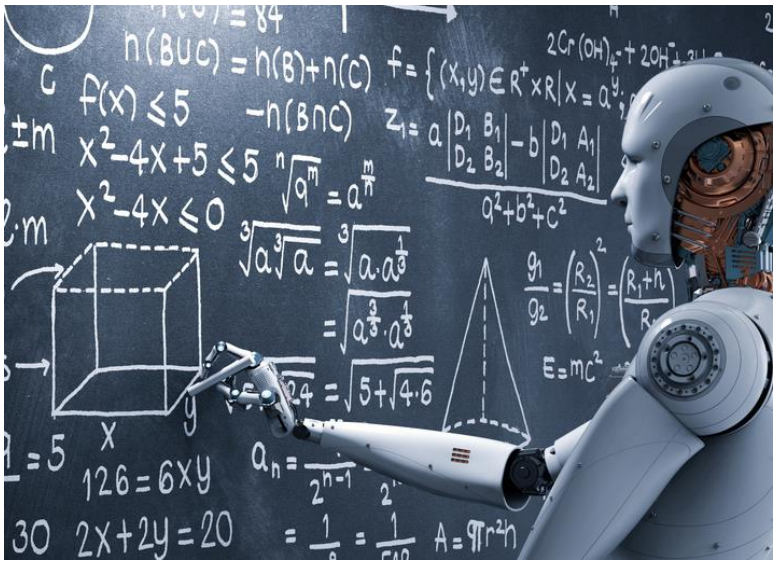


A VUELTAS CON LA IA Y LA RC: ¿DÓNDE CONVERGEN Y QUÉ PROBLEMÁTICA CONLLEVAN?

DESCRIPCIÓN BREVE

El presente ejercicio consta de dos partes. La primera resume el Libro Blanco sobre la Inteligencia Artificial en las cuestiones relativas a Responsabilidad Civil. En la segunda se plantean los problemas que arroja la aplicación de la legislación actual en materia de Inteligencia Artificial, concretamente en relación con la Responsabilidad Civil.

Macarena Azcárate, Leticia Amorós y David Ruiz

Índice:

---

1. Introducción

2. Resumen/análisis del Libro Blanco sobre la Inteligencia Artificial desde el punto de vista de la Responsabilidad Civil

a. ¿Qué es la IA?

b. ¿Qué es la Responsabilidad Civil?

c. Definición de los problemas

d. Riesgos para la seguridad jurídica y el funcionamiento eficaz del régimen de Responsabilidad Civil

e. Destinatarios

f. Cumplimiento y ejecución

g. Conclusión

3. Comentarios y propuestas sobre IA y RC

a. Introducción al problema

b. Fragmentación del mercado único y consecuencias sobre la RC

c. Problemas RC

d. Riesgos para la seguridad jurídica y el funcionamiento eficaz del régimen de Responsabilidad Civil

e. ¿Sobre quién recaería la RC? ¿Cobra sentido una Personalidad Jurídica para la IA?

f. Alcance temporal de la responsabilidad

g. Seguro de RC obligatorio

h. Conclusión

A vueltas con la IA y la RC: ¿Dónde convergen y qué problemática conllevan?

---

1. *Introducción*

Es indudable el rápido e imparable desarrollo que está teniendo la IA, pero esta transformación digital en la que estamos inmersos ofrece tantas ventajas como riesgos. El objetivo de la Comisión con este libro blanco es **movilizar recursos y crear los incentivos apropiados que aceleren la implantación de la IA**, con **un enfoque europeo, coordinando políticas entre los Estados Miembros y la comunidad investigadora.** Se trata de atraer y retener el talento, creando un marco regulatorio óptimo que aborde los problemas y los riesgos asociados a determinados usos de esta nueva tecnología y que, además, **atraiga la inversión pública y privada necesaria** para promover su implantación.

Se debe crear un ***"ecosistema de excelencia",*** un marco político adecuado para establecer medidas que armonicen los esfuerzos a escala *regional, nacional y europea*, en colaboración con los sectores *públicos y privados,* para movilizar recursos y estimular la inversión. Esto solo puede llevarse a cabo dentro de un ***"ecosistema de confianza"*** basado en una "regulación adecuada y proporcionada" que evite cualquier tipo de inseguridad jurídica.

2. *Resumen/análisis Libro Blanco sobre la Inteligencia Artificial desde el punto de vista de la Responsabilidad Civil*

    a. *¿Qué es la IA?*

En abril de 2019 el grupo de expertos de alto nivel creado por la Comisión definió *los sistemas de IA como programas informáticos (y posiblemente también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de esos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado*."

Dado que el uso de la IA no solo se traduce en oportunidades sino que conlleva riesgos y amenazas, el legislador deberá estar atento a estos riesgos y alcanzar una regulación de la IA que permita disfrutar de sus ventajas minimizando los riesgos aparejados a su uso y que a la vez que asegure el respeto de los derechos de las personas y los valores en torno a los cuales se erige la **Unión Europea ("UE")** y los **Estados Miembros ("EEMM")**.

Uno de los mayores problemas que se refiere es la posible fragmentación en esta materia entre los distintos EEMM. Para evitarlo es imprescindible que esta regulación se acometa principalmente por la UE de forma que las legislaciones de los EEMM sigan la hoja de ruta marcada por la UE en pro del mercado único.

b. ¿Qué es la Responsabilidad Civil?

La **Responsabilidad Civil** (en adelante "RC"), de acuerdo a Díez Picazo, es la sujeción de quien vulnera un deber de conducta en interés de otro sujeto a la obligación de **reparar el daño producido**. Será **RC contractual** cuando surja de la vulneración de un contrato entre las partes y de las obligaciones que genera entre las mismas o **extracontractual** (aquiliana) si se causa un daño por un comportamiento culposo o doloso.

Dentro de la RC **extracontractual** debemos distinguir si deriva de una acción u omisión **culposa** (conducta reprochable de la persona fuente de responsabilidad), o si deriva del **riesgo** (diferenciando entre la responsabilidad civil objetiva y la responsabilidad civil por riesgo.

En los casos complejos que no se pueda determinar a primera vista esta conducta culposa, se deberá demostrar culpa, teniendo como parte preponderante la **diligencia en el actuar**. De este modo se protege al damnificado en mayor medida (salvo excepciones de culpa exclusiva de la víctima o fuerza mayor), debiendo probar estos puntos el agente que haya causado el daño, mientras tanto se entenderá que es responsable. Esto obligará a los agentes a contratar seguros de responsabilidad civil para cubrir estos daños.

Actualmente, los desarrolladores e implementadores de la IA ya están sujetos a la legislación europea en materia de **derechos fundamentales** (protección de datos personales, privacidad, no discriminación y otros) **de protección de los derechos de los consumidores** y **normas sobre la seguridad de los productos** y **responsabilidad civil** y el **Acta Europea de Accesibilidad** aplicable a partir de 2025 a los bienes y servicios. Sin embargo, estas normas no son específicas para la IA y son previas a la existencia de la misma. Consecuentemente, no son del todo eficientes para cumplir con su finalidad dadas las características de la IA haciendo difícil su aplicación y ejecución.

Por ello, hay que estudiar la legislación actual y ver si es necesario legislar *Ad hoc* para afrontar los retos que plantea la IA, evitando una fragmentación entre las soluciones de los EEMM que, de facto, ya empieza a hacerse patente: a) Alemania propone un sistema de RC según el nivel de riesgo que lleve aparejado la aplicación de IA con (5 niveles), b) Dinamarca apuesta por un "sello de ética de los datos" para dar más confianza a los productos y servicios IA a los que se les conceda y c) Malta ofrece una certificación voluntaria que logra este mismo efecto.

c. Definición de los problemas

La aplicación de la IA puede causar tanto daños **materiales** (para la seguridad y la salud de las personas, con consecuencias como la muerte y menoscabos al patrimonio) como **inmateriales** (pérdida de privacidad, limitaciones al derecho de libertad de expresión, dignidad humana, discriminación en el acceso a empleo, etc…). Estos daños pueden estar vinculados a **gran variedad de riesgos,** defectos en el diseño general de los sistemas de IA, por uso de datos sesgado, fallos de ciberseguridad o conectividad en infraestructuras clave, usos malintencionados...

Determinados riesgos afectan principalmente a la protección de los **derechos fundamentales** (protección de datos personales, privacidad o no discriminación). Los ciudadanos temen quedarse indefensos a la hora de proteger sus derechos y su seguridad frente a los desequilibrios informativos de la toma de decisiones mediante algoritmos.

Algunas de las características de la IA como su opacidad ("efecto caja negra"), su complejidad, su imprevisibilidad y un comportamiento parcialmente autónomo pueden dificultar la tarea de las autoridades a la hora de controlar que se dé un eficaz cumplimiento normativo. La problemática principal oscila en encontrar mecanismos fiables de control que evite estos riesgos y el funcionamiento eficaz del régimen de RC.

d. Riesgos para la seguridad jurídica y el funcionamiento eficaz del régimen de Responsabilidad Civil

La **falta de disposiciones claras** en materia de seguridad y algunas características de las tecnologías de la IA puede crear **inseguridad jurídica** tanto a las *empresas que comercializan* productos con IA en la UE como a *las autoridades encargadas* de supervisar el mercado o de ejecutar las normas que puede resultarles confuso cómo intervenir, pueden no estar facultadas para tomar medidas o no contar con las capacidades técnicas adecuadas para examinar los sistemas de IA.

Esta inseguridad jurídica afecta también a las *personas damnificadas* para recibir compensaciones en materia de RC en los distintos países de la UE, al encontrar dificultad para hacer un seguimiento retrospectivo de las decisiones potencialmente problemáticas adoptadas mediante IA y para acceder las pruebas necesarias para llevar un caso ante los tribunales. En definitiva, la probabilidad de obtener la reparación efectiva será menor que si los daños son causados por tecnologías tradicionales.

Por ello, para no reducir los niveles globales de seguridad y minar la competitividad de las empresas europeas, urge alcanzar una regulación de la IA que ofrezca seguridad jurídica a los distintos agentes del mercado, incluyendo al consumidor final.

L*as directrices para una IA fiable* del grupo de expertos de alto nivel sobre la IA (de abril de 2019) son clave para un futuro marco normativo europeo de la IA. Establecen siete requisitos fundamentales que deben cumplirse y evaluarse a lo largo de todo su ciclo de vida útil:

1º. **Intervención y supervisión humanas**: Los sistemas de IA deben facilitar sociedades equitativas, apoyando la intervención humana y los derechos fundamentales, y no disminuir, limitar o desorientar la autonomía humana.

2º. **Solidez y seguridad técnicas**: La fiabilidad de la IA requiere que los algoritmos sean seguros, fiables y sólidos para resolver errores durante toda la vida útil de los sistemas de IA y hacer frente adecuadamente a los resultados erróneos con un plan de contingencia. Deben de ser resilientes frente a ataques abiertos o tentativas de manipular datos o los propios algoritmos.

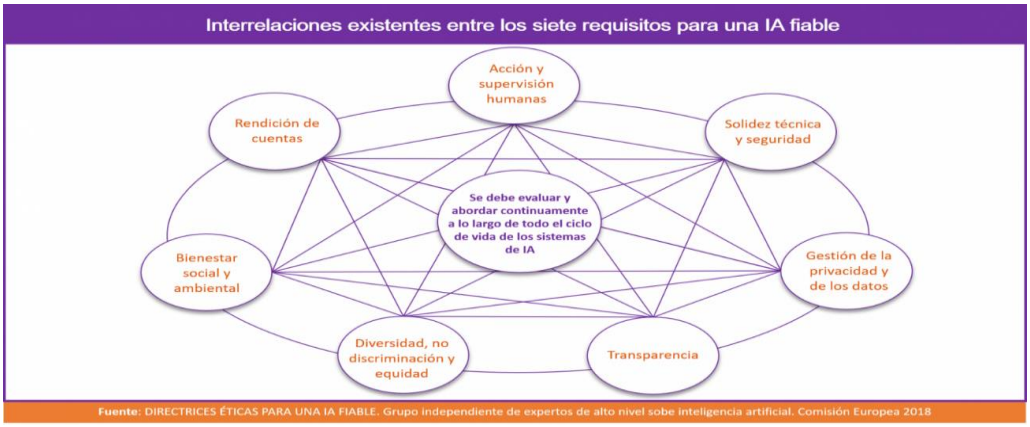
3º. **Privacidad y gestión de datos**: Para que las personas puedan confiar en el tratamiento de datos, los ciudadanos deben tener pleno control sobre sus propios datos y los datos que les conciernen no deben utilizarse para perjudicarles o discriminarles. Además deben garantizarse la privacidad y la protección de datos en todas las fases del ciclo vital del sistema de IA.

4º. **Transparencia**: Debe garantizarse la trazabilidad de los sistemas de IA, documentando las decisiones tomadas y la totalidad del proceso (descripción de la recogida, etiquetado de datos y algoritmo utilizado) que dio lugar a las decisiones. Si fuera posible debe aportarse la *explicabilidad* del proceso de toma de decisiones algorítmico, las opciones de diseño del sistema, y la justificación de su despliegue, garantizando transparencia al modelo de negocio.

5º. **Diversidad, no discriminación y equidad**; Los datos utilizados para el entrenamiento y funcionamiento de la IA, deben tener en cuenta las capacidades, competencias y necesidades humanas, y garantizar la accesibilidad. No pueden incluir sesgos o modelos de gobernanza deficientes que den lugar a una discriminación (in)directa. *El sesgo* también puede afectar a la forma en que está escrito el código de programación. Estos problemas deben abordarse desde el inicio del desarrollo del sistema.

6º. **Bienestar social y medioambiental**: Los sistemas de IA deben utilizarse para mejorar el cambio social positivo y aumentar la sostenibilidad y la responsabilidad ecológicas. Debe tomarse en cuenta su impacto sobre el medio ambiente y sobre otros seres sensibles.

7º: **Rendición de cuentas**: Deben implantarse mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de IA y de sus resultados antes y después de su implementación. La posibilidad de evaluación de los sistemas de IA por parte de auditores internos y externos y la disponibilidad de los informes de evaluación, contribuye a su fiabilidad especialmente en aplicaciones que afecten a los derechos fundamentales.



La IA es una tecnología transformadora y disruptiva que ha evolucionado en los últimos años gracias a la disponibilidad de un gran volumen de datos digitales, los avances computacionales, la capacidad de almacenamiento, la innovación científica y de ingeniería en métodos y herramientas de IA. Advierten de su impacto en la sociedad y en los ciudadanos en formas que aún no podemos imaginar.

Los **riesgos más notables** incluyen el *reconocimiento facial*, el *uso de datos biométricos involuntarios*, la *identificación automática*, los *sistemas clasificatorios de ciudadanos* y, por último, los sistemas de *armas autónomas letales* con habilidades cognitivas para decidir quién, cuándo y dónde luchar sin intervención humana. Todos ellos plantean muchos problemas éticos además de los legales ya que son susceptibles de vulnerar los derechos fundamentales.

En sus **conclusiones** resaltan la importancia de construir sistemas de IA en los que la tecnología, incluyendo los procesos y las personas que están detrás de la tecnología, sea fiable, trazando unas normas de juego y marcando los límites y consecuencias de un mal uso (culposo o reprochable) de la IA, cobrando importancia **la RC y su relación con la IA**.

La *Directiva sobre responsabilidad por los daños causados por productos defectuosos* atribuye al fabricante la responsabilidad de los daños que cause por un producto defectuoso. En los casos en los que aplique IA será difícil demostrar el nexo causal entre defecto y daño por las características de estos sistemas. Para los consumidores será igualmente difícil acceder a las pruebas que demuestren que efectivamente los daños que han padecido son responsabilidad de la empresa detrás del producto defectuoso. La

Comisión considera conveniente mejorar el marco normativo actual para abordar los riesgos y situaciones siguientes:

- **Aplicación y cumplimiento efectivos de la legislación nacional y de la UE en vigor**: La opacidad de la IA hace difícil detectar y probar incumplimientos de la legislación sobre derechos fundamentales, imputación de responsabilidades y reclamación de indemnizaciones. Hay que clarificar la normativa actual y adaptarla a nuevos escenarios, para que en casos de RC se ofrezca una solución real a las personas que sufran un perjuicio causado por un producto o servicio marcado por la IA.

- **Limitaciones del ámbito de aplicación de la legislación vigente de la UE**: si bien la legislación sobre seguridad de los productos de la UE se aplica al software cuando forma parte de un producto final, no está claro si el software independiente, como una IA, está cubierto por esta regulación o no. La legislación general de la UE en materia de seguridad en vigor es de aplicación a **los productos** pero **no a los servicios**, y, por consiguiente, *a priori* no se aplica tampoco a los servicios basados en las tecnologías de IA (como servicios sanitarios, financieros o de transporte).

- **Funcionalidad cambiante de los sistemas de IA**: Dado que la IA se actualiza o incluso por su aprendizaje automático, se pueden añadir nuevas funciones durante la vida útil de la IA que den lugar a nuevos riesgos no contemplados en el momento de su comercialización. La velocidad de la tecnología no permite una reforma normativa rígida sino que deberá poder amoldarse a los constantes cambios y actualizaciones que sufren los sistemas de IA. Actualmente la legislación en vigor se centra únicamente en los riesgos de seguridad en el momento de la comercialización.

- **Incertidumbre para imputar la responsabilidad entre los distintos agentes económicos:** La legislación de la UE imputa la responsabilidad al productor del producto comercializado, lo que plantea dudas con la IA porque algunos riesgos nacen *a posteriori*. Además, la legislación de la UE sobre la RC por los productos, deja que las normas nacionales en materia de RC se encarguen de los demás participantes en la cadena de suministro. La legislación de la UE en materia de seguridad solo aplica a productos y no a servicios, lo cual, si lo extrapolamos a servicios de IA, podremos concluir que tampoco aplica a estos.

- **Cambios en el concepto de seguridad**: el uso de la IA puede dar lugar a riesgos no previstos actualmente de forma específica por la legislación (ciberamenazas, seguridad personal, pérdida de conectividad…). Estos riesgos pueden estar presentes en el momento de su comercialización o llegar después, tras una actualización o por aprendizaje automático del producto. **Minimizar los riesgos para los derechos fundamentales,** especialmente la protección de datos personales, la privacidad y la no discriminación, así como, los **riesgos para la seguridad y el funcionamiento eficaz del régimen de RC**, es la dificultad a la que se enfrentan los sistemas basado en la IA.

Es necesario prestar especial atención a las aplicaciones de IA de alto riesgo, es decir, aquellas que se emplean en **sectores** en los que es previsible que existan o puedan surgir riesgos significativos, desde la perspectiva de la protección de la seguridad, derechos de los consumidores y derechos fundamentales (la sanidad, el transporte, la energía y en determinados ámbitos del sector público), así como en **determinados usos** que pueden considerarse críticos como los ligados a conducción automáticas o los procesos de contratación laboral.

Por otro lado, la Comisión también se refiere a los **requisitos legales que se les debe de imponer a los "actores relevantes" que desarrollen IAs de alto riesgo**. Los campos que se contemplan, acompañados por sus posibles criterios, son los siguientes:

- **Datos de entrenamiento**: los datos utilizados para entrenar los sistemas de IA han de ser suficientemente amplios para evitar situaciones peligrosas, que no generen discriminación y que protejan la privacidad de los datos personales.
- **Conservación de registros y datos**: la complejidad y la opacidad de muchos sistemas de IA, hacen necesario mantener un registro de los datos usados y por qué se han seleccionado, documentar la programación, entrenamiento, procesos y técnicas usadas para construir la IA, incluso conservar los propios conjuntos de datos.
- **Suministro de Información**: se requiere transparencia más allá de la conservación de datos. Se debe facilitar información clara sobre las capacidades y limitaciones de la IA, o informar "claramente" a los usuarios de que están interactuando con una IA y no con un humano.
- **Robustez y precisión**: Los sistemas de IA sobre todo en sus aplicaciones de riesgo elevado, para que sean fiables deben de ser sólidos y exactos todas las fases de su vida útil. Los resultados han de ser replicables y que son resilientes ante ataques abiertos o intentos de manipulación de los propios datos o algoritmo.
- **Supervisión humana**: Ayuda a garantizar que un sistema de IA no socave la autonomía humana o provoque otros efectos adversos. Los resultados de la IA no deben de ser efectivos hasta que un humano los valide o si lo son, deben poder supervisarse después.
- **Requisitos específicos en el caso de identificación biométrica remota**: en la normativa europea el reconocimiento facial a distancia dependiendo de los usos y de su tratamiento está muy limitado por el GDPR. En principio, está prohibido salvo en condiciones específicas principalmente por motivos de interés público significativo.

e. Destinatarios

La cuestión es establecer cómo repartir las obligaciones entre los distintos agentes económicos que participen en todo el proceso de creación del producto o servicio: Desarrollador, implementador, otras partes potenciales (productor, distribuidor, proveedor de servicios y usuario). La Comisión considera a tal efecto que cada obligación deberá dirigirse a la parte que esté en mejor posición para abordar todo posible riesgo. Recordemos que, en la actualidad, la normativa de la UE sobre RC establece que será el productor sobre quien recaiga la RC por productos defectuosos, independientemente de que la normativa nacional de los EEMM contemple en su normativa una indemnización a cargo de otras partes involucradas.

f. Cumplimiento y ejecución

Tal y como ya ha destacado la Comisión, uno de los mayores retos será el de generar confianza alrededor de la IA, garantizando un cumplimiento y ejecución efectivo de las normas existentes que se adapten a la realidad que vivimos y a las de nueva redacción. Se considera necesario un *control objetivo previo* que compruebe y asegure que se cumplen los requisitos que la normativa marque como obligatorios en materia de IA cuando su aplicación sea considerada de alto riesgo.

Este control podrá realizarse *ex ante* o *ex post* y deberá servir para facilitar un resarcimiento efectivo para los casos en los que a través de un sistema de IA se ocasione un daño o un perjuicio, garantizando una acción judicial efectiva, especialmente en los casos de aplicaciones de IA en sectores o actividades que se consideren de riesgo elevado.

g. Conclusión

Un uso diligente de la IA, traerá a los ciudadanos, empresas y a la sociedad en general, múltiples beneficios. Sin embargo, es fundamental que la aplicación de la IA no contravenga los Derechos Fundamentales, los principios éticos y valores de la UE y de sus EEMM.

Debemos tener en cuenta que la regulación actual no cubre estos supuestos de manera precisa y clara. Por ello, deberá introducirse normativa específica capaz de regular la IA de forma satisfactoria para ofrecer una mayor seguridad jurídica a todos los agentes del mercado. Los *pain points* que hay que solucionar a través de legislación específica son los siguientes:

- Algunas aplicaciones de IA requerirán supervisión humana que garantice un uso seguro.
- Adopción de medidas específicas si el daño deriva de datos incorrectos en la fase de diseño y mecanismos que garanticen la calidad de los datos durante la vida del producto.
- Establecer requisitos de transparencia para combatir la opacidad de los sistemas de IA para facilitar la viabilidad de cualquier pretensión jurídica que reclame RC.
- Adaptar normativa para los casos concretos en los que la IA se implemente tras la comercialización del producto, especialmente si pueda afectar a su seguridad.
- La complejidad de la cadena de suministros ha aumentado lo que dificulta depurar responsabilidades adecuadamente entre los distintos agentes implicados en el desarrollo.

Como ya se ha señalado, puede complicar la trazabilidad de los daños padecidos por la víctima debiendo de esta manera recurrir a un sistema de responsabilidad civil subjetiva. Esto podría aumentar los costes de litigación de las víctimas complicando demostrar la RC de otros partícipes del producto o servicio distintos del productor.

El camino aún será largo, pero la UE no puede descuidarse si no quiere que los EEMM emprendan su camino de manera individual, fragmentando el mercado único, lo que se traduciría en la pérdida de oportunidad de afrontar de manera conjunta el reto y la imposibilidad de que la UE se erija como una potencia mundial en este campo.

3. *Comentarios y propuestas sobre IA y RC*

a. Introducción al problema

La IA indudablemente va a traer ventajas a la sociedad, a las administraciones públicas, a las empresas privadas y, especialmente, a quienes exploten estas tecnologías, por los elevados beneficios económicos que va a reportar su uso a los distintos agentes del mercado.

Sin embargo, esto va a traer nuevas situaciones y problemas que tanto el derecho de la UE como el de los distintos EEMM tiene que poder solventar. La dificultad reside en cómo enfocar la RC de la IA de manera solvente, con seguridad jurídica y que, además no asfixie a fabricantes, desarrolladores y comercializadores de IA, fomentando su desarrollo e investigación sin una regulación muy severa que para proteger al consumidor haga que las empresas se lo replanteen.

Vamos a tratar de abordar estas cuestiones por medio de soluciones ya existentes como el tipo de responsabilidad que debe operar bajo estos presupuestos, si es o no pertinente un *seguro de RC obligatorio* y otros nuevos como por ejemplo la posible creación de un nuevo tipo de personalidad jurídica atribuible a las máquinas de IA con un patrimonio y una solvencia que los permita responder por el eventual daño causado.

b. Fragmentación del mercado único y consecuencias sobre la RC

El riesgo que conlleva la falta de una visión desde la UE, en relación a la RC y la IA, y una normativa europea para desarrollar una normativa Estatal, fomentaría consecuencias distintas para los agentes participantes en el desarrollo de productos con IA en función del EEMM. Por ello, es preponderante que se plantee un cuerpo legislativo fuerte desde la UE que prevea todos estos riesgos y marque un camino de acción por parte de los EEMM. A continuación intentaremos retratar estos riesgos y ofrecer posibles soluciones de acuerdo a los valores y derechos defendidos por la UE.

c. Problemas RC

La *complejidad* y *opacidad de los sistemas de IA* complica la tarea de discernir qué agente puede ser responsable de un daño ocasionado en el uso de productos IA o de la prestación de servicios de IA. Hacen muy difícil que un consumidor pueda hacer valer de manera eficaz sus derechos y reclamar una compensación por un daño sufrido, a través de un sistema subjetivo de responsabilidad en el que este deba demostrar la culpa del fabricante.

Por ello, esta *responsabilidad extracontractual* deberá descansar en un criterio de *imputación objetivo* o, al menos, de *presunción de culpa,* en el que el usuario que ha sufrido un daño deba demostrar este y el *nexo causal* entre el comportamiento del producto o servicio de IA y el daño, **debiendo ser los agentes detrás de la solución de IA los que deban encontrar alguna causa que pueda eximirles de responsabilidad**.

Las primeras soluciones que planteamos son:

1) la **inversión de la carga de la prueba** sobre las personas (físicas o jurídicas) que hayan participado en el desarrollo, producción y comercialización.
2) la **presunción de culpabilidad** como un **criterio de imputación objetiva** por el cual estos mismos agentes deberán demostrar que han actuado de manera diligente y que no se les puede responsabilizar por las consecuencias del evento dañoso.

Bajo este **criterio de imputación objetiva** o **presunción de culpa** de los agentes involucrados, estos serían los que tendrían que demostrar su hacer diligente y adecuado, facilitando al consumidor la reclamación de estos daños, puesto que solo tendrá que probar el daño que se le ha causado y la relación causal entre este y la solución de IA que presuntamente se lo ha ocasionado.

De otra forma estos procedimientos serían muy costosos y muchas acciones con fundamento no prosperarían porque muchos afectados no tendrían capacidad económica para afrontar el coste del procedimiento, perdiendo irremediablemente la acción. Sería necesaria la contratación de *peritos especializados* que pudieran discernir dónde ha estado el fallo que ha causado el daño.

A través de la **inversión de la carga de la prueba** son las empresas las que tienen que aportar la prueba y abogar por su diligencia. Tienen acceso a toda la prueba y pueden demostrar si han actuado de manera diligente, culposa o si han atendido de manera adecuada un posible riesgo. Conocen los códigos y algoritmos que hacen funcionar estos productos y servicios, los datos en los que se basan y sobre los cuales toman sus decisiones estas soluciones de IA. Es mucho más sencillo que sean ellas las que tengan que aportar la prueba a que sean los usuarios los que tengan que demostrar el daño, el nexo causal y la culpa de las empresas.

En consecuencia, creemos que cuando estemos antes soluciones de IA que puedan tener un riesgo relevante que pueda causar un daño, deberá de estarse a estas dos cuestiones: *la inversión de la carga de la prueba* y *la presunción de culpabilidad*. De esta manera las empresas que hayan causado un daño deberán de probar que han actuado de acuerdo la diligencia exigida o que, por el contrario, el daño ha surgido como consecuencia de fuerza mayor, que se trate de un caso fortuito, el hacer de un tercero o que la culpa recaiga exclusivamente sobre la víctima.

d. Responsabilidad por hechos propios (responsabilidad objetiva, doctrina del riesgo) y responsabilidad por hechos ajenos

Para poder determinar la concurrencia responsabilidad civil extracontractual deben de cumplirse los siguientes requisitos:

- Una acción u omisión
- Causación de un daño
- Nexo causal entre la acción u omisión y el daño
- Existencia de un criterio que permita imputar la responsabilidad extracontractual

Dadas las características de la IA (que en ocasiones el hacer de esta diverge de la intención inicial de su creador y se desarrolla y razona de acuerdo a su algoritmo) y de manera más concreta a aquellas IAs que conlleven un riesgo elevado para los usuarios y por la opacidad para poder demostrar la concurrencia de culpa y a quién corresponde debemos de considerar qué solución se aproxima más a ser justa.

Presentamos tres soluciones las cuales presentan ventajas enfocadas a facilitar el resarcimiento de daños causados por soluciones de IA pero, a su vez, también tienen sus desventajas como podría ser un régimen demasiado gravoso y exigente a la hora de marcar un nivel de diligencia adecuado. Estas tres posibilidades serían aplicar: 1) una responsabilidad objetiva, 2) la doctrina del riesgo o 3) un régimen similar o comparable al de los padres, madres o tutores en relación con sus hijos.

a) Responsabilidad por hechos propios

1. Responsabilidad objetiva

Como fundamento de la responsabilidad objetiva suele admitirse que no existe un único argumento sino un conjunto de criterios determinados por un riesgo anormal o extraordinario. Lo que motiva este criterio de determinación objetivo de la responsabilidad es *el riesgo extraordinario o anormal inherente a una acción u omisión*. Los criterios de la responsabilidad objetiva son una probabilidad especialmente alta de que el riesgo se materialice, la probabilidad de que el daño sea catastrófico o que pueda existir un riesgo potencial que *a priori* no se pueda descartar y que pudiera acaecer. Todos los anteriores son posibles resultados de la aplicación de la IA en determinados sectores y para determinadas tareas. Pensamos que son aplicables a este sector, al menos cuando el riesgo sea elevado.

Que la responsabilidad no dependa de la culpa no debe entenderse como una forma de repartir socialmente ciertos riesgos. Quienes deciden llevar estas actividades anormalmente peligrosas para poner en marcha una actividad o servicio para lucrarse y causan un daño, pese a haber actuado de manera diligente, han aceptado la existencia de estos riesgos de antemano, por lo que cobra sentido que sean estos sujetos privados los que soporten la responsabilidad.

El potencial económico de todos los negocios que apliquen IA va a ser exponencial e ingente. De modo que tiene sentido que sean los agentes detrás de un producto o servicio IA quienes deban responder por los posibles daños que puedan acaecer como consecuencia de la explotación de la IA a pesar de que hayan actuado de forma diligente.

El punto negativo de la objetivación de la responsabilidad es que no premia la diligencia del empresario o no castiga la falta de cuidado y puede provocar que el empresario no cuide tanto "no cometer errores" y "no proteja al consumidor de una manera tan exhaustiva" dado que en cualquier caso va a recaer sobre él la RC.

Esta solución no está libre de problemas. Sin embargo, dado el beneficio económico que van a reportar los negocios que implementen soluciones IA a sus productos y servicios, parece apropiado que sean objetivamente responsable en los casos en los que la aplicación de la IA implique que se den los criterios para la aplicación de este tipo de responsabilidad civil extracontractual.

2. Doctrina del Riesgo

Cobra sentido para los casos de aplicación de la IA en los que exista un riesgo considerable, un principio de precaución. La doctrina del riesgo acepta que *el riesgo sea el fundamento de una eventual responsabilidad civil extracontractual*. No se objetiva la responsabilidad sino que, debido al elevado riesgo de la actividad, se exigen cánones de diligencia más elevados y se invierte la carga de la prueba para que sea el posible responsable quien deba de demostrar que su actuar era diligente y concurría con todas las previsiones

y precauciones debidas en relación el riesgo en cuestión, medidas de precaución y de cuidados mayores en pro de evitar el daño.

Sin embargo, se concede al potencial responsable del daño la posibilidad de liberarse de la responsabilidad demostrando que, efectivamente, ha actuado con la diligencia exigible y con el suficiente cuidado de acuerdo al riesgo que estaba en juego. Para el supuesto de que no se cumpliera con esta diligencia exigible de acuerdo al riesgo, se entendería probado el nexo causal tanto desde el punto de vista físico como desde el jurídico.

Por lo tanto, la responsabilidad por riesgo es una de las posibles soluciones al problema que arroja la IA a la RC. Para aquellas actividades de riesgo que puedan ser peligrosas para los usuarios tanto por el sector en el que operen como por la actividad que desempeñen, habremos de estar a una elevación del estándar de diligencia en proporción al potencial riesgo. En caso de que estos agentes no sean capaces de probar su diligencia y falta de cuidado en función del riesgo se les tendrá como responsables de daño.

b) Responsabilidad por hechos ajenos

El artículo 1.903 del Código Civil prevé la responsabilidad por hecho ajeno, una responsabilidad por culpa en cuanto a una falta de diligencia. De esta manera, una persona distinta de la que ha ocasionado el daño es directamente responsable del mismo. Está previsto para aplicarse a padres, tutores o empresario. Esta negligencia puede concretarse en una falta de vigilancia dada la relación de subordinación o dependencia existente entre el autor material del daño y la persona que será directamente responsable del daño. Esta responsabilidad será directa, por lo que podrá reclamarse directamente contra las personas que refiere este art. 1.903.

Destaca el marcado carácter de culpa subjetivo ya que se responsabiliza directamente a otra persona de la que depende el agente que ha cometido la acción que ha dado lugar a la responsabilidad por una actitud pasiva, de omisión o de falta de vigilancia que ha permitido que se cause el daño en cuestión.

Aterrizando esto a la IA son escenarios similares. En ambos casos se trata de entes subordinados y dependientes cuya voluntad se escinde de la de su creador o persona de la que dependen. Por medio de este sistema se pretende *cuidar la falta de diligencia de vigilancia y de cuidado* por la persona directamente responsable a la que se le puede cargar con este deber de vigilancia.

En el caso de los sistemas de IA (siempre y cuando no se le atribuya una personalidad jurídica con un patrimonio que pudiera responder de los daños causados) no van a estar en condiciones de responder por un daño que hayan podido causar. Por eso, tiene sentido que se responsabilice de manera directa a la persona de la cual dependen, la que tiene este deber de vigilancia y que no puede permitir todo, sino que tiene que limitar el hacer de estas. El hacer de la IA, al igual que el de un menor, está marcado por unos patrones (basados en código y algoritmo) pero su voluntad se escinde de la de su creador ya que razona de manera independiente para alcanzar un fin lo cual lo dota de una cierta imprevisibilidad. Así, el fabricante, comercializador o agente que use esta solución IA deberá ejercer este control, llegando a retirarlo si fuera necesario del mercado para solucionar cualquier riesgo que pudiera haber o, por el contrario, afrontar la responsabilidad directa de la materialización del riesgo en daños.

La conducta de los sistemas de IA con capacidad de aprendizaje no supervisado, en ocasiones puede ser imprevisible, no pudiendo incluso prever algunos riesgos o situaciones que pueden darse. Esto va a concretarse en muchas ocasiones en daños y en situaciones que pueden poner en jaque los sistemas de responsabilidad civil y en los que, además, deberemos determinar los parámetros por los que se va a determinar quién es responsable de estos daños.

a) Fabricante

Considerando la incertidumbre y los riesgos inherentes a la IA debe prevalecer un principio de precaución que obligue al fabricante o al propietario que lo controla a actuar de manera especialmente diligente y tomando las medidas posibles para minimizar el riesgo.

Hacer responsable al fabricante de los daños o riesgos que puedan materializarse por el uso de sistemas de IA fomentará que el fabricante operé con un especial cuidado. Sin embargo, un régimen demasiado férreo puede ser un obstáculo para que el sector privado invierta en la UE en investigación y desarrollo. La dificultad oscila en encontrar el equilibrio.

La UE aboga por marcar un límite cuantitativo a esta responsabilidad el cual debemos recordar que aplicará para daños materiales, pero no a los personales. De nuevo, la determinación de la responsabilidad deberá de atender a criterios objetivos. Se invierte la carga de la prueba para que el fabricante pueda argumentar cualquier cuestión que le exima de responsabilidad (actuación correcta del robot, fuerza mayor, culpa del perjudicado, etc.).

Una limitación o exoneración de la responsabilidad puede encontrarse en que el fabricante haya compartido unas limitaciones de expectativas de seguridad o instrucciones, si de acuerdo a la evolución del sistema de IA y de los conocimientos del fabricante este puede vaticinar un riesgo o la consecución de un potencial daño.

Será interesante la **imposición de un seguro de responsabilidad obligatorio**, al menos en los supuestos catalogados de riesgo, a pesar de que esto en un último término se traduzca en un aumento en el precio del producto o servicio.

b) Empresario que se sirve del robot inteligente

El empresario que se sirva de los servicios del robot inteligente en la esfera profesional con la finalidad de obtener una ganancia económica deberá responder por los daños cometidos por el robot de acuerdo a criterios objetivos.

Podrán darse dos situaciones, una responsabilidad contractual o una responsabilidad por hecho ajeno cuando no exista contrato entre las partes. La responsabilidad estará basada en la teoría del riesgo atendiendo a dos criterios: la probabilidad de que el riesgo se materialice y la gravedad del mismo.

El empresario deberá tener la obligación controlar y vigilar el robot y su desempeño y, de acuerdo al rango de peligrosidad concreto deberá atenderse a criterios de responsabilidad objetiva. El perjudicado deberá, únicamente probar el daño y el nexo con el sistema de IA.

c) Responsabilidad del usuario del robot:

Si entendemos por el usuario a la persona que adquiere el sistema de IA para su uso personal, este puede ser o no el propietario del mismo. En el supuesto en el que poseedor y propietario coincidan en una misma persona estaremos a los criterios de responsabilidad objetiva o por riesgo que hemos referido.

Para el caso de que propietario y poseedor del robot no coincidan deberemos distinguir entre los siguientes supuestos:

- Cesión de uso a un tercero o pérdida de la máquina: la responsabilidad deberá ser solidaria por partes iguales entre el propietario (obligación de vigilancia) y el usuario-poseedor que deberá de actuar con diligencia y precaución para reducir los riesgos.
- En caso de robo o apropiación indebida el único responsable será el ladrón que se está valiendo del sistema de IA.

d) Responsabilidad del Robot Autónomo Inteligente con Personalidad Jurídica

Otro mecanismo a valorar en relación con las IA de Alto riesgo es la creación de una personalidad jurídica propia para los robots (e-personality). Hay un sector favorable a la creación de un nuevo vehículo apropiado y a medida, acorde a las necesidades que permita a los sistemas de IA tener personalidad jurídica propia de una manera *Ad hoc. O*tro sector, en cambio, no lo ven necesario porque el ordenamiento jurídico ya ofrece soluciones de este tipo. Por muy completa y autónoma que sea la IA nunca podrán ser consideradas auténticas personas.

Si se acepta la *e-personality* a las soluciones de IA, se les podría atribuir un estatus jurídico específico para proteger determinados intereses de la sociedad, similar a la ya existente personalidad jurídica societaria. Serían sujetos susceptibles de adquirir derechos y contraer obligaciones, podrían ser acreedoras o contraer deudas, poseer patrimonio propio y representar un interés social o económico. Supondría un mecanismo de control para evitar los riesgos de la nueva realidad, con unas finalidades que determinan sus condiciones de uso y sus límites, específica a determinados robots (a los sistemas de IA más autónomos o avanzados), como invención puramente técnica, formal y abstracta, con el objeto de proteger determinados intereses de la humanidad, teniendo muy presente su condición de sistema sometido y subordinado en todo momento al beneficio e interés de los humanos.

Un robot autónomo no es un ente libre e independiente, no se le puede imputar por el momento ningún tipo de culpabilidad, ni de responsabilidad que derive de la conciencia de sus actos. Siempre va a pertenecer a personas físicas o jurídicas, que son las que en última instancia van a permitir o decidir que siga funcionando o que cese en su empleo. Su voluntad no se ha formado de manera completamente libre, sino más bien es dependiente y sometido a la voluntad de otro.

No obstante, *The Expert Group on Liability and New Technologies*, en su informe de 2019, establecen que no es necesario el atribuir esta personalidad legal a los sistemas autónomos de IA a efectos de atribuirles RC.

La creación de un fondo de compensación de los daños y perjuicios sería útil en los casos en los que no exista la cobertura de seguro, a cargo del fabricante, del comercializador o, en general, de cualquier agente interviniente en el proceso productivo del robot o sistema de inteligencia artificial; como acto único, o mediante dotaciones periódicas; disponibilidad del fondo y requisitos para la gestión y, en su caso, rentabilización del mismo.

En ocasiones la personalidad jurídica puede llegar a emplearse para defraudar a los acreedores ("abuso de la personalidad jurídica"). Para combatir existe la doctrina del levantamiento del velo la cual podríamos trasladar y aplicar en estos casos. Cuestión muy relevante puesto que esta suerte de persona electrónica no deberá de incurrir en infracapitalización, teniendo en cuenta el riesgo de la actividad, la gravedad de los daños que pueda ocasionar y la probabilidad de los mismos o un seguro de responsabilidad civil obligatorio que pueda afrontar con solvencia eventual los daños que haya podido causar.

La cuestión no es pacífica y parece una solución viable pero lo cierto es que la responsabilidad objetiva por parte de los distintos agentes que participen en el desarrollo de la solución de IA puede también ser una solución adecuada a este problema.

f. Alcance temporal de la responsabilidad

¿Hasta qué momento deben de responder los agentes detrás de una solución de IA por los daños que cause el mismo? No hay un referente actual en el mercado que pueda proveernos con una solución adecuada y que además haya sido contrastada y demostrada o no su viabilidad.

Al tratarse de sistemas que funcionan con código y algoritmo que hace que la voluntad del sistema de IA se escinda de la de su creador, el deber de vigilancia y cuidado de este no puede tener un límite temporal. El fabricante deberá llevar a cabo un seguimiento de la solución IA observando el funcionamiento del mismo y estando pendiente de posibles riesgos que puedan surgir a lo largo de la vida del mismo.

Por ello recae sobre el fabricante una obligación de vigilancia o seguimiento. Esta obligación incluye un deber de información y de adopción de medidas para reducir los posibles riesgos, incluso retirando el producto o servicio con el fin de modificar lo que sea necesario para asegurar la seguridad de la solución IA.

g. Seguro de RC obligatorio

Teniendo en consideración todo lo expuesto y a su vez el ***Informe sobre responsabilidad derivada de la IA y otras tecnologías digitales emergentes*** del *Grupo de Expertos sobre responsabilidad y nuevas tecnologías de la Comisión Europea*, que dentro identificaba, entre las **características esenciales** que deberán tener los regímenes responsabilidad derivada de la IA y el uso de otras tecnologías digitales emergentes para proteger a las víctimas de los daños sufridos, ya señala que *"En situaciones que exponen a terceros a un riesgo incrementado de daños, un **seguro de responsabilidad civil obligatorio** podría darles a las víctimas un mejor acceso a la compensación y proteger a los potenciales causantes contra el riesgo de responsabilidad". Concluyendo "33) Cuanto más frecuente o grave sea el daño potencial resultante de la tecnología digital emergente y cuanto menos probable sea que el operador pueda indemnizar a las víctimas; más adecuado será obligar a contar con un **seguro de responsabilidad civil para la cobertura** de tales riesgos.*

Consideramos que sí sería prudente implantar el seguro obligatorio pero haciendo especial atención al riesgo inherente a la aplicación de la solución de IA en cuestión y no como un criterio general aplicable a cualquier solución de IA, dado que algunas de sus posibles aplicaciones o funcionalidades podrían no llevar riesgos aparejados a su desempeño.

Habrá muchas situaciones en las que exigir la contratación de un seguro de responsabilidad civil pueda ser contraproducente. Si en el mercado de seguros, además, las compañías no estuvieran dispuestas

suscribir pólizas de este tipo porque supone cubrir riesgos aún desconocidos o que se ofrezcan coberturas de seguro para tecnologías digitales emergentes que limiten la cobertura de ciertos riesgos atendiendo a la dificultad de prever estos o de acuerdo a estadísticas de siniestralidad podríamos encontrarnos con el mismo problema un riesgo que queda sin protección y además se frenaría el avance del desarrollo de soluciones IA por una imposibilidad sobrevenida para cumplir con los requisitos marcados.

En cualquier otro escenario, **el seguro obligatorio de responsabilidad civil** puede ser una solución positiva. En concreto, y de acuerdo a la experiencia en otros sectores con riesgos inherentes a la actividad como puede ser el transporte, con un alto potencial de siniestralidad, la experiencia nos ha demostrado que el mecanismo del seguro obligatorio en el tráfico motorizado ofrece una solución solvente a un problema similar.

Por lo tanto, atendiendo a lo anteriormente mencionado, las soluciones de IA de alto riesgo, tanto por el sector en el que se emplean como por el uso critico que se les pueda atribuir, se deberán crear nuevas coberturas de seguro basadas en nuevos estándares y requisitos de entrenamiento de datos, registros de los mismos, que la información en la que se basan sea clara y esté libre de errores y que se desempeñe con supervisión humana, entre otros. Esto sería especialmente relevante para vehículos autónomos, drones no tripulados, prótesis robóticas, robots para el cuidado de las personas, o sistemas quirúrgicos o de cirugía computerizada, todos a título de ejemplo y sin ser una lista *numerus clausus*, dado que en el punto en el que nos hallamos parece que lo único que limita la aplicación de IA es nuestra imaginación y su aplicación irá aumentándose e incorporándose en nuevos sectores y actividades económicas.

h. Conclusiones

De acuerdo con todo lo anterior, el riesgo en principio es una cuestión inherente a la aplicación de IA. Puede variar en función del sector y de la actividad para la que se utiliza pudiendo ser inexistente hasta suponer un riesgo extraordinario. Cobra sentido marcar una escala o una división de las aplicaciones de IA en función del riesgo de mayor a menor, debiendo adecuarse en función de este riesgo a unas reglas u otras.

Hemos alcanzado el quorum de que la RC aparejada a la IA debe de estar a criterios objetivos, dejando atrás los criterios subjetivos de determinación de culpa. Habremos de estar a cuestiones como la posibilidad de que se materialice el riesgo y la gravedad del mismo. La carga de la prueba deberá invertirse, lo cual tiene sentido de acuerdo al principio de disponibilidad probatoria, dependiendo del responsable civil demostrar que ha actuado con la suficiente diligencia.

Dentro de los regímenes propuestos por esta parte para atender la RC en casos de daños por IA debemos recordar que hemos propuesto: a) responsabilidad objetiva, b) teoría del riesgo y c) responsabilidad ajena aparejada a la determinada por el 1.903 del Código Civil español.

De los daños ocasionados por IA, el responsable civil podrá variar y podrá ser: 1) el fabricante (entendiendo por fabricante todos los agentes que participen en la creación o desarrollo de la solución en cuestión), 2) el empresario que comercializa el producto o servicio, 3) consumidor privativo (incluidos los poseedores que no coincidan con el propietario) y 4) la propia máquina de IA en tanto en cuanto disponga de una suerte de personalidad jurídica acompañada de un patrimonio o seguro de responsabilidad civil obligatorio que soporte estos daños.

En este mismo sentido, cabe atender a que la responsabilidad de los agentes que ponen el producto o servicio de IA en el mercado no termina con la venta del producto sino que deben de actuar con cuidado, diligencia y vigilando el desarrollo de la IA para poder advertir de cualquiera problemas que pudieran surgir durante la vida del producto o servicio a razón de su actuar autónoma. Recordemos que este deber de información únicamente involucra riesgos previsibles.

El seguro obligatorio es una buena solución a la responsabilidad objetiva propuesta para los daños causados por IA. Esto se verá reflejado en los precios de mercado finales pero a su vez es garante de que las reclamaciones por responsabilidad civil sean atendidas.

En último lugar, como resulta obvio, una especialización en relación con estas cuestiones en los juzgadores que van a discernir a quién corresponde la responsabilidad en estos supuestos va a ofrecer mayor seguridad jurídica ya que las sentencias serán congruentes y acordes a la realidad presentada dado que en temas complicados como son los tecnológicos una correcta comprensión del supuesto de hecho y de las circunstancias es preponderante para que la sentencia sea ajustada a los hechos y a derecho.

Por último, y como cierre a esta reflexión, podemos ver como la IA presenta incontables problemas ya que aquí sólo hemos tratado un ínfimo porcentaje de ellos y todos relacionados con la RC. Sin embargo, esto no debe frenar a las empresas a trabajar en la implementación de esta en sus productos y servicios y a los consumidores en procurar confiar en la misma por los incontables beneficios que puede aportar.

Es esencial como venimos diciendo una regulación que fomente una atmósfera adecuada para el cultivo, crecimiento y desarrollo de la IA teniendo en cuenta que a su vez deberá ser suficientemente flexible como para poder adaptarse a los cambios que sufran los sistemas de IA que, al ser autónomos, son imprevisibles.

En este contexto es necesario adaptar los Ordenamientos Jurídicos tanto europeo como los Estatales para una correcta adaptación de la IA al mercado único europeo y sólo desde una regulación común se podrá garantizar una adopción común y en condiciones de equidad en los distintos EEMM que pueda situar a la UE como referencia mundial en el campo de la IA.

Entre los desafíos jurídicos que plantea el uso de sistemas de IA destaca el marco de responsabilidades que derivan de su uso. Las instituciones de la UE están creando un marco normativo sobre la tecnología. El comité de Asuntos jurídicos del Parlamento Europeo ha propuesto recientemente unas Recomendaciones para la Comisión (2020/2014(INL)), sobre el Régimen de responsabilidad civil derivada del uso de sistemas inteligentes entre los que está la elaboración de un Reglamento sobre esta materia, que armonice los diferentes aspectos, basándose en una necesaria combinación de sólidas normas éticas con un sistema sólido y justo de compensación de daños.

En su exposición de motivos habla del doble papel del concepto de "responsabilidad": por un lado, una persona que ha sufrido un daño tiene derecho a reclamar una indemnización de la persona responsable de causar ese daño y, por otro lado, proporciona incentivos para que las personas eviten causar daños en primer lugar o cualquier responsabilidad orientada al futuro.

El marco normativo debe buscar el equilibrio entre proteger eficientemente posibles víctimas de daños y, al mismo tiempo, proporcionar suficiente margen de maniobra para desarrollo de nuevas tecnologías, productos o servicios posibles. Especialmente al comienzo del ciclo de vida de nuevos productos y servicios, hay un cierto grado de riesgo para el usuario y para terceros de que algo no funciona correctamente.

La idea que debe de perseguirse es el principio de que "*toda persona que sufra un daño causado por un sistema de IA debe de disfrutar del mismo nivel de protección que aquella que los sufra por un sistema o dispositivo convencional, no inteligente".* Es decir, las características inherentes de la IA como son cierta opacidad de su funcionamiento o de su algoritmo y la dificultades que pueden agravarse por la posible conectividad entre diferentes sistemas de IA y otros que no lo son, dependencia de datos externos, vulnerabilidades de ciberseguridad y en algunos casos su creciente autonomía provocada por un aprendizaje automático (machine learning) o un *Deep learnig*, no pueden menoscabar los derechos de la persona que haya sufrido un daño a ser resarcido por ello.

A día de hoy hay ya cierto consenso entre las diferentes instituciones europeas y no consideran necesario sustituir algunos de los regímenes de responsabilidad ya existentes y que funcionan bien, son útiles, pero resultan insuficientes:

1) **Directiva 85/374/CEE** sobre **responsabilidad derivada de productos defectuosos**, sino que tan solo hacerse algunos ajustes en la misma para adaptarla al nuevo contexto de los sistemas de IA.

    a. Si una persona sufre un daño causado por un sistema de IA defectuoso y se quiere solicitar una indemnización al productor, sin duda el cauce legal para lograrlo es esta Directiva. Pero solo cubre los daños ocasionados por defectos de fabricación a condición de que el perjudicado pueda demostrar el daño real, el defecto del producto y la relación causa efecto entre defecto y daño.

        En la medida en que a los sistemas de IA se les puede dotar de capacidades de adaptación y aprendizaje y el número de interrelaciones se complica, porque aprende de manera autónoma o interactúe con su entorno de forma imprevisible, esta legislación es insuficiente.

    b. Si, por el contrario, el daño es causado por un tercero que interfiere, sería de aplicación el sistema de responsabilidad basado en la culpa de los diferentes EEMM. Es aquí donde habría que buscar la armonización de los diferentes marcos jurídicos teniendo como objeto que al fin y al cabo se trata de establecer el marco regulatorio de un mercado único o común.

    c. En cualquier caso, no se debe limitar el tipo de alcance de los daños y perjuicios que puedan ser objeto de compensación, ni limitar la naturaleza de dicha compensación, por el único motivo de que los daños y perjuicios hayan sido causados por un agente no humano.

    d. Una vez que las partes en las que incumba la responsabilidad última hayan sido identificadas, dicha responsabilidad debería de ser proporcional al nivel real de las instrucciones impartidas a la IA y a su grado de autonomía.

    En España, además la responsabilidad por daños causados por productos defectuosos está regulada por el **TRLCU** (Texto refundido de la Ley de **consumidores y usuarios**) en sus art. 128 a 149 establece la responsabilidad civil tanto por bienes como por servicios defectuosos.

2) **RGPD** (Reglamento general de Protección de datos) o la **normativa de protección del consumidor vigente**, es la adecuada en el caso de que los daños que causen los sistemas de IA afecten a derechos personales y/o a otros intereses importantes protegidos por ley incluidos aquellos relativos al uso de datos biométricos o por técnicas de reconocimiento facial.

3) **La atribución de personalidad jurídica a la IA,** es un debate superado y una opción que parece ya considerada obsoleta por la mayoría de las instituciones europeas, aunque no se descarta quizás más a largo plazo, cuando los sistemas devengan más autónomos. No obstante, un **seguro de responsabilidad civil adecuado según el riesgo** que sea exigible a los desplegadores de sistemas de IA, es una opción que cobra más sentido, en tanto en cuanto el riesgo de provocar daños vaya en aumento. Queda descartado en aquellas situaciones en las que el uso o aplicaciones de IA no lleven aparejado ningún riesgo.

4) Este informe pone de manifiesto un vacío legal en cuanto a la **responsabilidad de los implementadores o utilizadores** de los sistemas de IA. Aunque estas personas están decidiendo sobre su uso de sistemas, son quienes ejercen control sobre los riesgos asociados y se benefician de sus operaciones, muchas de las reclamaciones de responsabilidad contra ellos fracasarían debido a la incapacidad de las personas afectadas para probar la culpa del implementador.
   Es muy difícil establecer un nexo de unión que pruebe su culpa por el daño sufrido en la mayoría de los casos, sobre todo si el daño fue causado en un ámbito público, donde no existe una relación contractual con enorme grupo de personas afectadas.

   El *Parlamento Europeo* propone dos formas de resolver este vacío según el nivel de riesgo que conlleve el sistema de IA:

   a. Si se trata de un sistema de IA de alto riesgo, el implantador debe de estar sujeto a un **régimen de responsabilidad objetiva estricta** e indemnizar a la víctima por cualquier daño sufrido en sus derechos legalmente protegidos (vida, salud, integridad física y propiedad) provocados por una actividad física o virtual de esos sistemas.

   b. Para el resto de los sistemas (todos los que no sean de alto riesgo) se prevé un sistema de responsabilidad basada en la culpa que admitirá prueba en contrario si el sistema fue activado sin su consentimiento o si hubiera desplegado la diligencia exigible en la elección, utilización y mantenimiento del sistema.

5) Los **tres elementos que componen los sistemas de IA** son al menos un **software**, el **algoritmo** y los **datos tratados**. Hay que añadir aquí la casi total ausencia de responsabilidad de los productores de *software* por programas inseguros o defectuosos. La gran mayoría del *software* que utilizamos hoy en día se rige por *contratos de licencia* que excluyen la responsabilidad por daños en el que no los desarrolladores ni los vendedores asumen su responsabilidad por sus productos. Todas estas licencias incluyen la **cláusula *"as is"*** o "***tal cual***" que excluye no solo cualquier garantía sobre el software licenciado sino que traslada el riesgo al usuario.

   El TRLC de protección de los consumidores establece que ninguna cláusula contractual ha de disminuir la responsabilidad del productor frente al perjudicado, lo que, es práctica habitual en la redacción de contratos de licencia de *software*, incluido el embebido en producto, lo que hace entrar en colisión la normativa de producto defectuoso con la práctica avalada jurisprudencialmente en el mundo del desarrollo de *software*.

   Por ello, parece que tanto la Directiva de productos defectuosos como el propio acervo comunitario dista de ser apto para los fines de determinar la responsabilidad del productor o prestador de los dispositivos o servicios IoT (también aplicable a sistemas de IA), y necesita revisión.

6) Se deberán **de crear mecanismos para la evaluación y mitigación de los riesgos** asociados a la IA que afectan directamente a la protección de los derechos fundamentales (protección de datos personales, privacidad o no discriminación). Que pueden estar originados por defectos en el diseño general de los sistemas de IA, por uso de datos sesgados, fallos de ciberseguridad o conectividad en infraestructuras clave, usos malintencionados, problemas de interacción entre personas y máquinas…

   La implantación de **planes de evaluación de los riesgos** en el que se identifiquen los más críticos, instaurando controles generales estrictos para guiar el desarrollo y el uso de los sistemas de IA, asegurar una supervisión adecuada y crear procedimientos y planes de contingencia sólidos. Siendo necesario el **ajuste de las normas de seguridad** comunitarias sobre seguridad de los productos y a la vez garantizar la información de los usuarios sobre cómo utilizar esos productos y protegerles contra posibles daños.

   Estos controles deberán abordar temas como los datos y su análisis o la ciberseguridad, para evitar posibles quiebras de la seguridad, un elevado nivel de seguridad y protección de los datos personales, en el que se asegure aplicar los principios de "*accountability*", "*privacy by design*" y "*by default*" y obligatoriedad de la Evaluación de Impacto en la Protección de Datos Personales (EIPD) que consiste en un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y en función del resultado obtenido se adoptaran las medidas necesarios para la gestión de dichos riesgos y así eliminarlos o mitigarlos.

   Por otra parte, y como último apunte a este ensayo, dada la funcionabilidad cambiante de los sistemas de IA que se actualiza o por su aprendizaje automático puede añadir nuevas funciones a la vida útil de la IA generando nuevos riesgos no contemplados en el momento de la comercialización. Es conveniente el establecimiento controles ex *ante y ex post*, que se amolden a los constantes cambios y actualizaciones de estas que actualmente no están contemplados en las legislaciones europeas.