea es acogida por la DRPD al exonerar al fabricante si "es probable que el defecto que causó el daño no existiera en el momento en que el producto fue introducido en el mercado [...]" o si "el estado objetivo de los conocimientos científicos y técnicos [...] no permitía descubrir el carácter defectuoso [del producto]" (art. 11, lits. c y e).

En su momento la resolución de 1985 se refería a normas específicas del producto, vigentes en el acervo comunitario. En aquel momento no existía, como ahora, una cláusula general que estableciera el deber de comercializar solo mercancías seguras. Esto cambiaría en 1992 con la primera Directiva General de Seguridad de los Productos (DGSP)[51] que dispuso una cláusula general de este tipo[52].

La conformidad del producto no depende del estricto cumplimiento de las normas o estándares *armonizados* por parte del fabricante. Este queda en libertad de escoger los medios con los que satisface las expectativas públicas. No obstante, si opta por cumplir los estándares armonizados lo beneficiará una *presunción de conformidad* de seguridad, *i.e.*, una presunción desvirtuable de que su producto cumple con las expectativas europeas. De lo contrario, debe demostrar que las medidas tomadas son suficientes y adecuadas para los riesgos que su producto refleja.

En síntesis, el fabricante tiene libertad para escoger los medios con que garantiza la seguridad de sus productos; lo cual resulta conveniente para la innovación. Le está permitido, así, al fabricante apartarse del consenso técnico descrito en el estándar armonizado. Incluso, cuando por el riesgo se dispone la intervención de *organismos notificados* que certifican su conformidad, y sin perjuicio de normas tan específicas que su cumplimiento no da lugar a alternativas, *e.g.*, el empleo de un material ignífugo.

[50] Así se analizó en el asunto Boston Scientific contra AOK por unos marcapasos y unos desfibriladores cuya extracción había sido necesaria para evitar daños ante una posible defectuosidad no corroborada del producto. Véase Tribunal de Justicia de la Unión Europea (2015).

[51] Consejo de las Comunidades Europeas (1992).

[52] La DGSP: "buscó llenar cualquier vacío relativo a productos de consumo, estableciendo un requisito general de seguridad dirigido a productores y distribuidores", véase Fairgrieve & Howells (2006) p. 59.

Este enfoque es importante a efectos de lo antes planteado, debido a que para verificar el incumplimiento de normas de seguridad no basta constatar la directiva europea o la norma armonizada. Puede ser necesario estudiar la declaración de conformidad emitida y evaluar las medidas adoptadas para conocer si la infracción existió.

Lo que sigue es identificar cómo los principios del nuevo enfoque se convirtieron en un marco jurídico. El NML constituye la materialización de tal política.

IV. La sistematización del nuevo enfoque: El Nuevo Marco Legislativo de Seguridad para los Productos

Con el paso de los años y la experiencia adquirida se hizo evidente la necesidad de un marco armonizador del nuevo enfoque legislativo. En palabras de la Comisión:

> "la negociación de los primeros textos de armonización de la Unión en virtud del nuevo enfoque destacó inmediatamente el hecho de que la determinación de los requisitos esenciales y las normas armonizadas no eran suficientes para crear el grado necesario de confianza entre los Estados miembros y que debían desarrollarse instrumentos y una política de evaluación de la conformidad horizontales"[53].

El NML recogió la armonización y la normalización, y le añadió nuevos ingredientes para complementar el ciclo de control de seguridad sobre los productos. En un principio, estaba compuesto por el reglamento 765/2008/CE, sobre requisitos de acreditación y vigilancia del mercado para la comercialización de productos[54] y la decisión 768/2008/CE, sobre un marco común para la comercialización de los productos.

1. La decisión 768/2008/CE, sobre comercialización de productos

La decisión 768/2008/CE (la decisión) es un modelo legislativo, un patrón que deben seguir las normas armonizadas. Plantea definiciones, procedimientos

[53] Comisión Europea (2022c) p. 8.

[54] Parlamento Europeo y el Consejo (2008).http://data.europa.eu/eli/reg/2008/765/oj/spa.", "plainCitation": Parlamento Europeo y el Consejo, Reglamento (CE Reglamento derogado de forma parcial en sus arts. 15 a 29 en aspectos relacionados con la vigilancia del mercado y el control *ex post* de las autoridades. Véase Parlamento Europeo y el Consejo (2019).

y deberes dirigidos a operadores económicos y autoridades; sin embargo, no es de obligatorio cumplimiento. Es una norma sui géneris y un compromiso político asumido por el Parlamento Europeo, la Comisión y el Consejo[55]. Su objetivo principal es que las eventuales directivas de armonización tengan una plantilla coherente que dé continuidad a la política de nuevo enfoque.

Es una herramienta para acoplar las normas armonizadas a la estrategia de seguridad. Por una parte, permite que en lo sucesivo se adopte una terminología uniforme, por ejemplo, acogiendo definiciones como "evaluación de conformidad" u "organismo de evaluación". Por otra parte, permite que las normas de seguridad se ajusten al objetivo estratégico de equilibrar la protección y las libertades económicas. Con ese fin, establece mecanismos como los "módulos" de análisis de la conformidad, los cuales son criterios agrupados que sugieren requisitos cuya complejidad aumenta en proporción a los riesgos del producto. Esto permite que los instrumentos armonizadores establezcan requisitos con un enfoque diferenciado, en el que los fabricantes de artículos menos peligrosos son exonerados de cumplir los requisitos más gravosos. Entre otras ventajas, brinda una plantilla que agiliza los procesos legislativos y estandariza, hasta cierto punto, los derechos y deberes de los operadores económicos.

A. El nivel de riesgo y la evaluación de la conformidad

Según se ha mencionado, el fabricante debe evaluar la conformidad de su producto haciendo un análisis de sus riesgos. La decisión 768/2008/CE propone un *menú de módulos, i.e.*, requisitos y procedimientos de seguridad que la norma europea –directiva o reglamento– puede adoptar. Los procedimientos más estrictos están reservados para los productos de mayor riesgo. Siguiendo este patrón, las directivas europeas establecen requisitos que van desde la evaluación independiente del fabricante hasta la intervención de un *organismo de evaluación de la conformidad*. Estos organismos descentralizados verifican que esté conforme con la legislación europea en seguridad.

B. Los organismos de evaluación de la conformidad y los organismos notificados

La confianza en la declaración autónoma del fabricante disminuye cuanto más riesgoso es su producto. En ciertos casos es necesario restringir la libertad del fabricante a efectos de aumentar la protección. Para ello, la decisión introduce una entidad ajena a este que se encarga de verificar su seguridad. Estas entida-

[55] Comisión Europea (2022c).

des reciben el nombre de *organismos notificados* y su competencia la adquieren luego de cumplir con una *designación* a cargo de las autoridades nacionales[56].

Para ser un organismo notificado, el reglamento 765/2008 establece un procedimiento de acreditación que versa sobre su competencia técnica[57]. Entre las funciones de verificación encomendadas está la calibración, certificación, pruebas de laboratorio o inspección de los productos. Por la naturaleza de sus funciones, sus actuaciones responden a principios de imparcialidad, eficiencia, especialidad e interés público. Quien que acuda a un organismo notificado no habilitado para el producto de que se trate, u obtenga una certificación emitida por fuera de su competencia, podría estar incumpliendo el marco de seguridad.

C. Los operadores económicos y su definición

Uno de los aspectos más importantes de la decisión 768/2008/CE fueron sus definiciones. Ya se había visto cómo el concepto de operador económico, aquí "agentes económicos" (art. R1-7) irriga la normativa europea de mercado. El valor de la decisión está en haber incluido los sujetos que la componen y sus obligaciones: fabricante, representante autorizado, importador y distribuidor son actores que, a pesar de algunas variaciones, han sido fuente de armonización y coherencia legislativa[58].

2. El reglamento (UE) 765/2008, sobre vigilancia del mercado

El otro componente del NML es el reglamento 765/2008/CE. Contrario a la decisión, es una norma de aplicación directa y de obligatorio cumplimiento, *i.e.*, no requiere de transposición en leyes nacionales[59]. El reglamento se ocupa de la base jurídica del *proceso de acreditación* de los organismos notificados, aunque

[56] Comisión Europea.

[57] El usuario selecciona entre la lista vigente en la Web NANDO. En esta se informa sobre la competencia de cada organismo notificado. Así se evita, por ejemplo, el pago por "certificaciones voluntarias" que son ineficaces frente al cumplimiento de normas de seguridad. Véase https://webgate.ec.europa.eu/single-market-compliance-space/#/ home [fecha de consulta: 2 de julio de 2024].

[58] De la intención de coherencia legislativa a partir de las definiciones da cuenta la DRPD, que descartó el término 'productor' que traía la anterior directiva y adoptó el de 'fabricante'.

[59] En el sistema jurídico de la UE, la transposición es un proceso de incorporación legislativa nacional de las normas comunitarias. Por su naturaleza, los reglamentos, a diferencia de las directivas comunitarias, son de aplicación directa en los términos que la legislación indique. Al contrario, las directivas requieren de una ley nacional que las incorpore y su grado de obligatoriedad varía de acuerdo con el tipo de directiva: de máxima o mínima armonización.

su aspecto más relevante es el marco de vigilancia del mercado. A efectos de la responsabilidad, según se mencionó, su importancia radica en que una intervención administrativa de la autoridad de mercado –*e.g.* mediante el retiro o recuperación de las mercancías– permite calificar el producto de defectuoso; por supuesto, atendiendo a todas las demás circunstancias (art. 7g de la DRPD).

A. La vigilancia del mercado

El comercio de productos representa el 25 % del PIB europeo y equivale a la sexta parte del mercado mundial: una suma aproximada de tres mil sesenta millones de euros a 2015[60]. Estas cifras hacen en extremo atractiva la importación de productos inseguros y la fabricación sin el cumplimiento de los requisitos legales. Dado que los controles de seguridad son, por regla general, posteriores a la comercialización de los productos y que las aduanas se ven desbordadas por el flujo de mercancías, la UE requería un marco legislativo para ejecutar controles adecuados de seguridad.

En su origen desarrollado por el reglamento 765/2008 y luego modificado por el reglamento (UE) 2019/1020, la vigilancia del mercado estructura el marco administrativo para prevenir y sancionar por infracciones en la seguridad de los productos. Se trata de otro de los pilares del marco de seguridad, esta vez a cargo de las autoridades y sus funciones principales son las siguientes:

- exigir que los operadores económicos aporten la documentación técnica del producto, así como los detalles de la red de distribución empleada,
- realizar inspecciones *in situ* y sin previo aviso al investigado, así como revisar los productos,
- realizar intervenciones por motivos de seguridad. Las más notorias son la prohibición de comercializar las mercancías, su retiro, su recuperación –del consumidor– o la imposición de sanciones "efectivas, proporcionadas y disuasorias".

Las medidas disuasorias han servido para generar una percepción pública de seguridad y de control institucional; algunas de ellas con un considerable impacto mediático. Así ocurrió, por ejemplo, con la sanción impuesta a Google LLC y su matriz Alphabet, Inc. con ocasión de los abusos identificados en su plataforma Android. Con más de cuatro mil cien millones de euros[61] ha sido la multa más cuantiosa impuesta a un operador económico en la historia de la UE.

[60] Comisión Europea (2017) p. 1.

[61] Si bien se trata de una sanción administrativa impuesta por abuso de posición dominante, responde a los mismos criterios establecidos en el reglamento (UE) 2019/1020. Véase Tribunal General de la Unión Europea (2022) C. 1082 y ss.

Luego de una década, el marco de vigilancia del mercado debió ser actualizado. El reglamento (UE) 2019/1020 adaptó esta institución a las necesidades del comercio moderno. En cumplimiento de la actualización:

- incrementó la coordinación europea de las autoridades de vigilancia nacionales, tanto aduaneras como de mercado,
- fortaleció el uso de los sistemas de información de seguridad de los productos, los eventos de riesgo y las sanciones impuestas[62],
- prescribió deberes de seguridad e incluyó a los prestadores de servicios logísticos en la categoría de operadores económicos.

B. El marcado "CE"

Por último, el Reglamento (UE) 765/2008 incorporó los principios generales del marcado "CE"[63]. Se trata de un símbolo que indica la conformidad del producto con la seguridad esperada. Ello no es una señal inequívoca de que este ha sido fabricado en la UE; pero sí distingue aquellos que cumplen con sus estándares de seguridad. El marcado "CE" facilita el control de seguridad a los operadores económicos que adquieren o modifican productos, dado que también pueden ser declarados responsables en desarrollo de sus actividades de importación o distribución.

3. Conclusión preliminar

En síntesis, el NML es la formalización legislativa de la política de nuevo enfoque. Esta se ocupó de introducir definiciones, deberes, procedimientos e instituciones relativas a la estrategia de seguridad europea[64]. Sin embargo, con todo y

[62] Así, por ejemplo, el art. 8 del reglamento establece que el portal "Tu Europa" debe informar sobre la seguridad de los productos. Allí se encuentra información especializada sobre los requisitos, normas y autoridades que intervienen en el control de seguridad de los productos. Véase https://europa.eu/youreurope/business/product-requirements/compliance/identifying-product-requirements/index_es.htm [fecha de consulta: 2 de julio de 2024].

[63] La función del sello CE se describe así por las autoridades: "Para poder venderse en la UE, muchos productos deben llevar obligatoriamente el marcado CE, que demuestra que el fabricante ha evaluado el producto y se considera que este cumple los requisitos de seguridad, sanidad y protección del medio ambiente exigidos por la UE. El marcado CE es obligatorio para los productos fabricados en cualquier lugar del mundo que vayan a comercializarse en la UE". Unión Europea (2024).

[64] Sobre la función que cumplen cada uno de estos elementos, ha dicho la Comisión Europea: "todos estos elementos diferentes están interrelacionados, funcionan juntos y son complementarios, formando una cadena de calidad de la UE. La calidad del producto depende de la calidad de fabricación, que en muchos casos se ve afectada por la calidad de los ensayos, internos o llevados a cabo por organismos externos, que depende de la calidad de los procesos de evaluación de la conformidad, que está influenciada por la calidad de los organismos, que a su vez depende de la calidad de sus controles, dependiente de la calidad de la notificación o la acreditación. El sistema

su complejidad, el NML responde a un contexto histórico donde las mercancías físicas y las cadenas logísticas no habían sido impactadas por la transformación digital. Por el contrario, los esfuerzos legislativos en los últimos años se han concentrado en proporcionar un marco de seguridad adecuado para las características que exhiben los nuevos productos digitales.

V. El Mercado Único Digital: los desafíos de los nuevos productos digitales

Quizá uno de los principales desafíos que ha afrontado la UE en este siglo ha sido el de promover condiciones políticas para el desarrollo tecnológico. La UE despertó tarde a la cuarta revolución industrial: solo hasta 2010 formuló una agenda digital[65] y tardó cinco años más para presentar su estrategia de Mercado Único Digital (MUD)[66]. Una vez admitió su letargo, se ocupó de producir una impresionante colección de normas y propuestas para promover las libertades del mercado. De allí que se diga que Estados Unidos diseña, China produce y la UE legisla.

1. Las tecnologías digitales y los nuevos retos en seguridad

Las tecnologías digitales han cambiado algunas de las percepciones tradicionales sobre los riesgos de los productos. Esto es consecuencia de la desmaterialización que genera la digitalización; la creciente interacción producto-servicio; la incorporación de novedosas funcionalidades que dependen de procesos de información y la complejidad técnico-científica que resulta de la mezcla de los anteriores elementos, entre otros motivos.

2. Los problemas identificados

En 2020 la Comisión Europea publicó un informe en el que analizaba el impacto de la IA, internet de las cosas y la robótica en el marco de seguridad y la

en su conjunto depende de la calidad de la vigilancia del mercado y de los controles de los productos procedentes de terceros países [...] Si un elemento se perdiera o mostrara debilidad, la solidez y la efectividad de toda la 'cadena de calidad' quedarían en entredicho". Comisión Europea (2022c) p. 12.

[65] Comisión Europea (2010).

[66] Comisión Europea (2015).

responsabilidad civil europea[67]. En su análisis, la Comisión concluyó que las normas de seguridad vigentes podían hacer frente a los cambios tecnológicos. Esto, en primer lugar, por el carácter tecnológicamente neutro de sus disposiciones y, en segundo, porque ya algunas normas habían incorporado disposiciones relativas a estos productos, *e.g.*, el Reglamento de Productos Sanitarios (UE) 2017/745 o la directiva 2014/32/UE sobre instrumentos de medida.

Con todo, la Comisión reconoció que algunas características de la nueva generación de productos, o no estaban reguladas, o las normas vigentes carecían de claridad. A continuación, presentaré cómo dichas características impactan el marco de seguridad vigente y cuáles son algunos de los remedios adoptados. Para el efecto describiré los riesgos partiendo de los tres elementos que integran todo producto digital: programa informático, equipo informático y datos o información[68]. Aunque en la práctica los tres conforman un sistema y, como tal operan de forma conjunta, trataré de explicar sus desafíos de manera individual.

3. *El programa informático o* software

A. Los elementos esenciales de una definición de *software*

El programa informático o *software* se ha definido como la "parte de un sistema electrónico de información consistente en un código informático"[69]. Como *parte*, el *software* se complementa con equipos informáticos y con información. Cuando se aísla de su componente material y del flujo de datos que alimenta su funcionamiento, el *software* adquiere una forma inmaterial que la definición legal citada designa "código informático"[70].

[67] Señala que: "Una gran parte del marco de la Unión en materia de seguridad de los productos se redactó antes de la aparición de tecnologías digitales tales como la IA, el internet de las cosas o la robótica [lo cual] [...] no implica que no pueda aplicarse a los productos que incorporan estas tecnologías". Comisión Europea (2020) p. 5.

[68] Se podría señalar que los datos son los símbolos y la información es el fin de utilizar los datos. Esta última requiere un sujeto analice su sentido.

[69] Así, en el art. 3-6 de la propuesta de Reglamento sobre Ciberseguridad, véase Comisión Europea (2022d).

[70] La directiva 2009/24/CE sobre programas de ordenador no define con claridad en qué consiste el *software* (programa de ordenador). Se adopta mejor la definición de la propuesta del Reglamento sobre Ciberseguridad. No obstante, menciona que el programa de ordenador son expresiones del intelecto y su protección legal versa sobre "la expresión del programa de ordenador y [...] las ideas y principios implícitos en los elementos del programa [no está protegida] [...]" (C. 11). Lo anterior da cuenta de la naturaleza abstracta del concepto y su origen humano. Véase Parlamento Europeo y el Consejo (2009).

El código es lenguaje, instrucciones transmitidas en lenguaje de máquina –*Machine code*– que el equipo informático interpreta con el objetivo de desempeñar una tarea. Como lenguaje e idea se podría afirmar que el código informático tiene dos características esenciales: intangibilidad y racionalidad.

Por *intangibilidad* me refiero a la forma inmaterial del *software*. Un programa informático contiene instrucciones; código en lenguaje de máquina que guía la actuación del producto. De su naturaleza intangible da cuenta la ley: el código está protegido por la directiva 2009/24/CE sobre protección a programas de ordenador, ya que es una "creación intelectual propia de su autor" (art. 1-3)[71].

Por *racionalidad* se señala la cualidad de ser un objeto que responde a determinada lógica, a un orden implícito con sentido para las personas. Por su naturaleza intelectual, la protección legal del *software* incluye los "trabajo[s] preparatorio[s] de concepción que conduce[n] al desarrollo" (C. 7)[72]. De allí que se diga:

> "La programación es un oficio. En su forma más elemental, es hacer que una computadora haga lo que tú quieres que haga (o lo que el usuario quiera que haga)"[73].

B. Los riesgos de la intangibilidad y la racionalidad implícita en el *software*

Contemplando los elementos anteriores, el *software* genera riesgos que el marco de seguridad no habría podido prever. En primer lugar, la *intangibilidad* es ajena a la regulación tradicional de la seguridad en productos, la cual se había ocupado de riesgos asociados a la producción industrial en masa[74], a la fuerza mecánica o la complejidad intrínseca de los productos *tangibles*[75]. En este escenario, la seguridad se ocupa del proceso productivo y de la información de uso ofrecida al usuario. Este trasfondo llevó a que la regulación de productos se enfocara en objetos muebles *tangibles*, excluyendo al *software* independiente (*stand alone software*) y a cualquier otra manifestación intangible como los servicios.

---

[71] Parlamento Europeo y el Consejo (2009).

[72] *Ibid*.

[73] Hunt & Thomas (2020) p. xix.

[74] Primero, alimentos y productos de consumo o artículos de aplicación humana como venenos, talcos o bebidas; luego, con vehículos y maquinaria. Para una perspectiva histórica de las garantías de calidad y seguridad alrededor de los bienes, véase Jaeger (1963) pp. 501-556.

[75] Muestra de ello es la catástrofe de la Talidomida, que provocó la creación de un régimen de responsabilidad objetiva en Alemania, *i.e.*, la Ley de Productos Medicinales o Arzneimittelgesetz. Este escándalo también motivó la expedición de la directiva 85/374/CEE sobre responsabilidad por productos defectuosos. Véase Magnus (2018) pp. 103-114.

Tal enfoque parece haber seguido la división de las libertades del mercado que trae el Tratado de Funcionamiento de la Unión Europea (TFUE), *i.e.*, mercancías, personas, servicios y capitales[76]. Antes de la vigente definición de producto se entendía que el *software* independiente, *i.e.*, aquel no incorporado en un continente material, era un servicio. Esta concepción seguía el TFUE, que define los servicios como prestaciones ejecutadas en actividades de carácter industrial o de profesiones liberales[77]. Como resultado, con excepción de la electricidad, las definiciones de producto adoptadas por normas como la DGSP de 2001 descontaban cualquier objeto intangible[78].

Esto fue cambiando a medida que se dimensionó el impacto del *software* en el mercado. Además de otras normas sectoriales, el RGSP incluyó al *software* en la definición de productos en 2023. En adelante se entiende que son productos, tanto el *software*-componente como el *software*-independiente[79].

Otro riesgo relacionado con la intangibilidad, cuya regulación ha requerido de un intenso debate –sobre todo en la Ley de IA–, es el de las afectaciones silenciosas del *software* a la salud mental y a otros derechos fundamentales. La seguridad ya no solo gravita alrededor de productos en los que "la percepción del usuario [es] de una amenaza de daño físico"[80]. Efectos imperceptibles como el estrés, la discriminación o la afectación a la dignidad humana son ahora objeto de una amplia regulación en el ámbito de los productos.

Por su parte, lo que aquí he llamado *racionalidad*, lógica u orden del *software* ha ocasionado importantes reacciones legislativas en materia de seguridad. Una de las causas de la popularidad del *software* es su capacidad para utilizar información. El nivel de sofisticación con que se emplee esta capacidad depende de diferentes factores como la información de que se disponga o el equipo informático. Para lo que tiene que ver con el *código* es preciso analizar las *técnicas* empleadas para utilizar la información. Dependiendo de la elección del desarrollador, el *software* será más o menos transparente, autónomo o complejo. Las técnicas escogidas también han sido objeto de amplias consideraciones legislativas en materia de seguridad.

---

[76] Art. 26-2 del Tratado de Funcionamiento de la Unión Europea (TFUE) señala: "El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones de los Tratados". Unión Europea (2016).

[77] Art 57 del TFUE.

[78] Sobre discusiones anteriores de si el *software* podría ser considerado producto, por ejemplo, interpretando sus similitudes con la electricidad, véase Machnikowski (2016).

[79] No siempre será un producto. El *software* también se puede prestar como servicio (SaaS). Un ejemplo de ello es la suscripción a una plataforma de vídeos.

[80] Aunque se mencionó que el concepto de salud como interés protegido comprendía la salud mental. Comisión Europea (2020) p. 9.

El ejemplo paradigmático de los riesgos que produce una técnica específica es la IA: no todo *software* es IA, aunque toda IA es *software*. Ello se explica, según la Ley de IA, en que esta difiere de "planteamientos de programación tradicionales y más sencillos" (C. 12) que dependen de reglas exhaustivas y deterministas previamente transmitidas por personas físicas. En la actualidad, la IA se identifica con ciertas técnicas de programación asociadas al aprendizaje automático o *Machine Learning* (ML), y a los sistemas lógicos basados en conocimiento (C. 12).

El ML es una técnica donde, entre otros acercamientos, el programa *aprende* realizando inferencias a partir de patrones obtenidos de grandes cantidades de datos[81]. Por los elementos que intervienen en su aprendizaje –entrenamiento– y operación, el ML exhibe sus propios riesgos.

Uno de ellos es el que deriva de los datos. Por motivos relacionados con su desempeño o *aprendizaje*, la calidad de los datos y su adecuada gestión inciden en la precisión, transparencia, explicabilidad y legalidad del sistema. Algunos problemas identificados son:

i) datos sesgados o insuficientes que se traducen en modelos imprecisos y peligrosos;
ii) la inadecuada gestión de los datos o la utilización de algoritmos complejos que afectan la transparencia del sistema o
iii) el empleo indebido de datos personales para el entrenamiento de sistemas.

Hasta la formulación de la Ley de IA no existían normas de seguridad que introdujeran parámetros de calidad para la gobernanza y la gestión de los datos (art. 10) o que desarrollaran deberes de transparencia (art. 13) y supervisión humana (art. 14).

El ML y otras técnicas de programación son, también, fuente de opacidad y de complejidad. Esto implica desafíos tanto para la prevención como para la responsabilidad civil. Los fabricantes deben poder entender y explicar el funcionamiento del producto, pero, además, facilitar herramientas al usuario para que entiendan la causa de una decisión de la IA. En un entorno donde los vehículos son autónomos, se diagnostican enfermedades con ayuda de IA y las personas utilizan asistentes virtuales para todo tipo de tareas, es indispensable permitir ciertos niveles de control y comprensión sobre su funcionamiento. Lo contrario conduce a declinar libertades, impactando la auditabilidad del sistema, las reclamaciones de las víctimas y el control de las autoridades. Para corregir lo anterior se han desarrollado deberes de documentación, su-

[81] El *Big Data* se explica como una base de datos cuya complejidad o cantidad impiden su tratamiento mediante tecnologías convencionales. Joint Research Centre, Estévez, Fernández, Gómez & Martínez (2022) p. 17.

pervisión humana, transparencia, conservación de registros y de trazabilidad, que se deben cumplir durante todo el ciclo de vida del sistema (art. 9).

Debe decirse, no obstante, que la opacidad y la complejidad de los sistemas pueden ser una cualidad inherente: un tómalo o déjalo. Una técnica que ejemplifica este dilema son las redes neuronales profundas[82], *i.e.*, algoritmos que replican las conexiones nerviosas –sinapsis– del cerebro humano. Al imitar los principios del cerebro para procesar información, la cantidad de capas y conexiones que se utilizan pueden ser tan complejas que sus resultados son incomprensibles. Este efecto de caja negra sustenta, en parte, los clamores de la industria para limitar su responsabilidad civil y las sanciones por falta de seguridad. Ello, por los riesgos que se deben tomar si se pretende generar un entorno de desarrollo técnico y científico[83].

Para finalizar, otra característica asociada al ML es la *autonomía*, *i.e.*, la capacidad del producto de ejecutar tareas con poca o ninguna influencia externa[84]. Se trata de una característica que ha concentrado la atención pública. La autonomía es, quizá, una de las más notorias funcionalidades de los productos modernos. El riesgo que comporta consiste en la imprevisibilidad inherente a su capacidad de aprendizaje, que dificulta al fabricante el análisis *ex ante* de sus riesgos. Si el fabricante no puede anticipar cómo se comportará el producto, su capacidad para evitar o reaccionar frente al daño se ve afectada[85].

Además del control que le proporciona la conectividad al fabricante, la autonomía ha contribuido a otro cambio sustancial en la estrategia de segu-

[82] Se explica como una rama del ML basada en redes neuronales artificiales de múltiple nivel, *op. cit.* p. 26.

[83] El art. 11-1(e) de la DRPD señala: "Los operadores económicos [...] no serán responsables [...] si demuestran que: [...] e) que el Estado objetivo de los conocimientos científicos y técnicos en el momento en que fue introducido en el mercado, puesto en servicio, o durante el período en el que el producto estaba bajo el control del fabricante no permitía descubrir el carácter defectuoso".

[84] Joint Research Centre, Estévez, Fernández, Gómez & Martínez (2022) p. 15.

[85] Además de la Ley de IA, otra norma que regula los efectos de la autonomía es el reglamento (UE) 2023/1230 relativo a las máquinas. Su considerando 12 lo explica así: "Recientemente se han introducido en el mercado máquinas más avanzadas, que no dependen tanto de los operadores humanos. Estas máquinas trabajan en tareas definidas y en entornos estructurados, pero pueden aprender a realizar nuevas acciones en este contexto y hacerse más autónomas. Otras mejoras que ya se han incorporado o cabe esperar que se incorporen a las máquinas tienen que ver con el tratamiento de la información en tiempo real, la resolución de problemas, la movilidad, los sistemas de sensores, el aprendizaje, la adaptabilidad, y la capacidad de operar en entornos no estructurados (por ejemplo, obras de construcción). El informe de la Comisión sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero de 2020, establece que la aparición de nuevas tecnologías digitales, como la inteligencia artificial, el internet de las cosas y la robótica, entraña nuevos retos para la seguridad de los productos". Parlamento Europeo y el Consejo (2023).

ridad: el monitoreo poscomercialización. Según se vio, el fabricante debía garantizar la conformidad *antes* de su introducción en el mercado. Aunque la evaluación tenía en cuenta el periodo de uso, descartaba el deber de ejercer vigilancia sobre el desempeño del producto. La nueva generación de productos digitales exige tal monitoreo, tanto por el control que ejerce el fabricante como por su autonomía característica. De allí que la responsabilidad del productor dependa, también, del control ejercido durante el periodo de uso, así como de la capacidad del producto para "seguir aprendiendo o adquirir nuevas características" (art. 7-2, lits. c y e de la DRPD). De acuerdo con el RGSP y la Ley de IA, los fabricantes deben velar por la seguridad del producto durante todo su ciclo de vida; en especial, cuando sus características pueden conducir a cambios sustanciales del producto con efectos en su seguridad.

4. El equipo informático o hardware

El *hardware* se ha definido como un: "sistema electrónico de información físico, o partes de este, capaz de tratar, almacenar o transmitir datos digitales"[86]. El concepto incluye cualquier dispositivo físico cuya función sea el tratamiento de información. Gracias a su condición física, es el componente del sistema que más se aproxima a la definición tradicional de producto. Esto ha permitido que las adecuaciones legales en seguridad en su mayoría apunten al *software* o al tratamiento de la información.

Debe decirse, no obstante, que el fabricante debe anticipar que el éxito de otras medidas de seguridad depende del equipo informático. Así ocurre, por ejemplo, con los deberes de registro o almacenamiento de la información, que exigen contar con equipos apropiados y cuyos resultados luego pueden ser objeto de exhibición en procesos sancionatorios o de responsabilidad.

Asimismo, los equipos informáticos deben contar con medidas apropiadas de seguridad electrónica. Así lo señala el reglamento (UE) 2023/1230 relativo a las máquinas que impone la instalación de medios para recabar "pruebas de toda intervención legítima o ilegítima" en el producto (anexo III, num. 1. 1.9). De forma similar se regulan los equipos radioeléctricos en la directiva (UE) 2014/53 (RED)[87], que exige la instalación de instrumentos para proteger los sistemas de información, la privacidad y el riesgo de fraude al usuario (art. 3-3). Un equipo radioeléctrico es cualquier producto que utilice ondas de radio para transmitir información, *e.g.*, dispositivos con Bluetooth o Wi-Fi, lo cual implica que tales medidas se tomen en un importante rango de equipos. En conclusión, ahora se exige que los equipos informáticos cuenten con

[86] Comisión Europea (2022d) arts. 3-7.

[87] Parlamento Europeo y el Consejo (2014).

los medios apropiados para el desempeño seguro de las funciones del *software* y el tratamiento de los datos.

5. La conectividad o el carácter "sistémico" de los productos digitales

El último elemento por revisar es la conectividad. Los sistemas digitales funcionan en constante interacción. El equipo recibe y emite señales de datos con información destinada a personas o cosas. Según la Directiva de Protección de Programas de Ordenador, su función "es comunicarse y trabajar con otros componentes del sistema de ordenador y con sus usuarios" (C. 10). Este trabajo conjunto va más allá del entorno tecnológico del usuario. Con el nivel actual de integración de los sistemas digitales, la conectividad se debe entender en un sentido más amplio. En el caso de los productos digitales, la finalidad de tal comunicación es "[interactuar] con el entorno físico o [administrar] dispositivos que interactúan con el entorno físico"[88] o virtual.

La comunicación entre equipos es consecuencia de tecnologías como internet. Los equipos informáticos incorporan puertos físicos o lógicos que envían y reciben datos a través de redes públicas y privadas. La información transmitida puede servir para que el producto exhiba un comportamiento, proyecte un contenido audiovisual o se comunique con otro dispositivo. Todas estas interacciones han generado una cadena de suministro compleja cuya seguridad también ha tenido que ser regulada.

La manifestación más evidente de tales riesgos es la de la seguridad electrónica o *ciberseguridad*. Al ser transmitida por redes públicas, la información puede ser alterada, destruida o explotada por personas sin autorización. Tales alteraciones amenazan derechos fundamentales como la libertad de expresión o la intimidad; asimismo, pueden generar daños físicos a pequeña y gran escala. Una de las principales preocupaciones legislativas en esta materia ha sido la de regular los sistemas críticos, *i.e.*, la infraestructura sensible que emplea sistemas digitales para actividades de gran importancia: infraestructura eléctrica, sanitaria o fiscal[89].

Una visión clásica de la ciberseguridad señala que su objetivo es la confidencialidad, integridad y disponibilidad de la información[90]. La confidencialidad se refiere al secreto de la información. Nadie más que las personas auto-

[88] Comisión Europea (2022d) arts. 3-5.

[89] SRI1 y ahora SRI2 han constituido el marco principal de protección a la infraestructura crítica de la UE. Parlamento Europeo y el Consejo (2022).

[90] Chiara (2022) pp. 118-137. Una visión moderna incluye, además, la seguridad electrónica de las personas y sus derechos, véase González & Jasmontaite (2020) pp. 97-115.

rizadas deben tener acceso a los datos almacenados, transmitidos o recibidos por un producto. Por su parte, la integridad se refiere a la originalidad y exactitud de la información que este utiliza en su funcionamiento. Por último, la referencia a la disponibilidad sugiere tener en cuenta dos facetas: como la posibilidad de acceder a la información con fines de exhibición o como el uso que de ella hace un sistema. Para que un producto opere de forma segura debe tener acceso a la información pertinente. Piense en un sistema de información biométrico que sufra un ataque de denegación de servicio (DoS) que impida el acceso a su base de datos o en una aplicación bancaria cuyos servidores colapsen. En síntesis, la seguridad electrónica conduce a valorar que: "la mayoría de productos digitales incorporan una multitud de componentes de diferentes proveedores de hardware y software"[91] cuya corrupción o ataque puede afectar a los demás.

Esta red de participantes genera otro desafío: la complejidad operativa del producto. Ya se había mencionado la complejidad de ciertas técnicas de programación como las redes neuronales; aquí nos referimos a la complejidad que deriva de la interacción de múltiples productos, servicios y componentes que se influyen mutuamente a través de datos. Si bien el fabricante siempre ha tenido que evaluar la forma en que su producto afecta los demás, la interacción moderna de los sistemas de información eleva las exigencias en seguridad para atender a eventos virtuales cuya previsibilidad es casi nula.

Lo anterior genera dos situaciones de riesgo. Por un lado, el fabricante debe garantizar la seguridad de su dispositivo a través de medidas dirigidas a los servicios o componentes que emplee. En otras palabras, debe tener el control de todo su entorno operativo. Este control es determinante para la responsabilidad por productos, ya que amplía la expectativa de seguridad de una manera que no tiene antecedentes (art. 7-1 de la DRPD). La ampliación es además interesante en lo que allí define como "servicios conexos", *i.e.*, un servicio digital integrado o interconectado, cuya ausencia impediría que el producto funcionara. Este interés surge de la variedad y frecuencia de las interacciones que produce el servicio, así como de la dificultad práctica para distinguirlo del producto.

La otra cara de la moneda es el cuidado que debe tener el fabricante frente a los demás dispositivos. Es necesario contar con políticas claras en materia de ciberseguridad y uso adecuado del producto, informando a los usuarios acerca de las medidas de prevención y las amenazas del entorno operativo. El mismo deber pesa sobre las autoridades cuando conozcan un evento de riesgo. Los fabricantes, entre otras medidas, deben diseñar los productos y adop-

[91] Chiara (2022) p. 129.

tar las actualizaciones de seguridad de forma que permitan un control adecuado de su seguridad.

En conclusión, la triada programa informático, equipo e interconexión constituye el núcleo de las actualizaciones legislativas en seguridad. Cada uno de ellos es fuente de situaciones de riesgo que aquí solo es posible enunciar. En la medida que la integración continúe, las autoridades se verán obligadas a desarrollar más normas y a acelerar la emisión de estándares armonizados que atiendan las necesidades específicas de las cada vez más complejas tecnologías que inundan el mercado.

Conclusiones

Las propuestas de responsabilidad civil con disposiciones sobre productos digitales han optado por incorporar múltiples remisiones a las normas de seguridad. Ambos grupos de normas son el resultado de la política de actualización y adecuación europea a los retos de la era digital.

Al analizarlas en conjunto se advierte una estrecha relación que parece hacer parte de una estrategia. Tal estrategia sugiere que el modelo proteccionista europeo regula cada vez más la seguridad de los productos y, al hacerlo, define estándares que son empleados para los fines de las directivas de responsabilidad. Este uso puede consistir en la configuración de un indicio que luego se convierte, por orden legal, en presunciones *iuris tantum* en contra de quien incumple. En otros casos, el conocimiento y cumplimiento de las normas de seguridad son medidas fundamentales para satisfacer el deber de exhibición a cargo del demandado.

Desde otra perspectiva, las normas de seguridad pretenden servir de guía a los operadores económicos quienes, para no someterse al albur de la decisión judicial *ad hoc*, identifican sus deberes en relación con los productos que fabrican o utilizan. Sin embargo, la cantidad de instrumentos legislativos involucrados en la seguridad, sobre todo en el ámbito digital, hacen de este un escenario cada vez más técnico y complejo. De hecho, parece que la nutrida legislación de seguridad puede hacer más sencillo para la víctima demostrar un incumplimiento a fines de solicitar una presunción, que probar la culpa del demandado o el defecto del producto.

Lo anterior demuestra el interés que tiene la comprensión del marco de seguridad europeo: sus principios, estructura y componentes. Este ha transitado por varias etapas que han generado un modelo que ahora muchos países siguen. Con este marco, la UE apuesta a la seguridad como ventaja competitiva en el mercado tecnológico; por lo menos mientras adquiere las condiciones para asumir el liderazgo que allí pretende asumir.

Bibliografía

Borghetti, Jean-Sébastien (2023): "Taking EU Product Liability Law Seriously: How Can the Product Liability Directive Effectively Contribute to Consumer Protection?", *French Journal of Legal Policy* No. 1.

Calvo Caravaca, Alfonso-Luis y Carrascosa González, Javier (2003): *Mercado único y libre competencia en la Unión Europea* (Madrid, Colex).

Chiara, Pier Giorgio (2022): "The IoT and the new EU cybersecurity regulatory land scape", *International Review of Law, Computers & Technology* vol. 36 No. 2. Disponible en https://doi.org/10.1080/13600869.2022.2060468 [fecha de consulta: 4 de mayo de 2022].

Corones, Stephen. G. & Clarke, Philip H. (1997): *Consumer Protection and Product Liability Law: Commentary and Materials*. LBC Casebooks (Sydney: LBC Information Services).

Danneman, Gerhard & Schulze, Reiner (2020): *German Civil Code. Bürgerliches Gesetzbuch. Article-by-article Commentary. Books 1-3: §§1-1296* vol. I (Baden-Baden, Beck & Nomos).

Fairgrieve, Duncan & Howells, Geraint (2006): "General Product Safety: A Revolution through Reform?", *The Modern Law Review* vol. 69 No. 1.

Farr, Sebastian (1992): *Harmonisation of Technical Standards in the EC*. European Practice Library (London, Chancery Law Pub).

Faure, Michael; Goodwin, Morag & Weber, Franziska (2014): "The Regulator's Dilemma: Caught between the Need for Flexibility & the Demands for Foreseeability. Reassessing the Lex Certa Principle", *Albany Law Journal of Science & Technology* vol. 24 No. 2.

Franklin, Marc A. (2016): *Cases and Materials on Tort Law and Alternatives* (New York, The Foundation Press, 10th. ed. University Casebook Series).

González Fuster, Gloria & Jasmontaite, Lina (2020): "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights", in Christen, Markus; Gordijn, Bert & Loi, Michele (eds.), *The Ethics of Cybersecurity*. The International Library of Ethics, Law and Technology (Cham, Springer International Publishing). Disponible en https://doi.org/10.1007/978-3-030-29053-5_5 [fecha de consulta: 2 de julio de 2024].

Gasòliba, Carles A. (1989): *L'Acta Única Europea*. Col·lecció Europa (Barcelona, Tibidabo).

Gormley, Laurence (2006): "The Internal Market: History and Evolution", in Nic Shuibhne, Niamh, *Regulating the Internal Market* (Cheltenham, Edward Elgar).

Howells, Geraint G. (1999; 2000): "The Relationship between Product Liability and Product Safety - Understanding a Necessary Element in European Product Liability through a Comparison with the U.S. Position International Torts: A Comparative Study", *Washburn Law Journal* vol. 39 No. 3.

Hunt, Andrew & Thomas David (2020): *The Pragmatic Programmer: Your Journey to Mastery*. 20th Anniversary Edition (Glasgow: Pearson, 2nd Edition).

Institute for European Tort Law; Winiger, Bénédict; Karner, Ernst & Oliphant, Ken (2018): *Digest of European Tort Law Volume 3: Essential Cases on Misconduct* (Berlin/Boston, De Gruyter).

Jaeger, Walter H. E. (1963): "Product Liability: The Constructive Warranty", *Notre Dame Lawyer* vol. 39 No. 5.

Joint Research Centre (European Commission); Estévez Almenzar, Marina; Fernández Llorca, David; Gómez, Emilia & Martínez Plumed, Fernando (2022): *Glossary of Human-Centric Artificial Intelligence* (LU: Publications Office of the European Union). Disponible en https://data.europa.eu/doi/10.2760/860665 [fecha de consulta: 2 de julio de 2024].

Machnikowski, Piotr (ed.) 2016: *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*.

Magnus, Ulrich (2018): "Product Liability for Medicinal Pharmaceutical in Germany", in Martín-Casals, Miquel & Valverde, J. L. (eds.), *Towards the Harmonisation of the Pharmaceuticals Liability Systems*, , Pharmaceuticals Policy and Law 20 (Amsterdam, IOS Press).

Martín-Casals, Miquel (2023): "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *InDret* n.º 3. Disponible en https://doi.org/10.31009/InDret.2023.i3.02 [fecha de consulta: 2 de julio de 2024].

Shapo, Marshall (2007): "Tort and Regulatory Law in the United States of America", in Van Boom, Willem H.; Lukas, Meinhard & Kisslin, Christa (eds.), *Tort and Regulatory Law*. Tort and Insurance Law vol. 19 (Wien, Springer).

Trivium (1998): *Diccionario Trivium - Derecho y Economía* (Madrid, Trivium).

Von Bar, Christian (1998): *The Common European Law of Torts* vol. 2 (New York, Clarendon Press/Oxford).

Weatherill, Stephen (2017): *The Internal Market as a Legal Concept*. The Collected Courses of the Academy of European Law XXV/1 (Oxford, University Press, First Edition).

Normas

Comisión Europea (2010): "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Una Agenda Digital para Europa". Disponible en https://eur-lex.europa.eu/legal content/es/ALL/?uri=CELEX:52010DC0245 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2015): "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una

Estrategia para el Mercado Único Digital de Europa". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52015DC0192 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2017): "Propuesta de Reglamento del Parlamento Europeo y del Consejo que establece normas y procedimientos para el cumplimiento y la garantía de cumplimiento de la legislación de armonización de la Unión sobre productos y modifica los Reglamentos (UE) Nº 305/2011, (UE) Nº 528/2012, (UE) 2016/424, (UE) 2016/425, (UE) 2016/426 y (UE) 2017/1369 del Parlamento Europeo y del Consejo y las Directivas 2004/42/CE, 2009/48/CE, 2010/35/UE, 2013/29/UE, 2013/53/UE, 2014/28/UE, 2014/29/UE, 2014/30/UE, 2014/31/UE, 2014/32/UE, 2014/33/UE, 2014/34/UE, 2014/35/UE, 2014/53/UE, 2014/68/UE y 2014/90/UE del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0795 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2018): "Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the member states concerning liability for defective products". Available in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0157&qid=1664878769484 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2020): "Informe de la Comisión al Parlamento, al Consejo y al Comité Económico y Social Europeo. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica". Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020DC0064 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2021): "Commission Staff Working Document. Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and Repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council". Available in https://doi.org/10.5040/9781782258674 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2021): "Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados Actos Legislativos de la Unión. 2021/0106 (COD)., Pub. L. No. COM (2021) 206 final (2021). Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2022a): "Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0495&qid=1709810593012 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2022b): "Propuesta de directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0496 [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2022c): "Comunicación de la Comisión 'Guía azul' sobre la aplicación de la normativa europea relativa a los productos". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022XC0629(04) [fecha de consulta: 2 de julio de 2024].

Comisión Europea (2022d): "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE)2019/1020". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0454 [fecha de consulta: 2 de julio de 2024].

Consejo de las Comunidades Europeas (1983): "Directiva 83/189/CEE del Consejo, de 28 de marzo de 1983, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas". Disponible en http://data.europa.eu/eli/dir/1983/189/oj/spa [fecha de consulta: 2 de julio de 2024].

Consejo de las Comunidades Europeas (1985): "Resolución del Consejo, de 7 de mayo de 1985, relativa a una nueva aproximación en materia de armonización y de normalización". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:3198 5Y0604(01) [fecha de consulta: 2 de julio de 2024].

Consejo de las Comunidades Europeas (1992): "Directiva 92/59/CEE del Consejo, de 29 de junio de 1992, relativa a la seguridad general de los productos". Disponible en http:// data.europa.eu/eli/dir/1992/59/oj/spa [fecha de consulta: 2 de julio de 2024].

Consejo Europeo (1985): "Directiva del Consejo de 25 de junio de 1985 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabiliad por los daños causados por productos defectuosos". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31985L0374 [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2001): "Directiva 2001/95/CE del Parlamento Europeo y del Consejo de 3 de diciembre de 2001 relativa a la seguridad general de los productos. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32 001L0095&qid=1668076395961&from=EN [fecha de consulta: 02 de julio de 2024].

Parlamento Europeo y el Consejo (2008): "Reglamento (CE) No. 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) No. 339/93". Disponible en http://data.europa.eu/eli/reg/2008/765/oj/spa [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2009): "Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:320 09L0024 [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2014): "Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE". Disponible en http://data.europa.eu/eli/dir/2014/53/oj/spa [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2019): "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) No. 765/2008 y (UE) No. 305/2011". Disponible en www.boe.es/doue/2019/169/L00001-00044.pdf [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2022): "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) No. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)". Disponible en http://data.europa.eu/eli/dir/2022/2555/oj/spa [fecha de consulta: 2 de julio de 2024].

Parlamento Europeo y el Consejo (2023): "Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo". Disponible en http://data.europa.eu/eli/reg/2023/1230/oj/spa [fecha de consulta: 2 de julio de 2024].

Unión Europea (2016): "Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea". Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016ME%2FTXT [fecha de consulta: 2 de julio de 2024].

Unión Europea (2024): "Marcado CE: obtención del certificado, requisitos de la UE". Disponible en https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_es.htm [fecha de consulta: 29 de abril de 2024].

Jurisprudencia

Tribunal de Justicia de las Comunidades Europeas (1979): sentencia del 20 de febrero de 1979, *Rewe-Zentral AG* contra *Bundesmonopolverwaltung für Branntwein*, No. asunto 120/78, ECLI:EU: C:1979:42, (1979). Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61978CJ0120&qid=1696245206286 [fecha de consulta: 2 de julio de 2024].

Tribunal de Justicia de la Unión Europea (2015): sentencia del Tribunal de Justicia (Sala Cuarta) de 5 de marzo de 2015. Asuntos C-503/13 y C-504/13. *Boston Scientific Medizintechnik GmbH v. AOK Sachsen-Anhalt - Die Gesundheitskasse y Betrieb skrankenkasse RWE* - ECLI:EU:C:2015:148, (2015). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62013CJ0503&qid=1663677324293&from=ES. [fecha de consulta: 2 de julio de 2024].

Tribunal General de la Unión Europea (2022): sentencia del Tribunal General (Sala sexta ampliada) del 14 de septiembre de 2022. Google LLC y Alphabet, Inc contra Comisión Europea, No. Asunto T-604/18, ECLI:EU:T:2022:541, (2022). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62018TJ0604&qid=1712832601736 [fecha de consulta: 2 de julio de 2024].