COMISIÓN
EUROPEA

Bruselas, 19.2.2020
COM(2020) 64 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO, 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

INFORME SOBRE LAS REPERCUSIONES EN MATERIA DE SEGURIDAD Y RESPONSABILIDAD CIVIL DE LA INTELIGENCIA ARTIFICIAL, EL INTERNET DE LAS COSAS Y LA ROBÓTICA

1. Introducción

La inteligencia artificial («IA»)[1], el internet de las cosas[2] y la robótica crearán nuevas oportunidades y ventajas para nuestra sociedad. La Comisión ha reconocido la importancia y el potencial de estas tecnologías y la necesidad de invertir de manera significativa en estos ámbitos[3], y se ha comprometido a convertir a Europa en líder mundial en los ámbitos de la IA, el internet de las cosas y la robótica. Para lograr este objetivo es preciso un marco jurídico claro y predecible que trate los aspectos difíciles de índole tecnológica.

1.1. Marco existente en materia de seguridad y responsabilidad civil

El objetivo general de los marcos jurídicos en materia de seguridad y de responsabilidad civil es garantizar que todos los productos y servicios, incluidos aquellos que incorporan tecnologías digitales emergentes, funcionen de manera segura, fiable y coherente y que los daños que puedan ocasionarse se reparen de forma eficiente. Contar con niveles elevados de seguridad de los productos y sistemas que incorporan nuevas tecnologías digitales y con mecanismos solventes de reparación de los daños (esto es, el marco en materia de responsabilidad civil) contribuye a proteger mejor a los consumidores y, por otra parte, genera confianza en estas tecnologías, que es una condición previa para que las adopten la industria y los usuarios. Esto, a su vez, potenciará la competitividad de nuestra industria y contribuirá a los objetivos de la Unión[4]. La existencia de un marco claro en materia de seguridad y responsabilidad civil es particularmente importante cuando surgen nuevas tecnologías como la IA, el internet de las cosas y la robótica, para así garantizar tanto la protección de los consumidores como la seguridad jurídica para las empresas.

La Unión tiene un marco regulador solvente y fiable en materia de seguridad y responsabilidad civil por los daños causados por productos defectuosos, así como un conjunto sustancial de normas de seguridad, complementado por la legislación nacional no armonizada en materia de responsabilidad civil. Juntos garantizan el bienestar de nuestros ciudadanos en el mercado único y fomentan la innovación y la asimilación tecnológica. Sin embargo, la IA, el internet de las cosas y la robótica están transformando las características de muchos productos y servicios.

En la Comunicación sobre la inteligencia artificial para Europa[5], adoptada el 25 de abril de 2018, se anunció que la Comisión presentaría un informe en el que se evaluarían las

---

1 La definición de inteligencia artificial del grupo de expertos de alto nivel sobre la IA puede consultarse en: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

2 La definición del internet de las cosas contenida en la Recomendación UIT-T Y.2060 puede consultarse en: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 y COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_es.

5 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2018%3A237%3AFIN.
En el documento de trabajo de los servicios de la Comisión anejo, SWD(2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137), se hizo una recopilación inicial de los problemas en materia de responsabilidad civil que plantean las tecnologías digitales emergentes.

repercusiones de las tecnologías digitales emergentes en los marcos existentes en materia de seguridad y responsabilidad civil. El presente informe tiene por fin determinar y analizar las repercusiones de carácter general y los posibles resquicios jurídicos de los marcos en materia de responsabilidad civil y de seguridad de la IA, el internet de las cosas y la robótica. Las directrices que figuran en el presente informe, que acompaña al Libro Blanco sobre la inteligencia artificial, sirven como elemento de debate y forman parte de una consulta más amplia de las partes interesadas. La sección sobre seguridad se basa en la evaluación[6] de la Directiva sobre máquinas [7] y la colaboración con los grupos de expertos pertinentes[8]. La sección sobre responsabilidad civil se basa en la evaluación[9] de la Directiva sobre responsabilidad por los daños causados por productos defectuosos[10], las aportaciones de grupos de expertos pertinentes[11] y las consultas con las partes interesadas. El presente informe no pretende ofrecer una perspectiva exhaustiva de la normativa vigente en materia de seguridad y responsabilidad civil, sino que se centra en las cuestiones clave señaladas hasta ahora.

1.2. Características de las tecnologías de la IA, el internet de las cosas y la robótica

La IA, el internet de las cosas y la robótica comparten muchas características. Combinan la **conectividad**, la **autonomía** y la **dependencia de datos** para llevar a cabo tareas con poco o ningún control o supervisión humanos. Los sistemas equipados con IA pueden mejorar la ejecución de sus propias tareas aprendiendo de la experiencia. Su **complejidad** se refleja tanto en la pluralidad de agentes económicos que participan en la **cadena de suministro** como en la multiplicidad de partes, componentes, programas informáticos, sistemas y servicios que forman conjuntamente los nuevos ecosistemas tecnológicos. A ello hay que añadir que su **código está abierto** a actualizaciones y mejoras tras su comercialización. Los enormes volúmenes de datos, la dependencia que tienen de los algoritmos y la **opacidad** que lleva aparejada la toma de decisiones por parte de la IA hacen más difícil predecir el comportamiento de un producto basado en la IA y comprender cuáles han podido ser las causas de los daños causados. Por último, la conectividad y el hecho de que su código esté abierto también pueden exponer a **ciberamenazas** a los productos de IA y de internet de las cosas.

---

6 Documento SWD(2018) 161 final.

7 Directiva 2006/42/CE.

8 La Red de Seguridad de los Consumidores establecida en virtud de la Directiva 2001/95/CE relativa a la seguridad general de los productos y los grupos de expertos sobre la Directiva 2006/42/CE relativa a las máquinas y la Directiva 2014/53/UE sobre equipos radioeléctricos compuestos por los Estados miembros, la industria y otras partes interesadas, como las asociaciones de consumidores.

9 COM(2018) 246 final.

10 Directiva 85/374/CEE.

11 El grupo de expertos sobre responsabilidad y nuevas tecnologías se creó para que la Comisión cuente con conocimientos especializados sobre la aplicabilidad de la Directiva sobre responsabilidad por los daños causados por productos defectuosos y de las normas nacionales en materia de responsabilidad civil, y con ayuda para elaborar principios rectores para posibles adaptaciones de la normativa aplicable a las nuevas tecnologías. Se compone de dos formaciones, la formación sobre responsabilidad civil por los daños causados por productos defectuosos y formación sobre nuevas tecnologías; consúltese el enlace siguiente: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1&Lang=ES.
Para consultar el informe sobre la formación de nuevas tecnologías en relación con la responsabilidad civil por la inteligencia artificial y otras tecnologías emergentes, véase https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

1.3. Oportunidades que brindan la IA, el internet de las cosas y la robótica

El aumento de la confianza de los usuarios y de su aceptación social de las tecnologías emergentes, la mejora de los productos, los procesos y los modelos empresariales y la posibilidad de que los fabricantes europeos sean más eficientes son solo algunas de las oportunidades que brindan la IA, el internet de las cosas y la robótica.

Además de aumentar la productividad y la eficiencia, la IA también promete que los seres humanos podrán alcanzar cotas de inteligencia aún ignotas, al facilitar nuevos descubrimientos y ayudar a resolver algunos de los mayores problemas del mundo: desde el tratamiento de enfermedades crónicas, la predicción de brotes de enfermedad o la reducción de las tasas de mortalidad por accidentes de tráfico hasta la lucha contra el cambio climático o la anticipación de las amenazas a la ciberseguridad.

Estas tecnologías pueden aportar numerosas ventajas al mejorar la seguridad de los productos y hacerlos menos propensos a ciertos riesgos. Por ejemplo, los vehículos conectados y automatizados podrían mejorar la seguridad vial, ya que la mayoría de los accidentes de tráfico se deben en la actualidad a errores humanos[12]. Por otra parte, los sistemas basados en el internet de las cosas están diseñados para recibir y tratar enormes volúmenes de datos procedentes de distintas fuentes. Esta mayor cantidad de información podría utilizarse para que los productos sean autoadaptativos y, por lo tanto, más seguros. Las nuevas tecnologías pueden contribuir a mejorar la eficacia de las recuperaciones de productos, ya que, por ejemplo, los productos podrían alertar a los usuarios para evitar problemas de seguridad[13]. Si se plantea un problema de seguridad al usar un producto conectado, los productores pueden comunicarse directamente con los usuarios para, en primer lugar, advertir a los usuarios sobre los riesgos y, en segundo lugar, si es posible, arreglar directamente el problema facilitando, por ejemplo, una actualización de seguridad. Por ejemplo, en una operación de recuperación de uno de sus productos en 2017, un productor de teléfonos inteligentes llevó a cabo una actualización del sistema para reducir a cero la batería de los teléfonos en cuestión[14], de modo que los usuarios no pudiesen utilizarlos.

Por otra parte, las nuevas tecnologías pueden contribuir a mejorar la trazabilidad de los productos. Por ejemplo, gracias a las funcionalidades de conectividad del internet de las cosas las empresas y las autoridades de vigilancia del mercado pueden encontrar los productos peligrosos y detectar riesgos en las cadenas de suministro[15].

Si bien la IA, el internet de las cosas y la robótica pueden generar oportunidades para la economía y nuestras sociedades, también pueden crear un riesgo de perjuicio de intereses jurídicamente protegidos, tanto materiales como inmateriales. El riesgo de que se produzcan tales perjuicios aumentará a medida que adquieran mayor implantación las diferentes aplicaciones informáticas. En este contexto, resulta esencial analizar si el actual marco

[12] Se calcula que alrededor del 90 % de los accidentes de tráfico se debe a errores humanos. Véase el informe de la Comisión «Salvar vidas: impulsar la seguridad de los vehículos en la UE» [COM(2016) 0787 final].

[13] Por ejemplo, se puede advertir al conductor de un automóvil que frene si ha producido un accidente más adelante.

[14] OCDE (2018), «Measuring and maximising the impact of product recalls globally: OECD workshop report», *OECD Science, Technology and Industry Policy Papers*, n.º 56, OECD Publishing, París (https://doi.org/10.1787/ab757416-en).

[15] OCDE (2018), «Enhancing product recall effectiveness globally: OECD background report», *OECD Science, Technology and Industry Policy Papers*, n.º 58, OECD Publishing, París (https://doi.org/10.1787/ef71935c-en).

jurídico en materia de seguridad y responsabilidad civil sigue siendo adecuado para proteger a los usuarios y en qué medida.

2. Seguridad

En la Comunicación de la Comisión «Generar confianza en la inteligencia artificial centrada en el ser humano» se dice que «**los sistemas de IA deben integrar mecanismos de seguridad y de seguridad desde el diseño para garantizar que sean verificablemente seguros en cada fase**, teniendo muy presente la **seguridad física y psicológica** de todos los afectados»[16].

La evaluación de la normativa de la Unión en materia de seguridad de los productos que se realiza en la presente sección analiza si el marco legislativo actual de la Unión contiene los elementos necesarios para garantizar que las tecnologías emergentes y los sistemas de IA en particular integran funcionalidades de seguridad y de seguridad desde el diseño.

El presente informe examina principalmente la Directiva sobre seguridad general de los productos[17], así como la normativa sobre productos armonizada que sigue las normas horizontales del «nuevo enfoque»[18] y/o el «nuevo marco legislativo» (en lo sucesivo, «el marco o la normativa de la Unión en materia de seguridad de los productos»)[19]. Las normas horizontales garantizan la coherencia entre las normas sectoriales sobre seguridad de los productos.

La normativa de la Unión en materia de seguridad de los productos tiene por objeto garantizar que los productos comercializados en el mercado de la Unión cumplan unos requisitos elevados en materia de salud, seguridad y medio ambiente, y que dichos productos puedan circular libremente por toda la Unión. La normativa sectorial[20] se complementa con la Directiva sobre seguridad general de los productos[21], que exige que todos los productos de consumo, aunque no estén regulados por la normativa sectorial de la Unión, sean seguros. Las normas de seguridad se complementan con la vigilancia del mercado y la atribución de competencias a las autoridades nacionales en virtud del Reglamento sobre la vigilancia del mercado[22] y la Directiva sobre seguridad general de los productos[23]. En el ámbito del transporte, hay normas de la UE y nacionales adicionales para la puesta en circulación de un

---

16 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Generar confianza en la inteligencia artificial centrada en el ser humano» [COM(2019) 168 final].

17 Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DO L 11 de 15.1.2002, p. 4).

18 DO C 136 de 4.6.1985, p. 1.

19 Reglamento (CE) n.º 765/2008 y Decisión n.º 768/2008/CE.

20 No se incluye la normativa de la Unión en materia de transporte y turismos.

21 Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (DO L 11 de 15.1.2002, p. 4).

22 Reglamento (CE) n.º 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) n.º 339/93 (DO L 218 de 13.8.2008, p. 30) (https://eur-lex.europa.eu/eli/reg/2008/765/oj?locale=es) y, de 2021 en adelante, el 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) n.º 765/2008 y (UE) n.º 305/2011 (DO L 169 de 25.6.2019, p. 1) (https://eur-lex.europa.eu/eli/reg/2019/1020/oj?locale=es).

23 Artículo 8, apartado 1, letra b), y apartado 3, de la Directiva sobre seguridad general de los productos.

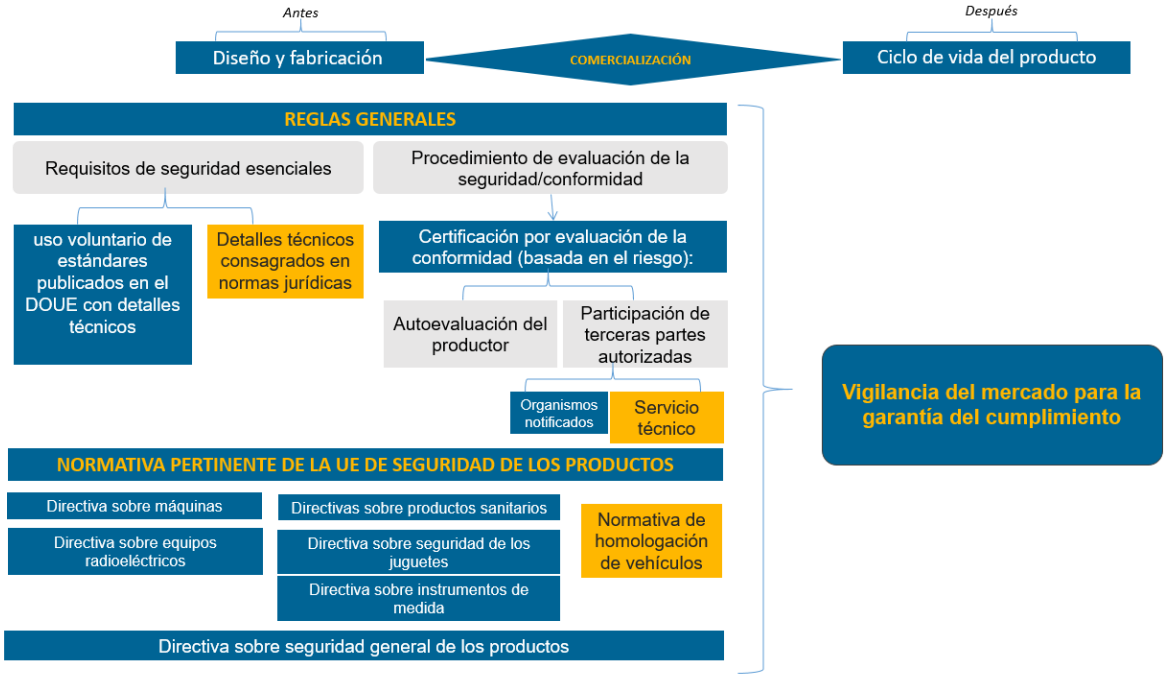
vehículo de motor[24], una aeronave o un buque y normas claras que rigen la seguridad durante el funcionamiento, con indicación de tareas para los operadores, así como tareas de vigilancia para las autoridades.

La normalización europea es otro elemento fundamental de la normativa de la Unión en materia de seguridad de los productos. Dado el carácter mundial de la digitalización y de las tecnologías digitales emergentes, la cooperación internacional en el ámbito de la normalización reviste una importancia especial para la competitividad de la industria europea.

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. Por lo tanto, no incorpora en todos los casos disposiciones que traten explícitamente los nuevos riesgos y dificultades de estas tecnologías emergentes; sin embargo, dado que el marco actual en materia de seguridad de los productos es tecnológicamente neutro, ello no implica que no pueda aplicarse a los productos que incorporan estas tecnologías. Por otra parte, los actos normativos posteriores de dicho marco, como ocurre en los sectores de los productos sanitarios o de los automóviles, ya han tenido en cuenta explícitamente algunos aspectos ligados a la aparición de las tecnologías digitales, como, por ejemplo, la automatización de las decisiones, la consideración de los programas informáticos como productos independientes y la conectividad.

[24] Por ejemplo, la Directiva 2007/46/CE por la que se crea un marco para la homologación de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos, y el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y por el que se deroga la Directiva 2007/46/CE.

Lógica en que se basa la normativa en vigor de la Unión en materia de seguridad de los productos[25]



A continuación, se describen las dificultades que las tecnologías digitales emergentes presentan para el marco de la Unión en materia de seguridad de los productos.

La **conectividad** es una funcionalidad fundamental de un número cada vez mayor de productos y servicios. Esta funcionalidad pone en jaque el concepto tradicional de seguridad, ya que la conectividad puede, directamente, comprometer la seguridad del producto e, indirectamente, cuando es susceptible de ser pirateado, dar lugar a amenazas para la seguridad y afectar a la seguridad de los usuarios.

Sirva de ejemplo la notificación de Islandia en el Sistema de alerta rápida para productos peligrosos no alimenticios de la UE («RAPEX», por sus siglas en inglés) en relación con un reloj de pulsera inteligente para niños[26]. Si bien el producto no podía causar un daño directo al niño, sin un nivel mínimo de seguridad, podía utilizarse fácilmente como medio para tener acceso al niño. Dado que una de las funciones previstas del producto es mantener seguros a los niños al tenerlos localizados, el consumidor tiene la expectativa legítima de que no supone una amenaza para la seguridad de los niños debido a la posibilidad de ser rastreados y/o contactados.

Otro ejemplo válido es el de una notificación de Alemania en relación con un turismo[27]. La radio del vehículo presentaba ciertas deficiencias de seguridad en el *software* que hacían posible el acceso de terceros no autorizados a los sistemas de control interconectados del vehículo, con lo que, si un tercero con ánimo doloso se sirviese de estas deficiencias, podría producirse un accidente de tráfico.

[25] No se incluyen los requisitos normativos relativos al ciclo de vida de los productos, es decir, el uso y el mantenimiento; solo sirve para fines ilustrativos generales.
[26] Notificación RAPEX de Islandia publicada en el sitio web EU Safety Gate (A12/0157/19).
[27] Notificación RAPEX de Alemania publicada en el sitio web EU Safety Gate (A12/1671/15).

Las aplicaciones industriales también pueden estar expuestas a ciberamenazas que afecten a la seguridad de las personas a mayor escala cuando tales aplicaciones carezcan de los niveles de seguridad necesarios, como, por ejemplo, los ciberataques contra un sistema de control crítico de una planta industrial con el fin de desencadenar una explosión que pueda ocasionar muertes.

La normativa de la Unión en materia de seguridad de los productos no establece, por norma general, requisitos esenciales obligatorios específicos frente a las ciberamenazas que afecten a la seguridad de los usuarios. Sin embargo, existen disposiciones en materia de seguridad en el Reglamento sobre los productos sanitarios[28], la Directiva sobre instrumentos de medida[29], la Directiva sobre equipos radioeléctricos[30] y la Directiva sobre homologación de tipo de los vehículos[31]. El Reglamento sobre la ciberseguridad[32] establece marcos voluntarios de certificación de la ciberseguridad para productos, servicios y procesos de tecnologías de la información y la comunicación, y la normativa pertinente de la Unión en materia de seguridad de los productos establece requisitos obligatorios.

Por otra parte, el riesgo de pérdida de conexión de las tecnologías digitales emergentes también puede entrañar riesgos relacionados con la seguridad. Por ejemplo, si una alarma contra incendios conectada pierde la conexión, podría no alertar al usuario en caso de incendio.

La seguridad en la normativa actual de la Unión en materia de seguridad de los productos es un objetivo de orden público. El concepto de seguridad está vinculado al uso del producto y a los riesgos, por ejemplo, mecánicos, eléctricos, etc., que deben tratarse para garantizar la seguridad del producto. Cabe señalar que, según el acto normativo de la Unión en materia de seguridad de los productos de que se trate, el uso del producto abarca no solo el uso previsto sino también el uso previsible y, en algunos casos, como en la Directiva sobre máquinas[33], incluso el mal uso razonablemente previsible.

El concepto de seguridad de la normativa en vigor de la Unión en materia de seguridad de los productos es un concepto amplio de seguridad, para proteger a los consumidores y los usuarios. Por tanto, el concepto de seguridad de los productos abarca la protección contra todo tipo de riesgos derivados del producto, incluidos no solo los riesgos mecánicos, químicos y eléctricos, sino también los riesgos cibernéticos y los riesgos relacionados con la pérdida de conexión de los productos.

Se podría contemplar adoptar disposiciones explícitas en relación con el ámbito de aplicación de los actos normativos de la Unión pertinentes con el fin de ofrecer una mejor protección a los usuarios y una mayor seguridad jurídica.

[28] Reglamento (UE) 2017/745, sobre los productos sanitarios.
[29] Directiva 2014/32/UE, sobre la comercialización de instrumentos de medida.
[30] Directiva 2014/53/UE, sobre equipos radioeléctricos.
[31] Directiva 2007/46/CE, sobre la homologación de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos. La Directiva será derogada y sustituida por el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y por el que se deroga la Directiva 2007/46/CE, que comenzará a desplegar efectos a partir del 1 de septiembre de 2020.
[32] Reglamento (UE) 2019/881.
[33] Directiva 2006/42/CE, sobre máquinas.

La **autonomía**[34] es una de las funcionalidades principales de la IA. Los resultados no deseados producidos por la IA podrían perjudicar a los usuarios y a las personas expuestas a ella.

Puesto que el «comportamiento» de los productos de IA puede determinarse previamente mediante la evaluación del riesgo realizada por el fabricante antes de la comercialización de los productos, el marco de la Unión en materia de seguridad de los productos ya establece obligaciones para que los productores tengan en cuenta en la evaluación del riesgo el «uso»[35] de los productos a lo largo de su vida útil. También dispone que los fabricantes deben ofrecer instrucciones e información de seguridad para los usuarios o advertencias[36]. En este contexto, por ejemplo, la Directiva sobre equipos radioeléctricos[37] exige al fabricante que incluya instrucciones sobre cómo utilizar el equipo radioeléctrico de conformidad con su uso previsto.

También pueden darse situaciones en las que los resultados de los sistemas de IA no puedan determinarse por completo por adelantado. En tales situaciones, la evaluación del riesgo realizada antes de comercializar el producto no puede seguir reflejando el uso, el funcionamiento o el comportamiento del producto. En estos casos y siempre que se vea modificado el uso inicialmente previsto por el fabricante[38] debido al comportamiento autónomo y ello tenga repercusiones para el cumplimiento de los requisitos de seguridad, se puede contemplar la necesidad de exigir una nueva evaluación del producto que incorpora aprendizaje automático[39].

De acuerdo con el marco actual, cuando los productores tengan conocimiento de que un producto, a lo largo de todo su ciclo de vida, presenta riesgos en materia de seguridad, deben informar inmediatamente a las autoridades competentes y tomar medidas para prevenir los riesgos para los usuarios[40].

---

[34] Si bien los productos basados en la IA pueden actuar de manera autónoma sirviéndose de su percepción del entorno sin seguir una serie de instrucciones predeterminadas, su comportamiento está limitado por el objetivo que se les ha asignado y otras opciones de diseño pertinentes decididas por sus desarrolladores.

[35] En la normativa de la Unión en materia de seguridad de los productos, los productores hacen la evaluación del riesgo basándose en el uso previsto del producto, en el uso previsible y/o en el mal uso razonablemente previsible.

[36] Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82). El anexo I, artículo R2, apartado 7, dice: «[l]os fabricantes garantizarán que el producto vaya acompañado de las instrucciones y la información relativa a la seguridad en una lengua fácilmente comprensible para los consumidores y otros usuarios finales, según lo que decida el Estado miembro de que se trate».

[37] El artículo 10, apartado 8, relativo a las instrucciones para el usuario final y el anexo VI, relativo a la declaración UE de conformidad.

[38] Hasta ahora, el aprendizaje automático se ha utilizado, en el contexto de la IA, principalmente para indicar que las máquinas son capaces de aprender durante su entrenamiento. Todavía no se exige que las máquinas basadas en la IA sigan aprendiendo después de su puesta en funcionamiento; por el contrario, y especialmente en el ámbito de la asistencia sanitaria, las máquinas basadas en la IA, por norma general, dejan de aprender una vez finalizan con éxito su entrenamiento. Así pues, que, en esta fase, los sistemas de IA tengan un comportamiento autónomo no significa que el producto desempeñe tareas no previstas por los desarrolladores.

[39] Esta exigencia está en consonancia con la Guía azul sobre la aplicación de la normativa de la UE relativa a los productos, de 2016, sección 2.1.

[40] Artículo 5 de la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos.

Además de la evaluación del riesgo realizada antes de comercializar un producto, podría establecerse un nuevo procedimiento de evaluación del riesgo cuando el producto sufra cambios importantes durante su vida útil; por ejemplo, distinta función del producto, no prevista por el fabricante en la evaluación inicial del riesgo. Dicha evaluación debería centrarse en las repercusiones en la seguridad derivadas del comportamiento autónomo durante la vida útil del producto. La evaluación del riesgo debe ser realizada por el agente económico correspondiente. Con carácter adicional, se podrían añadir en los actos normativos pertinentes de la Unión requisitos reforzados para los fabricantes sobre las instrucciones y advertencias para los usuarios.

Ya se exigen evaluaciones del riesgo similares en la normativa en materia de transporte[41]; por ejemplo, en la normativa sobre transporte ferroviario, cuando se modifica un vehículo ferroviario después de su certificación, el autor de la modificación tiene la obligación de someterse a un procedimiento específico y se definen criterios claros para determinar si la autoridad debe intervenir o no.

La funcionalidad de aprendizaje automático de los productos y sistemas de IA puede posibilitar que la máquina tome decisiones que varíen respecto de lo inicialmente previsto por los productores y, en consecuencia, lo que esperan los usuarios. Esto plantea dudas sobre el control humano, a saber, que los seres humanos puedan elegir si delegan, y cómo, la toma de decisiones en productos y sistemas de IA, para lograr objetivos determinados por el ser humano[42]. La normativa en vigor de la Unión en materia de seguridad de los productos no trata explícitamente la supervisión humana en el contexto de los productos y sistemas de IA que incorporan aprendizaje automático[43].

Los actos normativos pertinentes de la Unión pueden contemplar requisitos específicos de supervisión humana, que sirvan como salvaguarda, desde el diseño y durante todo el ciclo de vida de los productos y sistemas de IA.

El «comportamiento» futuro de las aplicaciones de IA podría generar **riesgos para la salud mental**[44] de los usuarios, derivados, por ejemplo, de su colaboración con robots y sistemas con IA humanoide, en el hogar o en entornos de trabajo. A este respecto, en la actualidad, la seguridad se refiere normalmente a la percepción del usuario de una amenaza de daño físico que puede derivarse de la tecnología digital emergente. Al mismo tiempo, en el marco

---

41 En el anexo I del Reglamento de Ejecución (UE) 2015/1136 de la Comisión (DO L 185 de 14.7.2015, p. 6) se describe el proceso a seguir de producirse un cambio en el sistema ferroviario que pueda afectar a la seguridad (por ejemplo, un cambio técnico u operativo o un cambio organizativo que pueda afectar al proceso operativo o de mantenimiento).
En caso de «cambio significativo», un organismo de evaluación independiente, que podría ser la autoridad nacional de seguridad u otro organismo competente técnicamente, debe presentar un informe de evaluación de la seguridad al proponente del cambio.
Tras el proceso de análisis del riesgo, el proponente aplicará medidas adecuadas para mitigar los riesgos (si el proponente es una empresa ferroviaria o una infraestructura gestionada, la aplicación del Reglamento forma parte de su sistema de gestión de la seguridad, cuya aplicación es supervisada por la autoridad nacional de seguridad).

42 Recomendaciones estratégicas y de inversión para una IA fiable, grupo de expertos de alto nivel sobre la IA, junio de 2019.

43 Sin embargo, ello no es óbice para que pueda ser necesaria la supervisión en situaciones concretas en virtud de algunas de las obligaciones más generales existentes en materia de comercialización del producto.

44 Constitución de la OMS, primer punto: «La salud es un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades» (https://www.who.int/es/about/who-we-are/constitution).

jurídico de la Unión se define como producto seguro aquel que no presenta ningún riesgo o solo el riesgo mínimo para la seguridad y la salud de las personas. Existe un consenso bastante extendido acerca de que la definición de «salud» incluye tanto el bienestar físico como el bienestar mental. No obstante, los riesgos para la salud mental deben incluirse explícitamente en el concepto de seguridad de los productos en el marco legislativo.

La autonomía no debe provocar ni estrés ni malestar excesivos por períodos prolongados y tampoco debe perjudicar la salud mental. En este sentido, los factores que favorecen la sensación de seguridad de las personas de más edad[45] suelen ser: tener control sobre sus rutinas diarias, ser informados sobre ellas y contar con una relación segura con el personal sanitario. Los productores de robots que interactúen con personas mayores deben tener en cuenta estos factores para prevenir los riesgos para la salud mental.

Podría contemplarse incluir en la normativa pertinente de la UE obligaciones explícitas de los productores de, por ejemplo, robots con IA humanoide, para que valoren expresamente el daño mental que sus productos pueden causar a los usuarios, en particular los usuarios vulnerables como las personas mayores en entornos sanitarios.

Otra característica fundamental de los productos y sistemas basados en la IA es la **dependencia de datos**. La exactitud y pertinencia de los datos es esencial para garantizar que los sistemas y productos basados en la IA tomen las decisiones previstas por el productor.

La normativa de la Unión en materia de seguridad de los productos no trata explícitamente el tema de los riesgos para la seguridad derivados de datos erróneos. Sin embargo, según cuál sea el «uso» del producto, los productores deben anticipar durante las fases de diseño y ensayo la exactitud de los datos y su pertinencia para las funciones de seguridad.

Por ejemplo, un sistema basado en la IA diseñado para detectar objetos específicos puede tener dificultades para reconocer objetos en condiciones de iluminación deficientes, por lo que los diseñadores deben incluir datos procedentes de ensayos de productos en entornos tanto típicos como mal iluminados.

Otro ejemplo es el de los robots agrícolas, como los robots de recogida de frutas, que tienen por objeto reconocer y localizar las frutas maduras en rama o sobre el terreno. Si bien los algoritmos correspondientes ya muestran unas tasas de acierto superiores al 90 %, un defecto en los conjuntos de datos de los que se nutren dichos algoritmos puede hacer que dichos robots tomen una decisión errónea y acaben lesionando a un animal o a una persona.

La cuestión que se plantea es si la normativa de la Unión en materia de seguridad de los productos debe incluir requisitos específicos en la fase de diseño en relación con el riesgo para la seguridad derivado de datos erróneos, así como mecanismos para garantizar la calidad de los datos cuando se usan con productos y sistemas de IA.

La **opacidad** es otra característica principal de algunos de los productos y sistemas basados en la IA, que puede derivar de la capacidad de mejorar la ejecución de sus tareas aprendiendo de la experiencia. En función del enfoque metodológico, los productos y sistemas basados en la IA pueden caracterizarse por diversos grados de opacidad, lo que puede hacer que el proceso de toma de decisiones sea difícil de determinar («efecto caja negra»). Si bien los humanos no tienen por qué comprender todos y cada uno de los pasos del proceso de toma de decisiones, dado que los algoritmos de la IA se van volviendo más avanzados e introduciendo

[45] Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, pp.237-264, Research, Neziha Akalin, Annica Kristoff ersson y Amy Loutfi, julio de 2019.

en ámbitos críticos, es fundamental que los humanos puedan comprender cómo toma el sistema las decisiones algorítmicas. Este aspecto reviste especial importancia para el mecanismo de control *a posteriori*, ya que hará posible que las autoridades de garantía del cumplimiento puedan localizar al responsable original de los comportamientos y opciones de los sistemas de IA. Así se reconoce también en la Comunicación de la Comisión «Generar confianza en la inteligencia artificial centrada en el ser humano»[46].

La normativa de la Unión en materia de seguridad de los productos no trata explícitamente el tema del aumento de los riesgos derivados de la opacidad de los sistemas basados en algoritmos. Por consiguiente, es necesario contemplar la posibilidad de introducir requisitos de transparencia de los algoritmos, así como de solidez, rendición de cuentas y, cuando proceda, supervisión humana y resultados imparciales[47], lo cual reviste especial importancia para el mecanismo de control *a posteriori* y para generar confianza en el uso de estas tecnologías. Una forma de afrontar esta cuestión puede ser imponer obligaciones a los desarrolladores de los algoritmos de modo que tengan que revelar los parámetros de diseño y los metadatos de los conjuntos de datos si se producen accidentes.

Otros riesgos adicionales que pueden afectar a la seguridad son los derivados de la **complejidad de los productos y los sistemas**, ya que una serie de componentes, dispositivos y productos pueden integrarse e influir en el funcionamiento de los otros (p. ej., productos que forman parte de un ecosistema doméstico inteligente).

Esta complejidad ya se trata en el marco jurídico de la Unión en materia de seguridad al que se hace referencia al principio de esta sección[48]. En concreto, cuando el productor lleve a cabo la evaluación del riesgo del producto, debe considerar el uso previsto, el uso previsible y, en su caso, el mal uso razonablemente previsible.

Por ello, **si el productor prevé que su dispositivo estará interconectado e interactuará con otros dispositivos, debe considerar estos aspectos en la evaluación del riesgo**. Los usos o malos usos se determinan sobre la base, por ejemplo, de la experiencia de usos pasados del mismo tipo de producto, las investigaciones de accidentes o el comportamiento humano.

La complejidad de los sistemas también se trata más específicamente en la normativa sectorial de seguridad, como el Reglamento sobre los productos sanitarios y, en cierto grado, la Directiva relativa a la seguridad general de los productos[49]. Por ejemplo, el productor de un dispositivo conectado, destinado a formar parte de un ecosistema doméstico inteligente, debe poder prever razonablemente que sus productos tendrán un efecto en la seguridad de otros productos.

Por otra parte, la normativa en materia de transporte trata esta complejidad a nivel del sistema. En el caso de los automóviles, los trenes y los aviones, se homologan y certifican tanto cada componente como todo el vehículo o aeronave. La aptitud para circular, la aeronavegabilidad y la interoperabilidad ferroviaria forman parte de la evaluación de la

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.

[47] Sobre la base de los requisitos clave propuestos en las directrices éticas para una IA fiable del grupo de expertos de alto nivel sobre la IA: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

[48] Reglamento (CE) n.º 765/2008 y Decisión n.º 768/2008/CE y la normativa sectorial armonizada sobre seguridad de los productos, por ejemplo, la Directiva 2006/42/CE, sobre máquinas.

[49] El artículo 2 de la Directiva sobre seguridad general de los productos especifica que un producto seguro tendrá en cuenta el «efecto sobre otros productos cuando razonablemente se pueda prever la utilización del primero junto con los segundos».

seguridad. En materia de transporte, los «sistemas» deben ser «autorizados» por una autoridad, bien sobre la base de una evaluación de la conformidad con requisitos técnicos claros realizada por una tercera parte, bien tras una demostración sobre cómo se afrontan los riesgos. Por lo general, la solución combina elementos de producto y de sistema.

La normativa de la Unión en materia de seguridad de los productos, incluida la normativa en materia de transporte, ya tiene en cuenta, en cierta medida, la complejidad de los productos y sistemas para hacer frente a los riesgos que pueden afectar a la seguridad de los usuarios.

Los sistemas complejos suelen incorporar **programas informáticos**, que son un componente esencial de un sistema basado en la IA. Por lo general, como parte de la evaluación inicial del riesgo, el fabricante del producto final tiene la obligación de prever los riesgos de los programas informáticos integrados en ese producto en el momento de su comercialización.

Determinadas normas de la Unión en materia de seguridad de los productos hacen una referencia explícita a los programas informáticos integrados en el producto. Por ejemplo, la Directiva sobre máquinas[50] exige que los posibles fallos de los programas informáticos del sistema de control no den lugar a situaciones peligrosas.

En la normativa de la Unión en materia de seguridad de los productos, las actualizaciones de los programas informáticos podrían compararse a las operaciones de mantenimiento por razones de seguridad, siempre que no modifiquen significativamente un producto ya comercializado ni introduzcan riesgos nuevos que no estaban previstos en la evaluación inicial del riesgo. Sin embargo, si la actualización de los programas informáticos modifica sustancialmente el producto en el que se descarga, la totalidad del producto podría considerarse un nuevo producto y el cumplimiento de la normativa pertinente en materia de seguridad de los productos debe volver a evaluarse en el momento en que se realice la modificación[51].

La normativa armonizada sectorial de la Unión en materia de seguridad de los productos no contiene, en general, disposiciones específicas para los programas informáticos autónomos, en la versión en que fueron comercializados originalmente o en la versión en que han sido cargados tras la comercialización del producto. Sin embargo, algunos actos normativos de la Unión regulan estos programas informáticos autónomos; por ejemplo, el Reglamento sobre los productos sanitarios. Además, los programas informáticos autónomos cargados en los productos conectados que se comunican a través de determinados módulos de radio[52] también pueden regularse por la Directiva sobre equipos radioeléctricos mediante actos delegados. Esta Directiva exige que determinadas categorías o clases de equipos de radio sean compatibles con funcionalidades que garanticen que la conformidad de dichos equipos no se vea comprometida cuando se carguen programas informáticos[53].

[50] Sección 1.2.1 del anexo I de la Directiva sobre máquinas.
[51] Guía azul sobre la aplicación de la normativa de la UE relativa a los productos, de 2016.
[52] Los módulos de radio son dispositivos electrónicos que transmiten y/o reciben señales de radio (Wifi, Bluetooth, etc.) entre dos dispositivos.
[53] Artículo 3, apartado 3, letra i), de la Directiva sobre equipos radioeléctricos.

Si bien la normativa de la Unión en materia de seguridad de los productos tiene en cuenta los riesgos para la seguridad derivados de los programas informáticos integrados en un producto en el momento de su comercialización y, posiblemente, de actualizaciones posteriores previstas por el fabricante, pueden ser necesarios requisitos específicos y/o explícitos para los programas informáticos autónomos (por ejemplo, una aplicación que se descargue). Deben tenerse especialmente en cuenta los programas informáticos autónomos que garantizan las funciones de seguridad de los productos y sistemas de IA.

Pueden ser necesarias obligaciones adicionales para los fabricantes a fin de garantizar que ofrezcan funcionalidades para evitar la introducción de programas informáticos que afecten a la seguridad durante la vida útil de los productos de IA.

Por último, las tecnologías digitales emergentes se ven afectadas por las **cadenas de valor complejas**. Sin embargo, esta complejidad no es nueva ni solo un problema planteado por las nuevas tecnologías digitales emergentes como la IA o el internet de las cosas. Es el caso, por ejemplo, de productos como los ordenadores, los robots de servicios o los sistemas de transporte.

En el marco de la Unión en materia de seguridad de los productos, independientemente de la complejidad de la cadena de valor, la responsabilidad de la seguridad del producto recae en el productor que lo comercializa. Los productores son responsables de la seguridad del producto final, incluidas las partes integradas en el mismo, por ejemplo, los programas informáticos de un ordenador.

Algunos actos de la normativa de la Unión en materia de seguridad de los productos ya contienen disposiciones que se refieren explícitamente a situaciones en las que varios agentes económicos intervienen en un producto concreto antes de su comercialización. Por ejemplo, la Directiva sobre ascensores[54] obliga al agente económico que diseña y fabrica el ascensor a proporcionar al instalador «toda la documentación y la información necesarias para que pueda hacerlo de manera correcta y segura»[55]. La Directiva sobre máquinas obliga a los fabricantes de equipos a proporcionar información al operador sobre cómo montar dicho equipo con otra maquinaria[56].

La normativa de la Unión en materia de seguridad de los productos tiene en cuenta la complejidad de las cadenas de valor e impone obligaciones a una serie de agentes económicos en consonancia con el principio de «responsabilidad compartida».

Si bien la responsabilidad del productor respecto de la seguridad del producto final ha resultado ser adecuada para las cadenas de valor complejas actuales, contar con disposiciones explícitas que pidan específicamente la cooperación entre los agentes económicos de la cadena de suministro y los usuarios puede aportar seguridad jurídica quizás hasta en cadenas de valor más complejas. En particular, cada agente de la cadena de valor que influya en la seguridad del producto (por ejemplo, los productores de programas informáticos) y los usuarios (al modificar el producto) asumirían su responsabilidad y proporcionarían al siguiente agente de la cadena la información y las medidas necesarias.

[54] De conformidad con lo dispuesto en el artículo 16, apartado 2, de la Directiva 2014/33/UE.

[55] En la Directiva 2014/33/UE, sobre ascensores, el instalador es el equivalente del fabricante y debe asumir la responsabilidad del diseño, fabricación, instalación y comercialización del ascensor.

[56] La Directiva sobre máquinas, anexo I, artículo 1.7.4.2, dice: «Cada manual de instrucciones contendrá como mínimo, cuando proceda, la información siguiente:» [...] i) «las instrucciones de montaje, instalación y conexión, incluidos los planos, diagramas y medios de fijación y la designación del chasis o de la instalación en la que debe montarse la máquina».

3. Responsabilidad civil

A nivel de la Unión, las disposiciones en materia de seguridad de los productos y de responsabilidad civil por los productos son dos mecanismos complementarios que persiguen el mismo objetivo estratégico: un mercado de bienes único y operativo que garantice niveles elevados de seguridad, es decir, que reduzca al mínimo el riesgo de daños para los usuarios y contemple indemnizaciones de los daños originados por mercancías defectuosas.

En el ámbito nacional, los marcos de responsabilidad civil no armonizados complementan estas normas de la Unión garantizando la indemnización de los daños por causas diversas (como productos y servicios) y regulando la responsabilidad civil de distintas personas (como los propietarios, los agentes o los proveedores de servicios).

Por más que la optimización de las normas de seguridad de la Unión en materia de IA puede coadyuvar a evitar accidentes, estos pueden seguir ocurriendo. En estos casos entra en juego la responsabilidad civil. Las normas en materia de responsabilidad civil tienen una doble función en nuestra sociedad: por un lado, garantizan que las víctimas de un daño causado por otros perciban una indemnización y, por otro, proporcionan incentivos económicos a la parte responsable para que no cause dicho perjuicio. Las normas en materia de responsabilidad civil deben garantizar siempre un equilibrio entre la protección de los ciudadanos frente a los daños y la posibilidad de que las empresas innoven.

Los marcos de responsabilidad civil en la Unión han funcionado bien. Se basan en la aplicación paralela de la Directiva sobre responsabilidad por los daños causados por productos defectuosos (Directiva 85/374/CEE), que armonizó la responsabilidad civil de los fabricantes de productos defectuosos, y otros regímenes nacionales no armonizados.

La Directiva sobre responsabilidad por los daños causados por productos defectuosos proporciona un nivel de protección que no garantizan por sí solos los regímenes nacionales de responsabilidad subjetiva. Introduce un sistema de responsabilidad civil objetiva del productor por los daños causados por los defectos de sus productos. En caso de daño material o físico, la parte perjudicada tiene derecho a indemnización si puede probar el daño, el defecto del producto (es decir, que no ofrecía la seguridad que el público tiene derecho a esperar) y el nexo causal entre el producto defectuoso y el daño.

Los regímenes nacionales no armonizados tienen normas en materia de responsabilidad civil subjetiva, según las cuales las víctimas de daños deben probar la culpa de la persona responsable, el daño y la causalidad entre la culpa y el daño, para tener derecho a indemnización. También contemplan regímenes de responsabilidad objetiva, en los que el legislador nacional ha atribuido la responsabilidad civil por un riesgo a una persona concreta, sin necesidad de que la víctima pruebe la existencia de culpa o defecto o de causalidad entre la culpa o el defecto y el daño.

Los regímenes nacionales de responsabilidad civil proporcionan a las víctimas de daños causados por productos y servicios varias acciones indemnizatorias paralelas, basadas en la culpa o en la responsabilidad objetiva. Estas acciones se dirigen a menudo contra distintas personas responsables y se rigen por condiciones diferentes.

Por ejemplo, quien sufre un accidente de tráfico está legitimado, por lo general, para reclamar una indemnización al propietario del vehículo, independientemente de la culpa de este (es decir, la persona que contrata el seguro de responsabilidad civil obligatoria del vehículo), y reclamar al conductor por su responsabilidad subjetiva, ambas en virtud del Derecho civil nacional, así como para reclamar al fabricante, en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, si el coche tenía algún defecto.

De conformidad con las normas armonizadas en materia de seguro de vehículos automóviles, el uso del vehículo debe estar asegurado[57] y el asegurador es siempre, en la práctica, la primera persona a la que reclamar un indemnización por lesiones o daños materiales. Según estas normas, el seguro obligatorio compensa a la víctima y protege al asegurado, cuando en virtud de las normas del Derecho civil nacional[58] le corresponde pagar una indemnización por daños y perjuicios por el accidente del automóvil. Los productores no están sujetos a un seguro obligatorio en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos. Los vehículos autónomos no se tratan en la normativa de la Unión de forma diferente a los vehículos no autónomos en lo que se refiere al seguro del vehículo. Tales vehículos, como los demás vehículos, deben estar cubiertos por el seguro de responsabilidad civil obligatorio frente a terceros, que es la manera más sencilla de que la parte perjudicada obtenga una indemnización.

La suscripción de un seguro adecuado puede paliar los perjuicios de un accidente, ya que posibilita la indemnización expedita de la víctima. La existencia de normas claras en materia de responsabilidad civil ayuda a las aseguradoras a calcular sus riesgos y solicitar el reembolso a la parte responsable en última instancia de los daños. Por ejemplo, si un accidente es originado por un defecto, el asegurador del vehículo puede solicitar el reembolso al fabricante después de indemnizar a la víctima.

Sin embargo, las características de las tecnologías digitales emergentes, como la IA, el internet de las cosas y la robótica, ponen en entredicho aspectos de los marcos de responsabilidad civil nacionales y de la Unión y podrían menoscabar su eficacia. Algunas de estas características pueden dificultar la determinación de la relación causal entre los daños y un comportamiento humano, que es uno de los elementos necesarios para presentar una reclamación por responsabilidad subjetiva, de conformidad con las normas nacionales. Esto significa que, en las reclamaciones basadas en las normativas nacionales de responsabilidad civil, la cuestión probatoria puede ser gravosa o excesivamente onerosa y, por lo tanto, es posible que las víctimas no reciban una compensación adecuada. Es importante que las víctimas de accidentes ocasionados por productos y servicios basados en tecnologías digitales emergentes, como la IA, no gocen de un nivel de protección inferior al que tienen respecto de otros productos y servicios similares, por los que recibirían una indemnización conforme a la normativa nacional de responsabilidad civil, porque podría disminuir la aceptación social de estas tecnologías emergentes y generar vacilación en cuanto a su uso.

Será preciso valorar si las dificultades que las nuevas tecnologías plantean para los marcos existentes también podrían generar inseguridad jurídica en cuanto a cómo aplicar las normas en vigor (por ejemplo, cómo se aplicaría el concepto de culpa a los daños causados por la IA). Estas, a su vez, podrían desincentivar las inversiones, así como aumentar los costes de la información y los seguros para los productores y otras empresas de la cadena de suministro, especialmente las pymes europeas. Además, si los Estados miembros hiciesen frente a estos problemas para sus marcos nacionales de responsabilidad civil, podría aumentar la fragmentación, lo que incrementaría los costes de poner en práctica soluciones innovadoras en materia de IA y reduciría el comercio transfronterizo en el mercado único. Es importante que las empresas conozcan sus riesgos en materia de responsabilidad civil a lo largo de toda la cadena de valor y puedan reducirlos o prevenirlos y asegurarse eficazmente contra ellos.

[57] Armonizadas en materia de vehículos de motor por la Directiva 2009/103/CE, relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad.

[58] En la mayoría de los Estados miembros, la responsabilidad civil objetiva se aplica a la persona a cuyo nombre esté matriculado el vehículo.

En el presente capítulo, se explican algunas de las dificultades que las nuevas tecnologías plantean para los marcos existentes y cómo podrían solucionarse. Por otra parte, las características singulares de ciertos sectores, por ejemplo, el de la asistencia sanitaria, pueden merecer consideraciones adicionales.

Complejidad de los productos, los servicios y la cadena de valor: La tecnología y la industria han evolucionado de forma radical en las últimas décadas. Ejemplo paradigmático es que la línea divisoria entre productos y servicios ya no es tan nítida como antes; de hecho, están cada vez más interrelacionados. Aunque los productos y cadenas de valor complejos no son algo novedoso para la industria europea o su modelo regulador, los programas informáticos y también la IA merecen una atención específica en relación con la responsabilidad civil derivada de los productos. Los programas informáticos son esenciales para el funcionamiento de un gran número de productos y pueden afectar a su seguridad; vienen integrados en los productos, pero también se pueden instalar por separado para posibilitar el uso previsto del producto. La utilidad de los ordenadores y los teléfonos inteligentes se vería seriamente menguada si no tuviesen programas informáticos. Ello también implica que un programa informático puede hacer defectuoso un producto físico y provocar daños físicos (véase el recuadro sobre los programas informáticos en la parte dedicada a la seguridad), lo que podría dar lugar finalmente a que se exigiese responsabilidad civil al fabricante del producto en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

Sin embargo, dado que hay programas informáticos de muchos tipos y formas, las respuestas relativas a la clasificación de los programas informáticos como servicio o como producto no siempre son claras. Por lo tanto, si bien el programa informático que dirige las operaciones de un producto físico puede considerarse una parte o componente de este, algunos tipos de programas informáticos autónomos podrían ser más difíciles de clasificar.

Aunque la definición de producto de la Directiva sobre responsabilidad por los daños causados por productos defectuosos es amplia, podría precisarse su ámbito de aplicación para reflejar mejor la complejidad de las tecnologías emergentes y garantizar que haya una indemnización por los daños causados por productos defectuosos debido a sus programas informáticos u otras características digitales. Con ello se mejoraría la capacidad de los agentes económicos, como los desarrolladores de programas informáticos, de valorar si pueden considerarse productores en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

Las aplicaciones de IA suelen estar integradas en **entornos de internet de las cosas complejos**, en los que interactúan muchos dispositivos y servicios conectados. La combinación de distintos componentes digitales en un ecosistema complejo y la pluralidad de agentes implicados pueden dificultar evaluar dónde se puede producir un perjuicio y quién es el responsable. Debido a la complejidad de estas tecnologías, puede resultar muy difícil para las víctimas saber quién es la persona responsable y probar todas las condiciones que el Derecho nacional exige para la concesión de la indemnización. El coste de estas pesquisas puede ser prohibitivo y disuadir a las víctimas de reclamar una indemnización.

Por otra parte, los productos y servicios basados en la IA interactuarán con las tecnologías tradicionales, lo que dará lugar también a una mayor complejidad en materia de responsabilidad civil. Por ejemplo, los automóviles autónomos compartirán la red viaria con los tradicionales durante cierto tiempo. Una complejidad similar debida al solapamiento de interactuaciones se producirá en algunos sectores de servicios (como la gestión del tráfico y

la asistencia sanitaria), en los que los sistemas parcialmente automatizados de IA contribuirán a la toma de decisiones de humanos.

Según el informe[59] de la formación sobre nuevas tecnologías del grupo de expertos sobre responsabilidad y nuevas tecnologías, debería contemplarse la posibilidad de adaptar las leyes nacionales para facilitar la carga de la prueba de las víctimas de daños relacionados con la IA. Por ejemplo, la carga de la prueba podría vincularse al cumplimiento (por el agente pertinente) de obligaciones específicas en materia de ciberseguridad u otras obligaciones en materia de seguridad establecidas por ley: si no cumple estas normas, podría modificarse la carga de la prueba por lo que se refiere a la culpa y la causalidad.

La Comisión está recabando opiniones acerca de si, y en qué medida, puede ser necesario para paliar las consecuencias de esta complejidad reducir o invertir la carga de la prueba exigida por las normas nacionales en materia de responsabilidad civil por los daños causados por el funcionamiento de las aplicaciones de IA, a través de una iniciativa adecuada de la UE.

Por lo que se refiere a la normativa de la Unión, de conformidad con la Directiva sobre responsabilidad por los daños causados por productos defectuosos, un producto que no cumple las normas de seguridad obligatorias se considera defectuoso, independientemente de la culpa de los productores. No obstante, también pueden existir razones para reflexionar sobre cómo facilitar la carga de la prueba de las víctimas con arreglo a la Directiva: la Directiva depende de las normas nacionales probatorias y sobre el establecimiento de la relación de causalidad.

Conectividad y apertura de código: No está claro en la actualidad qué expectativas de seguridad cabe tener en relación con los daños derivados de violaciones de la ciberseguridad del producto y acerca de si dichos daños serán adecuadamente indemnizados en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

Puede haber deficiencias en materia de ciberseguridad desde el principio, cuando el producto se pone en circulación, pero también pueden aparecer en un momento posterior, mucho después de que el producto se haya puesto en circulación.

En los marcos de responsabilidad civil subjetiva, al establecerse obligaciones claras en materia de ciberseguridad los agentes pueden saber exactamente lo que deben hacer para evitar que se les exija responsabilidad civil.

En virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, la cuestión de si un productor podría haber previsto una serie de cambios teniendo en cuenta el uso razonablemente previsible del producto puede adquirir mayor relevancia. Por ejemplo, los productores podrían invocar más el principio de aparición posterior del defecto, por el cual un productor no es responsable si el defecto no existía en el momento en que el producto se puso en circulación, o el de los riesgos del desarrollo, según el cual no es responsable si, de acuerdo con los conocimientos más avanzados en ese momento, no se podía haber previsto el defecto. Además, la responsabilidad civil del productor puede verse reducida si la parte perjudicada no descargó todas las actualizaciones pertinentes para la seguridad, ya que se consideraría una negligencia concurrente del perjudicado. Dado que el concepto de uso razonablemente previsible y las cuestiones relativas a la negligencia concurrente, como el no haber descargado una actualización de

[59] Informe «Liability for Artificial Intelligence and other emerging technologies» (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

seguridad, pueden hacerse más frecuentes, los perjudicados podrían tener más dificultades para obtener una indemnización por los daños causados por el defecto de un producto.

Autonomía y opacidad: Que una aplicación que se apoye en la IA actúe de manera autónoma quiere decir que lleva a cabo una tarea sin que cada paso esté predefinido y que lo hace con menos o, en última instancia, sin ningún control o supervisión humanos inmediatos. Los algoritmos basados en el aprendizaje automático de la máquina pueden ser difíciles, si no imposible, de comprender («efecto caja negra»).

Además de la complejidad expuesta anteriormente, debido al efecto caja negra de algunas IA, puede resultar difícil obtener una indemnización por los daños causados por aplicaciones de IA autónomas. Para comprender el algoritmo y los datos utilizados por la IA hacen falta una capacidad analítica y unos conocimientos técnicos que pueden ser excesivamente costosos para las víctimas. Es más, sin la cooperación de la parte aparentemente responsable puede resultar del todo imposible acceder al algoritmo y a los datos. Como consecuencia, es posible que, en la práctica, las víctimas no puedan presentar una demanda viable de responsabilidad civil. Por otra parte, sigue sin quedar claro cómo demostrar la culpa de una IA que haya actuado de manera autónoma, ni en qué consiste la culpa de una persona que se sirve de la IA.

Los ordenamientos jurídicos nacionales ya han elaborado una serie de soluciones para reducir la carga de la prueba de las víctimas en situaciones similares.

Sigue siendo un principio rector para la seguridad de los productos y la responsabilidad civil por los productos en la Unión que los productores garanticen que todos los productos comercializados sean seguros, a lo largo de todo su ciclo de vida y respecto del uso del producto que cabe razonablemente esperar. Esto significa que el fabricante de un producto basado en la IA tendría que asegurarse de que respete determinados parámetros de seguridad. Las funcionalidades de la IA no son óbice para que exista un derecho a tener expectativas de seguridad respecto de los productos, independientemente de que se trate de una cortadora de césped automática o un robot de cirugía.

La autonomía puede afectar a la seguridad del producto, ya que puede alterar sustancialmente sus características, incluidas sus funcionalidades de seguridad. Queda por esclarecer en qué condiciones las funcionalidades de aprendizaje automático pueden ampliar la responsabilidad civil del productor y en qué medida debe el productor haber previsto algunos cambios.

De forma coordinada con los cambios correspondientes en el marco en materia de seguridad de la Unión, podría revisarse el concepto de «puesta en circulación» utilizado actualmente por la Directiva sobre responsabilidad por los daños causados por productos defectuosos, a fin de tener en cuenta que los productos pueden cambiar y ser modificados, lo que podría ayudar a aclarar quién es el responsable civil de los cambios introducidos en el producto.

Según el informe[60] de la formación sobre nuevas tecnologías del grupo de expertos sobre responsabilidad y nuevas tecnologías, el funcionamiento de algunos dispositivos y servicios autónomos de IA puede tener un perfil de riesgo específico en términos de responsabilidad civil, ya que pueden perjudicar seriamente bienes jurídicos importantes, como la vida, la salud y la propiedad privada, y exponer al público en general a riesgos. Esto puede afectar principalmente a los dispositivos basados en la IA que circulen en espacios públicos (por

[60] Informe «Liability for Artificial Intelligence and other emerging technologies» (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

ejemplo, vehículos totalmente autónomos, drones[61] y robots de mensajería) o a servicios basados en la IA con riesgos similares (por ejemplo, servicios de gestión del tráfico que orienten o controlen los vehículos o la gestión de la distribución eléctrica). Las dificultades que plantean la autonomía y la opacidad a las normativas nacionales de responsabilidad civil podrían tratar de solucionarse siguiendo un enfoque basado en el riesgo. Los regímenes de responsabilidad civil objetiva pueden garantizar que, siempre que se materialice dicho riesgo, la víctima sea indemnizada con independencia de exista o no culpa, aunque deben valorarse ponderadamente las consecuencias de la elección de quién debe ser el responsable civil objetivo de las operaciones de desarrollo y asimilación de la IA, y debe asimismo considerarse un enfoque basado en el riesgo.

En relación con el funcionamiento de las aplicaciones de IA con un perfil de riesgo específico, la Comisión está recabando opiniones sobre si puede ser necesario, y en qué medida, establecer una responsabilidad civil objetiva, tal como existe en las normativas nacionales respecto de riesgos similares a los que está expuesto el público (por ejemplo, para automóviles, aeronaves o centrales nucleares), a fin de indemnizar eficazmente a las posibles víctimas. La Comisión también está recabando opiniones sobre la posibilidad de vincular el establecimiento de una responsabilidad civil objetiva con la obligación de suscribir un seguro, siguiendo el ejemplo de la Directiva sobre el seguro de vehículos automóviles, con el fin de garantizar el pago de la indemnización con independencia de la solvencia de la persona civilmente responsable y contribuir a reducir los costes asociados a los daños.

En relación con el funcionamiento de las demás aplicaciones de IA, que son la gran mayoría, la Comisión está reflexionando sobre si procede adaptar la carga de la prueba relativa a la causalidad y la culpa. A este respecto, una de las cuestiones señaladas por el informe[62] de la formación sobre nuevas tecnologías del grupo de expertos sobre responsabilidad y nuevas tecnologías es la situación en la que la parte presuntamente responsable civilmente no ha registrado los datos pertinentes para valorar la responsabilidad civil o no está dispuesto a compartirlos con la víctima.

4. Conclusión

La aparición de nuevas tecnologías digitales como la IA, el internet de las cosas y la robótica plantean nuevas dificultades en materia de seguridad de los productos y responsabilidad civil por los mismos, como la conectividad, la autonomía, la dependencia de datos, la opacidad, la complejidad de los productos y los sistemas, las actualizaciones de los programas informáticos y la mayor complejidad que supone la gestión de la seguridad y las cadenas de valor.

La normativa actual en materia de seguridad de los productos presenta una serie de resquicios jurídicos que deben corregirse, en particular en la Directiva sobre seguridad general de los productos, la Directiva sobre máquinas, la Directiva sobre equipos radioeléctricos y el nuevo marco normativos. Los futuros trabajos de adaptación de los distintos actos normativos de este marco se llevarán a cabo de manera coherente y armonizada.

[61] Véanse los sistemas de aeronaves no tripuladas a que se hace referencia en el Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas.

[62] Informe «Liability for Artificial Intelligence and other emerging technologies» (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199).

Las nuevas dificultades en materia de seguridad plantean también otras dificultades en materia de responsabilidad civil. Deben solucionarse esas dificultades en materia de responsabilidad civil para garantizar el mismo nivel de protección que tienen las víctimas de las tecnologías tradicionales, manteniendo al mismo tiempo el equilibrio con las necesidades de la innovación tecnológica. Ello contribuirá a generar confianza en estas nuevas tecnologías digitales emergentes y a crear estabilidad en la inversión.

Si bien, en principio, las normativas en vigor de la Unión y nacionales en materia de responsabilidad civil pueden hacer frente a las vicisitudes jurídicas derivadas de las tecnologías emergentes, la dimensión y el efecto combinado de las dificultades que plantea la IA podrían dificultar la indemnización de las víctimas en todos los casos en que esté justificada[63]. Por lo tanto, el reparto de los costes cuando se produce un daño puede ser injusto o ineficiente con arreglo a las normas actuales. A fin de corregir esta situación y atender a las posibles incertidumbres del marco existente, podría contemplarse hacer algunos ajustes a la Directiva sobre responsabilidad por los daños causados por productos defectuosos y a los regímenes de responsabilidad civil nacionales a través de iniciativas adecuadas de la UE, sobre la base de un enfoque específico basado en el riesgo, es decir, teniendo en cuenta que las distintas aplicaciones de IA presentan riesgos diferentes.

[63] Véase el informe de la formación de nuevas tecnologías, p. 3, y la recomendación estratégica 27.2 del grupo de expertos de alto nivel sobre la IA.