La aplicación de la inteligencia artificial y el derecho: La gestión de riesgos como fundamento de la diligencia debida frente a los riesgos de la inteligencia artificial

Alfonso Ortega Giménez
Profesor doctor de Derecho Internacional Privado. Universidad Miguel Hernández de Elche
alfonso.ortega@umh.es | https://orcid.org/0000-0002-8313-2070
Juan José Gonzalo Domenech
Consultor GRC. Eulen Seguridad
jjgonzalo.seguridad@eulen.com | https://orcid.org/0000-0002-6213-9871
José Bonmatí Sánchez
Abogado. Ayuela Jiménez Legal, SLP
jbs@ayuelajimenez.es | https://orcid.org/0000-0002-0491-8738

Este trabajo ha sido finalista en el **Premio «Estudios Financieros» 2020** en la modalidad de **Derecho Civil y Mercantil**.

El jurado ha estado compuesto por: don Javier Avilés García, don Francisco Javier Arias Varona, doña María Isabel Candelario Macías, doña Icíar Cordero Cutillas, don Fernando Díez Estella, doña Paula Fernández Ramallo y don Antonio Serrano Acitores.

Extracto

Como resultado de la globalización, la expansión de los mercados y el uso masivo de datos, las empresas se enfrentan a un mercado que evoluciona hacia la digitalización de la prestación de los servicios y la distribución de bienes. Como consecuencia de las posibilidades que ofrece el análisis masivo de datos y el uso de algoritmos de aprendizaje, las empresas pueden aumentar su capacidad competitiva mediante el desarrollo e implementación de nuevas soluciones tecnológicas, encaminadas a la mejora de la prestación de servicios y distribución de bienes al mercado, a través de la personalización de la experiencia de los usuarios mediante el uso de sistemas de recomendación, la automatización de la atención al cliente y la mejora en los procedimientos logísticos. Pero los beneficios y ventajas que implica el uso de la inteligencia artificial no deben desviar la atención de los retos y riesgos que genera para todos los operadores que intervienen en su ciclo de vida, adquiriendo especial importancia la adopción de una conducta proactiva.

Palabras clave: inteligencia artificial; cuarta revolución industrial; revolución 4.0; gestión de riesgos; *accountability*; transformación digital.

Fecha de entrada: 01-06-2020 / Fecha de aceptación: 18-09-2020

Cómo citar: Ortega Giménez, A., Gonzalo Domenech, J. J. y Bonmatí Sánchez, J. (2021). La aplicación de la inteligencia artificial y el derecho: La gestión de riesgos como fundamento de la diligencia debida frente a los riesgos de la inteligencia artificial. *Revista CEFLegal*, *241*, 5-36.

The application of artificial intelligence and law: Risk management as a foundation for due diligence in the face of artificial intelligence risks

Alfonso Ortega Giménez

Juan José Gonzalo Domenech

José Bonmatí Sánchez

Abstract

As a result of globalization, the expansion of markets and the massive use of data, companies are facing a market that is evolving towards the digitization of the provision of services and the distribution of goods. As a consequence of the possibilities offered by massive data analysis and the use of learning algorithms, companies can increase their competitive capacity through the development and implementation of new technological solutions, aimed at improving the provision of services and distribution of goods to the market, through the personalization of the user experience through the use of recommendation systems, the automation of customer service and the improvement in logistics procedures. But the benefits and advantages that the use of artificial intelligence implies should not divert attention from the challenges and risks that it generates for all the operators involved in its life cycle, with the adoption of proactive behavior becoming especially important.

Keywords: artificial intelligence; fourth industrial revolution; revolution 4.0; risk management; accountability; digital transformation.

Citation: Ortega Giménez, A., Gonzalo Domenech, J. J. y Bonmatí Sánchez, J. (2021). La aplicación de la inteligencia artificial y el derecho: La gestión de riesgos como fundamento de la diligencia debida frente a los riesgos de la inteligencia artificial. *Revista CEFLegal*, *241*, 5-36.

Sumario

1. La cuarta revolución industrial y la digitalización del mercado

La cuarta revolución industrial ha pasado de ser un fenómeno novedoso y desconocido, al día a día de las empresas que intervinieren en el mercado, ya sea mediante la prestación de servicios, o mediante la producción y distribución de bienes.

La cuarta revolución industrial se construye sobre la implementación y uso de las nuevas tecnologías por los operadores del mercado en sus procedimientos internos y externos, permitiendo a las empresas organizar mejor sus medios de producción, adaptándose con mayor agilidad a las necesidades de la demanda y gestionando de forma más eficiente sus recursos, mediante el procesamiento masivo de datos.

Sin perjuicio de que la cuarta revolución industrial se construya sobre el uso de una gran variedad de tecnologías, cabe destacar el protagonismo de tres de ellas respecto del resto: (a) el internet de las cosas (IoT por sus siglas en ingles), (b) el *big data* y (c) la inteligencia artificial (IA).

A pesar de que las mismas tengan finalidades distintas y se construyan sobre la base distintos y variados componentes tecnológicos, es la coordinación en el uso de estas tecnologías la que ha permitido desarrollar una gran variedad de aplicaciones que ofrecen a las empresas la posibilidad de, mediante la acumulación y análisis masivo de datos, la extracción de *insights* que permiten tomar decisiones más informadas, incrementando así la posibilidad de que la decisión adoptada sea la más beneficiosa para el curso de la empresa.

Resulta evidente, por tanto, que el motor de la cuarta revolución industrial pasa por la captación, análisis y uso masivo de los datos captados, ya sea mediante la interacción entre personas (P2P, del inglés *people to people*), entre maquinas (M2M, *machines to machine*) y entre personas y maquinas (P2M, *people to machine*).

Sin duda, es el actual ecosistema digital el que ha permitido la generación de las grandes masas de datos, y así lo refleja la infografía de la consultora Domo titulada *Data never sleeps 7.0*, arrojando que, en el año 2019, a través de la red, se generaron 4 millones de datos por minuto (Domo, 2019).

En la misma red en la que se generan los datos, las empresas llevan años desarrollando e implementando sus planes de actuación para poder ofrecer sus productos y servicios en el nuevo mercado: el mercado digital.

Los operadores de mercado no son ajenos al potencial desarrollo y oportunidades que brinda el mercado digital, no solo por poder llegar a clientes y usuarios de todos los rincones del mundo, también por la posibilidad de implementar, a su actuación en el mercado, las soluciones que las nuevas tecnologías ofrecen, buscando adquirir mayores niveles de competencia frente al resto de los operadores.

Pero, actualmente, las empresas no solo se enfrentan a una transformación del mercado sin precedentes, también al cambio de mentalidad de los usuarios y consumidores de los bienes y servicios, que se han transformado en clientes caracterizados por la información, la comparativa, la agilidad y la disminución de la fidelidad.

Es en este punto donde las empresas que hayan implementado herramientas o soluciones basadas en IA podrán adaptarse a la nueva demanda y mejorar su posición en el mercado. En este sentido, y sin ánimo de ser exhaustivos, la IA puede ofrecer a los operadores del mercado los siguientes beneficios:

- **Personalización de la experiencia**: La captación, almacenamiento y análisis de grandes cantidades de datos declarados por el propio usuario o generados en la propia red permite generar perfiles de los usuarios y, en consecuencia, el desarrollo y despliegue de soluciones de IA que permitan personalizar el trato de los usuarios, a través de sistemas de recomendaciones y avisos basados en sus preferencias e intereses. En este sentido, Netflix dispone de soluciones de IA que permiten, a través de variables como el tiempo medio de conexión de los usuarios, franja horaria de conexión, películas y series vistas con anterioridad y edad, entre otras, habilitar un sistema de recomendaciones personalizado que avisa al usuario sobre nuevo material audiovisual que podría ser de su interés.
- **Agilización en la atención y resolución de controversias**: Mediante el entrenamiento y uso de *chatbots*, las empresas pueden ofrecer a sus usuarios una herramienta que permita resolver las dudas que los usuarios puedan plantear, algo que hasta el momento cumplían las ya tan conocidas FAQ (*frequently asked questions*) pero que, a diferencia de los actuales *chatbots*, no se actualizan de forma automática con las cuestiones que puedan ir planteando los usuarios. De esta forma, los usuarios pueden resolver sus dudas en cualquier momento, sin importar si la cuestión la plantean un día festivo o si la hora de la consulta es antes o después del horario comercial, evitando así las, a veces, tan incompletas FAQ o los tiempos medios de respuesta que, en caso de tener que ser respondidas por personas, podrían demorarse en función del número de consultas y el momento en el han sido planteadas.

- **Mejora en los procesos internos y logísticos**: El uso de soluciones basadas en IA permite a las empresas poder adoptar decisiones respecto de su actividad en el mercado, ya sea desde la cantidad de productos de los que disponen en oferta, hasta el desarrollo de nuevas áreas de negocio, pasando por el tipo de publicidad en función de las características de los usuarios que adquieres sus bienes o servicios. En este sentido puede destacarse el sistema *Method and System for Anticipatory Package Shipping* de la empresa Amazon, que, a partir del análisis de los datos de los usuarios (p. ej. historial de compras, hábitos de consumo, etc.), permite adoptar un modelo predictivo del comportamiento del consumidor a partir de su historial de compras y de sus hábitos de consumo. De esta forma, se podrá anticipar la demanda en una determinada área geográfica y abastecer los almacenes más cercanos con carácter previo al incremento previsto de la demanda.

Partiendo de lo expuesto en el apartado anterior, es innegable la cantidad de beneficios que el uso de herramientas basadas en IA ofrece a sus implementadores, es decir, a quienes la utilizan; una serie de ventajas que pueden implicar la diferencia entre ser un operador competitivo o no, pero, como dice el refranero español, toda moneda tiene dos caras.

La IA, identificada con la moneda del refrán, tiene dos caras: por un lado, las de los beneficios y ventajas derivadas de su uso y, por otro lado, los retos y riesgos que genera su desarrollo e implementación.

Es en este sentido, no es difícil encontrar ejemplos sobre los daños y perjuicios que puede ocasionar el uso de IA, ya sea de forma intencionada o por falta de diligencia. En el caso de los supuestos intencionados pueden destacarse los casos de *deepfakes*, material audiovisual que, mediante el uso de IA permite crear situaciones ficticias con un grado de realismo que impide o dificulta gravemente la distinción entre lo real y lo ficticio (Merino, 2019).

Por otro lado, también existe la posibilidad de que el daño ocasionado no sea consecuencia de un acto intencionado, como por ejemplo la posibilidad de que, mediante el uso de un sistema de IA para la clasificación de los clientes, el diseño de los algoritmos o como consecuencia de los datos utilizados para su entrenamiento, se utilice como elemento diferenciador alguna característica discriminatoria. A modo de ejemplo puede destacarse el ya conocido caso de Amazon, con un sistema de IA cuya función relacionada con la selección de personal discriminaba a las mujeres respecto de ciertos puestos de trabajo, o el sistema de IA de Google, entrenado para clasificar personas pero que, debido a una falta de datos de entrenamiento de calidad, no aprendió a identificar a las personas de raza negra y, por tanto, las discriminaba en las herramientas de clasificación de fotos.

Estos son ejemplos que permiten acercarse al concepto de riesgo en el uso de sistemas de IA y, aunque puedan parecer casos aislados, el cada vez mayor uso de IA en nuestras vidas cotidianas incrementa la posibilidad de sufrir un perjuicio o, si nos encontramos en el otro lado del muro, ser responsables del mismo.

Por tanto, afrontar los riesgos que genera el uso de la IA supone un gran reto jurídico, ya sea por el cada vez mayor uso de la misma, debido a la transversalidad en su aplicación y el constante desarrollo, lo que incrementa el riesgo de que, derivado de su uso, se pueda ocasionar un daño a terceros, o por la cantidad de sujetos que intervienen a lo largo de su ciclo de vida, debido a la complejidad en el diseño, desarrollo, implementación y uso de la IA, que amplía y complica la identificación del sujeto que debe responder por los daños provocados.

A consecuencia de lo anterior, al Unión Europea ha elaborado y publicado, a lo largo de los últimos dos años, una serie de informes, recomendaciones y propuestas que buscan arrojar luz sobre una gran cantidad de cuestiones relativas a la IA, que van desde el propio concepto de IA, hasta sus posibles usos, pasando por, probablemente, la cuestión más relevante: la IA como fuente de riesgos y cómo afrontarlos.

2. Análisis de la inteligencia artificial desde la perspectiva europea

2.1. Concepto jurídico de la inteligencia artificial y la fiabilidad durante su ciclo de vida

Ya lo anunciaba la actual presidenta de la Comisión Europea, Ursula von der Leyen, con carácter previo a su elección, y es que durante los 100 primeros días de su mandato presentaría propuestas de legislación para un enfoque europeo coordinado sobre las implicaciones éticas y humanas de la IA.

Hacía apenas unos años, en 2017, las instituciones de la Unión Europea adoptaban una de las primeras iniciativas de la Unión Europea, con relevancia jurídica y regulatoria, en el marco de la IA; concretamente el Parlamento Europeo remitió a la Comisión Europea un informe con recomendaciones sobre normas de derecho civil sobre robótica (Parlamento Europeo, 2017).

Durante los años siguientes, y ante la pérdida de la carrera por la IA frente a otras potencias como Estados Unidos o China, la Unión Europea ha decidido incrementar su intervención, consciente de que el mercado europeo necesita normas que reduzcan la incertidumbre y la inseguridad jurídica derivada de la ausencia de regulación o guías en el desarrollo y uso de la IA.

En este sentido, la UE se enfrenta un reto regulatorio cada vez más frecuente como resultado de la cada vez mayor implementación de soluciones o herramientas basadas en las nuevas tecnologías: el equilibrio de los intereses de todos los intervinientes en el ciclo de vida de la tecnología.

Por un lado, el regulador debe atender la necesidad de dotar al ordenamiento jurídico con un marco de protección, que reduzca los riesgos y proteja a los destinatarios frente a daños y perjuicios que puedan sufrir. Por otro lado, el regulador también debe garantizar la creación de un marco favorable del desarrollo y progresos de las nuevas tecnologías, incentivándolo mediante un marco regulatorio flexible y adaptativo.

En este marco, y con el objetivo de dotar de mayor seguridad jurídica el desarrollo y uso de la IA en el mercado europeo, las instituciones de la Unión Europea han centrado su actividad en emitir una serie de directrices que permitan resolver o reducir la incertidumbre respecto de las dos grandes fuentes de riesgos: (a) afrontar los riesgos inherentes al uso de la IA y (b) establecer las reglar para determinar el o los responsables de los daños que pudiera ocasionar el uso de la IA.

Respecto de la primera de las cuestiones, y debido a la transversalidad funcional de la IA, ya citada, la Unión Europea considera necesario, para reducir o eliminar los riesgos derivados del desarrollo y uso de la IA, la adopción de una serie de medidas por parte de los sujetos intervinientes, destinada a convertir la IA en IA Fiable (Comisión Europea, 2019, p. 14).

La IA Fiable es aquella IA de la cual puede asegurarse que, durante su ciclo de vida, cumple con el ordenamiento jurídico (licitud), respeta los valores éticos y morales (ética) y dispone de una infraestructura segura (robustez). En conclusión, la IA Fiable es aquella IA que, debido a las medidas implementadas, se puede catalogar como licita, ética y robusta.

En este sentido, e independientemente del uso de la IA (p. ej. predecir, clasificar o prescribir, entre otros) y del campo en el que se despliegue (p. ej. *ecommerce*, *retail* y financiero, entre otros), los sujetos intervinientes a lo largo del ciclo de vida de la IA deben adoptar las medidas necesarias que permitan acreditar que la IA cumple y garantiza: (a) la autonomía del ser humano, (b) la prevención de la generación de daños, (c) la equidad y (d) la explicabilidad.

Sin perjuicio del establecimiento de los cuatro pilares que deben garantizarse en el uso de cualquier sistema de IA a lo largo de su ciclo de vida, la Unión Europea no establece medidas *numerus clausus*, sino que recoge una serie de actividades o políticas que, de ser implementadas por los sujetos intervinientes en el ciclo de vida de la IA, aumentarían su fiabilidad. Entre las medidas propuestas por la Unión Europea, esta diferencia entre las técnicas y las no técnicas: (a) supervisión humana de las decisiones tomadas por la IA antes de su aplicación a terceros, (b) desplegar sistemas de IA cuya precisión supere un porcentaje mínimo, (c) asegurar la explicabilidad de las decisiones tomadas por la IA, y (d) auditorías algorítmicas encaminadas a detectar y solventar posibles sesgos y errores derivados del aprendizaje automático, entre otras.

Por tanto, y a falta de normas de carácter vinculante, la Unión Europea ha establecido una guía a seguir por aquellos sujetos que intervienen en el ciclo de vida de la IA, y que se construye sobre la adopción de una conducta proactiva o *accountability*, al ser necesario

asumir, en la práctica, una serie de medidas que se estimen convenientes para reducir los riesgos derivados del uso de la IA.

Es precisamente en este momento donde la inexistencia de una definición universal de IA podía generar conflicto, pues la ausencia de una definición de la IA permitía que los sujetos consideraran que la tecnología desarrollada o implementada podría no considerarse IA y, en consecuencia, no adoptar ninguna medida encaminada a garantizar su fiabilidad.

A consecuencia de lo anterior, y aunque actualmente no existe un consenso único sobre una definición de la IA, el Grupo de Expertos de Alto Nivel en IA de la UE (AI HLEG, por sus siglas en inglés) definen la IA como (Comisión Europea, 2019, p. 6):

- Sistemas de *software*, y en algunos casos también de *hardware*, diseñados por seres humanos, es decir, la IA no requiere de entidad corpórea (p. ej. robot) para ser identificada como IA, siendo, en muchos casos, programas informáticos sin soporte físico.
- Estos sistemas, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivado de esos datos.
- Como consecuencia de la captación y análisis de los datos, llevan a cabo la acción o acciones óptimas para lograr el objetivo establecido.

Esta definición también ha sido utilizada en la propuesta enviada por el Parlamento Europeo a la Comisión Europea relativa al régimen de responsabilidad civil de la IA. Concretamente, en su artículo 3, relativo a las definiciones, se recoge que la IA es:

> Todo sistema que presenta un comportamiento inteligente al analizar determinadas entradas y actuar, con cierto grado de autonomía, con vistas a alcanzar objetivos específicos. Los sistemas de IA pueden basarse exclusivamente en programas informáticos, que actúen en el mundo virtual, o estar integrados en dispositivos físicos.

2.2. Riesgos inherentes al desarrollo y uso de la inteligencia artificial: responsabilidad en la cadena de valor

Una vez definida la IA y el establecimiento de una guía que orientara la actuación de los sujetos que intervienen en su ciclo de vida, las instituciones de la UE y el AI HLGE han emitido más informes y guías encaminadas a ayudar a los sujetos a identificar más riesgos y a su tratamiento, como, por ejemplo, el informe *Liability for Artificial Intelligence and other*

emerging digital techonologis, publicado en diciembre de 2019, y que ha servido como base para el establecimiento de los principales riesgos a los que se enfrenta el uso de la IA y los posibles sistemas de responsabilidad aplicables (Comisión Europea, 2019).

Pero ha sido en febrero de 2020 cuando la Unión Europea publicó una serie de informes y guías encaminadas a definir la política oficial que adoptará la Unión Europea frente al desarrollo y uso de la IA en territorio comunitario. Entre ellas cabe destacar el Libro Blanco sobre la IA.

En el Libro Blanco, la Comisión Europea focaliza el desarrollo de la IA sobre la base de dos conceptos: excelencia y confianza. Cada principio se enfoca en una visión distinta de la IA: (a) la excelencia se encuentra dirigida al desarrollo y evolución técnica de la IA, concretamente mediante el incentivo de la investigación y la innovación que permita crear soluciones de IA y erigir al mercado europeo como referente mundial; y (b) la confianza se encuentra orientado a la adopción de medidas que permitan reducir los riesgos de la IA (fiabilidad) y, en consecuencia, genere confianza en su uso.

Para nuestro caso, el principio relevante es el de la confianza, es decir, el relacionado con el cumplimiento normativo. En este sentido, la Unión Europea diferencia, respecto del cumplimiento normativo, dos tipos de IA: alto riesgo y otras.

Para la diferenciación entre ambos tipos de IA, la Unión Europea se focaliza en la mayor o menor posibilidad de que, derivado de la aplicación de la IA en un sector y actividad concreta, se generen riesgos significativos; por tanto, y para definir la IA de alto riesgo (*high risk*) la UE exige la confluencia de dos requisitos:

- La aplicación de la IA en un sector en el que, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos. Estos sectores serán determinados por la Unión Europea a través del desarrollo normativo, pero ya se adelantan sectores como la sanidad, la energía y el transporte.
- La aplicación de la IA en el sector en cuestión se use de manera que puedan surgir riesgos significativos.

Por tanto, no cualquier uso de IA puede considerarse de alto riesgo, incluso cuando se utilice en un sector señalado como de alto riesgo, pues se requiere además que el uso concreto también sea de alto riesgo. En el caso del sector del transporte, considerado de alto riesgo, el uso de la IA para identificar los productos alimenticios que transporta y adaptar la temperatura difiere, en cuanto al riesgo, en el uso de la IA para facilitar la conducción autónoma del vehículo. En ambos casos nos encontramos ante el uso de IA en el sector del transporte, pero uno de ellos parece, *a priori*, no generar riesgos significativos (control de la temperatura) y, sin embargo, la otra funcionalidad sí que podría catalogarse como generador de riesgos significativos (control del vehículo).

No obstante, hay casos excepcionales que, *per* se, implican un alto riesgo, como es la identificación biométrica remota, independientemente del sector en el que se use (Comisión Europea, 2020, p. 23).

En definitiva, y desde una perspectiva jurídica, diferenciar entre IA de alto riesgo e IA normal es primordial, pues en función de la consideración que tenga el sistema de IA desplegado, las obligaciones impuestas por la normativa serán distintas.

Mientras que en el caso de la IA de alto riesgo le será de aplicación el marco normativo existente y la normativa específica que será elaborada y publicada por la Unión Europea, introduciendo nuevas medidas y requisitos, el resto de usos de la IA quedarán sometidos a la aplicación de la normativa actual, sin perjuicio de posibles adaptaciones que se puedan llevar a cabo.

De esta forma, a los sujetos que intervengan en el ciclo de vida de la IA les serán de aplicación, entre otras, la normativa de protección de datos, para aquellos casos en los que se utilicen datos personales durante el entrenamiento, ajuste, prueba y uso de la IA; la normativa de protección y defensa de los consumidores y usuarios, en aquellos casos en los que el uso de la IA se encuentra vinculado con la prestación de servicios o producción y distribución de bienes a consumidores, o la normativa de servicios de la sociedad de la información y comercio electrónico si el uso de la IA se realiza en el marco de la actuación en el mercado digital.

Por tanto, y como resultado de todo lo anterior, resulta innegable que la transversalidad en el desarrollo y uso de la IA y, por ende, su aplicación en una gran variedad de ámbitos de la realidad tiene, como consecuencia directa, el incremento de los riesgos a generar algún daño o llevar a cabo alguna conducta considerada como infracción y, en consecuencia, sancionable por la autoridad competente.

Es en este punto donde los supuestos de responsabilidad adquieren mayor complejidad al sumarse, a la existencia de una gran variedad de riesgos, la intervención de varios sujetos que podrían dificultar la imputación de la conducta causal y, en consecuencia, resarcir al perjudicado.

Debido a la complejidad técnica de la mayoría de herramientas y sistema de IA, el ciclo de vida de la IA comprende muchas fases, en las cuales intervendrán varios operadores en función de las tareas asumidas. Entre los operadores que intervienen en el ciclo de vida de un sistema de IA pueden destacarse, en función de las distintas competencias que pueden ser asumidas: (a) diseño y desarrollo, (b) entrenamiento, (c) validación, (d) despliegue, (e) explotación y (f) retirada.

Independientemente del número de etapas que conforman el ciclo de vida de un sistema de IA, no existe una relación directa entre estas y el número de operadores que intervienen, pues habrá ocasiones en las que un solo operador aborde la mayoría de las etapas, y otros casos en los que la división funcional se encuentre más dispersa.

En consecuencia, la Unión Europea reconoce que si los riesgos derivado del uso de la IA se materializan, la intervención de varios operadores puede complicar la trazabilidad de la verdadera causa o causas del daño y los sujetos a los que se les puede imputar, perjudicando así: (a) a las empresas o profesionales que forman parte del mercado de la IA, por la inseguridad jurídica sobre su responsabilidad frente a posibles daños que pudiera ocasionar la IA, y (b) al destinatario final que, como posible damnificado, podría ver dificultada sus posibilidades de reclamar y recibir compensaciones. Esta situación genera, por tanto, tres escenarios de responsabilidad:

- **Responsabilidad mancomunada**: Los sujetos intervinientes durante el ciclo de vida de la IA responderán proporcionalmente a su intervención en la provocación de los daños. Este régimen, aunque beneficioso para los sujetos que intervienen en el desarrollo y despliegue de la IA, perjudica gravemente a los damnificados, que tendrán que probar, salvo en la existencia de un sistema de responsabilidad objetiva, la responsabilidad individual de cada uno de los intervinientes, sobre la base de las funciones asumidas, el daño generado y el nexo causal entre ambos.
- **Responsabilidad solidaria**: El damnificado podrá dirigirse contra cualquier de los sujetos intervinientes por el hecho de haber intervenido en el proceso de desarrollo, puesta a disposición y uso de la IA. En este régimen, a diferencia del anterior, son las imputadas las que tienen que probar que su intervención no fue la generadora del daño.
- **Responsabilidad del sistema de IA**: En la propuesta presentada por el Parlamento Europeo a la Comisión Europea en el año 2017, se barajaba la posibilidad de reconocer personalidad jurídica específica para los robots. De esta forma, los robots autónomos más complejos serían considerados personas electrónicas responsables de reparar los daños que puedan causar y aplicar la personalidad electrónica en aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente.

Esta última posibilidad ya fue rechazada por la Unión Europea en el informe sobre IA y responsabilidad, publicado en diciembre de 2019, al recoger de forma expresa que, de cara a los efectos de la responsabilidad, no sería necesario dotar a los sistemas autónomos de personalidad propia (Comisión Europea, 2019, p. 37).

En consecuencia, son dos los regímenes de responsabilidad que podrían ser de aplicación: mancomunado o solidario. Sin perjuicio de que la Unión Europea no se haya pronunciado formalmente sobre el tipo de régimen de responsabilidad aplicable, es muy probable que se decante por el sistema de solidaridad entre los sujetos intervinientes en el ciclo de vida de la IA, dado que garantiza, en mayor medida, la protección del damnificado.

A favor de esta interpretación ya se ha pronunciado el Parlamento Europeo en el Proyecto de Informe con recomendaciones destinadas a la Comisión sobre un régimen de res-

ponsabilidad civil en materia de inteligencia artificial (Parlamento Europeo, 2020, p. 24). El artículo 11 del citado informe establece que, en caso de que haya más de un implementador de un sistema de IA, estos serán responsables conjuntos y solidarios. El informe define como implementador la persona que decide sobre el uso del sistema de IA, ejerce control sobre el riesgo asociado y se beneficia de su utilización.

De esta forma parece que los sujetos que intervengan en el procedimiento de diseño, desarrollo y uso de sistemas de IA se encuentran irremediablemente avocados a tener que asumir una serie de riesgos, de los cuales responderán de manera solidaria junto a otros sujetos, sin perjuicio de la posibilidad de repetir contra otros de los sujetos intervinientes en el ciclo de vida de la IA, estableciendo así un sistema de responsabilidad en la cadena de suministro. Este sistema se basa en tres pasos lógicos para imputar la responsabilidad al agente (Terwindt, Leader, Vastardis, Wright, 2018, pp. 269-271):

- Establecer la **existencia de un indelegable deber de cuidado, o diligencia debida** basado en tres requisitos: (a) que el daño era previsible; (b) proximidad de la relación entre el demandante y el demandado, y (c) que es justo, justo y razonable que la ley imponga un deber de un alcance determinado a una de las partes en beneficio de la otra.
- El **quebrantamiento** de ese deber de cuidado, cuando efectivamente se ha atribuido al agente.
- Que ese quebrantamiento del deber de cuidado haya **causado el resultado ilícito**.

En ese deber de cuidado, se espera que la organización adopte como una práctica adecuada por parte del agente un proceso de apreciación y tratamiento de riesgos como parte de su responsabilidad personal; y como se analizará en el próximo apartado, si el sujeto concreto actúa, dentro de las funciones asumidas respecto del ciclo de vida de la IA, con la debida diligencia.

2.3. Proactividad y debida diligencia como conducta sancionada como circunstancia tendente a la reducción o eliminación de la responsabilidad

Con la llegada de las nuevas tecnologías han aflorado una gran cantidad de retos y riesgos derivados del uso de las mismas, convirtiendo la seguridad jurídica que ofrece la exhaustiva regulación a través de normas que requieren de un procedimiento de elaboración, enmienda y aprobación en un auténtico obstáculo para el verdadero desarrollo de las nuevas tecnologías y sus oportunidades.

En síntesis, el regulador se enfrente a un marco donde la tecnología avanza y evoluciona a un ritmo que nuestro sistema normativo actual no puede seguir, por estar construido,

mayoritariamente, sobre un sistema basado en formalismos inherentes a la elaboración y aprobación de normas, lo que, en la práctica, dificulta y obstaculiza el desarrollo y uso de las nuevas soluciones tecnológicas, incluida la IA, al no contar los interesados (diseñadores, desarrolladores, usuarios, etc.) con un marco que permita generar seguridad en el uso de la IA y confianza en las consecuencias.

Como resultado de lo anterior, y ante la cada vez mayor implementación de la IA en el mercado, el regulador, tanto nacional como comunitario, ha decidido adoptar una vía de regulación, similar a la que actualmente es aplicable a la protección de datos y la privacidad: dentro de un marco legal mínimo impuesto por el regulador (p. ej. normas marco), la persona o entidad interesada en la implementación de sistemas tecnológicos en su modelo de negocio debe asumir una conducta proactiva (*accountability*), destinada a la adopción de medidas que garanticen el despliegue y uso dentro de unos estándares de fiabilidad y seguridad.

Aunque pueda ser objeto de regulación más específica, todos los informes, guías y propuestas publicadas por la Unión Europea en materia de IA coinciden en que uno de los requisitos que se exige a todos los sujetos que intervengan en el ciclo de vida de la IA es el de adoptar una conducta proactiva, es decir, orientada a la actuación diligente en la implementación, mantenimiento, uso y responsabilidad que pudiera ocasionar la IA (Comisión Europea, 2019, p. 10).

En este sentido, el regulador articula el cumplimiento legal a través de una serie de normas donde de define el objetivo a alcanzar (p. ej. disponer una IA fiable), pero delegando en la organización los medios para alcanzarlo. Este método regulatorio, ya utilizado en campos como el de la protección de datos de carácter personal, se construye sobre un sistema basado en la gestión, por parte de cada organización, de los riesgos que soporta derivado de su contexto y actividad desarrollada.

De esta forma, y ante una realidad cambiante, como consecuencia del cada vez mayor desarrollo de las tecnologías, el regulador delega en los operadores la tarea de adoptar las medidas que consideren necesarias, en función de las circunstancias propias de cada operador, para alcanzar un objetivo prefijado en vez del mero cumplimiento de hitos regulatorios (Kishnani, Turley y Eggers, 2018, p. 9), es decir, se obliga a los operadores a asumir un papel proactivo: una debida diligencia.

No en pocos casos, la materialización de un riesgo y la responsabilidad del operador como sujeto causante del daño puede verse reducida o eliminada si se prueba que, a través de la debida diligencia, se han adoptado las medidas necesarias para identificar, analizar y tratar los riesgos derivados del contexto y la actividad desarrollada.

En definitiva, la debida diligencia se sanciona, en muchas ocasiones, con una reducción de la responsabilidad o su eliminación, en el menor de los casos. Este modelo no es exclusivo de la Unión Europea, pues otros países, como Japón, de amplia tradición tecnológica, también han adoptado esta estrategia de regulación de los riesgos (Turner, 2019, p. 299).

La figura de la debida diligencia adquiere especial relevancia en el campo del desarrollo y uso de la IA pues, como ya se ha expuesto previamente, la transversalidad en el uso y aplicación de la IA y la orientación del sistema de responsabilidad a un régimen de solidaridad incrementan el número de riesgos y, en consecuencia, de las probabilidades de encontrarse ante un supuesto de responsabilidad por daños o la comisión de una infracción sancionable.

Sin embargo, y con el objetivo de acreditar la adopción de las citadas medidas proactivas en el marco de la IA, la Unión Europea plantea la consecución de certificaciones (validación obligatoria para los sistemas de IA de alto riesgo) o etiquetado (validación voluntaria para los sistemas de IA no considerados como de alto riesgo) con el objetivo de permitir a los agentes económicos mostrar que la IA utilizada es fiable. Ello contribuirá a incrementar la confianza de los operadores en los sistemas de IA.

Más allá de la mera aproximación teórica realizada en los párrafos anteriores, y como se analizará en los siguientes aparatos, la adopción de una conducta proactiva por parte de los sujetos intervinientes en el ciclo de vida de la IA se encuentra ampliamente amparada por la normativa que, como ya se ha visto unos apartados anteriores, es de aplicación a la IA.

3. Aplicación práctica de la diligencia debida como elemento para la reducción de la responsabilidad

3.1. El concepto de riesgo legal

La implicación de los sistemas de IA y la interactuación con los usuarios supone de por sí ejercer una actividad de riesgo en las operaciones de la organización. La existencia de sistemas de IA dentro del comercio electrónico implica la aplicación de diversos regímenes jurídicos, como puede ser la Ley de servicios de la sociedad de la información (LSSI), protección de datos y seguridad de la información.

Dentro de la gestión jurídica de una organización, deben tenerse en cuenta los riesgos legales derivados del uso del sistema de IA. En este sentido, la norma ISO 31022, estándar internacional y aceptado internacionalmente por la International Standard Organization, sobre la gestión de riesgos legales, aporta una definición de riesgo legal[1], que queda estipulado como «el efecto de la incertidumbre sobre los objetivos en relación con las materias

[1] La definición de «riesgo legal» es similar a la estipulada por el Comité de Basilea de Supervisión Bancaria (2005, p. 137), que lo define como «riesgo de sanciones legales o normativas, pérdida financiera material, o pérdida de reputación que un banco puede sufrir como resultado de incumplir con las leyes, regulaciones, normas, estándares de auto-regulación de la organización, y códigos de conducta aplicables a sus actividades bancarias».

legales, regulatorias, y no contractuales». A continuación, la norma crea una clasificación de las fuentes de riesgos legales[2] que, a su vez, podemos clasificarlas según el impacto en la organización, según sean riesgos directos o indirectos (Ceballos, 2007, p. 3):

Como **riesgo indirecto**, destacamos las incidencias legales que puedan tener su origen en decisiones políticas, leyes nacionales o internacionales, incluyendo leyes estatutarias, jurisprudencia o derecho consuetudinario, actos administrativos, órdenes regulatorias, sentencias y laudos, reglas procesales, memorandos de entendimiento o contratos. El riesgo legal crece con la incertidumbre sobre las leyes, normativa y acciones legales aplicables. Por tanto, el riesgo legal incluye la exigibilidad legal, la legalidad de los instrumentos y la exposición a cambios no anticipados en leyes y regulaciones (Puyol, 2018, p. 82).

En cuanto a **riesgos directos**, destacamos los siguientes:

- El riesgo respecto a asuntos contractuales que se relacionan con las situaciones en que la organización no cumple con sus obligaciones contractuales no hace cumplir sus derechos contractuales o celebrar contratos con términos y condiciones onerosos, inadecuados, injustos o inaplicables.
- El riesgo de los derechos no contractuales es el riesgo de que la organización no haga valer sus derechos no contractuales. Por ejemplo, el hecho de que una organización no haga cumplir sus derechos de propiedad intelectual, como sus derechos relacionados con derechos de autor, marcas registradas, patentes, secretos comerciales e información confidencial contra un tercero.
- El riesgo de las obligaciones no contractuales es el riesgo de que el comportamiento y la toma de decisiones de la organización puedan dar lugar a un comportamiento ilegal, un incumplimiento del deber de cuidado no legislativo a terceros. Esto podría incluir una organización que infringe los derechos de propiedad intelectual de terceros, el incumplimiento de las normas de atención requeridas debido a los clientes (como la venta incorrecta) o el uso o la administración inapropiados de las redes sociales que resulten en un reclamo de difamación o difamación de terceros.

3.2. Los riesgos sobre los derechos y libertades de los interesados en la legislación de datos personales

La gestión del cumplimiento de la legislación de protección de datos está basada en el riesgo existente sobre los derechos y libertades de los interesados. Este concepto deriva

[2] En este sentido, el concepto de riesgo legal es asimilable al concepto de riesgo de cumplimiento de la ISO 37301:2020.

del principio de responsabilidad proactiva, que otorga libertad al responsable para evidenciar el cumplimiento de las disposiciones (Martínez Martínez, 2018, p. 268).

Para obtener el riesgo, la Asociación Española de Protección de Datos (AEPD) propone los siguientes criterios para su identificación (2020, p. 32):

- Los riesgos que se derivan del tratamiento en sí mismo, siendo el más característico el que se deriva del sesgo en los sistemas de toma de decisiones sobre las personas o su discriminación.
- Los riesgos que se derivan del tratamiento con relación al contexto social y los efectos colaterales que se puedan derivar de él, indirectamente relacionados con el objeto de tratamiento.

Como cualquier tecnología que se base en el tratamiento de datos personales, no deja de tener una afección en los principios rectores de la legislación de protección de datos consagrados en el artículo 5 del Reglamento general de protección de datos (RGPD). Es, sobre la base de estos principios, donde surgen los principales riesgos (Leenes y De Conca, 2018, p. 299).

Si bien es reiterado varias a lo largo del RGPD, que, debido al modelo de responsabilidad objetiva, el cual rige el sistema de responsabilidad civil, impide limitar la responsabilidad del responsable en los supuestos de reclamación civil (Rubí Puig, 2018, p. 83)[3], no significa que se aplique análogamente a los supuestos de responsabilidad administrativa.

El principio de licitud y limitación de la finalidad es el primer principio al que un implementador se debe enfrentar. Tras exponer las distintas fases del ciclo de vida, cada una de ellas consiste en un proceso ejecutado en un macroproceso que los engloba, siendo el macroproceso el servicio prestado por el sistema de IA. En el caso de que, durante la ejecución del proceso, se tratasen datos personales, en cualquiera de sus formas, estaríamos ante una actividad de tratamiento de datos personales.

Las actividades de tratamiento son atribuidas siempre al responsable del tratamiento, que será quien determine la finalidad y los medios con los cuales se efectúa el tratamiento; sin embargo, si el responsable decide contratar a terceras partes para el desarrollo del sistema, estos pueden convertirse en encargados del tratamiento, cuyo rol se adquiere cuando el responsable subcontrata parte del proceso de tratamiento a un tercero. Es decir,

[3] No sería suficiente acreditar una debida diligencia respecto a la comisión de un hecho dañoso, ni utilizar un mecanismo de certificación o códigos de conducta. En concreto, el artículo 42.4 del RGPD estipula que la certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente reglamento.

si un responsable encarga a un tercero la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[4], este se convertirá en encargado del tratamiento.

Podemos destacar la existencia de las siguientes actividades de tratamiento que suceden en el desarrollo de un sistema de IA, para las cuales se necesita una base jurídica individual:

- El entrenamiento o validación del modelo.
- El uso de datos de terceros en la inferencia.
- La comunicación de datos implícitos en el modelo.
- El tratamiento de los datos del interesado en el marco del servicio prestado por la IA.
- El tratamiento de datos del interesado para la evolución del modelo.

Y por encima de estas actividades, reside la principal finalidad para la cual el sistema de IA ha sido desarrollado: la finalidad operacional establecida. Esta última finalidad, y las anteriores, deben basarse en una base de legitimación del artículo 6 del RGPD y, a su vez, informar al usuario de todas las finalidades existentes.

El principio de **transparencia** resulta ser crítico en los tratamientos basados en sistemas de IA, puesto que el interesado tiene el derecho de conocer las condiciones en las que se realiza el tratamiento. Pero la transparencia se concreta también en obligaciones a los operadores para prestar de una manera adecuada la información en un formato que permita ser entendible al interesado. El RGPD contiene en su articulado medidas concretas respecto a la obligatoriedad del deber de transparencia a los responsables, y de forma adecuada para cubrir los conflictos legales existentes. En concreto, el artículo 13.2 f) del RGPD obliga a ofrecer al interesado una información significativa sobre la lógica aplicada, así como respecto a la importancia y las consecuencias previstas de un tratamiento cuando implica la adopción de decisiones automatizadas de las que deriven efectos jurídicos o le afecten significativamente de modo similar, obligación que va dirigida a tratar los problemas de explicabilidad del algoritmo (Martínez Martínez, 2018, p. 275).

La transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución (AEPD, 2020, p. 36).

[4] *Vid*. artículo 4.2 del RGPD.

Íntimamente ligado con la transparencia, el responsable deberá informar sobre la finalidad para la cual el sistema de IA trata los datos personales, cuestión que se torna difícil debido a la gran multitud de tratamientos que intervienen.

En segundo lugar, el principio de **exactitud** incide principalmente sobre la existencia de sesgos en los modelos de inferencia. En concreto, según el considerando 71 del RGPD, los datos asociados a los interesados, ya sean los datos directamente recogidos o los inferidos, han de ser exactos. En particular, se hace explícito que el responsable del tratamiento ha de utilizar «procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles» que garanticen que los datos vinculados con el interesado son exactos. Es obligatorio demostrar y documentar que los procedimientos empleados para la inferencia de información sobre un interesado son precisos y, por tanto, estables y predecibles de acuerdo con el artículo 24 del RGPD.

Respecto a los datos inferidos, datos derivados de la interpretación realizada por el sistema de IA, y su exactitud, se destacan tres factores influyentes (AEPD, 2020, p. 56):

- La propia implementación del sistema IA. Las reglas implementadas que permiten a los sistemas de IA introducir inferencias erróneas, o los errores de programación que afectan a la implementación práctica, creando un sesgo que no puede ser alterado por un cambio de código (*hardwired*).
- El conjunto de datos utilizado para a validación y entrenamiento está viciado de manera intencionada, lo que se conoce como inyección de *bad data*.
- La evolución sesgada del modelo de IA.

Por último, el principio de **minimización** choca directamente con el principio rector del *big data*, tecnología que alimenta al sistema de IA, el cual es la maximización de tratamiento de los datos personales (Gil González, 2015, p. 52). Esa limitación se puede conseguir mediante:

- Limitar la extensión de las categorías de datos que se utilizan en cada fase del tratamiento a aquellas que son estrictamente necesarias y relevantes.
- Limitar el grado de detalle o precisión de la información, la granularidad de la recogida en tiempo y frecuencia y la antigüedad de la información utilizada.
- Limitar la extensión en el número de interesados de los que se tratan los datos.
- Limitar la accesibilidad de las distintas categorías de datos al personal del responsable/encargado o incluso al usuario final (si hay datos de terceros en los modelos de IA) en todas las fases del tratamiento.

En este ámbito, es relevante la influencia de la **seguridad de la información**. Podemos entenderla como una dimensión relacionada con la protección de datos. No en

vano, el artículo 32 del RGPD contempla la obligación de implementar las medidas de seguridad adecuadas para asegurar la integridad, disponibilidad, confidencialidad y resiliencia de la información sobre la base del artículo 5 del mismo respecto al principio de confidencialidad.

Pero no todo el marco de la seguridad de la información se limita únicamente a la legislación de protección de datos personales. El Real Decreto-Ley 12/2018, de seguridad de las redes y sistemas de información regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establece un sistema de notificación de incidentes.

La seguridad de la información puede definirse como el proceso tendente a prevenir, responder y corregir los incidentes de seguridad, protegiendo así la confidencialidad, integridad y disponibilidad de la información. Dentro de este concepto, se encuentra la ciberseguridad, una dimensión incluida en la seguridad de la información que persigue los anteriores objetivos en los ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas y comunicación por cable (NIST, 2018, p. 96).

La existencia de riesgos de seguridad de la información está asociada a la pérdida de dichas cualidades, por ejemplo;

- Los ciberatacantes podrían hacer mal uso de los datos recabados o generados por los dispositivos al comprometer la **disponibilidad** de los datos. Cuando no hay datos disponibles, puede provocar un fallo en el sistema; podrían producirse daños.
- Cambiar los datos, causando problemas de **integridad** de datos; y el uso de conocimientos de *big data* para reforzar o crear resultados discriminatorios. La integridad de los datos puede causar problemas más sustanciales. Cuando los atacantes cambian datos, como la codificación, el cambio de valores o el reemplazo de datos con los suyos, la información proporcionada a los usuarios puede ser engañosa, o los límites establecidos previamente o los algoritmos que dirigen la funcionalidad del dispositivo pueden cambiar (Tschider, 2018, p. 97).
- Comprometer la **confidencialidad** de la información mediante una intrusión indebida en los sistemas o una difusión a terceros no autorizados para su recepción.
- La imposibilidad de recuperar los datos tras un incidente que ha conllevado a eliminación de estos, comprometiendo la **resiliencia** de la organización.

La existencia de una autoridad administrativa que controle el cumplimiento de la legislación sobre protección de datos mediante la aplicación de un régimen administrativo de responsabilidad, y la convivencia con un régimen de responsabilidad civil, nos lleva a plantearnos la aplicación privada del derecho de la protección de datos de manera aná-

loga al régimen de competencia (Díez Estella, 2019) mediante la existencia de acciones *follow-on* y *stand alone*.

El deber de responsabilidad proactiva debe demostrarse también respecto de los riesgos en materia de seguridad de la información, y esto se consigue mediante una adecuada gestión del riesgo, tal y como recoge el artículo 32.1[5] del RGPD. Como veremos más adelante[6], la gestión de riesgos supone un proceso que abarca la identificación, análisis, evaluación y tratamiento de los riesgos, con el fin de adoptar una decisión estratégica respecto a estos.

3.3. Los riesgos directos sobre la responsabilidad civil del prestador de servicios de la sociedad de la información

Por último, debido al fin del sistema de IA, la LSSI juega un papel crucial respecto al conjunto de obligaciones que incorpora. Esta norma contiene no solo un conjunto de obligaciones, sino también un régimen de responsabilidad civil en los artículos 13 y siguientes. En concreto, los artículos 16 y 17 dibujan escenarios de riesgos legales muy concretos que pueden generar responsabilidad civil respecto al almacenamiento de datos que vulnerasen derechos de terceros, o la facilitación de contenidos.

En ambos supuestos, la LSSI basa la responsabilidad en los siguientes elementos:

- La inexistencia de un conocimiento efectivo del contenido ilícito o indexado, y
- Que una vez verificado el contenido ilícito, el prestador sea diligente en el momento de la retirada.

Es decir, el implementador del sistema de IA debe intervenir sobre los actos ejecutados por el sistema de IA; una mala configuración del sistema derivada de la programación del algoritmo, o la alimentación del sistema mediante *bad data*. Sobre la base de estas situaciones, es posible que contenidos de terceros que vulneren sus derechos se embeban en la página de comercio electrónico del prestador de manera automática, generando un daño al sujeto. En cualquier caso, la LSSI establece un control *a posteriori*; el prestador no está obligado a supervisar *ex ante* el contenido (Carnero Sobrado, 2012, p. 4). La debida diligencia se limita, en este caso, a una actuación *a posteriori*, siendo el concepto de diligencia debida diferente al de responsabilidad proactiva del RGPD.

---

5 «Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo».

6 Véase apartado 4 del presente trabajo.

3.4. El futuro sistema de responsabilidad en la Directiva de productos defectuosos a raíz de la estrategia europea: el cambio de paradigma

La IA tiene multitud de manifestaciones, ya sea mediante la inclusión de bienes muebles, o mediante la ejecución de un *software* en sistemas informáticos, pudiendo en ambas situaciones ser explotados por los consumidores o por personas jurídicas para la prestación de sus servicios finales. Estas posibilidades modifican profundamente las normas de responsabilidad aplicables en cada caso.

En el caso de que tratemos a los sistemas de IA incorporados en bienes muebles[7], los postulados doctrinales (Navas Navarro, 2019, p. 3), y también derivados de la Unión Europea (Comisión Europea, 2019a, 2019b), actuales abogan por que se encuentren sujetos a la Directiva (UE) 85/374/CEE, de 25 de julio de 1985, sobre responsabilidad por productos defectuosos. 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, y el nexo causal entre el producto defectuoso y el daño. Este es el principal marco regulatorio que la Unión Europea plantea para hacer frente a los retos regulatorios, pero, aunque contemos con él, no afronta totalmente todos retos que la IA presenta:

- **Debido a la complejidad de los productos y los sistemas**, la Directiva sobre responsabilidad por daños de producto no proporciona una definición de «producto» y «productor» que cubra de manera conceptual los productos o servicios derivados de la IA; puesto que resulta difícil encasillarlos debido a la fina línea de separación entre ellos.
- **La compleja cadena de valor** soportada por los sistemas de IA hace que participen numerosos actores en su diseño, creando una compleja cadena de valor de responsabilidad difusa.
- **Las aplicaciones de IA se encuentran en entornos multiconectados** entre varios dispositivos, lo que provoca un ecosistema complejo y la existencia de una pluralidad de agentes, generando problemas en la determinación del hecho que ha causado el perjuicio, soportando las víctimas un gran coste para demostrar el perjuicio.

[7] Puede resultar aplicable el nuevo régimen estipulado en la nueva regulación digital de la Unión Europea mediante la aprobación de la Directiva (UE) 2019/771, del Parlamento europeo y del Consejo de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes, donde en su artículo 3.e incluye en su ámbito de aplicación aquellos servicios digitales que son incorporados en bienes muebles suministrados por un tercero, en los contratos de compraventa de bienes.

- **La conectividad y apertura de código.** La existencia de vulnerabilidades en los sistemas compromete la seguridad, pudiendo ser fuente de riesgos que generen daños a los usuarios, habiendo dudas en la aplicación del concepto de seguridad, centrado en un ámbito industrial. Por otro lado, es aplicable 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, haciendo que la indemnización civil que pueda recibir un usuario se reduzca, por no haber instalado las actualizaciones que eliminan dichos defectos, pudiendo considerarse como una actitud negligente del usuario.
- **La autonomía y opacidad** de la IA es una fuente de riesgos en el sentido de que esta puede ejecutar una tarea no predefinida, sin que exista supervisión humana inmediata. Esta característica hace que sea difícil reclamar una indemnización por la falta de conocimientos técnicos para la compresión de la decisión, e imposibilitando a las víctimas la interposición de una reclamación.

Debido a los retos presentados, la Unión Europea propone los siguientes cambios en la directiva:

- Modificar las definiciones de «productor» y «seguridad» para precisar su ámbito de aplicación con el fin de 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.
- Plantear un enfoque de «responsabilidad compartida», en el cual cada agente de la cadena de valor y los usuarios asumirá su responsabilidad y proporcionará al agente siguiente la información necesaria.
- Invertir la carga de la prueba en las situaciones en las que los agentes han vulnerado las obligaciones mínimas de seguridad impuestas por la directiva.
- Un modelo de responsabilidad objetiva basada en el riesgo aplicable a aquellos sistemas que operen en espacios públicos, que 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.

En resumen, la Unión Europea ha propuesto un sistema de responsabilidad subjetiva basado en la diligencia debida de los intervinientes en la cadena de valor del sistema de IA, basado en el riesgo como método de imputación objetiva (Navas Navarro, 2019, p. 5) a lo largo de la cadena de valor, y estas operaciones de debida diligencia deben alcanzar los riesgos propios de los diferentes productores intervinientes. Sin embargo, se contem-

pla una regla especial en los casos en los que se adoptara un sistema de responsabilidad objetiva en las situaciones de alto riesgo.

3.5. La propuesta de Reglamento de responsabilidad civil para los daños contra la vida, la integridad física y los bienes derivados del uso de la IA

La aprobación, por parte de la Comisión Europea, tanto del Libro Blanco como del Informe sobre Responsabilidad Civil, el Proyecto de Informe con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial[8], el cual propone un reglamento para abordar el sistema de responsabilidad civil en los supuestos de daños contra la vida, la integridad física o los bienes de una persona física o jurídica, junto con la Directiva (UE) 85/374/CEE, pretenden ser un marco de responsabilidad civil coherente para los sistemas de IA[9]. El articulado del proyecto distingue aquí la intervención de dos sujetos[10]:

- El implementador. La persona que decide sobre el uso del sistema de IA, ejerce control sobre el riesgo asociado y se beneficia de su utilización, y
- El productor. El desarrollador o el operador final de un sistema de IA o el productor tal como se define en el artículo 3 de la Directiva 85/374/CEE.

Por lo tanto, será sobre la figura del implementador sobre la que recaerá la aplicación del futuro reglamento, y será propietario de los riesgos sujetos a este[11].

Sobre la base del objeto de la norma, prevé dos situaciones derivadas del uso de un sistema de IA, que determina la aplicación de un régimen de responsabilidad civil diferente:

- Un sistema basado en la responsabilidad objetiva del implementador respecto de cualquier daño o perjuicio causado por una actividad física o virtual cuando este opere un sistema de IA de alto riesgo[12], con la consecuencia de no poder alegar la aplicación de medidas de diligencia debida para la exclusión de la responsable.

8 2020/2014(INL).

9 Considerando 21 del Proyecto de Informe.

10 Artículo 3 del Proyecto de Informe.

11 Artículo 2 del Proyecto de Informe.

12 Los sistemas de alto riesgo considerados son, hasta que las instituciones de la Unión Europea los hayan ampliado y desarrollado, los relativos al transporte, sanidad y energía.

- Un sistema basado de responsabilidad subjetiva, donde el implementador no será responsable si, entre otras posibilidades, demuestra una debida diligencia a través de la selección de un sistema de IA apropiado para las tareas y con las capacidades adecuadas, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles.

Atendiendo al considerando 16 de la propuesta, el programa de diligencia debida debe efectuarla el implementador de la solución de IA sobre la base de los siguientes elementos:

- La naturaleza del sistema de IA. Las finalidades, la infraestructura informática utilizadas y los procesos existentes que lo operan.
- El derecho protegido jurídicamente potencialmente afectado. La identificación de los derechos fundamentales en los que el sistema de IA pueda incidir.
- El daño o perjuicio potencial que podría causar el sistema de IA, y
- La probabilidad de dicho perjuicio.

4. La debida diligencia mediante la gestión de los riesgos en el ciclo de vida de la inteligencia artificial

Las operaciones de debida diligencia están orientadas fundamentalmente a obtener información de una parte interesada, evaluarla, y tomar una decisión al respecto. Este proceso deberá regirse mediante un principio de proporcionalidad y adecuación (Spedding, 2008, p. 18) respecto a la materia a auditar, tamaño de las organizaciones, recursos y prioridades establecidos, por lo que su contenido puede variar respecto al objetivo que se persigue. Pero podemos establecer como un elemento básico de un programa de debida diligencia la existencia de un proceso de gestión de riesgos.

En cualquier caso, el proceso de diligencia debida se presenta como un objetivo más que como una serie de elementos a cumplir. Consiste en que el propietario de los riesgos consiga mediante sus medidas tener un control sobre los procesos operacionales, y con ello evaluar y efectuar las decisiones adecuadas para gobernar los riesgos del sistema de IA, siendo los conceptos de «gobernanza» y «gestión de riesgos» un binomio inherente al proceso de debida diligencia (Spedding, 2008, p. 45).

A falta de un modelo, o estándares para entender los requisitos de un programa de diligencia debida, podemos presentar, como ejemplo, las obligaciones en materia de diligencia debida en la cadena de suministro del Reglamento (UE) 2017/821, por el que se establecen obligaciones en materia de diligencia debida en la cadena de suministro por lo que respec-

ta a los importadores de la Unión de estaño, tantalio y wolframio, sus minerales y oro originarios de zonas de conflicto o de alto riesgo[13]. Según este reglamento, la debida diligencia en la cadena de suministro está formada por:

- Las medidas en materia de gestión de riesgos.
- Las auditorías externas, siendo estas tanto de segunda parte como de tercera parte, y
- La comunicación de información con el fin de identificar y abordar los riesgos reales y potenciales para impedir o reducir los efectos negativos asociados.

Debemos entender la mención a este reglamento como ejemplo ilustrativo de las exigencias en materia de gestión de riesgos en la cadena de suministros, como es recogido en el artículo 5, pero que, análogamente, la presentación de un programa siguiendo estas directrices puede poner al implementador en una posición ventajosa a la hora de demostrar su debida diligencia.

No solo durante el articulado de la propuesta se hace una mención continua al concepto de riesgo en el sistema de IA. Podemos encontrar en diferente legislación aplicable la obligación de efectuar un proceso de gestión de riesgos. La legislación en materia de protección de datos, como hemos explicado anteriormente, el cumplimiento con el RGPD, tiene su base en la gestión del riesgo (considerando 74 del RGPD).

Si bien el término de gestión de riesgos no nos es desconocido a los juristas por su inclusión en diferentes normas, su construcción va más allá de la obligación recogida en la norma, debiéndonos atener a metodologías y estándares internacionalmente reconocidos para definirlo. Para ello, utilizaremos la definición del estándar ISO 31000:2018 sobre gestión de riesgos, emitida por la International Standard Organization, organización internacional reconocida por sus estándares mundialmente reconocidos, puesto que, para su elaboración, intervienen los organismos nacionales de estandarización de todo el mundo. Este estándar define la gestión de riesgos como «actividades coordinadas para controlar la organización en relación con el riesgo». A pesar de la definición corporativa recogida en su cláusula 3, la gestión es entendida como un proceso que se encuentra embebido en el sistema de gobernanza y, siguiendo el presente estándar, para la correcta adopción del proceso de gestión de riesgos, la organización que posea un sistema de IA debe identificar, analizar, evaluar, comunicar y tratar los riesgos relacionados con los sistemas de IA.

El concepto de riesgo que la propuesta contempla se refiere a una concepción basada en la combinación de las consecuencias sobre los derechos protegidos y la probabilidad de ocurrencia de estos. Esta formulación del concepto de riesgo, derivada del considerando 16,

[13] DOUE L 130/1 de 19 de mayo de 2017.

promueve una concepción negativa del riesgo, que si bien es fruto de una concepción tradicional de riesgo respecto a modelos más antiguos (Kaplan y Garrick, 1975), difiere de la concepción ambivalente presentada por la norma ISO 31000:2018, donde lo define como «el efecto de la incertidumbre sobre los objetivos», concretando que la incertidumbre es «cualquier variación, positiva o negativa, que afecta al cumplimiento de los objetivos». Por lo que el implementador deberá identificar, analizar, evaluar y tratar los riesgos que puedan generar un daño indemnizable sobre la base de la vulneración de un derecho. Estos derechos, como se ha mencionado, pueden ser los relacionados con la seguridad de la información o protección de datos personales que, en caso de un incumplimiento que genere un daño, puede generar un derecho a indemnizar al sujeto.

El Reglamento (UE) 2017/821 coincide con la norma ISO 31000:2018 respecto a los elementos que un programa de debida diligencia debe tener, y las actividades del proceso de gestión de riesgos que recomienda aplicar:

- Una política de cadena de suministro con el compromiso de adoptar un sistema de gestión de riesgos.
- Adoptar las estrategias para la gestión de los riesgos, y comunicando el resultado de la evaluación de los riesgos a la alta dirección y a las partes interesadas.
- Adoptando las medidas de gestión de riesgos.
- Aplicando el plan de tratamiento del riesgo, supervisando y registrando la eficacia de los esfuerzos de reducción de riesgos; informando a los altos directivos designados a ese fin.
- Llevando a cabo nuevas evaluaciones de los hechos y riesgos en relación con los riesgos que deban reducirse, o a raíz de un cambio de circunstancias.

La intervención de numerosos actores en la cadena de suministro conlleva la existencia de dificultades en la atribución de responsabilidad ante la existencia de un daño cuya atribución es difusa; sin embargo, no todos los intervinientes en la cadena de suministro poseen el mismo grado de «importancia» en el desarrollo del producto, ni mucho menos independencia entre las partes, pudiendo influir en los procesos de una parte a otra de la misma cadena de suministro, por diferentes motivos, ya sean económicos, laborales o estratégicos. Bajo este axioma, se ha desarrollado el concepto de «esfera de influencia» para atribuir dicha intervención en los procesos de una parte sobre la otra. Este concepto fue introducido, dentro del mundo corporativo, por la United Nations Global Compact. Esta teoría permite entender que la parte que ejerce la influencia sobre la otra puede llegar a ser responsable por los daños atribuidos a esta última (Chen, 2013, p. 369). Sin embargo, este concepto ha sido aclarado posteriormente por el Consejo de Derechos Humanos en el Informe del Representante Especial del Secretario General: *Aclaración de los conceptos de «esfera de influencia» y «complicidad»*. En este informe, diferencia el concepto de influencia (*leverage*) en dos significados diferentes:

- El «impacto», es decir, el perjuicio que las actividades o las relaciones de las empresas causan en la materia concreta, y
- La «autoridad» que una empresa puede ejercer sobre otros agentes que causan un perjuicio.

El impacto siempre entra en el ámbito de la responsabilidad de respetar la ley, mientras que la autoridad solo en circunstancias determinadas. No se puede responsabilizar a las empresas del impacto derivado del incumplimiento ejercido por cada entidad sobre la que tengan alguna autoridad, pues comprendería también los casos en que no están contribuyendo al daño ni son causa de él. Tampoco es conveniente exigir a las empresas que actúen siempre que tengan influencia. La esfera de influencia debe entenderse como la relación causal sobre la materialización de un impacto. Sin embargo, el propio informe especifica que, si no existe una situación legal de control a un proveedor, no tendría sentido incluirlo dentro del alcance del programa de debida diligencia.

Sin embargo, el modelo de la propuesta de Reglamento relativo a la responsabilidad civil por el funcionamiento de los sistemas de inteligencia artificial, ha establecido diversas habilitaciones legales para que el implementador realice programas de debida diligencia respecto al productor del sistema, tal y como se establece en el considerando 17 sobre el deber del productor de cooperar.

Una vez determinada la relación de la gestión de riesgos dentro del deber de diligencia que debe existir en la cadena de suministro, se plantean por parte de las organizaciones herramientas concretas que permitan una adecuada apreciación del riesgo y fácilmente integradas en los sistemas de gobernanza, de manera que esta herramienta no se convierta en un requerimiento burocrático que obstaculice la consecución de los objetivos operativos de la organización, y sea fácilmente demostrable ante terceros la debida diligencia que una entidad aseguradora soporta. En este contexto, el concepto de «debida diligencia» se torna en un concepto jurídico indeterminado, que podemos entender como la intención deliberada del legislador de no cerrar las opciones que un implementador posee a la hora de poder demostrar la debida diligencia (Martínez Estay, 2019, p. 164) ante esos terceros, ya sean clientes, órganos jurisdiccionales o Administraciones públicas.

El Proyecto de Informe contempla unas presunciones *iuris tantum* que los implementadores pueden utilizar, según el considerando 16, como (a) el futuro sistema voluntario de certificación del Libro Blanco, sobre la adecuada diligencia debida[14]; (b) la demostración por parte del implementador de que ha supervisado real y periódicamente el sistema de IA durante su funcionamiento y se ha informado al fabricante sobre posibles irregularidades durante el mismo, o (c) como que el implementador ha prestado la debida atención en lo

[14] Actualmente, se ha propuesto un modelo propuesto para ser candidato a mecanismo de sistema voluntario de certificación, propuesto por Carlos Galán (2019, p. 7).

que se refiere al mantenimiento de la fiabilidad operativa, si ha instalado todas las actualizaciones disponibles proporcionadas por el productor del sistema de IA. La demostración de estos elementos se antoja difícil por parte del implementador, puesto que estas posibilidades se encuentran bajo la valoración de la sana crítica, de acuerdo con la legislación procesal.

A todo esto, surgen soluciones como las evaluaciones de la conformidad realizadas por entidades de certificación acreditadas por un organismo nacional de acreditación como mecanismo de control respecto al cumplimiento y los riesgos (Galán, 2019, p. 10). Existen estándares certificables que pueden cubrir adecuadamente los riesgos identificados que afectan al sistema de IA, como son:

- ISO/IEC 27001:2013 - Sistemas de Gestión de Seguridad de la Información (SGSI). El objetivo de la norma es prestar guías y directrices a una organización para que adopte un SGSI basado en la mejora continua, que proteja la confidencialidad, integridad y disponibilidad de la información.
- ISO 22301:2019 - Sistemas de Gestión de Continuidad de Negocio (SGCN). La norma aporta guías y directrices para la adopción de un SGCN con el fin de asegurar la continuidad de los servicios tras la existencia de un incidente.
- ISO/IEC 20000-1:2018 - Sistemas de Gestión de Servicios de TI (SGSTI). La norma presenta guías y directrices para la implementación de un SGSTI con el fin de gestionar un servicio de TI sobre la base de diferentes prácticas que sostienen un servicio de TI con el fin de generar valor.

Estos estándares, creados por la International Standard Organization, están dirigidos a aquellas organizaciones que pretendan adoptar un sistema de gestión basado en la mejora continua sobre la base del objeto concreto que pretendan gestionar, como puede ser la calidad, la seguridad de la información o la continuidad de las operaciones. Estos estándares imponen los siguientes requisitos para su implementación de manera adecuada en una organización:

- La implicación de la alta dirección mediante la asignación de recursos, establecimiento de políticas y supervisión del desempeño del sistema.
- La gestión de los riesgos que afectan a los objetivos de la organización relacionados con la seguridad de la información, la continuidad de negocio, etc.
- Aseguramiento de la condición de los proveedores de acuerdo con los requisitos de seguridad de la información o continuidad de negocio establecidos por el implementador.
- La exigencia de auditar la eficacia del sistema anualmente.
- La necesidad de establecer indicadores de eficacia y desempeño para determinar el cumplimiento de los objetivos.

Se puede demostrar la conformidad con el estándar mediante una auditoría externa de una entidad de certificación acreditada por un organismo nacional de acreditación, como puede ser la Entidad Nacional de Acreditación (ENAC) según el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y el 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. La certificación acreditada por ENAC, o entidad similar, si bien tiene el valor probatorio de un documento privado, el Tribunal Supremo, en la STS 1623/2016, de 4 julio, de la Sala Tercera, establece que merece de un valor añadido por la intervención de un organismo nacional de acreditación[15].

5. Conclusiones

La cuarta revolución industrial ha brindado al mercado y a los usuarios la posibilidad de aprovechar todo el potencial de las nuevas tecnologías para el desarrollo y uso de nuevas herramientas, cuyas funcionalidades y aplicaciones mejoran la experiencia de los intervinientes en el mercado, a través de un trato más personalizado y la mejora en los procesos internos y externos.

Entre las tecnologías más disruptivas sobresale la IA, cuyas ventajas y beneficios han suscitado un incremento significativo durante los últimos años respecto de su desarrollo y despliegue. Sin embargo, los retos y riesgos derivados de la aplicación de la misma están ocasionando más de un quebradero de cabeza, fundamentalmente en lo que respecta a los riesgos y la responsabilidad de los sujetos intervinientes.

La urgencia de abordar los riesgos que implica el uso de la IA es cada vez más evidente, consecuencia, sin duda, del imparable avance de la IA y la falta de agilidad de los sistemas normativos para adaptar el ordenamiento jurídico a los nuevos retos que van surgiendo.

Por ello, nos aproximamos cada vez más a regímenes jurídicos donde el tradicional modelo regulatorio basado en el cumplimiento de requisitos legales para poner en circulación un servicio o producto en el mercado está evolucionando a otro basado en la conducta responsable de los operadores del mercado, con el fin de proporcionar un marco jurídico flexible y dinámico que no limite la evolución de las tecnologías disruptivas.

La IA no se queda atrás, y tras observar la estrategia elaborada por la Unión Europea, se apuesta por criterios de gestión de riesgos y debida diligencia en las operaciones y de-

[15] FJ 14.º: «La consecuencia de lo expuesto es que los trabajos - documentos de inspección y certificaciones - de las entidades de inspección y certificación acreditadas no tienen el valor de documento público, sino privado, pero con el valor de que en ellos se hacen constar datos por unas entidades que si han sido acreditadas para tal fin es porque la ENAC como acreditadora entiende que reúnen las condiciones de imparcialidad y suficiencia técnica para asumir tal cometido».

sarrollos de sistemas de IA. En caso de que los sujetos intervinientes en el ciclo de vida de la IA no adopten estos modelos de diligencia debida, pueden enfrentarse a la totalidad de la responsabilidad, ya sea civil o administrativa.

Actualmente, estos sujetos se enfrentan a la indeterminación del concepto de «debida diligencia» , y hasta que no se estandaricen modelos o procedimientos, se propone la adopción de mecanismos de certificación de renombre y acreditados por organismos nacionales de acreditación, con el fin de gestionar los riesgos propios del uso de sistemas IA, como pueden ser riesgos sobre la seguridad o la calidad del proceso, que si bien no tienen el valor de documentos públicos, no puede obviarse el valor añadido que la acreditación por los organismos nacionales de acreditación suponen para acreditar la adopción de una conducta proactiva.

Referencias bibliográficas

AEPD. (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. AEPD.

Carnero Sobrado, J. I. (2012). Consideraciones en torno a la responsabilidad civil de los prestadores de servicios por comentarios alojados en sus páginas web. *Diario La Ley*, *7782*, 1-7.

Ceballos, D. (2007). Una propuesta de indicador de riesgo legal. *2.ª Reunión de Investigación en Seguros y Gestión de Riesgos*, Cantabria.

Chen, S. (2018). Multinational Corporate Power, Influence and Responsability in Global Supply Chains. *Journal of Business Ethics*, *148*, 365-374.

Comisión Europea. (2019). *A definition of AI: Main Capabilities and Disciplines*: Comisión Europea.

Comisión Europea. (2020a). *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza*. Comisión Europea.

Comisión Europea. (2020b). *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*. Comisión Europea.

Comité de Basilea de Supervisión Bancaria. (2005). *El cumplimiento y la función de cumplimiento en los bancos*. Comité de Basilea.

Díez Estella, F. (2019). La aplicación privada del derecho de la competencia: acciones de daños y pronunciamientos judiciales. *Cuadernos de Derecho Transnacionales*, *11*(1), 267-305.

Domo. (2019). Data never sleeps 7.0. Domo web.

Galán, C. (2019). La certificación como mecanismo de control de la inteligencia artificial en Europa. *IEEE*, *46*, 1-19.

Gil González, E. (2015). *Big data, privacidad y protección de datos*. AEPD.

Kaplan, S. y Garrick, B. J. (1981). *On the Quantitative Definition of Risk. Risk Analy-*

sis. Rasmussen (1975). An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. US Nuclear Regulatory Commission.

Kishnani, P., Turley, M. y Eggers, M. (2018). *El futuro de la regulación. Principios para regular tecnologías emergentes*. Deloitte Insights.

Leenes, R. y De Conca, S. (2018). Artificial Intelligence and Privacy. En W. Barfield y U. Pagallo (Eds.), *Research Handbook on the Law of Artificial Intelligence* (pp. 279-307). Edward Elgar Publishing.

Martínez Estay, J. I. (2019). Los conceptos jurídicos indeterminados en el lenguaje constitucional. *Revista de Derecho Político*, *105*. 162-194.

Martínez Martínez, R. (2018). Inteligencia artificial, derecho y derechos fundamentales. En T. de la Quadra Salcedo, y J. L. Piñar Mañas (Dirs.), *Sociedad digital y Derecho* (pp. 259-279). Boletín Oficial del Estado.

Merino, M. (2019). Ha comenzado la carrera para crear la tecnología capaz de detectar los *deepfakes*, pero los falsificadores llevan ventaja. *Xataka*.

Navas Navarro, S. (2019). Responsabilidad civil del fabricante y tecnología inteligente. *Diario La Ley*, *35*, 1-11.

Navas Navarro, S. (2019). Sistemas expertos basados en Inteligencia Artificial y Responsabilidad civil: Algunas cuestiones controvertidas. *Diario La Ley*, 1-15.

NIST (National Institute of Standards and Technology). (2018). *Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy*. NIST.

Parlamento Europeo. (2017). *Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*. Parlamento Europeo.

Puyol, J. (2018). *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*. Tirant lo Blanch.

Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil, 5*(4), 53-87.

Spedding, L. (2008). Introduction and traditional due diligence. En L. Spedding (Ed.), *The Due Diligence Handbook: Corporate Governance, Risk Management and Business Planning* (pp. 1-49). Elsevier.

Terwindt, C., Vastardis, A. y Wright, J. (2018). Supply chain liability: pushing the boundaries of the common law?», *Journal of European Tort Law*, *8*(3), pp. 261-296.

Tschider, C. (2018). Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age. *Denver Law Review*, *96*(1), 87-143.

Turner, J. (2019). *Robot Rules: Regulating Artificial Intelligence*. Palgrave Macmillan.