

Decálogo de la inteligencia artificial ética y responsable en la Unión Europea

Alberto J. Tapia Hermida

Catedrático de Derecho Mercantil. UCM

Socio de Estudio Jurídico Sánchez Calero

Diario La Ley, Nº 9749, Sección Tribuna, 4 de Diciembre de 2020, Wolters Kluwer

Normativa comentada
Comentarios

I. El falso mito de lo alortinos neutrales y la necesaria regulación de la inteligencia artificial

Aun cuando no existen análisis estadísticos certeros, podemos aventurar —sin miedo a errar en exceso— que entre el 80 y el 90 por ciento de nuestras actividades de la vida diaria están condicionadas por el uso de la inteligencia artificial. Y podemos constatar también que estos usos de la inteligencia artificial permanecen, en una grandísima medida, como «terra ignota» de la regulación y el control público. Por si este dato no fuera relevante de por sí, hemos de añadir que tales usos se realizan por entidades que, en la mayoría de los casos, carecen de personalidad y están localizadas «en las nubes» (y no sólo en sentido informático). *Item* más, usamos y padecemos los usos de la inteligencia artificial de forma mayoritariamente inconsciente, desnudando nuestras intimidades ante «cookies» que nos invaden con el uso de algoritmos que detectan y redirigen nuestros consumos e ideas sin que nosotros seamos más que pequeños barcos de papel en la tormenta global orquestada por las grandes corporaciones que operan a modo de elites extractivas de nuestro esfuerzo.

Lo anterior viene a cuento porque nos parece que no debemos comenzar a hablar de la inteligencia artificial ética y responsable sin traer a colación una idea que llevamos madurando un cierto tiempo en el ámbito de la digitalización financiera. Se trata del «**mito de los algoritmos neutrales**», que acompaña a la «*paradoja de la transparencia digital*» (1). Con el «*mito de los algoritmos neutrales*» nos hemos referido al contraste entre:

- a) La afirmación generalizada de que el uso de algoritmos en las finanzas tiene un impacto neutral en el sentido de que no afecta a los riesgos que se generan para el consumidor porque se asientan sobre registros interconectados imposibles de manipular (por ejemplo, en el caso del blockchain). Es más, las campañas publicitarias de las grandes entidades financieras anuncian de manera idílica, pomposa e insistente la digitalización de sus servicios bancarios como un remedo del paraíso terrenal, sin advertir del enorme efecto que tiene de exclusión de grandes capas de población que —por razones de edad o de capacidad económica— carecen de acceso a la red y de conocimientos para utilizarla; amén de los enormes costes labores y el cierre masivo de sucursales.
- b) La realidad tozuda y constatable —por ejemplo, cuando se examina la jurisprudencia sobre delincuencia financiera digital— de que los algoritmos pueden mentir, engañar y manipular (y ser manipulados) —y de hecho lo hacen— mediante, por ejemplo, prácticas en el mercado de valores de multiplicación patológica de órdenes («quote stuffing»), de indicios falsos («spoofing»), de órdenes contradictorias prácticamente simultáneas («churning») y de anticipación parasitaria («sniffers»). Procede mencionar, en este sentido, la advertencia de la CNMV de 18 de noviembre de 2020 sobre nuevos fraudes informáticos en el mercado financiero al calor del COVID 19 que constata como, en los últimos meses, se están recibiendo en la CNMV testimonios de inversores españoles sobre el uso de nuevas herramientas informáticas por parte de los conocidos como chiringuitos financieros que recurren a dos herramientas digitales: el *software* de acceso remoto (como AnyDesk, LogMeIn, TeamViewer, etc.) y las redes privadas virtuales (servicios de VPN).

Sin llegar al ámbito estrictamente delincencial, podemos constatar como, durante la pandemia del COVID 19, los algoritmos han sido instrumentos decisivos para las estrategias inversoras «bajistas» que han atacado, dentro del IBEX 35, las cotizaciones de ACS, CIE, AUTOMOTIVE, MELIA, NATURGY, etc.

Por lo anterior, cuando decimos que llevamos algunos años intentando destruir el «*mito de los algoritmos neutrales*» aplicamos el siguiente silogismo elemental: si el ser humano puede mentir, manipular y ser manipulado; y si los algoritmos son obra del ser humano; entonces, los algoritmos pueden mentir, engañar, manipular y ser manipulados.

Es precisa una labor regulatoria que identifique a los responsables del uso de algoritmos, prevenga y sancione este tipo de prácticas en defensa de los consumidores

Por ello, es precisa una labor regulatoria que identifique los responsables del uso de los algoritmos y prevenga y sancione este tipo de prácticas en defensa de los consumidores, sean estos clientes bancarios, inversores o asegurados.

Con todo lo anterior, nos parece que hemos justificado sobradamente el interés y la necesidad de regular la inteligencia artificial para garantizar su uso ético y responsable.

II. Las dos resoluciones el Parlamento Europeo de 20 de octubre de 2020 sobre una inteligencia artificial ética y responsable

El 20 de octubre de 2020, el Parlamento Europeo (PE) aprobó dos Resoluciones que se refieren a la Inteligencia Artificial (2) :

- a) La Resolución del Parlamento Europeo, de 20 de octubre de 2020 (LA LEY 22995/2020), con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)) que lleva por título «Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas» (p9_ta-prov(2020)0275). La denominaremos Resolución sobre la Inteligencia Artificial Ética (RIAE).
- b) La Resolución del Parlamento Europeo, de 20 de octubre de 2020 (LA LEY 19743/2020), con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) que lleva por título «Régimen de responsabilidad civil en materia de inteligencia artificial» (P9_TA-PROV(2020)0276). La denominaremos Resolución sobre la Inteligencia Artificial Responsable (RIAR).

III. Decálogo de los principios regulatorios de la inteligencia artificial en la UE

Ofrecemos seguidamente una síntesis (3) de estas Resoluciones del PE preparatorias de una nueva regulación de la UE para implantar una inteligencia artificial ética y responsable en forma de un decálogo de diez principios regulatorios de la IA en la UE que inferimos de la RIAE y de la RIAR; todo ello para facilitar su exposición y su comprensión:

1. Control de riesgos

Este primer enfoque regulatorio tan sensible para la digitalización financiera —porque recordemos que el mercado financiero es un mercado que gestiona riesgos futuros (por ejemplo, en su sector asegurador o del mercado de valores)— se manifiesta en varias partes de la RIAE (LA LEY 22995/2020). Así, el PE «*hace hincapié en que toda futura regulación ha de seguir un enfoque basado en el riesgo y orientado al futuro para regular la inteligencia artificial, la robótica y las tecnologías conexas, con normas tecnológicamente aplicables a todos los sectores y con normas sectoriales cuando proceda*».

En este último aspecto el PE destaca que —para «*garantizar la aplicación uniforme del sistema de evaluación de riesgos y el respeto de las obligaciones jurídicas conexas y para asegurar la igualdad de condiciones entre los Estados miembros y prevenir la fragmentación del mercado interior*»— hay que diferenciar dos grandes sectores de la IA atendiendo el criterio del riesgo que producen para sus usuarios (apartado 12 (LA LEY 22995/2020) y ss.):

- a) Los sectores de alto riesgo, determinados por inclusión mediante la elaboración de una lista exhaustiva y acumulativa de sectores de alto riesgo y de usos o fines de alto riesgo; lista debe someterse a una reevaluación periódica. A tal efecto, el PE considera que, para determinar si la inteligencia artificial, la robótica y las tecnologías conexas deben considerarse de alto riesgo, es necesario basarse siempre en una evaluación *ex ante* imparcial, regulada y externa apoyada en criterios concretos y definidos. De tal manera que la inteligencia artificial, la robótica y las tecnologías conexas deben considerarse de alto riesgo cuando

su desarrollo, despliegue y uso entrañen un riesgo significativo de causar lesiones o daños a particulares o a la sociedad, vulnerando los derechos fundamentales y las normas de seguridad establecidas en el Derecho de la Unión. En concreto, para evaluar si las tecnologías de inteligencia artificial entrañan un riesgo de ese tipo, el PE considera que deben tenerse en cuenta el sector en el que se desarrollan, despliegan o utilizan, su uso o finalidad específicos y la gravedad de la lesión o daño que cabe esperar que se produzca de forma acumulativa.

b) Los sectores que no son de alto riesgo, determinados por exclusión lógica respecto de los anteriores.

2. Protección de los consumidores amplio en sentido subjetivo, geográfico y funcional

Este segundo principio regulatorio de la IAE relacionado con la digitalización financiera se manifiesta en esta RIAE cuando el PE se refiere a los «consumidores y mercado interior» subrayando la importancia de que haya una protección amplia de los consumidores porque el marco regulador para la inteligencia artificial se aplique con amplitud en sentido (apartado 78 (LA LEY 22995/2020) y ss.):

a) Subjetivo, para que comprenda aquellos casos en que los consumidores se vean afectados por un sistema algorítmico en sus diferentes papeles: como usuarios de un sistema algorítmico, estén sujetos a tal sistema, sean los destinatarios de tal sistema o estén orientados a él.

b) Geográfico, ya que se protegerá al consumidor independientemente del lugar en que estén establecidas las entidades que desarrollen, comercialicen o utilicen el sistema de IA.

c) Funcional, porque el marco de protección del consumidor debe aplicarse a todos los desarrolladores y a toda la cadena de valor de los sistemas de IA, a saber: el desarrollo, el despliegue y el uso de las tecnologías pertinentes y sus componentes).

3. Seguridad, transparencia y rendición de cuentas

Este tercer principio regulatorio relevante para la digitalización financiera —porque recordemos que el mercado financiero es, en esencia, un mercado cibernético cuya materia prima es, en última instancia, la información— se manifiesta en varios apartados de esta RIAE cuando el PE *«recuerda que el derecho a la información de los consumidores constituye un principio fundamental en virtud del Derecho de la Unión, y subraya que, en consecuencia, debe respetarse plenamente en relación con la inteligencia artificial, la robótica y las tecnologías conexas»*. De esta idea general deriva dos consecuencias sobre el alcance de la transparencia que debe abarcar (apartado 17 (LA LEY 22995/2020) y ss.):

a) La interacción con los sistemas de inteligencia artificial, incluidos los procesos de automatización.

b) Su modo de funcionamiento y sus capacidades (por ejemplo la manera en que se filtra y presenta la información) su exactitud y sus limitaciones.

c) La forma en que dicha información debe ser facilitada a las autoridades nacionales de control y a las autoridades nacionales de protección de los consumidores.

4. Igualdad: prevención de la discriminación automatizada

Este cuarto principio regulatorio relacionado con la digitalización financiera (por ejemplo, en la selección de asegurados por las entidades aseguradoras) también se manifiesta en varios apartados de esta RIAE cuando el PE se refiere a una regulación «sin sesgo y sin discriminación» (apartado 27 (LA LEY 22995/2020) y ss.).y *«recuerda que la inteligencia artificial, dependiendo de su desarrollo y de su uso, puede crear y reforzar sesgos, también a través de sesgos inherentes a los conjuntos de datos subyacentes, y, por lo tanto, crear diversas formas de discriminación automatizada, incluida la discriminación indirecta, en particular en relación con grupos de personas con características similares»*. Por lo tanto, el PE pide a la Comisión y a los Estados miembros que adopten todas las medidas posibles para evitar tales sesgos y para garantizar la plena protección de los derechos fundamentales. En concreto, el PE hace hincapié en la necesidad evitar que los sesgos culturales y de género se incluyan involuntariamente en los algoritmos, sistemas y aplicaciones de la inteligencia artificial.

5. Responsabilidad

Este quinto principio regulatorio especialmente sensible para la digitalización financiera se manifiesta en dos formas:

A) Responsabilidad social

En primer lugar, en una forma genérica de responsabilidad social, donde las entidades financieras juegan un rol de liderazgo, cuando esta RIAE se refiere a la «responsabilidad social y paridad de género» y recoge que el PE «*hace hincapié en que la inteligencia artificial, la robótica y las tecnologías conexas socialmente responsables tienen un papel que desempeñar en la búsqueda de soluciones que salvaguarden y promuevan los valores fundamentales de nuestra sociedad*» (4) . En el ámbito financiero destaca, en especial, la importancia que reviste conseguir un alto nivel de alfabetización digital general y formar profesionales altamente cualificados en este ámbito, así como garantizar el reconocimiento recíproco de estas formaciones en toda la Unión (apartado 37 (LA LEY 22995/2020) y ss.).

B) Responsabilidad civil

En segundo lugar, este principio regulatorio se expresa en una forma específica de responsabilidad civil, donde las entidades financieras deben garantizar la cobertura por los daños que puedan causar a su clientela a resultados del empleo de la inteligencia artificial (por ejemplo, los daños exigibles a un banco por ejecución errónea de servicios de pagos digitales). Se desarrolla específicamente en la Resolución del Parlamento Europeo, de 20 de octubre de 2020 (LA LEY 19743/2020), con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(IN)).

6. Imputabilidad

Este principio regulatorio específico de una Inteligencia Artificial Responsable (IAR) —que guarda relación directa con el presupuesto regulatorio de la potencialidad dañina de los sistemas de IA y resulta especialmente relevante en materia de digitalización financiera— se establece en la RIAR (LA LEY 19743/2020) con un doble alcance:

A) Imputabilidad general a un agente: la lucha contra indefensión en la que se encuentran los consumidores

En primer lugar, como imputabilidad general a un agente que prevenga la indefensión en la que se encuentran los consumidores que usan de ingenios basados en la IA. Así, en su parte introductoria, la RIAR (LA LEY 19743/2020) advierte de la indefensión en la que se encuentran los consumidores que usan de ingenios basados en la IA para exigir responsabilidad a las entidades que operan con ellos (por ejemplo, las entidades financieras cuando prestan servicios de pago digitalizados) (5) . Después, la RIAR, al referirse a la «responsabilidad civil del operador» insiste en la idea de la indefensión en la que se encuentran los consumidores que usan de ingenios basados en la IA (6) (apartado 11 (LA LEY 19743/2020)).

B) Imputabilidad específica al operador de la inteligencia artificial: operador inicial, operador final y ejercicio de control

En segundo término, se expresa como imputabilidad específica que identifique de forma unívoca al agente de la IA causante del daño y responsable de indemnizarlo cuando el PE considera adecuado que establecer una noción amplia de «operador» que abarque tanto al operador final (7) como al operador inicial (8) . En ambos casos, estas identificaciones deben basarse en el concepto de «ejercicio del control» (9) abarcando todo el desarrollo del proceso de aplicación de la inteligencia artificial (10) .

Después, la RIAR (LA LEY 19743/2020) matiza este principio de imputabilidad específica en situaciones complejas en las que haya más de un operador, por ejemplo, un operador final y un operador inicial. *Porque*, entonces, la protección de la víctima perjudicada exige que todos los operadores deban ser responsables civiles solidarios. Lo que, a su vez, plantea el derecho a reclamar en la vía de regreso unos de otros de forma proporcional conforme a los porcentajes de responsabilidad determinados por los respectivos niveles de control que tengan los operadores sobre el riesgo relacionado con la operación y el funcionamiento del sistema de IA, lo que exige, a su vez, garantizar la trazabilidad de los productos con el fin de identificar mejor a los que intervienen en las distintas fases (apartado 12 (LA LEY 19743/2020) y ss.)

7. Adaptabilidad: Adecuación del régimen de responsabilidad civil a los sistemas de IA de alto riesgo y de riesgo normal

Este principio regulatorio específico de una Inteligencia Artificial Responsable (IAR) —que también resulta especialmente relevante en materia de digitalización financiera, por cuanto el mercado financiero está plagado de sistemas de IA autónomos de alto riesgo— se establece en el RIAR (LA LEY 19743/2020) cuando, al referirse a las

«normas en materia de responsabilidad civil diferentes para riesgos diferentes», comienza recordando que el tipo de sistema de IA sobre el que el operador ejerce control es un factor determinante en lo que respecta a la responsabilidad y de ahí deduce una necesidad de asumir una distinción básica entre dos tipos de sistemas de IA: los de alto riesgo y los de riesgo normal.

La distinción básica mencionada obedece a que un sistema de IA que conlleve un alto riesgo inherente y actúe de manera autónoma pone en peligro potencial en mucha mayor medida al público en general. De lo que el PE infiere *«habida cuenta de los retos jurídicos que plantean los sistemas de IA para los regímenes de responsabilidad civil existentes, parece razonable establecer un régimen común de responsabilidad objetiva para los sistemas de IA autónomos de alto riesgo»* (11) (apartado 14 (LA LEY 19743/2020) y ss.).

8. Cobertura preventiva

A) Especial relevancia para la digitalización financiera

Este tercer principio regulatorio específico de una Inteligencia Artificial Responsable (IAR) resulta especialmente relevante en materia de digitalización financiera por concurrir las dos circunstancias siguientes:

- a) Porque el alto riesgo de los sistemas de IA implicados en la digitalización financiera hace especialmente necesario prever la cobertura preventiva de la responsabilidad civil en que puedan incurrir los operadores financieros.
- b) Porque los instrumentos de cobertura preventiva tienen carácter financiero, como el seguro de responsabilidad civil o las garantías bancarias.

En este punto, el RIAR (LA LEY 19743/2020) — al referirse a los «seguros y sistemas de IA»— manifiesta que el PE *«considera que la cobertura de la responsabilidad civil es uno de los factores clave que define el éxito de las nuevas tecnologías, productos y servicios; observa que una cobertura de la responsabilidad civil adecuada es también esencial para garantizar que el público pueda confiar en la nueva tecnología, a pesar de las posibilidades de sufrir un daño o de hacer frente a demandas judiciales por parte de las personas afectadas; observa, al mismo tiempo, que este sistema regulador se centra en la necesidad de explotar y potenciar las ventajas de los sistemas de IA, a la vez que se establecen sólidas salvaguardias»* (apartado 23 (LA LEY 19743/2020)).

B) Exigencia de un seguro obligatorio de responsabilidad civil para los operadores de sistemas de IA de alto riesgo

Esta cobertura preventiva mediante un seguro de responsabilidad civil obligatorio parte de la consideración general de que la cobertura de la responsabilidad civil es uno de los factores clave que definirá el éxito de las nuevas tecnologías, productos y servicios y concreta esta idea general en otras dos derivadas:

- a) La apreciación específica de la necesidad de establecer una cobertura preventiva de la responsabilidad civil por el uso de la IA mediante un seguro obligatorio para los sistemas de IA de alto riesgo que debe cubrir los importes y el alcance de la indemnización establecidos legalmente. De tal manera que todos los operadores de sistemas de IA de alto riesgo deberán ser titulares de un seguro de responsabilidad civil cuyos perfiles resultan difíciles de precisar en la actualidad porque, en la actualidad, dicha tecnología es todavía muy inusual, ya que presupone un alto grado de toma de decisiones autónomas. En todo caso, el PE considera que la incertidumbre relacionada con los riesgos no debe hacer que las primas de seguro sean prohibitivamente elevadas y convertirse así en un obstáculo para la investigación y la innovación. En este sentido, el PE considera que la falta de datos sobre los riesgos asociados a los sistemas de IA, unida a la incertidumbre sobre su evolución en el futuro, dificulta al sector de los seguros elaborar productos de seguro nuevos o adaptados y que, por lo tanto, es probable que dejar el desarrollo de un seguro obligatorio plenamente al mercado resulte en un enfoque de «talla única» con primas desproporcionadamente elevadas y los incentivos equivocados, alentando a los operadores a optar por el seguro más barato en lugar de por la mejor cobertura, lo que podría convertirse en un obstáculo para la investigación y la innovación.
- b) La estimación del PE de que «un mecanismo de indemnización a escala de la Unión, financiado con fondos públicos, no es la manera adecuada de colmar posibles lagunas en materia de seguros».

Una vez establecida esta necesidad de un seguro obligatorio para los sistemas de IA de alto riesgo análogo al

seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles; la RIAR (LA LEY 19743/2020) apunta las dificultades que su implantación conllevará que pueden exponerse en forma de causa y efecto:

- a) La causa será la falta de estadísticas de siniestralidad, porque esta ausencia de datos sobre los riesgos asociados a los sistemas de IA, unida a la incertidumbre sobre su evolución en el futuro, dificulta al sector de los seguros elaborar productos de seguro nuevos o adaptados.
- b) El efecto consistirá en el riesgo de que el mercado asegurador diseñe un seguro obligatorio de «talla única» con primas desproporcionadamente elevadas y los incentivos equivocados, alentando a los operadores a optar por el seguro más barato en lugar de por la mejor cobertura, lo que podría convertirse en un obstáculo para la investigación y la innovación. De ahí infiere *«que la Comisión debe colaborar estrechamente con el sector de los seguros para estudiar la forma de poder utilizar datos y modelos innovadores para crear pólizas de seguro que ofrezcan una cobertura adecuada a un precio asequible»*.

9. Sostenibilidad

Este principio regulatorio específico de la Inteligencia Artificial Ética (IAE) parte de la estimación de que el desarrollo de la inteligencia artificial, la robótica y las tecnologías conexas puede contribuir asimismo a alcanzar los objetivos de sostenibilidad del Pacto Verde Europeo en gran diversidad de sectores; puede potenciar el impacto de las políticas en la protección medioambiental; y pueden contribuir a reducir la congestión del tráfico y las emisiones de gases de efecto invernadero y de contaminantes atmosféricos.

10. Gobernabilidad

A modo de conclusión, podemos citar la referencia que hace el PE en el RIAE (LA LEY 22995/2020) a la «buena gobernanza» diciendo que «hace hincapié en que una gobernanza adecuada del desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas, especialmente las tecnologías de alto riesgo, también mediante la adopción de medidas centradas en la rendición de cuentas y el tratamiento de los posibles riesgos de sesgo y discriminación, puede hacer que aumente la seguridad y la confianza de los ciudadanos en dichas tecnologías».

En este punto, destaca, por último, la Certificación Europea de Conformidad Ética al que se refiere, en especial, el PE en la RIAE cuando propone que, en el marco de la coordinación al nivel de la Unión, se elaboren criterios comunes y un procedimiento de solicitud para la concesión de un certificado europeo de conformidad ética, que fomentaría la ética por diseño a lo largo de toda la cadena de suministro de los ecosistemas de inteligencia artificial. Certificación que podría ser, en el caso de las tecnologías de alto riesgo, un requisito previo obligatorio para la admisibilidad en los procedimientos de contratación pública sobre inteligencia artificial, robótica y tecnologías conexas y, en el caso de cualquier operario o usuario de tecnologías no consideradas de alto riesgo, un instrumento para certificar la evaluación positiva de la conformidad que haya llevado a cabo la autoridad nacional de control correspondiente.

(1) Sobre ambos se puede ver nuestro estudio «Las tecnofinanzas (FINTECH). Retos a la regulación y a la supervisión financieras» publicado en la Revista Iberoamericana del Mercados de Valores (RIMV) n.º 54 (julio 2018), pp. 1 y ss.

(2) Ver Diario La Ley n.º 44, 10 de noviembre de 2020 «El Parlamento Europeo aprueba su propuesta de regulación de la Inteligencia Artificial» y las entradas de nuestro blog financiero (ajtapia.com) de 12 de noviembre de 2010 sobre «Digitalización financiera: Los 7 principios regulatorios de una Inteligencia Artificial Ética (IAE) en la UE. Resolución del Parlamento Europeo de 20 de octubre de 2020 sobre los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas» y de 13 de noviembre de 2020 sobre «Digitalización financiera: Los 3 principios regulatorios de una Inteligencia Artificial Responsable (IAR) en la UE. Resolución del Parlamento Europeo de 20 de octubre de 2020 sobre la responsabilidad civil en materia de inteligencia artificial».

(3) El contenido de ambas Resoluciones sobre una IA ética y responsable será objeto de un examen más extenso y detallado en el estudio sobre *«Regulación de la inteligencia artificial en la Unión Europea. Ética y responsabilidad»* que publicaremos en el próximo número 87 de diciembre de 2020 de La Ley Unión Europea.

(4) Se refiere, en especial a *«la democracia, el Estado de Derecho, la pluralidad e independencia de los medios de comunicación y una información objetiva y de libre acceso, la salud y la prosperidad económica, la igualdad de oportunidades, los derechos sociales y laborales de los trabajadores, una educación de calidad, la protección de la infancia, la diversidad cultural y lingüística, la paridad de género, la alfabetización digital, la innovación y la creatividad; recuerda la necesidad de velar por que los intereses de todos los ciudadanos, incluidos los que están marginados o en situación de vulnerabilidad, como las personas con discapacidad, sean tenidos en cuenta y estén representados debidamente»*.

- (5) En este sentido, la RIAR (LA LEY 19743/2020) dice: «Considerando que ciertos sistemas de IA presentan importantes retos jurídicos para el actual marco de responsabilidad civil y podrían dar lugar a situaciones en las que su opacidad podría hacer extremadamente costoso, o incluso imposible, determinar quién controlaba el riesgo asociado al sistema de IA o qué código, entrada o datos han provocado en última instancia el funcionamiento lesivo; que este factor podría dificultar la identificación de la relación entre el daño o perjuicio y el comportamiento que lo causa, con el resultado de que las víctimas podrían no recibir una indemnización adecuada».
-
- (6) Cuando refleja que el PE «opina que las normas en materia de responsabilidad civil que afectan al operador deben cubrir todas las operaciones de los sistemas de IA, independientemente de dónde se lleve a cabo la operación y de que esta sea física o virtual; observa que las operaciones en espacios públicos que exponen a muchas personas a un riesgo constituyen, sin embargo, casos que requieren una consideración más profunda; considera que a menudo las víctimas potenciales de daños o perjuicios no son conscientes de la operación y no suelen disponer de derechos a reclamar por responsabilidad contractual contra el operador; señala que, si se produce un daño o perjuicio, esas personas solo tendrían una pretensión por responsabilidad subjetiva y podrían tener dificultades para demostrar la culpa del operador del sistema de IA, por lo que podrían fracasar las correspondientes demandas por responsabilidad civil».
-
- (7) «Debe entenderse la persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento».
-
- (8) «Debe entenderse la persona física o jurídica que define, de forma continuada, las características de la tecnología, proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA».
-
- (9) «Se entiende cualquier acción del operador que influya en el funcionamiento del sistema de IA y, por consiguiente, en la medida en que expone a terceros a sus potenciales riesgos».
-
- (10) El PE «considera que esas acciones podrían afectar al funcionamiento de un sistema de IA desde el inicio al fin, al determinar la entrada, la salida o los resultados, o podrían cambiar las funciones o procesos específicos dentro del sistema de IA».
-
- (11) Además, el PE «subraya que este enfoque basado en el riesgo, que puede incluir varios niveles de riesgo, debe basarse en criterios claros y una definición adecuada de «alto riesgo», así como ofrecer seguridad jurídica; (...) cree que un sistema de IA presenta un alto riesgo cuando su funcionamiento autónomo conlleva un potencial significativo de causar daño a una o más personas, de forma aleatoria y yendo más allá de lo que cabe esperar razonablemente; considera que, a la hora de determinar si un sistema de IA es de alto riesgo, también debe tenerse en cuenta el sector en el que cabe esperar que surjan riesgos importantes y la naturaleza de las actividades realizadas; considera que la magnitud del potencial depende de la relación entre la gravedad del posible daño, la probabilidad de que el riesgo cause un daño».
-