Intelética 2(4) (2025), 150-162
Revista de Inteligencia Artificial, Ética y Sociedad

INTELETICA

https://inteletica.iberamia.org/

La responsabilidad en el uso de los sistemas de inteligencia artificial

Antonio Merchán Murillo

Prof. Dº Internacional privado. Universidad de Cádiz.

antonio.merchan@uca.es

Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, de cuyo equipo de investigación es miembro

Abstract The present work aims to carry out a study in relation to liability and the challenges it presents in the use of Artificial Intelligence systems, paying special attention to Artificial Intelligence systems that are deterministic, through a comparative study of the Directives on liability for damage caused by defective products and by which Directive 85/374 / EEC is repealed and the one on the adaptation of non-contractual civil liability rules to artificial intelligence, the latter still proposed. Likewise, it is intended to emphasize the difficult fit that they will have around the determination of the applicable Law, through the rules of private international law, where in Spain the Hague Convention of October 2, 1973 on the Law Applicable to Product Liability must be applied, which has erga omnes effect.

Resumen El en presente trabajo se pretende hacer un estudio en relación a la responsabilidad y los retos que presenta en el uso de los sistemas de Inteligencia Artificial, dándose especial atención a los sistemas de Inteligencia Artificial que son deterministas, a través de un estudio comparativo de las Directivas sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE y la relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, esta última aún propuesta. Asimismo, se pretende hacer hincapié en el difícil encaje que tendrán en torno a la determinación de la Ley aplicable, a través de las normas de Derecho internacional privado, donde en España debe aplicarse el Convenio de la Haya de 2 de octubre de 1973 sobre Ley Aplicable a la Responsabilidad por Productos, que tiene eficacia erga omnes.

Palabras clave: Inteligencia artificial, productos defectuosos, responsabilidad, Ley aplicable.

Keywords: Artificial intelligence, defective products, liability, applicable law.

1 Introducción

Internet, si tenemos en cuenta que es un espacio donde es posible ponerse en contacto con gente (para charlar, estudiar, trabajar, hacer negocios; en definitiva, para encontrar información, incluso donde encontrar el amor o disfrutar y jugar, leer, escuchar música, etc.), podemos comprobar que es como una “ciudad”, global. La más grande del mundo, moderna, con millones de habitantes, pero invisible.

Si tenemos una nueva “ciudad”, necesitamos conocerla y saber cómo ser un buen ciudadano, lo que no es fácil, porque Internet, nuestra “ciudad” cambia. Direcciones prohibidas donde antes se podía circular, canales que crecen y cambian rápidamente. Todo casi sin darnos cuenta. Los que viven en Internet, considerémoslos ciudadanos digitales, tienen que aprender normas de comportamiento apropiadas y la responsabilidad en materia de uso de la tecnología.

ISSN: 3020-7444

En ese contexto lo primero que debemos tener en cuenta son los principios básicos que rigen la digitalización o la electrónificación:

a) Principio de equivalencia funcional: constituye el núcleo sobre el que gravita el reconocimiento jurídico de los actos realizados en el comercio electrónico. Sin su aplicación, carecería de eficacia. Se formula bajo la idea de que los actos jurídicos electrónicos poseen una equivalencia funcional con los actos jurídicos escritos.

b) Principio de inalterabilidad del derecho preexistente: todas aquellas reglas dirigidas a la regulación del comercio electrónico no supongan una modificación sustancial del Derecho existente. No obstante este hecho no debe impedir que las normas deban ser interpretadas y adaptadas.

c) Principio de neutralidad tecnológica: las nuevas normas que rigen el comercio electrónico abarquen con sus reglas no sólo la tecnología existente sino también toda tecnología futura sin que haya necesidad de modificar estas normas

d) Principio de la buena fe: principio que encuentra su justificación en la idea de que la ignorancia, ante la renovación tecnológica, genera desconfianza

e) Libertad contractual mantenida en el nuevo contexto electrónico: autonomía de la voluntad.

En relación a este principio se ha observado un cambio de terminología en las normas pasando de seguridad a fiabilidad:

a) El término utilizado antes era certificación; es decir, seguridad: induce dependencia, en relación con el origen o la conexión. Ahora, el primero espera una buena conducta. Esto nos va a llevar a problemas de prueba (por ejemplo, en relación a la probatio diabólica, en la propuesta de Directiva sobre responsabilidad de los sistemas de IA).

b) La fiabilidad como medio nos lleva a una probabilidad de buen funcionamiento. Lo que nos sitúa en la confianza. Desde el punto de vista de la transacción, cuando hablamos de fiabilidad, nos referimos a que un dispositivo trabaje correctamente durante un tiempo y en las condiciones en que se encuentre el servicio, de manera que quien una transacción tendrá que fijarse en los posibles riesgos. Por consiguiente, identificamos la fiabilidad como un conocimiento del estado del sistema.

c) La fiabilidad nos lleva a la confianza: Se pretende atraer la atención del usuario, creando un clima de confianza en un entorno determinado. De esta forma, se quiere dar a entender como un proveedor de servicios, con sus acciones y sus caracteres, va a conseguir, de Internet, un universo más o menos confiable para las personas.

Junto a los anteriores debe advertirse una estructura propia común a todas las transacciones. Son identificables los siguientes elementos, que pueden ser agrupados en dos apartados:

a) Elementos objetivos: que no necesariamente son materiales. Estos elementos son:

1) El mensaje de datos;

2) La norma técnica de estructuración;

3) La firma electrónica;

4) Los sistemas de información;

5) Las redes de transmisión de datos;

b) Elementos subjetivos: se comprenden en el mismo los distintos sujetos destinatarios de los mandatos y privilegios legales así como de los derechos y obligaciones contractualmente adquiridos en el marco jurídico del comercio electrónico. Estos son:

1) El iniciador o firmante del mensaje de datos;

2) El destinatario del mensaje de datos;

3) Los intermediarios y proveedores de servicios de certificación de firma electrónica o autoridad de certificación. Con lo comentado, se puede realizar una tarea de determinación y definición de cada uno de los elementos principales involucrados en la transacción electrónica, a la vez que se podrían tratar los múltiples problemas derivados de la dificultad de aplicar los diferentes conceptos y las categorías jurídicas.

Todo lo anterior no tiene sentido sin un marco de interoperabilidad: ¿Por qué? Se trata de que sistemas o componentes de software para intercambiar y utilizar información entre sí, de manera eficiente y sin problemas. En el ámbito de la tecnología de la información, la interoperabilidad es crucial para garantizar que diferentes sistemas, aplicaciones y dispositivos puedan trabajar juntos de manera armoniosa:

a) Organizativos: en los procesos de negocio y estructuras internas (por ejemplo, que actores participan y por tanto van a ser sujetos responsables. Por ese motivo, el ámbito personal de las normas es tan importante);

b) Semánticos: los datos comparten el mismo significado (por eso las definiciones son tan importantes: para garantizar no un buen nivel de comunicación sino de interpretación);

c) Técnicos: conexión de sistemas sean eficientes sin fallos en materia de ciberseguridad (por ejemplo, intercambio de datos);

d) Jurídicos: las normas deben ser neutrales tecnológicamente.

2 Construcción de un nuevo marco jurídico

En la construcción del nuevo marco jurídico (digital), puede apreciarse en primer lugar una estructura clara de las normas en función a carácter de la transacción según nos situemos en el origen, en el medio a través del que se va a desarrollar la transacción o en la consecución. En función a ello vamos a poder apreciar distintas normas que van a estar en relación y, por tanto, van a tener una clara incidencia entre todas ellas, tal y como reflejamos en el cuadro:

Si nos encontramos en el origen nos vamos a encontrar la 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (conocido como eIDAS 2.0) donde se va a pasar a regular cuestiones importantes en torno la identidad digital, identidad auto-soberanía, etc. Por otro lado, si nos situamos en el medo en el que se va a desarrollar la transacción va aparecer diferentes normas muy importantes: el Reglamento eIDAS 2.0, Reglamento 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD en relación a la información personal), Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, Directiva 2016/1148, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS) con el fin de garantizar la seguridad de las redes y sistemas de información en el territorio de la UE), 2019/881 relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad) (Reglamento sobre ciberseguridad) en el establecimiento de una Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información), Reglamento sobre gobernanza europea de datos, Reglamento Servicios Digitales, Reglamento 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital, que regula la actuación de las grandes plataformas digitales), etc. Finalmente, si nos situamos en la consecución de la transacción nos vamos a encontrar: el Reglamento eIDAS 2.0, Reglamento sobre datos no personales, Propuesta directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, Directiva 2024/2853, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos, Reglamento 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, Reglamento 2023/988 relativo a la seguridad general de los productos, el Reglamento 2023/1114 relativo a los mercados de criptoactivos (Reglamento MiCA), etc.

Las normas anteriores, entre otras, guardan relación entre sí. En cualquier caso, centrándonos en el objeto de nuestro trabajo, que es la Inteligencia Artificial (IA), podemos observar que en los últimos años, han sucedido

muchas cosas a nivel de la Unión Europea con respecto a la regulación de la IA. Los estudios de ha desentrañado los problemas de responsabilidad que surgen de las características distintivas de la IA, como su autonomía, complejidad, falta de transparencia y opacidad, que dificultan la aplicación de las normas de responsabilidad existentes y los requisitos asociados.

Las normas de responsabilidad actuales se formularon hace décadas basándose en conceptos antiguos que hacen que su idoneidad puede, por tanto, ser cuestionable cuando se apliquen a la IA. Además, muchos actores participan en la cadena de suministro de sistemas de IA, lo queo puede generar incertidumbre sobre quién será o debería ser considerado responsable en última instancia y, especialmente, a quién dirigirse cuando se produzca un daño. Es posible que las personas que hayan sufrido daños relacionados con sistemas de IA no tengan acceso adecuado a la información y, por lo tanto, a las pruebas para probar su caso ante los tribunales.

Los litigios podrían volverse gravosos y costosos para las víctimas, dejándolas "sin acceso efectivo a la justicia". En este contexto, es importante que las víctimas de accidentes que involucran IA no se enfrenten a un nivel de protección más bajo en comparación con otros productos y/o servicios (tradicionales) por los cuales recibirían compensación según la legislación nacional. De lo contrario, la aceptación social de esos sistemas de IA podría verse obstaculizada

Lo anterior, va a generar incertidumbres con respecto a la aplicación de las normas cuyo marco normativo elegido es una Directiva, por lo que habrá que ver las disposiciones nacionales que la transponen. Aunque ambas propuestas se están presentando a nivel de la UE, la responsabilidad extracontractual todavía está regulada en gran medida por la legislación nacional. Además, debe tenerse en cuenta que existe un Convenio de la Haya sobre Ley aplicable a productos defectuosos, del que es parte España, pudiendo haber casos, en los que no pueda aplicarse por determinar aplicable las normas de un tercer Estado.

2.1 El marco regulatorio en torno a la IA

La IA podría verse como una rama de la informática que “estudia las propiedades de la inteligencia mediante su síntesis informática”[1]. Ahora bien, qué constituye o entra dentro del alcance de la inteligencia. La IA requiere una máquina para realizar tareas cognitivas asociadas con la mente humana, que incluyen “percibir, razonar, aprender, interactuar con el entorno, resolver problemas, tomar decisiones e incluso demostrar creatividad”[2]. En este contexto la OCDE sugiere que un sistema de IA puede “hacer predicciones, recomendaciones o decisiones que influyan en entornos reales o virtuales”[3].

La dificultad de determinar en detalle qué se incluye en estas definiciones, qué se considera inteligencia y en qué momento un sistema debe considerarse IA ha llevado a adoptar definiciones bastante amplias, en particular, en un informe para el gobierno del Reino Unido sugiere que la IA es “un conjunto de tecnologías digitales avanzadas de propósito general que permiten que las máquinas realicen tareas altamente complejas de manera efectiva”[4]. Asimismo, la Comisión Europea en su Libro Blanco propuso que la IA “es una colección de tecnologías que combinan datos, algoritmos y poder de cómputo (o capacidad informática)”. Esta definición puede ser demasiado inclusiva, pero se debe a la dificultad de delimitar claramente el término.

[1] P. Stone, R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager,
2Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence”, *Computers and Society*, 2016, p. 13. Disponible en https://arxiv.org/abs/2211.06318 (Fecha de consulta 15 de julio de 2023).
[2] A. Rai, P. Constantinides, S. Sarker, “Next-generation digital platforms: toward human–AI hybrids”, Mis Quart, 43-1, 2019, pp. iii-x. Disponible en https://research.manchester.ac.uk/en/publications/next-generation-digital-platforms-toward-human-ai-hybrids (Fecha de consulta 15 de julio de 2023).
[3] OECD, Recommendation of the council on artificial intelligence (OECD Legal Instruments), 2019. Disponible en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (Fecha de consulta 15 de julio de 2023).
[4] W. Hall, J. Pesenti, *Growing the artificial intelligence industry in the UK Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy*, London, 2017. Disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf (Fecha de consulta 15 de julio de 2023).

En la actualidad en el Reglamento se dice de ella en el considerando 3 que es “un conjunto de tecnologías de rápida evolución que puede generar un amplio abanico de beneficios económicos y sociales en todos los sectores y actividades sociales”, concretando en el 71 decir que “es una familia de tecnologías de rápida evolución”. Por ello, la define en el artículo 3,1 como sistema de IA que integra “el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I[5] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa”.

Ahora bien, téngase claro que los sistemas de IA como dice la el Reglamento son sistemas de software, pero posiblemente también de hardware, diseñados por humanos que, dado un objetivo complejo, actúan en la dimensión física o digital al percibir su entorno a través de la adquisición de datos, interpretar los datos estructurados o no estructurados recopilados, razonar sobre el conocimiento, o el procesamiento de la información, derivado de estos datos y decidir las mejores acciones a tomar para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento analizando cómo el entorno se ve afectado por sus acciones anteriores. Como disciplina científica, la IA incluye varios enfoques y técnicas, como el aprendizaje automático (de los cuales el aprendizaje profundo y el aprendizaje por refuerzo son ejemplos específicos), el razonamiento automático (que incluye la planificación, la programación, la representación y el razonamiento del conocimiento , la búsqueda y la optimización) y la robótica (que incluye el control, la percepción, los sensores y los actuadores, así como la integración de todas las demás técnicas en sistemas ciberfísicos)[6].

De esta forma, si bien los aspectos que comentamos hacen que los sistemas de IA sean más complejos y capaces, y su combinación crea el llamado problema de la “caja negra”, que se describe en el texto provisional revisado de la taxonomía, la secretaría ha advertido que para analizar su importancia jurídica no es prudente utilizar analogías de fuerte contenido humano, como “aprendizaje” o “autonomía”. También cabe preguntarse si medidas cualitativas como la “complejidad” y la “capacidad” podrían servir de base para un tratamiento jurídico diferenciado.

En este sentido, como se señala en el texto provisional revisado de la taxonomía, el Reglamento de Inteligencia Artificial, en la que se adopta una definición de “sistema de IA” que sigue el modelo de la definición de la OCDE, establece normas especiales para los sistemas de IA de “alto riesgo” en función de la finalidad o los objetivos para los que se despliega el sistema de IA, o las tareas que realiza, en lugar de tener en cuenta algún aspecto intrínseco de su programación[7].

Con las definiciones anteriores, nuestra intención es observar la dificultad con la que nos encontramos, especialmente, para explicar en el marco normativo, que haremos más adelantes, sobre la fiabilidad de la IA, que además no será suficiente para lograr que los derechos fundamentales forman parte, de la IA fiable y con ello garantizar el cumplimiento de la legislación[8]. Por ello, el Grupo europeo de ética de la ciencia y de las nuevas tecnologías propuso un conjunto de principios básicos, apoyados en los valores fundamentales recogidos en los Tratados de la UE y en la Carta de los Derechos Fundamentales de la Unión Europea: respeto de la autonomía humana; prevención del daño; equidad; explicabilidad[9].

---

[5] Se refiere a “Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización

[6] Bernd Carsten Stahl, “A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values”, *Computer Law & Security Review*, Volume 45, July 2022.

[7] CNUDMI/UNCITRAL: *Cuestiones jurídicas relacionadas con la economía digital: las operaciones de datos*, Nueva York, 6 a 17 de julio de 2020.

[8] Grupo de expertos de alto nivel sobre inteligencia artificial, directrices éticas para una IA fiable, Bruselas, 2019. Disponible en https://digital-strategy.ec.europa.eu/es/node/1950 (Fecha de consulta 15 de julio de 2023).

[9] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, E. J. M. Vayena, “AI4People —An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations”, *Minds and Machines*, 2018, núm. 28, pp. 689-707.

La nueva norma que se aprobará en breve viene a establecer normas armonizadas para el desarrollo, la comercialización y el uso de sistemas de IA en la UE siguiendo un enfoque proporcionado basado en el riesgo. Determinando sistemas de IA que están prohibidos (art. 5), sistemas de IA que se consideran de alto riesgo (art. 6) y todos los demás sistemas (riesgo limitado o sin riesgo). La prohibición se refiere a determinadas prácticas de IA especialmente dañinas que contravienen los valores de la Unión, por ejemplo, al violar los derechos fundamentales. Las prohibiciones engloban aquellas prácticas que tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas.

Si lo anterior, lo relacionamos con la definición de "sistema de inteligencia artificial" vemos que es muy amplia, cubriendo una amplia gama de aplicaciones dedicadas o módulos, por ejemplo, un componente de seguridad, tal y como se establece en el considerando 55, "con independencia de si el sistema forma parte físicamente de él (integrado) o tiene una funcionalidad en el producto sin formar parte de él (no integrado)", en relación el considerando 6.

En este sentido, si bien en el artículo 6,1 se especifica con más detalle, puede verse como el Reglamento identifica dos tipos de sistema de IA sea considerando de alto riesgo: a) sistemas de IA destinados a ser utilizados como componentes de seguridad de productos que están sujetos a evaluación de conformidad ex ante por parte de terceros y b) otros sistemas de IA independientes con implicaciones para los derechos fundamentales que se enumeran explícitamente en el Anexo III.

La definición subyacente de sistema de IA pretende ser tecnológicamente neutral, lo que viene impulsada por la naturaleza de los sistemas de IA. Por ello, puede decirse que es deliberadamente abierta, con vista, además, a modificarse con miras al cambio tecnológico en curso. De conformidad con el artículo 4, la Comisión está facultada para más que modificar es actualizar "la lista de técnicas y estrategias que figura en el anexo I, con miras a adaptar dicha lista a la evolución del mercado y los avances tecnológicos". Además, en virtud del artículo 7, la Comisión está facultada para adoptar actos delegados para actualizar el anexo III añadiendo sistemas de IA de alto riesgo. El criterio es doble: "a) los sistemas de IA estén destinados a utilizarse en cualquiera de los ámbitos que figuran en los puntos 1 a 8 del anexo III y b) los sistemas de IA conlleven el riesgo de causar un perjuicio a la salud y la seguridad, o el riesgo de tener repercusiones negativas para los derechos fundamentales".

Tal como se establece en la exposición de motivos, la clasificación de sistemas de alto riesgo se basa en la finalidad prevista del sistema de IA, en consonancia con la legislación vigente de la UE sobre seguridad de los productos. Por lo tanto, esta clasificación no solo depende de la función del sistema, sino también del propósito específico y las modalidades para las que se utiliza.

En virtud del Reglamento, los sistemas considerados de "alto riesgo" están permitidos en el mercado europeo sujeto al cumplimiento de los requisitos obligatorios relacionados con [19] datos y gobernanza de datos, documentación y mantenimiento de registros, transparencia y suministro de información a los usuarios, supervisión humana, solidez, precisión y seguridad, así como la evaluación de la conformidad ex-ante.

Por lo demás, el alcance del Reglamento la propuesta está significativamente determinado por las cuarenta y cuatro definiciones establecidas en el artículo 3. Esto incluye, junto al elemento clave, el sistema de IA, dimensiones importantes como los actores involucrados (proveedor, usuarios, importador y distribuidor), las diversas etapas de puesta en el mercado o uso de los sistemas (introducción en el mercado, puesta a disposición en el mercado, puesta en servicio y retirada de un sistema de IA) y dimensiones de diseño y uso (finalidad prevista, uso indebido razonablemente previsible e incidente grave).

Ahora bien, desde nuestro punto de vista se queda corta y, por otro lado, apenas protege contra la IA de bajo y medio riesgo, por ejemplo, la moderación de los contenidos publicados y el análisis profundo del comportamiento de los usuarios quedan fuera del ámbito normativo de la Ley. El uso cada vez mayor de tecnologías de IA en el monitoreo de las redes sociales, que a veces se realiza con buenas razones para prevenir el discurso de odio y el acoso, deja abiertas preguntas importantes y muy debatidas con respecto a la equidad y la transparencia de los sistemas de IA que manejan estas tareas. Además, el riesgo de discriminación y violación de la libertad de expresión debido a malas interpretaciones que pueda realizar la IA es real, pero, según la interpretación de alto riesgo vista en el Reglamento, básicamente no queda dentro.

Otra cuestión serían las obligaciones de transparencia para determinados sistemas de IA, establecidas por el artículo 52, se aplican a una gama limitada de sistemas de IA y no son muy precisas en cuanto al contenido y la forma de la información que debe proporcionarse. En ausencia de directrices claras, existe un grave riesgo de que la información proporcionada varíe de un fabricante a otro. Además, Los códigos de conducta voluntarios establecidos en el artículo 69 no incluyen ningún proceso de verificación para asegurar que las entidades adheridas cumplan con el código

2.2 Los marcos de responsabilidad de la IA

El Reglamento de IA lleva aparejadas medidas para apoyar la adopción de la IA en Europa mediante el fomento de la excelencia y la confianza, a través de dos Directivas, una relativa a productos defectuosos y la otra, aún propuesta, relativa a la Responsabilidad de la IA. Los problemas que se asocian a ambas es que la regulación de la responsabilidad de la IA se basa en el artículo 114 TFUE. De hecho, esto se justifica para evitar la fragmentación del mercado único digital, costes legales prohibitivos para las empresas que suministran IA en toda la UE y obstáculos para las personas perjudicadas que pretenden demandar a los proveedores en entornos transfronterizos.

Actualmente, la responsabilidad extracontractual de los sistemas de IA se basa en un régimen de doble vía: responsabilidad en gran medida armonizada según la Directiva por productos defectuosos (en la medida en que actualmente se aplica al software); y una responsabilidad en gran medida no armonizada según las normas del derecho nacional de daños (cubierto por la propuesta Directiva de responsabilidad de la IA). Sin embargo, las mismas razones expuestas para el uso del artículo 114 del TFUE también hablan claramente a favor del establecimiento de un solo régimen europeo armonizado de responsabilidad extracontractual para los productos, incluidos los sistemas de inteligencia artificial. La elección actual de dos directivas, una dirigida específicamente a la IA y otra dirigida a la responsabilidad por productos defectuosos, incluida la IA, genera problemas importantes, ya que la mayoría de los Estados miembros siguen apreciando sus regímenes nacionales de responsabilidad civil.

Dado que la Comisión optó por trabajar con dos directivas, es necesario aclarar la relación entre ellas. Ambos se aplican en paralelo, pero cubren aspectos diferentes y, según la Comisión, aspectos mutuamente excluyentes, tal y como explicamos de manera esquemática:

PRODUCTOS DEFECTUOSOS	RESPONSABILIDAD DE LA IA
Reclamación basada en la legislación de la UE	Reclamación basada en el Derecho del Estado miembro (art. 4)
Aspectos materiales y procesales de la responsabilidad por productos defectuosos	Aspectos procesales de la responsabilidad por los sistemas de IA
Aplicable a productos físicos y, especialmente, software, incluidos sistemas de inteligencia artificial.	Aplicable únicamente a sistemas de IA
Responsabilidad supuestamente objetiva	Responsabilidad basada en culpa
Reclamaciones contra fabricantes y otras entidades de la cadena de suministro	Reclamaciones contra fabricantes, usuarios profesionales y consumidores
Daños elegibles: propiedad, muerte o lesiones personales y pérdida de datos	Daños subvencionables: potencialmente también derechos fundamentales y pérdidas económicas primarias
Armonización total (art. 3)	Armonización mínima

Visto lo anterior, cualquier instrumento diseñado específicamente para la IA debe garantizar que quienquiera que en declaraciones públicas afirme estar utilizando IA también pueda ser demandado bajo el régimen de responsabilidad de la IA. De manera similar, el alcance de las obligaciones contractuales en los contratos de compraventa de bienes o contenidos o servicios digitales está influenciado principalmente por la redacción de los anuncios. Una disposición de este tipo reduciría la fricción entre los dos regímenes y reduciría la inseguridad jurídica para los posibles demandantes.

Como decimos, incluso las directivas que armonizan plenamente siempre crean el riesgo de transposiciones divergentes. La Directiva de protección de datos ofrece un excelente ejemplo de esto. El panorama fragmentado de la protección de datos en los Estados miembros fue una de las razones clave para la elección de un reglamento como instrumento para el RGPD. Por lo tanto, para evitar la fragmentación y las transposiciones divergentes entre los Estados miembros en esta área tan sensible para la innovación, la responsabilidad de la IA debería detallarse igualmente en una regulación integral, no en dos directivas.

Un marco unificado y coherente no sólo beneficia a la industria de la IA; transposiciones divergentes entre los Estados miembros también tienden a exacerbar las dificultades para que los consumidores sepan qué régimen se aplica y cómo demandar a los proveedores ubicados en diferentes Estados miembros. En general, la competencia tradicional de los Estados miembros en materia de regímenes de responsabilidad debe, al menos en la esfera no contractual, dar paso a las realidades de un mercado único digital unificada. Por lo tanto, la competencia prevista en el artículo 114 del TFUE debería aprovecharse para proporcionar un marco integral a escala de la UE para la responsabilidad de la IA y el software en general.

2.3 Retos en la responsabilidad en materia de IA

En relación a la aún propuesta de Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial debemos ser conscientes de los numerosos desafíos a los que nos enfrentamos en la aplicación del derecho de responsabilidad civil en caso de daños relacionados con IA, en primer lugar en relación a carga probatoria de probar la culpa y el daño en relación a toda la información relevante necesaria para iniciar el proceso de reclamación, lo que se va a relacionar con un ecosistema tecnológico difuso y la complejo como es el de la propia IA, donde las empresas que utilizan o producen dichos sistemas tienen mucho control sobre los datos y la información.

En este contexto a pesar de la obligación de revelar las pruebas e información pertinentes, la interacción entre las diferentes disposiciones del artículo 3 no es del todo clara y requiere una mayor aclaración. Por ejemplo, según el artículo 3.1, el requisito de revelar pruebas solo se aplica a los proveedores de sistemas de IA, a ciertas personas sujetas a las obligaciones de estos (como el fabricante del producto) o a los usuarios. Esto parece implicar que no se aplica a otros "demandados", como los proveedores de servicios u operadores, salvo que, por supuesto, sean considerados usuarios, proveedores o fabricantes del producto. El artículo 3.5, por su parte, impone específicamente una presunción de incumplimiento para los "demandados", lo cual abarca un grupo más amplio que las partes identificadas en el artículo 3.1. Sin embargo, dado que otras partes, además de los proveedores de sistemas de IA, las personas sujetas a sus obligaciones y los usuarios no parecen estar obligadas inicialmente a revelar información, la presunción resulta algo vaga y de aplicación limitada.

Además, dicha presunción solo se refiere a las pruebas que estén "a disposición" del demandado en relación con sistemas de IA "de alto riesgo". Esto excluye, por ejemplo, los sistemas de reconocimiento de emociones que podrían causar daños significativos, al menos según la propuesta de la Comisión Europea.

Otro de los retos esenciales que presenta la Directiva propuesta es la relativa a la presunción refutable de relación de causalidad en caso de culpa establecida en el artículo 4, donde se recoge en el apartado1, a)que la culpa consiste en el incumplimiento de un deber de diligencia establecido en la legislación de la Unión o nacional, destinado directamente a proteger contra el daño, lo que también sirve como referencia para los apartados 1,b) (“que pueda considerarse razonablemente probable, basándose en las circunstancias del caso, que la culpa ha influido en los resultados producidos por el sistema de IA o en la no producción de resultados por parte del sistema de IA”) y 1,c) (“que el demandante haya demostrado que la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA causó los daños”), respectivamente. Posteriormente, conforme al artículo 4.2, se aborda el caso específico en que los demandados son proveedores de sistemas de IA de alto riesgo regulados por la Ley de IA, la “culpa” solo puede consistir en el incumplimiento de

una lista de requisitos establecidos de manera exhaustiva en el artículo 4.2. Por otro lado, el artículo 4.3, que regula las reclamaciones por daños contra un usuario de un sistema de IA de alto riesgo sujeto a la Ley de IA, establece que la culpa puede consistir, en particular, debido a la ausencia de una referencia explícita a "solo", en incumplimientos de requisitos relacionados conforme a lo dispuesto en la Ley de IA.

Ahora bien, dicho lo anterior, puede apreciarse un problema importante ante la falta de claridad lingüística; pues el termino "razonablemente probable", en función de las circunstancias del caso, que la falla haya "influido" en los "resultados" producidos por el sistema de IA o que el sistema de IA no haya podido producir un resultado, va a conllevar una evaluación subjetiva por parte de un juez, basada en cada caso particular, si se cumplen los requisitos de "razonablemente probable" e "influencia". Esto puede acabar afectando a la seguridad jurídica y causar fragmentación en la UE en función de las tradiciones nacionales en materia de responsabilidad civil. La noción de "resultado" tampoco está definida en la Directiva propuesta.

Además, la relación entre las nociones de "culpa" y "deber de cuidado" en virtud del 4,1, a) se refiere a la presunción de nexo causal tras una falta cometida por un demandado, al violar un deber de cuidado en virtud del derecho de la UE y nacional destinado directamente a proteger contra el daño que se produjo. Se trata de un ámbito bastante amplio. Por el contrario, los artículos 4.2 y 4.3, que tratan específicamente de los proveedores, las personas sujetas a las obligaciones de estos últimos o los usuarios de sistemas de IA de alto riesgo lo que podrían interpretarse de dos maneras diferentes[10]:

a) Como si exigieran únicamente el incumplimiento de los requisitos pertinentes del Reglamento de IA, de modo que se considere que se cumple la condición del artículo 4,1 a) para que el demandante se beneficie de la presunción, lo que implicaría unas obligaciones en función del resultado.

b) Como una exigencia *no solo* de una violación de los requisitos pertinentes de la Reglamento de IA, sino también de una violación de un deber de cuidado, siendo esta por la que nos decantaríamos.

2.4 Retos de la normativa sobre productos defectuosos

En relación con la Directiva 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo podemos observar una gran problemática en relación a la falta de claridad lingüística pues utiliza términos generales no definidos en la propia norma y que, por tanto, tendrán que se apreciado por el propio Tribunal conforme a su propia normativa aplicar, que atendiendo a su sistema de Derecho internacional privado podrá ser la ley extranjera, como se apreciará más adelante. De esta forma se aprecia terminología como: a) "razonablemente previsible" (artículo 7 en relación a la presunción de conformidad con el requisito general de seguridad), identificado como ejemplo en los considerandos 31 y 32 "por ejemplo el comportamiento previsible de un usuario de maquinaria derivado de una falta de concentración o el comportamiento previsible de determinados grupos de usuarios, como los niños o los efectos razonablemente previsibles de otros productos en el producto en cuestión, como por ejemplo en un sistema doméstico inteligente"; b) "sustancialmente" (Artículo 8,2 en relación a los elementos adicionales que deben tenerse en cuenta para la evaluación de la seguridad de los productos) aclarándose en el considerando 39 que este carácter sustancial debe determinarse de acuerdo con los criterios establecidos en el Derecho de la Unión y nacional aplicable en materia de seguridad de los productos, incluido el Reglamento (UE) 2023/988 relativo a la seguridad general de los productos; c) criterios "pertinentes" o "proporcionados", según la traducción, para evaluar su seguridad (artículo 9 en relación a las obligaciones de los fabricantes) del que no se aprecia nada aclaratorio; d) datos "necesarios" para que el fabricante investigue la reclamación sobre el supuesto producto peligroso (artículo 9, 13 sobre) indicando como aclaración en el considerando 33 que "podría requerir una descripción más amplia del producto".

Estas apreciaciones, entre otras, van a ser cruciales para la aplicación de disposiciones clave de la Directiva. Sin embargo, son conceptos no definidos y requerirán que los tribunales determinen su contenido y alcance. En última

[10] De Bruyne, J., Dheu, O., Ducuing, C., "The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive", *Computer Law & Security* Review, 51, 2023.

instancia, las definiciones proporcionadas por los tribunales pueden variar de un Estado a otro, lo que puede crear fragmentación jurídica y beneficiar a los propios destinatarios de las normas, diluyendo su posible responsabilidad.

Por otro lado, puede observarse que la Directiva pone el foco en obviamente abordar la IA, pero también sobre el Internet of Things (IoT). Esto se puede observar en como la IA puede proporcionarse como un servicio y no como un producto, especialmente, en relación a los híbridos; es decir, productos como cosas y servicios basados en IA[11]. Observemos que sigue un patrón visible en la norma sobre seguridad de los productos[12], motivo por el que se solicita cada vez más a los fabricantes que aseguren no solo el producto sino también su aspecto digital, por razones de ciberseguridad. Esta cuestión se observa en la adaptación de la nueva Directiva mediante una ficción jurídica, en el sentido de que esencialmente todo lo que está bajo el control del fabricante, a pesar de que el fabricante no haya instalado o realizado el sistema de IA. Este enfoque se produce a costa de desnaturalizar la función de "fabricación" y en relación con el producto en sí. Este hecho nos lleva a la definición del concepto de componente que puede generar incertidumbre en cuanto a la relación entre el producto y el componente pues parece que no solo establece un régimen de responsabilidad por productos defectuosos, sino también por componentes defectuosos, ya que es obvio que el componente constituye una parte del producto por la que también es responsable el fabricante del producto. Sin embargo, esto solo se observa de manera implícita, ya que no se establece claramente que el fabricante del producto pueda ser considerado responsable de los componentes defectuosos. Al referirse a la integración del componente en el producto o a su interconexión con él, la definición de un componente tampoco establece una relación clara e inequívoca entre el componente y el producto.

Lo anterior tiene sentido si observamos los actores que participan o pueden verse afectados por el sistema, a los efectos del análisis jurídico[13]:

a) El desarrollador: persona responsable del diseño teórico de alto nivel del sistema de IA, así como de la programación, la capacitación y la verificación de dicho sistema.;

b) El proveedor de datos: persona que proporciona datos al sistema (es decir, los datos necesarios para respaldar la capacitación, la implantación o el funcionamiento);

c) El implantador: persona que implanta el sistema integrándolo en sus operaciones (por ejemplo, en los bienes y servicios que suministra

d) El operador: la persona que hace funcionar el sistema

e) La persona afectada

A los anteriores se le pueden sumar, en un sistema de registro distribuido los siguientes participantes[14]:

a) Un desarrollador: persona o grupo de personas que diseñan, desarrollan y mantienen el código informático con el que se hace funcionar el sistema;

b) Un operador del nodo: persona que opera un nodo (es decir, una computadora que ejecuta el código informático)

c) Un administrador que controla: qué personas operan un nodo y qué operaciones realiza cada nodo

La gama de actores descrita puede coincidir o no. En cualquier caso, pueden surgir relaciones contractuales entre la persona que implementa el sistema de IA y la persona que lo opera (por ejemplo, un contrato de suministro de

[11] De Bruyne, J., Dheu, O., Ducuing, C., "The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive", *Computer Law & Security* Review, 51, 2023.

[12] Cita reiteradamente en la propuesta, y ahora en la Directiva menos, Reglamento (UE) 2019/1020 relativo a la vigilancia del mercado y la conformidad de los productos y Reglamento (UE) 2023/988 relativo a la seguridad general de los productos

[13] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: la inteligencia artificial*, Nueva York, 6 a 17 de julio de 2020.

[14] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: continuación de la labor relativa a la contratación automatizada y progresos en otros aspectos*, Nueva York, 27 de junio a 15 de julio de 2022

bienes con IA integrada) o entre la persona que opera el sistema de IA y alguien afectado por él (por ejemplo, mediante un acuerdo de uso para la provisión de servicios con IA integrada).

2.5 El difícil encaje con las normas de derecho internacional privado en la determinación de la ley aplicable en la contratación automatizada

Para hablar de esta cuestión nos centraremos en los errores de programación e interferencia de terceros en los sistemas de IA, donde puede darse que la interferencia física de una persona frustre, por ejemplo, la formación del contrato, al introducir los datos, o que la parte que utilizara un programa informático para formar un contrato, siendo éste el que interpretara mal los datos, por lo que la otra parte podría verse afectada por un error, aunque el programa funcionara tal y como estaba programado, provocando con ello, además, un daño a un tercero.

Para ello, partimos del caso *B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l)*[15], donde la decisión adoptada por un Tribunal de Singapur tiene implicaciones en relación a los contratos automatizados, la IA y si las criptomonedas son consideradas como propiedad. Nosotros solo nos vamos a centrar en las primeras cuestiones, en relación a la naturaleza automatizada de la Plataforma que, según el Tribunal, podría dar lugar a transacciones que tengan un efecto contractual legalmente vinculante y cómo se determina el conocimiento, a los efectos de establecer un error cuando los contratos se celebran de forma automatizada por ordenador y no a través de la toma de decisiones humana[16].

Conforme a lo anterior, el Tribunal señalo que "toda la información necesaria para la formación del contrato electrónico ha sido preprogramada, según estrictos parámetros establecidos por la empresa, en el software informático de la SSP". Por lo tanto, los datos relevantes se procesan automáticamente por medios electrónicos a través del software de un ordenador y las transacciones se ejecutan automáticamente dentro de los parámetros especificados predeterminados en el programa. Una vez realizado, usando su ordenador y accediendo al software SSP, se introducen los datos necesarios, la oferta es generada automáticamente por el propio programa sin más intervención humana y, una vez que se han tomado los pasos requeridos por el programa para una aceptación de la oferta, la aceptación es procesada automáticamente por el propio programa, de nuevo sin intervención humana adicional[17]. De esta forma, los usuarios que tenían acceso al software SSP, creado por una empresa programadora, podían usar el programa con el fin de formalizar el contrato, con la otra parte del contrato, comprometiéndose a que, si se seguían las instrucciones previas; es decir, conforme a los procedimientos programados, estarían obligados por el resultado generado automáticamente, incluso si la parte destinataria o un tercero, que podría identificarse como los usuarios finales, a quienes van destinados lo productos finales, que son terceros en discordia, desconocían temporalmente ese resultado. El proceso podría describirse en una empresa fábricas, otra las compra a través de una plataforma programada por un tercero quizá por encargo, esta misma la distribuye para un usuario final u otra y yo, usuario final utilizo el producto).

De esta forma, puede observarse que en el presente caso, una parte ofrece el software SSP como el medio automático para la formación del contrato. Una vez que la otra parte ha metido los datos necesarios en el programa informático, no se necesita más intervención humana para la formación de un contrato vinculante entre una y otra parte. Ahora bien, el producto que resulte puede ser presentado a un usuario final, siendo este defectuoso, si se produce un error o fallo del sistema en el programa[18], que pueden ser consecuencia de diversos errores de procesamiento de datos, entre ellos la falta de acceso a fuentes de datos externas que hizo que el tipo de cambio se

[15] Caso B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l) 3. Disponible en: https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/quoine-pte-ltd-v-b2c2-ltd.pdf

[16] D. Kiat Boon Seng, "Quoine Pte Ltd v B2C2 Ltd: A Commentary", *China-Singapore "One Belt One Road" International Business Cases Digest Part* 1. Disponible en: SSRN: https://ssrn.com/abstract=3960007 or http://dx.doi.org/10.2139/ssrn.3960007

[17] WongPartnership LLP, "Singapore Court of Appeal Clarifies Application of Unilateral Mistake in Algorithmic Trading", *Casewatch*, Julio, 2020. Disponible es: https://www.wongpartnership.com/upload/medias/KnowledgeInsight/document/15268/20200702_CaseWatch_SingaporeCourtofAppealClarifiesApplicationofUnilateralMistakeinAlgorithmicTrading.pdf

[18] CNUDMI/UNCITRAL, *Cuestiones jurídicas relacionadas con la economía digital: la inteligencia artificial*, Nueva York, 6 a 17 de julio de 2020.

apartara del tipo de mercado, y la ausencia de salvaguardas incorporadas en la programación destinadas a impedir que se realizaran las operaciones.

Como ya hemos comentado, hablamos de programas que operan cuando se les llama a hacerlo de manera preestablecida. Son meras máquinas que llevan a cabo acciones que en otra época habrían sido realizadas por un humano debidamente capacitado. No son diferentes, por ejemplo, a un robot de cocina que me puede ayudar a hacer un gazpacho Hablamos de máquinas que operan como han sido programadas una vez activadas. De esta forma, como dice la Sentencia "cuando es relevante determinar cuál era la intención o el conocimiento subyacente al modo de operación de una máquina en particular, es lógico tener en cuenta el conocimiento o la intención del operador o controlador de la máquina". En el caso del robot de cocina, nosotros como personas físicas seremos quienes coloquemos los ingredientes y la pune en funcionamiento. Su conocimiento o intención será contemporáneo a la operación que va a hacer la máquina, en nuestro ejemplo el gazpacho, "pero en el caso de los robots o el software de los ordenadores, esto no será así. El conocimiento o la intención no pueden ser los de la persona que lo enciende, sino los de la persona que fue responsable de hacerlo funcionar de la manera en que lo hizo, es decir, el programador". Esto necesariamente se habrá hecho en una fecha anterior a la fecha en la que el software del ordenador o del robot llevaron a cabo los actos en cuestión. En este sentido, rechazo el argumento de la parte demandada de que el único conocimiento relevante es el conocimiento al momento de contratar. Sin embargo, se muestra de acuerdo con el demandante en el sentido de que en que se debe tener en cuenta el conocimiento y la intención del programador del programa en cuestión cuando se escribió ese programa o la parte relevante del mismo.

En definitiva, el criterio aceptado por el tribunal fue remitirse al estado mental de la persona que programó el sistema automatizado; es decir, antes de que se formara el contrato. El criterio rechazado por el tribunal consistía en remitirse al estado mental que habría tenido la parte que operaba el sistema automatizado si hubiera conocido las circunstancias pertinentes que rodeaban la formación del contrato[19]. Estos criterios se pueden describir en los términos de que la ley puede exigir que el estado mental de una persona se determine subjetivamente, en función de lo que la persona sabe realmente o de su verdadera intención, u objetivamente, en función de lo que la persona parece saber o de su aparente intención[20].

En relación a ello, existe una relación contractual y, por tanto surge el problema de determinar, la ley aplicable a la responsabilidad contractual derivada de cuando en la contratación automatizada el sistema de IA se utiliza en el comercio, entre la persona que implanta el sistema y la persona que lo hace funcionar (por ejemplo, un contrato con IA incorporada) y/o entre la persona que hace funcionar el sistema de IA y una persona afectada (por ejemplo, un acuerdo de uso para el suministro de servicios con IA incorporada) o entre las partes, que siguiendo las pautas del programa se relacionan comercialmente entre ellos.

Por otro lado, puede existir una responsabilidad extracontractual por el daño que se ha producido al usuario final. Ahora bien, es difícil probar que un defecto del hardware fue el motivo por el cual el robot de cocina, por ejemplo explotó, y aún más difícil determinar que la causa del daño fue un algoritmo defectuoso, porque si el algoritmo que se sospecha que causó el daño fue desarrollado o modificado por algún sistema de IA creado con técnicas de aprendizaje automático. En cualquier caso, habrá que determinar la ley aplicable a la responsabilidad contractual.

De esta forma, en el ámbito extracontractual: responsabilidad por daños causados por productos, en el Derecho internacional privado, las obligaciones extracontractuales derivadas de daños causados por los productos no se rigen por el Reglamento Roma II ni por el artículo 10.9 CC, sino por el Convenio de La Haya de 2 octubre 1973, sobre la Ley aplicable a la responsabilidad por productos, en vigor para España desde el 1 febrero 1989. La Directiva 85/374/CEE sobre daños causados por los productos no contiene regla alguna sobre su aplicación en casos internacionales: armoniza las legislaciones nacionales de los Estados miembros sobre estas materia, pero no recoge ninguna regla sobre su ámbito de aplicación en el espacio[21].

[19] D. Seng, "Quoine Pte. v. B2C2 Ltd., recurso de apelación civil núm. 81 de 2019, sentencia de 24 de febrero de 2020", *Singapore Law Reports*, vol. 2020, núm. 2.

[20] CNUDMI/UNCITRAL, *Uso de la inteligencia artificial y la automatización en la contratación*, Nueva York, 4 a 8 de abril de 2022

[21] A-L. Calvo Caravaca/ J. Carrascosa González, *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018, p. 1345.

De esta forma, el Convenio de La Haya de 2 octubre 1973 se aplica para determinar la Ley aplicable a la responsabilidad de los fabricantes de productos acabados o de componentes, productores de productos naturales, proveedores de productos y otras personas, comprendidos los reparadores y almacenistas, que intervienen en la cadena comercial de preparación y de distribución de un producto, por los daños causados por un producto (artículos 1 y 3 convenio). Asimismo, debe indicarse que no se aplica a los daños producidos un producto si este ha sido transferido al destinatario final por la persona a la que se imputa la responsabilidad. La responsabilidad, en este caso, será contractual, y se regirá por la Ley aplicable al contrato de que se trate (artículo l).

De lo anterior se deduce en la contratación automatizada se excluye su aplicación ya que es posible que el defecto no existía cuando el producto se puso en circulación; pues en el ámbito del derecho de la responsabilidad civil extracontractual pueden plantearse dificultades probatorias respecto del nexo causal con el daño, es decir, determinar si los daños o perjuicios sufridos fueron causados por el funcionamiento del propio sistema de IA, y no por la calidad de los datos procesados[22] por el sistema de IA que sea atribuible a un tercero.

Por otro lado, si bien se aprecia se aplicaría para determinar la ley aplicable a la responsabilidad de por daños causados por productos los bienes y los servicios, al hacerse referencia a las personas que intervienen en la cadena comercial de preparación y de distribución de un producto, es posible que esos regímenes quizás sean aplicables a los bienes con IA incorporada, pero también a los servicios con IA incorporada, en base al principio de equivalencia funcional[23]. En este supuesto, se aplicaría el artículo 4 del Convenio[24] que determina que la legislación aplicable será el Derecho interno del Estado en cuyo territorio se haya producido el daño, en el caso de que dicho Estado sea también:

a) el Estado de residencia habitual de la persona directamente perjudicada, o

b) el Estado en el que se encuentre el establecimiento principal de la persona a quien se le imputa la responsabilidad, o

c) el Estado en cuyo territorio el producto ha sido adquirido por la persona directamente perjudicada.

3 Conclusiones

En este contexto surge la necesidad de analizar y profundizar en un marco jurídico adecuado, para que tanto los ciudadanos como las empresas puedan confiar en la tecnología con la que interactúan, disponer de un entorno jurídico predecible y contar con la garantía efectiva de que van a protegerse sus derechos y libertades. Por ello, en relacionadas con la Ley aplicable, surgiendo con ello situaciones de responsabilidad contractual y extracontractual, donde planteamos la necesidad de revisar todas las circunstancias dadas para evitar que la responsabilidad se diluya respecto de las operaciones llevadas a cabo por las partes, donde puede darse que nos encontremos con dificultades probatorias respecto del nexo causal con el daño.

Bibliografía

Las referencias bibliográficas están integradas en el texto.

[22] J. Sluijs; P. Larouche; W. Sauter, “Cloud Computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market”, *JIPITEC*, 2012, núm. 3, pp. 130 – 149

[23] R. Illescas Ortiz, “La equivalencia funcional como principio básico del derecho de la contratación electrónica”, *Revista Aranzadi de derecho y nuevas tecnologías*, Nº. 1, 2003, pp. 19-31.

[24] A. Rodríguez Benot; B. Campuzano Díaz; M.ª. A. Rodríguez Vázquez; A. Ybarra Bores: *Manual de Derecho Internacional Privado*, 9ª Ed. Tecnos, 2023.