ESTUDIOS

DERECHO PRIVADO Y TECNOLOGÍA

PILAR CÁMARA ÁGUILA
ALICIA AGÜERO ORTIZ
DIRECTORAS

Centro de Investigación en Propiedad Intelectual CIPI

INCLUYE LIBRO ELECTRÓNICO

ARANZADI

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/

Primera edición: 2025

Depósito Legal: M-8451-2025
ISBN versión impresa con complemento electrónico: 978-84-1163-866-1
ISBN versión electrónica: 978-84-1163-865-4

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

Índice general

Página

Página

Página

Página

Página

Página

Página

CAPÍTULO 7

LA NUEVA REGULACIÓN EUROPEA DE LOS CRIPTOACTIVOS: EL REGLAMENTO EUROPEO SOBRE MERCADOS DE CRIPTOACTIVOS (REGLAMENTO MICA)

Página

Página

Página

CAPÍTULO 8

NUEVOS PARADIGMAS EN EL ECOSISTEMA DE PAGOS DIGITALES: DINERO TOKENIZADO, TOKENS DE PAGO Y TRANSACCIONES A TRAVÉS DE SMART CONTRACTS. HACIA LA AUTOMATIZACIÓN DE LOS PAGOS MEDIANTE INTELIGENCIA ARTIFICIAL

Página

Página

CAPÍTULO 11

RÉGIMEN DE GARANTÍAS DE BIENES DIGITALIZADOS, CONTENIDOS Y SERVICIOS DIGITALES

Página

Página

Página

Capítulo 1

Marco jurídico europeo sobre inteligencia artificial

PASCUAL MARTÍNEZ ESPÍN
Catedrático de Derecho Civil
Universidad de Castilla-La Mancha

SUMARIO: I. INTRODUCCIÓN. *1. Objeto. 2. La UE y el Reglamento de Inteligencia Artificial.* II. REGLAMENTO EUROPEO DE IA. *1. Contexto y objetivos. 2. Estructura del Reglamento. 3. Principales aspectos del RIA.* 3.1. Ámbito de aplicación. 3.2. Definiciones Clave. 3.3. Clasificación de riesgos. A. Sistemas de IA de riesgo inaceptable. B. Sistemas de IA de Alto Riesgo. C. Sistemas de IA de riesgo limitado. D. Sistemas de IA de riesgo mínimo. E. Modelos de Uso Generalizado con Riesgos Sistémicos. F. Tabla de riesgos. G. Regulación de las Inteligencias Artificiales Generativas y Modelos Fundacionales. *4. Obligaciones de los Proveedores, Importadores y Distribuidores de Sistemas de IA de Alto Riesgo.* 4.1. Obligaciones de los Proveedores de Sistemas de IA de Alto Riesgo. 4.2. Obligaciones de los Importadores de Sistemas de IA de Alto Riesgo. 4.3. Obligaciones de los Distribuidores de Sistemas de IA de Alto Riesgo. *5. Obligaciones de los usuarios de sistemas de IA de alto riesgo. 6. Impacto sobre los Derechos Fundamentales.* 6.1. Protección de Datos. 6.2. No discriminación. 6.3. Explicabilidad y transparencia. *7. Protección de datos y ciberseguridad. 8. Mecanismos de supervisión.* 8.1. Agencias de Supervisión. 8.2. Régimen sancionador. 8.3. Oficina Europea de IA. 8.4. Comité Europeo de IA. 8.5. Otros órganos. 8.6. Las autoridades públicas de los Estados miembros de la UE. *9. Relación con otras normativas.* 9.1. Reglamento General de Protección de Datos. 9.2. Relación con la Directiva de Seguridad de Productos. 9.3. Protección del Consumidor en el Contexto de la IA. *10. Innovación. 11. Valoración crítica del Reglamento.* 11.1. Impacto en la Innovación. 11.2. Complejidad

I. INTRODUCCIÓN

1. OBJETO

El propósito de este trabajo es examinar las medidas de índole jurídico-privado implementadas por la Unión Europea (UE) con el fin de establecer un marco jurídico comunitario en el ámbito de la inteligencia artificial.

2. LA UE Y EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

La Unión Europea ha tomado el liderazgo en la regulación de la inteligencia artificial (IA) con la introducción del Reglamento de Inteligencia Artificial (RIA) en abril de 2021, alcanzando un acuerdo provisional en diciembre de 2023. El principal objetivo del reglamento es garantizar que los sistemas de IA en la UE sean seguros, respeten los derechos fundamentales y fomenten la innovación tecnológica.

El rápido avance de la IA, aunque ofrece beneficios en áreas como la salud y la educación, plantea riesgos significativos, como la falta de transparencia en los algoritmos, lo que complica la aplicación de las leyes de seguridad y derechos fundamentales. El RIA busca equilibrar estos riesgos con las oportunidades de la IA, regulando su desarrollo y comercialización dentro de la UE para asegurar un mercado confiable y seguro.

El Reglamento (UE) 2024/1689, que entrará en vigor el 1 de agosto de 2024, establece un marco normativo para la IA, con aplicación completa a partir de agosto de 2026. Este marco clasifica los sistemas de IA en función de su nivel de riesgo, imponiendo requisitos más estrictos a aquellos considerados de alto riesgo. Tanto desarrolladores como empresas deberán cumplir con las normativas para garantizar que sus tecnologías respeten los estándares de seguridad y derechos fundamentales.

II. REGLAMENTO EUROPEO DE IA

El Reglamento (UE) 2024/1689 establece un marco legal integral para regular los sistemas de inteligencia artificial (IA) en la Unión Europea, respondiendo al rápido crecimiento de esta tecnología y sus impactos en los derechos fundamentales, la seguridad y la competitividad en el mercado interno. Su objetivo principal es equilibrar la innovación tecnológica con la protección de los derechos humanos, estableciendo normas claras para el desarrollo, comercialización y uso de sistemas de IA. Publicado el 12 de julio de 2024 en el Diario Oficial de la UE, el reglamento entró en vigor el 2 de agosto de 2024.

1. CONTEXTO Y OBJETIVOS

En los últimos años, la inteligencia artificial (IA) ha ganado gran relevancia, evidenciada por su creciente presencia en múltiples sectores y su inclusión entre las palabras más usadas en 2022 según la Real Academia Española. Este auge ha destacado la necesidad de regularla para equilibrar sus beneficios con una gestión adecuada de riesgos.

La Unión Europea (UE) ha avanzado en la creación de un marco normativo para la IA, respondiendo al compromiso político de la Presidenta Von der Leyen de abordar las implicaciones éticas y humanas de esta tecnología. El Libro Blanco de 2020 estableció las bases para fomentar la adopción de la IA y mitigar sus riesgos. La propuesta de Reglamento, tras consultas con diversas partes interesadas, busca garantizar que la IA sea confiable y alineada con los valores y derechos fundamentales de la UE.

El RIA tiene como principal objetivo crear un ecosistema de confianza para promover el uso seguro y legal de la IA, beneficiando al bienestar humano. Sus metas clave incluyen asegurar que el desarrollo y uso de la IA respeten los derechos fundamentales, como la privacidad y la protección de datos, creando además un entorno que fomente la innovación en IA y mantenga la competitividad global de la Unión Europea. También impone obligaciones de transparencia y responsabilidad a los operadores de sistemas de IA para garantizar la confianza de los usuarios.

El artículo 1 del RIA establece un marco jurídico uniforme para el uso y desarrollo de la IA en la UE, promueve una IA fiable alineada con los valores de la Unión, garantiza la protección de la salud, la seguridad y los derechos fundamentales frente a los riesgos que plantea esta tecnología, y apoya a las pequeñas y medianas empresas (pymes) y startups en el desarrollo de

nuevas tecnologías. Asimismo, asegura la libre circulación de bienes y servicios basados en IA dentro de la UE, evitando restricciones injustificadas por parte de los Estados miembros.

2. ESTRUCTURA DEL REGLAMENTO

El RIA, compuesto por 180 considerandos, 113 artículos y 13 anexos, establece un marco legal integral y flexible para la regulación de la inteligencia artificial en la Unión Europea.

En su Título I, define los términos clave y delimita su alcance, orientándose hacia la neutralidad tecnológica y asegurando su adaptabilidad a los avances futuros. La definición de «sistema de IA» es amplia, permitiendo que el reglamento siga siendo relevante frente a los cambios tecnológicos.

El Título II prohíbe ciertas prácticas de IA que presentan riesgos inaceptables, como la manipulación subliminal o la calificación social por parte de autoridades públicas, y restringe el uso de sistemas de identificación biométrica remota en espacios públicos, salvo excepciones limitadas.

El Título III clasifica los sistemas de IA de alto riesgo y establece requisitos rigurosos para su desarrollo y uso, incluyendo obligaciones sobre la calidad de los datos, transparencia, supervisión humana y ciberseguridad. La lista de estos sistemas puede ser actualizada conforme evolucione la tecnología.

El Título IV regula los sistemas de IA que interactúan directamente con personas, detectan emociones o generan contenido sintético, imponiendo la obligación de informar claramente a los usuarios cuando están interactuando con IA o en casos de ultrafalsificaciones.

En el Título V se promueve la innovación mediante sandboxes regulatorios, donde las empresas pueden desarrollar, probar y validar sistemas en un entorno controlado. Estas pruebas, supervisadas por autoridades competentes, permiten el uso de datos personales en proyectos de interés público, asegurando siempre la seguridad y los derechos fundamentales. Las autoridades nacionales también tienen la facultad de gestionar estos sandboxes y establecer criterios de participación, eximiendo a las empresas de sanciones por infracciones durante la fase de pruebas.

El Título VI establece una estructura de gobernanza a nivel europeo y nacional, incluyendo la creación del Comité Europeo de IA, encargado de armonizar la implementación del reglamento y apoyar la supervisión de los

sistemas de IA. Cada Estado miembro designará autoridades competentes para garantizar la correcta aplicación de las normas. El Título VII establece la obligación de registrar los sistemas de alto riesgo en una base de datos gestionada por la Comisión Europea, promoviendo la transparencia y facilitando la supervisión. El Título VIII se centra en las obligaciones de los proveedores en cuanto a la vigilancia post-comercialización y el reporte de incidentes graves, asegurando el cumplimiento mediante la cooperación entre las autoridades nacionales de supervisión de mercado.

El Título IX introduce la posibilidad de que los proveedores adopten voluntariamente códigos de conducta para sistemas de IA no clasificados como de alto riesgo, fomentando un comportamiento ético y responsable en áreas como sostenibilidad y accesibilidad.

El Título X establece medidas para proteger la confidencialidad de la información intercambiada durante la aplicación del reglamento, mientras que el Título XI otorga a la Comisión la facultad de adoptar actos delegados y de ejecución para actualizar las disposiciones del reglamento y adaptarlas a los avances tecnológicos. Finalmente, el Título XII fija un calendario para la aplicación gradual del reglamento, con plazos específicos para la implementación completa y revisiones periódicas para garantizar su efectividad a largo plazo.

3. PRINCIPALES ASPECTOS DEL RIA

La Unión Europea establece principios clave para la regulación de la inteligencia artificial, centrados en asegurar la supervisión y control humano. Entre estos principios destacan la prioridad de la seguridad, la transparencia en el desarrollo y aplicación de la IA, y la rendición de cuentas de los actores involucrados. Se exige que los sistemas de IA operen sin prejuicios, sesgos o discriminación, promoviendo la responsabilidad social y la igualdad de género. También se enfatiza el compromiso con la sostenibilidad ambiental y la protección estricta de la privacidad y los datos personales de los ciudadanos.

3.1. Ámbito de aplicación

El RIA abarca todos los sistemas de IA comercializados o utilizados en la Unión Europea (UE), independientemente de su origen. Incluye tanto sistemas autónomos como aquellos integrados en productos o servicios,

prestando especial atención a los sistemas clasificados como de alto riesgo, sujetos a requisitos adicionales de conformidad, gestión de riesgos y supervisión post-comercialización. Desde el punto de vista subjetivo, se aplica a proveedores que introducen sistemas en el mercado o los ponen en servicio en la UE, sin importar su ubicación; responsables del despliegue establecidos en la UE; proveedores y responsables en terceros países cuyos sistemas se utilicen en la UE; importadores y distribuidores que comercialicen sistemas; fabricantes que introduzcan sistemas junto con sus productos bajo su marca; representantes autorizados que actúan en nombre de proveedores fuera de la UE; y personas afectadas ubicadas en la UE por el uso de IA. En cuanto al ámbito objetivo, el Reglamento incluye excepciones, como las competencias de los Estados miembros en seguridad nacional; sistemas de IA con fines militares, de defensa o seguridad; investigación y desarrollo científico; y sistemas bajo licencias libres o de código abierto, excepto si son de alto riesgo. No se aplica a responsables del despliegue que sean personas físicas usando IA para actividades personales no profesionales.

3.2. Definiciones Clave

El Reglamento introduce una serie de definiciones esenciales para su correcta interpretación, entre las que destacan:

- **Sistema de IA**: Un sistema basado en una máquina que opera con diversos niveles de autonomía y que puede adaptarse después de su implementación. Diseñado para alcanzar objetivos explícitos o implícitos, este sistema infiere de la información de entrada la manera de generar resultados de salida, tales como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.
- **Sistema de IA de Alto Riesgo**: Se refiere a aquellos sistemas cuyo diseño o ámbito de aplicación pueden tener un impacto significativo sobre los derechos fundamentales, la seguridad o la salud de las personas.
- **Operador**: Cualquier persona física o jurídica que desarrolle, comercialice o utilice un sistema de IA.
- **Riesgo**: La combinación de la probabilidad de que se produzca un daño y la gravedad de dicho daño.
- **Proveedor**: Una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso

general, o que introduzca en el mercado o ponga en servicio dicho sistema de IA o modelo bajo su propio nombre o marca, ya sea con pago o de forma gratuita.

- **Responsable del Despliegue**: Una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, excepto cuando su uso sea en una actividad personal de carácter no profesional.
- **Evaluación de la Conformidad**: El proceso mediante el cual se verifica si un sistema de IA de alto riesgo cumple con los requisitos establecidos en el capítulo III, sección 2 del reglamento.
- **Datos Biométricos**: Datos personales obtenidos a partir de un tratamiento técnico específico, relacionados con las características físicas, fisiológicas o conductuales de una persona, tales como imágenes faciales o datos dactiloscópicos.
- **Espacio de Acceso Público**: Cualquier lugar físico, ya sea de propiedad privada o pública, al que pueda acceder un número indeterminado de personas, independientemente de las condiciones de acceso o restricciones de capacidad.
- **Modelo de IA de Uso General**: Un modelo de IA, incluyendo aquellos entrenados con grandes volúmenes de datos mediante autosupervisión a gran escala, que posee un grado considerable de versatilidad y puede realizar una amplia variedad de tareas de manera competente. Este modelo puede ser integrado en diversos sistemas o aplicaciones posteriores, salvo aquellos utilizados exclusivamente para investigación, desarrollo o creación de prototipos antes de su introducción al mercado.

3.3. Clasificación de riesgos

El RIA establece un marco regulatorio graduado que clasifica los sistemas de IA según su nivel de riesgo, desde mínimo hasta inaceptable. A medida que aumenta el riesgo, se incrementan las obligaciones regulatorias, con restricciones más estrictas para garantizar la seguridad. Los sistemas de IA considerados de riesgo extremo, que representan una amenaza grave para los derechos humanos, están prohibidos[1].

1. BARRIO ANDRÉS, M., (Dir.), «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial», en BARRIO ANDRÉS (Dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 35 y ss.

A. Sistemas de IA de riesgo inaceptable

El artículo 5 del RIA prohíbe los sistemas de IA que representen amenazas graves a la seguridad pública, privacidad y derechos fundamentales, con excepciones limitadas. Entre ellas, se permite la identificación biométrica remota en tiempo real en espacios públicos, solo para fines legales específicos y bajo condiciones estrictamente reguladas.

B. Sistemas de IA de Alto Riesgo

Los sistemas de IA de alto riesgo son aquellos que impactan sectores críticos como infraestructuras, salud, educación, empleo, servicios esenciales, seguridad, migración, justicia y procesos democráticos. Incluyen tecnologías que influyen en el comportamiento humano, como el reconocimiento de emociones, la puntuación ciudadana y la predicción policial. Debido a su potencial para afectar derechos fundamentales y la seguridad pública, están sujetos a estrictos requisitos regulatorios y rigurosas evaluaciones de riesgos.

La clasificación de un sistema de IA como de alto riesgo se basa en su impacto en sectores regulados, como infraestructuras críticas (agua, energía, transporte), salud (diagnósticos y tratamientos), educación y empleo (contratación y evaluaciones), servicios esenciales (banca y telecomunicaciones), identificación biométrica, aplicación de la ley y procesos judiciales. Se excluyen los sistemas de recomendación en grandes plataformas, regulados por otras normativas.

Los sistemas de IA de alto riesgo deben cumplir requisitos clave: alta calidad de los datos para evitar sesgos y asegurar representatividad, trazabilidad y documentación exhaustiva, transparencia en el funcionamiento y la lógica, supervisión humana constante para evitar automatizaciones sin control, y precisión y robustez frente a fallos o ataques. Además, deben establecer un sistema de gestión de riesgos continuo, con monitoreo y medidas preventivas para mitigar posibles riesgos.

En el caso de tecnologías de identificación biométrica, deben mantener registros detallados de su uso. Para evitar la automatización excesiva y asegurar un comportamiento ético, se requiere supervisión humana efectiva. Asimismo, se deben implementar controles avanzados de ciberseguridad para proteger los sistemas de ataques.

El Reglamento prohíbe el uso de IA para manipular comportamientos de manera perjudicial, especialmente en menores o personas vulnerables,

y para la puntuación social. Los sistemas de alto riesgo deben pasar una evaluación de conformidad antes de su comercialización, con una fase de autoevaluación interna y otra de certificación externa por organismos acreditados. Tras su lanzamiento, se exige monitoreo continuo y actualizaciones para mantener la seguridad y el cumplimiento normativo.

Este marco asegura que los sistemas de IA de alto riesgo sean desarrollados y gestionados con altos estándares de seguridad, ética y protección de los derechos fundamentales.

C. Sistemas de IA de riesgo limitado

Los sistemas de IA de propósito general, como los chatbots, presentan riesgos controlados. Es obligatorio informar a los usuarios que están interactuando con una IA, y el contenido generado, incluidos los deepfakes, debe ser claramente identificado. Estos requisitos de transparencia tienen como objetivo prevenir el uso indebido de la IA, incluso en situaciones de bajo riesgo.

D. Sistemas de IA de riesgo mínimo

Estos sistemas, como los videojuegos con IA o los filtros de spam, no están regulados específicamente debido a su bajo impacto. Los usuarios tienen la libertad de decidir sobre su uso, dado que no presentan riesgos significativos.

E. Modelos de Uso Generalizado con Riesgos Sistémicos

Los modelos de inteligencia artificial de uso generalizado, también llamados modelos fundamentales o de propósito general, presentan un riesgo sistémico debido a su versatilidad e impacto en múltiples sectores. Si fallan o se utilizan indebidamente, pueden comprometer infraestructuras críticas, sistemas financieros y otras áreas clave. Ejemplos de estos modelos incluyen GPT-4 de OpenAI y Gemini de Google DeepMind, clasificados como de riesgo sistémico cuando su capacidad computacional supera los 10^25 FLOPS.

El Reglamento establece requisitos estrictos para estos modelos avanzados, como evaluaciones periódicas para identificar y mitigar riesgos, pruebas adversarias para detectar vulnerabilidades explotables y la obligación de notificar incidentes graves a la Comisión Europea. También se exige la implementación

de medidas de ciberseguridad robustas y eficiencia energética adecuada para minimizar impactos ambientales y operativos. Es esencial que incluyan sistemas de moderación de contenidos para prevenir discursos de odio, desinformación y otros usos nocivos, especialmente en áreas como la salud.

Aunque el umbral de 10^25 FLOPS define los riesgos sistémicos, el Reglamento sugiere que podría aplicarse un sistema de cumplimiento más riguroso a todos los modelos fundamentales, sin importar su capacidad, para evitar resultados ilegales. Este sistema debe adaptarse a diferentes escalas empresariales, incluyendo a proveedores más pequeños. La Comisión Europea promueve la creación de códigos de conducta voluntarios que complementen las obligaciones legales y fomenten prácticas éticas en la operación de estos sistemas. Los modelos también estarán sujetos a auditorías periódicas y supervisión humana para garantizar el cumplimiento normativo y la protección de los derechos fundamentales.

Este enfoque colaborativo busca garantizar que el desarrollo de la IA se realice de manera segura y responsable, minimizando riesgos sistémicos y protegiendo a los usuarios durante todo el ciclo de vida del modelo.

F. Tabla de riesgos

Analicemos las distintas categorías de riesgos, indicando los supuestos comprendidos en las mismas (con ejemplos), y las consecuencias o medidas que prevé el Reglamento. La siguiente tabla nos ilustrará:

Categoría de riesgo	Supuestos	Consecuencias/medidas
Riesgo inaceptable	Sistemas de evaluación social[2]. Sistemas que constituyan una clara amenaza para la seguridad, los medios de vida y los derechos de las personas[3]. Manipulación de comportamiento humano[4].	Prohibido
Alto riesgo	Identificación facial a distancia[5]; Infraestructuras críticas que podrían poner en riesgo la vida y la salud de los ciudadanos[6]; Formación educativa o profesional, que puede determinar el acceso a la educación y el curso profesional de la vida de una persona (por ejemplo, puntuación de exámenes)[7];	Sistemas adecuados de evaluación y mitigación de riesgos; Alta calidad de los conjuntos de datos que alimentan el sistema para minimizar riesgos y resultados discriminatorios;

Categoría de riesgo	Supuestos	Consecuencias/medidas
Alto riesgo *(cont.)*	Componentes de seguridad de los productos (por ejemplo, aplicación de IA en cirugía asistida por robot)[8]; Empleo, gestión de trabajadores y acceso al autoempleo (por ejemplo, *software* de clasificación de CV para procedimientos de contratación)[9]; Servicios públicos y privados esenciales (por ejemplo, calificación crediticia que niega a los ciudadanos la oportunidad de obtener un préstamo)[10]; Aplicación de la ley que pueda interferir con los derechos fundamentales de las personas (por ejemplo, evaluación de la fiabilidad de las pruebas)[11]; Gestión de la migración, el asilo y el control de fronteras (por ejemplo, verificación de la autenticidad de los documentos de viaje)[12]; Administración de justicia y procesos democráticos (por ejemplo, aplicación de la ley a un conjunto concreto de hechos)[13].	Registro de actividad para garantizar la trazabilidad de los resultados; Documentación detallada que proporcione toda la información necesaria sobre el sistema y su propósito para que las autoridades evalúen su cumplimiento. Información clara y adecuada al usuario; Medidas apropiadas de supervisión humana para minimizar el riesgo; Alto nivel de robustez, seguridad y precisión.
Riesgo limitado	ChatBots y sistemas de inteligencia artificial que interactúan con individuos[14].	Requerimiento de transparencia, la obligación de comunicar a los usuarios sobre su interacción con un sistema de inteligencia artificial.
Riesgo mínimo	Videojuegos que incorporan inteligencia artificial y sistemas de filtrado de contenido no deseado[15].	Uso sin restricciones y sin normativas particulares.

2. La inteligencia artificial (IA) se utiliza en la evaluación social para mejorar la comunicación y la comprensión de la información. Un ejemplo de esto es el sistema de IA analítica llamado Clara. Clara utiliza diferentes técnicas de clasificación y búsqueda de patrones para evaluar si un texto es comprensible o no. Además, maneja nueve métricas diseñadas por lingüistas computacionales para decidir si un texto cumple o no los requisitos mínimos de claridad. Clara devuelve una puntuación en porcentaje para indicar si el texto escrito está más o menos cerca de ser un texto claro. Esto permite al usuario corregir el texto en función de las indicaciones de Clara y someterlo a evaluación de nuevo. Otro ejemplo de IA en la evaluación social es la incorporación de herramientas de IA, como ChatGPT, en el proceso de aprendizaje. Los estudiantes pueden valorar la aportación de la herramienta, identificar los puntos débiles o complementar la respuesta que les ha proporcionado.

3. Algunos sistemas de IA que representan amenazas para la seguridad, los medios de vida y los derechos de las personas incluyen los sistemas de puntuación social, que evalúan el comportamiento individual y asignan puntuaciones que, en algunos países, determinan el acceso a servicios públicos como educación y atención médica. Los sistemas de reconocimiento facial se emplean para identificar a personas a partir de imágenes, pero su uso en vigilancia y control puede comprometer la privacidad y la libertad. Los sistemas de toma de decisiones automatizada, utilizados en áreas como contratación, evaluación crediticia y justicia penal, si no están bien diseñados, pueden perpetuar discriminación y sesgos.
4. La inteligencia artificial está desempeñando un papel cada vez más importante en la manipulación del comportamiento humano, aprovechando su capacidad para identificar vulnerabilidades en los hábitos y decisiones de las personas. Un estudio reciente demostró que la IA puede aprender a detectar esas vulnerabilidades y utilizarlas para influir en las elecciones humanas, un fenómeno que está siendo estudiado con preocupación en diversos ámbitos. Por ejemplo, las empresas recurren a la IA para personalizar la publicidad. Recopilan grandes cantidades de datos sobre los usuarios y luego adaptan los anuncios específicamente a sus intereses y necesidades, lo que incrementa la probabilidad de que realicen compras. De manera similar, los bots en las redes sociales se utilizan para difundir información falsa y manipular la opinión pública, afectando directamente cómo las personas perciben y reaccionan a ciertos eventos. En el ámbito de los juegos de azar, los casinos aplican la IA para analizar el comportamiento de los jugadores, ofreciéndoles incentivos diseñados a medida para mantenerlos jugando por más tiempo. Incluso los asistentes virtuales pueden ser programados para persuadir a los usuarios a realizar compras adicionales. En el ámbito de la vigilancia, los sistemas impulsados por IA están diseñados para predecir posibles amenazas al analizar los comportamientos humanos. Otra aplicación importante de la IA es el reconocimiento facial, una tecnología que ha evolucionado rápidamente. Estos sistemas, que detectan patrones faciales para identificar a personas, se utilizan en diversos campos, desde el desbloqueo de dispositivos móviles hasta la identificación de criminales en aeropuertos. En entornos comerciales, como los supermercados, esta tecnología puede ser utilizada para controlar el acceso a ciertas áreas, como cajas registradoras, impidiendo intentos de robo al no reconocer el rostro de personas no autorizadas. En la seguridad pública, las fuerzas del orden emplean el reconocimiento facial para identificar a sospechosos en lugares concurridos, como estaciones de tren o aeropuertos. Además, el marketing ha comenzado a beneficiarse de esta tecnología al personalizar la publicidad según características físicas como la edad o el estado de ánimo de los clientes. En las escuelas, el reconocimiento facial se utiliza para gestionar la asistencia de los estudiantes, y en los parques temáticos, para personalizar las experiencias de los visitantes. Finalmente, las infraestructuras críticas, como el suministro de agua, la energía eléctrica y los sistemas de transporte, se encuentran entre los sectores más vulnerables a la aplicación de la IA. La Unión Europea ha identificado algunas aplicaciones de IA que presentan un alto riesgo para la vida y la salud de los ciudadanos, como las que se utilizan en la gestión de infraestructuras críticas, la evaluación educativa y profesional, la seguridad de los productos mediante cirugía asistida por robots, la selección de trabajadores mediante programas informáticos y la evaluación crediticia que puede afectar el acceso a préstamos. Estas aplicaciones de IA, aunque poderosas, requieren una supervisión estricta para evitar que afecten negativamente a la vida de las personas.

5. Los sistemas de reconocimiento facial son una tecnología de detección y reconocimiento biométrico que se basa en detectar patrones y aspectos específicos de la fisiología de un rostro para reconocer o identificar a la persona. Estos sistemas se han utilizado en diversos campos, desde el desbloqueo de un móvil hasta la detección de criminales que intentan acceder al aeropuerto para escapar del país. Algunos ejemplos de uso de esta tecnología incluyen: Control de acceso: En un supermercado o en un establecimiento pequeño se podría llevar a cabo un control sobre quien abre la caja registradora mediante un reconocimiento facial previo, de esta manera también se pueden evitar intentos de robo ya que, al no reconocer el rostro, la caja permanecería cerrada; Seguridad pública: La policía puede utilizar sistemas de reconocimiento facial para identificar a sospechosos en lugares públicos, como estaciones de tren o aeropuertos; Marketing: Las empresas pueden utilizar sistemas de reconocimiento facial para recopilar información sobre los clientes, como su edad, género y estado de ánimo, para personalizar la publicidad y mejorar la experiencia del cliente; Educación: Las escuelas pueden utilizar sistemas de reconocimiento facial para tomar asistencia y garantizar la seguridad de los estudiantes; Entretenimiento: Los parques temáticos pueden utilizar sistemas de reconocimiento facial para identificar a los visitantes y personalizar la experiencia del usuario.
6. Los sistemas de reconocimiento facial son una tecnología biométrica avanzada que permite identificar a las personas mediante el análisis de patrones y características fisiológicas de sus rostros. Esta tecnología ha encontrado aplicaciones en una variedad de campos. Por ejemplo, se utiliza para desbloquear dispositivos móviles, así como en aeropuertos para identificar a criminales que intentan escapar. En entornos comerciales, como supermercados, el reconocimiento facial puede controlar quién tiene acceso a la caja registradora, impidiendo que personas no autorizadas la abran, lo que reduce los intentos de robo. En el ámbito de la seguridad pública, la policía emplea estos sistemas en estaciones de tren y aeropuertos para identificar a sospechosos entre la multitud. Además, las empresas están utilizando el reconocimiento facial para personalizar la publicidad, basándose en características como la edad, el género y el estado de ánimo de los clientes, mejorando así su experiencia. Las escuelas también han implementado esta tecnología para gestionar la asistencia de los estudiantes y garantizar su seguridad. Incluso en el entretenimiento, como en los parques temáticos, el reconocimiento facial se usa para identificar a los visitantes y personalizar su experiencia. Por otro lado, las infraestructuras críticas son esenciales para el funcionamiento de una sociedad, y su daño o destrucción tendría consecuencias significativas en la seguridad, la salud, el bienestar y la economía de la población. Estas infraestructuras incluyen el suministro de agua, la energía eléctrica, el transporte, las comunicaciones, las fuerzas de seguridad y los servicios de emergencia. La inteligencia artificial también desempeña un papel crucial en la gestión de estas infraestructuras críticas, pero puede representar riesgos significativos para la vida y la salud de los ciudadanos. La Unión Europea ha identificado varias aplicaciones de IA de alto riesgo, como las relacionadas con el transporte, la educación y la formación profesional, que pueden influir en el acceso a oportunidades educativas y laborales. Otros ejemplos incluyen los componentes de seguridad de productos, como en la cirugía asistida por robots, la gestión laboral mediante programas informáticos de selección de currículos y los servicios esenciales como la calificación crediticia, que puede afectar el acceso de los ciudadanos a préstamos. Estos ejemplos ilustran la necesidad de una regulación estricta de la IA para proteger a la sociedad de posibles impactos adversos.

7. La inteligencia artificial (IA) está transformando el ámbito educativo y profesional de manera significativa. Los sistemas de IA pueden automatizar la corrección de exámenes y el análisis de ensayos, lo que agiliza el proceso evaluativo y mejora la precisión. Además, la IA facilita la organización de horarios escolares y la administración de registros estudiantiles, aliviando la carga de gestión en las instituciones educativas. Más allá de las tareas administrativas, la IA tiene un impacto profundo al romper barreras geográficas y socioeconómicas, permitiendo que más personas accedan a una educación de calidad sin importar su ubicación o contexto. Este potencial transformador de la IA también contribuye a acelerar el logro de los objetivos globales en educación. Al automatizar procesos de gestión y optimizar los métodos de enseñanza, la IA mejora los resultados del aprendizaje y reduce las barreras al acceso educativo. Entre los sistemas más destacados en el ámbito educativo se encuentran los sistemas de tutoría inteligente, que proporcionan retroalimentación personalizada y adaptan los contenidos a las necesidades de cada estudiante, favoreciendo un aprendizaje más efectivo. Por otro lado, los sistemas de recomendación de cursos utilizan la IA para sugerir programas y materias alineadas con los intereses y habilidades de los estudiantes, personalizando aún más la experiencia educativa. Además, la IA también puede analizar el lenguaje natural de los estudiantes a través de sistemas de análisis de sentimientos, lo que permite identificar sus emociones y actitudes hacia el aprendizaje, ofreciendo una visión más completa de su progreso y bienestar.
8. Los sistemas de inteligencia artificial (IA) son cada vez más comunes en los productos que utilizamos en nuestra vida cotidiana. La seguridad de estos productos es una preocupación importante para los fabricantes y los consumidores. Según un artículo de KPMG Tendencias, los sistemas de IA que se utilizan en productos sujetos a la legislación de la UE sobre seguridad de los productos, incluyendo: juguetes, aviación, automóviles, dispositivos médicos y ascensores, deben cumplir con los requisitos de ciberseguridad establecidos por la Comisión Europea (Ciberseguridad en entornos de inteligencia artificial — KPMG Tendencias). La guía publicada por la Comisión Europea establece que el requisito de ciberseguridad de la Ley de IA se aplica al sistema de IA en su conjunto y no directamente a sus componentes internos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen sistemas de IA por sí solos. Para realizar una correcta evaluación de riesgos de ciberseguridad, y poder garantizar así su cumplimiento, se requiere un enfoque integrado y continuo que utilice prácticas y procedimientos probados de ciberseguridad combinados con controles específicos de IA. Es importante tener en cuenta que los sistemas de seguridad de los productos que utilizan IA pueden variar según el tipo de producto. Por ejemplo, la composición de los sistemas de seguridad como medios técnicos para garantizar la seguridad incluye un sistema integrado de medios técnicos de protección (CS TSO), un conjunto de medios técnicos y/o sistemas (alarmas, alarmas contra incendios, control de acceso, videovigilancia, etc.) que garantizan el cumplimiento de un conjunto de tareas del sistema de seguridad.
9. Los sistemas de inteligencia artificial están cada vez más presentes en los productos que utilizamos en nuestra vida diaria, y la seguridad de estos productos es una preocupación primordial tanto para fabricantes como para consumidores. De acuerdo con KPMG Tendencias, los productos que incluyen IA y están sujetos a la legislación de la UE en materia de seguridad, como juguetes, automóviles, dispositivos médicos, aviación y ascensores, deben cumplir con los requisitos de ciberseguridad establecidos por

la Comisión Europea. La normativa estipula que el requisito de ciberseguridad de la Ley de IA debe aplicarse al sistema de IA en su conjunto y no solo a sus componentes internos, reconociendo que aunque los modelos de IA son elementos fundamentales, no constituyen un sistema de IA por sí mismos. Para garantizar el cumplimiento de estos estándares, es necesario un enfoque continuo que combine prácticas probadas de ciberseguridad con controles específicos de IA, ajustados al tipo de producto, lo que puede implicar la implementación de medios técnicos de protección como alarmas, control de acceso y videovigilancia. Asimismo, la inteligencia artificial se está utilizando con creciente frecuencia en el ámbito laboral para mejorar la eficiencia y la productividad. En la selección de candidatos, por ejemplo, la IA ayuda a los empleadores a evaluar currículums y programar entrevistas de manera más ágil, facilitando la identificación de los perfiles más adecuados para los puestos de trabajo. Además, en la gestión de trabajadores, la IA optimiza la programación de turnos, la asignación de tareas y la supervisión del rendimiento, ayudando a los gerentes a detectar necesidades de formación o apoyo adicional. En cuanto al autoempleo, los sistemas de IA también juegan un papel clave al analizar datos y ofrecer recomendaciones personalizadas sobre oportunidades de negocio, contribuyendo a que más personas puedan acceder a trabajos independientes de manera efectiva.

10. Los sistemas de inteligencia artificial (IA) se están utilizando cada vez más en servicios públicos y privados esenciales. Algunos ejemplos de servicios públicos esenciales que utilizan IA son la educación, la asistencia sanitaria, la policía y la aplicación de la ley. En el caso de los servicios privados esenciales, la calificación crediticia es un ejemplo común de un servicio que utiliza IA.

11. Los sistemas de inteligencia artificial están cada vez más presentes en los productos que utilizamos en nuestra vida diaria, y la seguridad de estos productos es una preocupación primordial tanto para fabricantes como para consumidores. De acuerdo con KPMG Tendencias, los productos que incluyen IA y están sujetos a la legislación de la UE en materia de seguridad, como juguetes, automóviles, dispositivos médicos, aviación y ascensores, deben cumplir con los requisitos de ciberseguridad establecidos por la Comisión Europea. La normativa estipula que el requisito de ciberseguridad de la Ley de IA debe aplicarse al sistema de IA en su conjunto y no solo a sus componentes internos, reconociendo que aunque los modelos de IA son elementos fundamentales, no constituyen un sistema de IA por sí mismos. Para garantizar el cumplimiento de estos estándares, es necesario un enfoque continuo que combine prácticas probadas de ciberseguridad con controles específicos de IA, ajustados al tipo de producto, lo que puede implicar la implementación de medios técnicos de protección como alarmas, control de acceso y videovigilancia. Asimismo, la inteligencia artificial se está utilizando con creciente frecuencia en el ámbito laboral para mejorar la eficiencia y la productividad. En la selección de candidatos, por ejemplo, la IA ayuda a los empleadores a evaluar currículums y programar entrevistas de manera más ágil, facilitando la identificación de los perfiles más adecuados para los puestos de trabajo. Además, en la gestión de trabajadores, la IA optimiza la programación de turnos, la asignación de tareas y la supervisión del rendimiento, ayudando a los gerentes a detectar necesidades de formación o apoyo adicional. En cuanto al autoempleo, los sistemas de IA también juegan un papel clave al analizar datos y ofrecer recomendaciones personalizadas sobre oportunidades de negocio, contribuyendo a que más personas puedan acceder a trabajos independientes de manera efectiva.

12. Los sistemas de inteligencia artificial están desempeñando un papel cada vez más relevante en la gestión de la migración, el asilo y el control de fronteras. Según un informe de Amnistía Internacional, diversos gobiernos han implementado tecnologías avanzadas en estos sistemas, como es el caso de Estados Unidos, Reino Unido y la Unión Europea. Entre los ejemplos más destacados se encuentran los sistemas de verificación de autenticidad de documentos de viaje, que emplean IA para analizar y detectar elementos de seguridad en los documentos y, así, identificar posibles falsificaciones. Además, los sistemas de toma de decisiones biométricos y algorítmicos están siendo utilizados para evaluar solicitudes de asilo y migración, determinando de manera automatizada si las solicitudes deben ser aceptadas o denegadas. Asimismo, las tecnologías de externalización de fronteras, apoyadas en IA, están siendo utilizadas para controlar y vigilar los límites territoriales, a menudo mediante drones y sistemas de detección de patrones de movimiento, lo que permite una supervisión más rigurosa y automatizada en la gestión de las fronteras.
13. La inteligencia artificial está ganando terreno en la administración de justicia y los procesos democráticos, con aplicaciones que van desde chatbots conversacionales, que ayudan a responder preguntas frecuentes y aliviar la carga de trabajo de los empleados públicos, hasta sistemas más complejos como los de control de contratación pública, que detectan fraudes y corrupción. Además, se utilizan sistemas de alerta temprana para identificar irregularidades en los procesos judiciales y notificar a los jueces. En el ámbito de la predicción de sentencias, la IA ayuda a prever el posible resultado de un juicio, proporcionando a los jueces información adicional para sus decisiones. Finalmente, los sistemas de análisis de documentos permiten procesar grandes volúmenes de información, extrayendo datos clave que agilizan los procedimientos judiciales.
14. Los sistemas de inteligencia artificial que interactúan directamente con los usuarios se están volviendo cada vez más comunes, con los chatbots como ejemplo clave de esta tecnología. Los chatbots son programas que utilizan IA para simular conversaciones humanas, permitiendo interacciones fluidas a través de interfaces de chat. Estos sistemas automatizan diálogos, brindan asistencia inmediata, personalizan las experiencias de los usuarios y ofrecen entretenimiento. En 2024, algunos de los chatbots más populares incluyen ChatGPT, que destaca por su capacidad de manejar diversos temas y comprender el contexto, lo que hace que las interacciones sean más naturales y bien informadas. Nuevo Bing, por su parte, utiliza procesamiento del lenguaje natural para responder con precisión a las consultas y realizar búsquedas web en tiempo real. Tidio es otra herramienta de IA, enfocada en la atención al cliente, que se integra con sitios web para responder preguntas frecuentes y programar citas, mientras que Zendesk se especializa en la asistencia a clientes, respondiendo preguntas comunes, proporcionando información adicional y organizando citas a través de una plataforma integrada de atención al cliente. Estos chatbots muestran cómo la IA está transformando la forma en que las empresas y los individuos interactúan, mejorando la eficiencia y personalización en tiempo real.
15. Los videojuegos modernos integran la inteligencia artificial para ofrecer experiencias de juego más inmersivas y realistas. La IA permite la creación de personajes no jugables (PNJ) con comportamientos sofisticados y realistas, además de generar automáticamente mapas y niveles de juego. En juegos como *Metal Gear Solid*, la IA dota a los enemigos de estrategias avanzadas, permitiéndoles rastrear al jugador cuando se oculta. Títulos como *Rogue* y *Elite* emplean algoritmos para generar escenarios aleatorios, brindando

G. *Regulación de las Inteligencias Artificiales Generativas y Modelos Fundacionales*

En el marco del Reglamento Europeo, se han establecido normas específicas para los modelos fundacionales de inteligencia artificial (IA) generativa, que son sistemas avanzados y de gran escala capaces de realizar una amplia gama de tareas diversas con un alto grado de competencia. Estos modelos incluyen, entre otros, la generación de contenido creativo (textos publicitarios, guiones, música, y obras de arte originales), el diseño y la moda (creación de patrones, estilos y diseños innovadores), la conversión de lenguaje, la programación informática (generación de códigos y desarrollo de videojuegos), así como aplicaciones en medicina y descubrimiento de fármacos.

Los modelos fundacionales son grandes redes neuronales entrenadas en datos no etiquetados a gran escala mediante técnicas de aprendizaje autosupervisado. Este enfoque permite al modelo aprender de manera autónoma patrones complejos y representaciones generales del lenguaje o de otros tipos de datos, lo que lo hace altamente versátil y adaptable a una amplia gama de tareas posteriores con ajustes mínimos. Estos modelos sirven como base para diversas aplicaciones, desde procesamiento de lenguaje natural hasta visión por computadora, y pueden ser ajustados o especializados para tareas específicas mediante técnicas de transferencia de aprendizaje. Ejemplos destacados de modelos fundacionales incluyen GPT-4 de OpenAI, Gemini de Google, Llama 2 de Meta y Claude de Anthropic, todos los cuales representan avances significativos en la capacidad de la inteligencia artificial para comprender y generar contenido complejo en múltiples dominios.

El Reglamento impone obligaciones más estrictas en materia de transparencia para los sistemas de IA generativa, especialmente aquellos que crean contenido complejo, como textos, imágenes, audio o video con diversos grados de autonomía. Entre las principales obligaciones se exige que los proveedores ofrezcan información clara sobre el funcionamiento del sistema, incluyendo los procesos que intervienen en la generación de contenido y las limitaciones inherentes del modelo. Además, deben establecerse mecanismos para mitigar el riesgo de desinformación, garantizando que el con-

---

una experiencia única en cada partida. Además, los sistemas de filtrado de contenido no deseado se han vuelto esenciales para proteger a los jugadores de material inapropiado. Juegos como *Roblox* y *Minecraft* implementan estos sistemas para garantizar un entorno seguro, asegurando que el contenido inapropiado sea filtrado de manera efectiva, mejorando así la seguridad y la calidad de la experiencia de los usuarios.

tenido generado no sea engañoso ni utilizado con fines malintencionados. Los sistemas también deben estar diseñados para permitir una supervisión adecuada, asegurando que los usuarios puedan intervenir y corregir resultados que pudieran causar daño o ser utilizados de manera inapropiada. Asimismo, se exige una documentación exhaustiva que incluya detalles sobre el entrenamiento del modelo, los datos utilizados y los mecanismos de control de calidad y seguridad del contenido generado. No obstante, se percibe una importante laguna en la aplicación de las disposiciones de los Artículos 16 y siguientes de la Ley de Servicios Digitales, que contemplan mecanismos de denuncia y respuesta ante problemas, los cuales no se aplican expresamente a la IA generativa. Esta falta de alineación podría limitar la capacidad de abordar de manera efectiva los riesgos asociados con la generación automatizada de contenido y el mal uso de estos sistemas de IA. Por ello, la inclusión de mecanismos específicos de reporte y respuesta para la IA generativa sería esencial para completar el marco regulador y asegurar una supervisión efectiva.

4. OBLIGACIONES DE LOS PROVEEDORES, IMPORTADORES Y DISTRIBUIDORES DE SISTEMAS DE IA DE ALTO RIESGO

Los sistemas de IA de alto riesgo están sujetos a estrictas regulaciones en la Unión Europea, que asignan obligaciones claras a proveedores, importadores y distribuidores. Estas obligaciones garantizan la seguridad, transparencia, protección de derechos fundamentales y el cumplimiento de los más altos estándares éticos.

4.1. Obligaciones de los Proveedores de Sistemas de IA de Alto Riesgo

Los proveedores de sistemas de IA de alto riesgo deben garantizar el cumplimiento de las normativas vigentes, lo cual implica implementar un sistema de gestión de calidad documentado que abarque todo el ciclo de vida del sistema, desde su diseño hasta su despliegue y operación. Es imperativo mantener una documentación técnica completa, detallada y actualizada que cumpla con los requisitos legales, y conservar los archivos de registro generados por el sistema durante el tiempo estipulado por las leyes y contratos aplicables. Previo a la comercialización o puesta en servicio, el sistema debe someterse a una evaluación de conformidad exhaustiva. Una vez cumplidos todos los requisitos normativos, el sistema se debe registrar y marcar con el sello CE, certificando su conformidad con las regulaciones europeas. En caso de que el sistema no cumpla con los requisitos, el proveedor tiene la obliga-

ción de adoptar de inmediato medidas correctivas, como la modificación, retirada o recuperación del sistema, notificando a las autoridades competentes y a los organismos notificados las no conformidades y las acciones adoptadas. Además, los proveedores deben establecer un sistema de vigilancia post-comercialización que monitorice el rendimiento del sistema en situaciones reales, recolectando datos para implementar las actualizaciones necesarias. En los casos en que el proveedor se encuentre fuera de la UE, deberá designar un representante autorizado en el territorio comunitario, quien será responsable de asegurar el cumplimiento normativo y proporcionar la información requerida. Finalmente, los proveedores deben cumplir con las normas armonizadas establecidas por el Reglamento (UE) n.º 1025/2012 o, en su defecto, con las especificaciones técnicas adoptadas por la Comisión, para demostrar la conformidad del sistema con los requisitos reglamentarios.

4.2. Obligaciones de los Importadores de Sistemas de IA de Alto Riesgo

Los importadores de sistemas de IA de alto riesgo deben garantizar que, antes de su comercialización en el mercado de la UE, dichos sistemas cumplen con todas las normativas aplicables. Esto implica verificar que el proveedor ha realizado una evaluación de conformidad exhaustiva, ha elaborado la documentación técnica correspondiente y ha aplicado el marcado CE, lo que certifica la conformidad del sistema con los requisitos europeos. Los importadores también deben asegurarse de que su información, como nombre, marca y dirección, esté claramente indicada en el propio sistema de IA o en su embalaje, y de que las condiciones de almacenamiento y transporte no comprometan el cumplimiento normativo del sistema. Además, tienen la responsabilidad de colaborar estrechamente con las autoridades competentes, proporcionando toda la información y documentación necesaria para demostrar el cumplimiento del sistema con las regulaciones vigentes, lo que incluye facilitar el acceso a los archivos de registro generados por el sistema y cooperar en cualquier acción correctiva o investigación que pueda surgir en relación con su funcionamiento o conformidad normativa.

4.3. Obligaciones de los Distribuidores de Sistemas de IA de Alto Riesgo

Los distribuidores de sistemas de IA de alto riesgo deben verificar que los productos que comercializan cumplen con las normativas aplicables, asegurándose de que el marcado CE esté presente y de que exista la documentación técnica correspondiente. Asimismo, deben constatar que tanto el proveedor como el importador han cumplido con sus respectivas obligaciones. En caso

de detectar que un sistema no cumple con los requisitos normativos, los distribuidores están obligados a tomar las medidas correctivas necesarias para asegurar la conformidad del sistema, o bien retirarlo del mercado si no es posible subsanar los incumplimientos. Si el sistema supone un riesgo, deben informar a las autoridades competentes sin demora. Además, los distribuidores tienen la obligación de cooperar plenamente con las autoridades nacionales, proporcionando la documentación requerida que demuestre la conformidad del sistema y facilitando cualquier medida adicional que las autoridades consideren necesaria para garantizar el cumplimiento del Reglamento.

5. OBLIGACIONES DE LOS USUARIOS DE SISTEMAS DE IA DE ALTO RIESGO

El Reglamento impone estrictas obligaciones a los usuarios de sistemas de inteligencia artificial (IA) clasificados como de alto riesgo, con el objetivo de proteger los derechos fundamentales, garantizar la transparencia y permitir una supervisión humana eficaz. Los usuarios están obligados a realizar una exhaustiva evaluación del impacto del sistema sobre los derechos fundamentales antes de su implementación, identificando y mitigando cualquier riesgo potencial. Además, deben registrar los sistemas de IA en una base de datos centralizada de la Unión Europea, lo que es un requisito indispensable para su operación legal y facilita la supervisión por parte de las autoridades competentes. Es crucial que los usuarios proporcionen información clara y accesible sobre el funcionamiento del sistema, explicando cómo se toman las decisiones automatizadas y los algoritmos empleados, asegurando así que las personas afectadas comprendan su funcionamiento y puedan ejercer sus derechos. La supervisión humana efectiva es también una obligación, lo que implica que los usuarios deben poder intervenir, interrumpir o modificar el funcionamiento del sistema cuando sea necesario, particularmente ante decisiones inadecuadas. Además, deben mantener una documentación detallada y precisa del sistema de IA, incluyendo sus aspectos técnicos, operativos y cualquier modificación realizada a lo largo del tiempo, lo cual es esencial para garantizar la trazabilidad, un mantenimiento adecuado y la evaluación continua del sistema.

6. IMPACTO SOBRE LOS DERECHOS FUNDAMENTALES

6.1. Protección de Datos

El Reglamento amplía las salvaguardias del Reglamento General de Protección de Datos (RGPD), garantizando que los sistemas de inteligen-

cia artificial (IA) respeten plenamente la privacidad y la protección de los datos personales. Uno de los principios clave es la minimización de datos, que exige que los sistemas de IA limiten estrictamente la cantidad de datos personales que recopilan, procesando únicamente aquellos datos que sean absolutamente esenciales para su funcionamiento, y evitando cualquier tratamiento innecesario de información personal. Además, los operadores de estos sistemas deben obtener el consentimiento explícito, específico y plenamente informado de los usuarios antes de procesar sus datos personales. Este consentimiento debe ser otorgado de manera libre, tras una explicación clara de los fines del tratamiento, los datos involucrados y los posibles riesgos. Los usuarios también deben tener la opción de retirar su consentimiento en cualquier momento, sin que ello afecte la legitimidad del procesamiento previo.

6.2. No discriminación

El Reglamento prohíbe de manera tajante cualquier forma de discriminación derivada del uso de sistemas de inteligencia artificial (IA). Para cumplir con esta prohibición, los sistemas de IA deben ser diseñados y desarrollados siguiendo estrictos principios que aseguren la prevención de sesgos. Esto requiere la implementación de estrategias y controles sólidos para identificar, mitigar y eliminar cualquier sesgo inherente o adquirido que pueda influir en la toma de decisiones del sistema. Las medidas adoptadas deben garantizar que los resultados generados no conduzcan a decisiones discriminatorias, especialmente en función de características protegidas como raza, género, etnia, religión, orientación sexual, discapacidad u otras categorías susceptibles de discriminación. Además, es imprescindible que los desarrolladores y operadores realicen evaluaciones continuas a lo largo del ciclo de vida del sistema para detectar y corregir cualquier sesgo emergente, asegurando así la equidad y no discriminación en el uso de la IA.

6.3. Explicabilidad y transparencia

El RIA establece la transparencia como un principio esencial, exigiendo que los sistemas de IA sean trazables y explicables. Esto implica que las personas deben ser informadas cuando interactúan con una IA, y los responsables del despliegue deben comprender claramente sus capacidades y limitaciones. Además, las personas afectadas por decisiones automatizadas deben ser conscientes de sus derechos.

El Capítulo IV del RIA detalla las obligaciones de transparencia, especialmente para sistemas que impactan derechos fundamentales. El artículo 13 especifica que los responsables del despliegue deben informar sobre el uso de sistemas de categorización biométrica y reconocimiento de emociones, salvo en la persecución de delitos. También deben advertir sobre el uso de deep fakes y contenido manipulado, excepto cuando el contenido sea claramente satírico, creativo, o esté relacionado con investigaciones criminales.

La transparencia debe ser un elemento presente desde el diseño del sistema, incluyendo información detallada sobre los datos utilizados en su entrenamiento. Los modelos de uso general deben ofrecer resúmenes exhaustivos de los conjuntos de datos, en cumplimiento con la normativa de la UE y los Estados miembros.

La Comisión Europea fomenta la creación de códigos de buenas prácticas, con énfasis en la detección y etiquetado de contenido generado artificialmente. Los sistemas de IA deben ser configurados para que sus decisiones sean comprensibles tanto para usuarios como para terceros, proporcionando explicaciones claras sobre la lógica, los datos empleados y los criterios en la toma de decisiones, facilitando así la evaluación de su equidad y conformidad normativa.

El marco regulatorio establece principios estrictos para asegurar una operación transparente y responsable de los sistemas de IA. Los operadores deben proporcionar informes detallados sobre el funcionamiento del sistema, accesibles a los usuarios y partes interesadas, sobre todo cuando se impacten derechos fundamentales. La IA debe justificar coherentemente sus decisiones, evitando sesgos e injusticias. Además, los sistemas que afecten derechos fundamentales deben ser transparentes, precisos y no discriminatorios, especialmente en sectores sensibles como la seguridad y la justicia.

Es necesaria una documentación técnica exhaustiva que abarque desde el desarrollo hasta la implementación, detallando algoritmos, datos, capacidades, limitaciones y medidas de gestión de riesgos. Esta documentación debe ser acompañada de una supervisión humana continua.

Los proveedores de IA tienen la obligación de informar a los usuarios cuando interactúan con un sistema de IA, a menos que la artificialidad sea evidente. Esta obligación no se aplica en investigaciones criminales o en la prevención de delitos, siempre que el sistema no esté dirigido al público en general. Los operadores que utilicen sistemas de reconocimiento emocional o categorización biométrica deben informar sobre su uso, salvo cuando sea

necesario mantener la confidencialidad por razones de seguridad o aplicación de la ley.

Es obligatorio advertir sobre contenido simulado, salvo en casos de seguridad, investigaciones criminales o cuando se ejerzan derechos de libertad de expresión y creación artística, siempre respetando los derechos de terceros.

7. PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

El Reglamento establece la importancia de proteger los datos personales y la privacidad en los sistemas de inteligencia artificial (IA), que deben cumplir estrictamente con las normativas de protección de datos. En España, estos sistemas están regulados por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), que exigen el respeto a principios fundamentales como la licitud, transparencia, minimización de datos, exactitud, integridad y confidencialidad en el tratamiento de información personal. Además, se demanda una responsabilidad proactiva por parte de los responsables del tratamiento de datos para asegurar su cumplimiento.

Paralelamente, el Reglamento enfatiza la importancia de la ciberseguridad para garantizar que los sistemas de IA estén protegidos frente a amenazas cibernéticas, lo que es clave para mantener la integridad, confidencialidad y disponibilidad de los datos procesados. La protección contra ataques cibernéticos es fundamental tanto para la fiabilidad operativa de los sistemas de IA como para su seguridad general.

En respuesta a estos riesgos, la Comisión Europea publicó en septiembre de 2023 una guía con recomendaciones para entidades, operadores y empresas que implementan sistemas de IA de alto riesgo, con el fin de ayudarlas a cumplir con los requisitos de ciberseguridad. Esta guía ofrece lineamientos detallados para establecer medidas de seguridad robustas que protejan tanto los datos como las operaciones de los sistemas de IA avanzados[16].

8. MECANISMOS DE SUPERVISIÓN

La implementación y cumplimiento del RIA en la Unión Europea recaen sobre los Estados miembros, que deben designar autoridades nacionales competentes para supervisar su aplicación y la vigilancia del mercado.

16. Ciberseguridad en entornos de inteligencia artificial — KPMG Tendencias.

Además, cada Estado designará una autoridad nacional de supervisión, encargada de actuar como enlace entre los ciudadanos, las autoridades de otros países y el Comité Europeo de Inteligencia Artificial, representando a su país en las instancias europeas.

El sistema se fortalece con la creación de un foro consultivo que asegura la representación equilibrada de las partes interesadas y ofrece asesoramiento técnico especializado. A nivel europeo, la Comisión Europea establecerá la Oficina Europea de Inteligencia Artificial, encargada de la supervisión de los modelos de uso general de IA (GPAI) y de la coordinación con el Comité Europeo de Inteligencia Artificial. Esta oficina contará con el respaldo de una Comisión Científica de expertos independientes que proporcionarán conocimientos científicos especializados.

Las autoridades de supervisión tendrán facultades para realizar inspecciones, exigir correcciones y garantizar el cumplimiento riguroso del reglamento. Estas estructuras velarán por que los sistemas de IA operen bajo principios éticos y de responsabilidad.

El Reglamento (UE) 2024/1689 establece normas armonizadas sobre IA, delegando en la Comisión Europea la responsabilidad de supervisar los GPAI a través de la Oficina Europea de IA, mientras que los Estados miembros se encargan de la implementación en otros aspectos. El Comité Europeo de Inteligencia Artificial y el grupo de expertos científicos establecidos bajo el artículo 68 del RIA son actores fundamentales en la aplicación de este reglamento. Además, el Supervisor Europeo de Protección de Datos interviene cuando las instituciones de la UE utilicen IA en el marco del reglamento[17].

8.1. Agencias de Supervisión

El reglamento establece la creación de organismos de supervisión tanto a nivel nacional como en el ámbito de la Unión Europea con responsabilidades clave. La primera es la supervisión del cumplimiento, asegurando que los operadores de sistemas de inteligencia artificial se adhieran rigurosamente a las disposiciones del reglamento, y supervisando la correcta implementación de las normativas aplicables. La segunda es la investigación de infracciones, llevando a cabo investigaciones detalladas en casos de pre-

17. JIMÉNEZ SERRANÍA, V., «Medidas de apoyo a la innovación y arquitectura de gobernanza», en BARRIO ANDRÉS (Dir.) *El reglamento europeo de inteligencia artificial*, *op. cit.*, pp. 111 y ss.

sunto incumplimiento y, en caso de confirmarse una infracción, imponiendo sanciones proporcionales a la gravedad de la violación. Estos organismos garantizarán la correcta aplicación del marco regulatorio, promoviendo el uso ético y legal de la inteligencia artificial.

8.2. Régimen sancionador

El Reglamento establece un régimen sancionador integral para quienes incumplan sus disposiciones, combinando multas significativas con responsabilidad civil. Este sistema es proporcional, efectivo y disuasorio, ajustándose a la gravedad de cada infracción. En casos graves, como el incumplimiento de requisitos relacionados con datos o prácticas prohibidas, las multas pueden alcanzar hasta 35 millones de euros o el 7% del volumen de negocios anual global, aplicándose el monto más elevado. Además, los operadores son responsables civilmente por los daños causados por sus sistemas de inteligencia artificial, brindando un recurso adicional a las personas afectadas.

El régimen sancionador se organiza en tres niveles según la gravedad de la infracción. Las infracciones graves pueden acarrear multas de hasta 35 millones de euros o el 7% del volumen de negocios anual global. Las infracciones de requisitos menos graves, como los relacionados con modelos de IA de uso general, se sancionan con hasta 15 millones de euros o el 3% del volumen de negocios anual global. La presentación de información incorrecta, incompleta o engañosa se penaliza con hasta 7,5 millones de euros o el 1,5% del volumen de negocios anual global. Las pymes se acogen al umbral más bajo en cada categoría, mientras que las grandes empresas enfrentan el umbral superior.

Para garantizar una aplicación homogénea de estas sanciones, la Comisión Europea, con el asesoramiento del Comité, desarrollará directrices comunes. El Reglamento se aplica tanto a empresas como a instituciones y organismos de la Unión Europea, sujetos a las mismas normas y sanciones. El Supervisor Europeo de Protección de Datos tiene la facultad de imponer multas administrativas para asegurar el cumplimiento por parte de las entidades de la Unión. Además, las personas afectadas pueden presentar denuncias ante las autoridades nacionales encargadas de la vigilancia del mercado.

La Comisión Europea tiene potestad para adoptar actos que modifiquen aspectos específicos del Reglamento, previa consulta con expertos y en coor-

dinación con el Parlamento Europeo y el Consejo. También tiene poderes de ejecución para garantizar la aplicación uniforme de las disposiciones en toda la Unión, respetando los principios de subsidiariedad y proporcionalidad.

8.3. Oficina Europea de IA

La Oficina Europea de Inteligencia Artificial tiene como objetivo consolidar las capacidades de la Unión Europea en el campo de la inteligencia artificial (IA), especialmente en la implementación y supervisión de normativas para los modelos de IA de propósito general (GPAI). Entre sus funciones destacan la elaboración de códigos de conducta, la clasificación de modelos con riesgos sistémicos y la vigilancia del cumplimiento del RIA. Esto incluye la solicitud de documentación a proveedores, evaluaciones técnicas, investigaciones de riesgos y la exigencia de medidas correctivas cuando sea necesario.

Además, la Oficina desempeña un papel crucial como coordinador de la política de IA en la UE, fomentando la colaboración con instituciones públicas, expertos y la comunidad científica, proyectando a la Unión como líder global en esta tecnología. Aunque inicialmente se contemplaba su autonomía, la Oficina fue integrada en la Comisión Europea bajo la Dirección General de Redes de Comunicación, Contenidos y Tecnología (DG CNECT), con una línea presupuestaria independiente para asegurar su operatividad.

El grado de autonomía de la Oficina ha sido objeto de debate y su estructura se definirá antes de la entrada en vigor del RIA. Supervisará específicamente modelos de alto rendimiento, como los GPAI, incluyendo sistemas como GPT-4 de OpenAI, y tendrá un rol en la legislación secundaria y la coordinación de normas en sistemas ya regulados por otras leyes. Además, desarrollará códigos de conducta y buenas prácticas en toda la UE, con un enfoque clave en la cooperación con la comunidad de *software* de código abierto para promover la adopción ética y responsable de la IA generativa en sectores estratégicos.

La Oficina se encargará de consolidar un ecosistema innovador y confiable de IA en Europa, promoviendo un enfoque coherente frente a los desafíos internacionales. En cuanto a la aplicación del Reglamento, la Comisión Europea, a través de la Oficina, tiene competencias exclusivas para garantizar el cumplimiento de las disposiciones relativas a los GPAI y puede imponer sanciones por incumplimientos. También coordinará la cooperación entre las autoridades nacionales de los Estados miembros, especialmen-

te en investigaciones conjuntas. En caso de conflictos entre decisiones de autoridades nacionales, la Comisión puede intervenir y anular resoluciones conforme al «procedimiento de salvaguardia de la Unión» estipulado en el artículo 81 del RIA.

Con la estructura aprobada para la Oficina, la Comisión busca garantizar coherencia en la aplicación del Reglamento. La Oficina se ha organizado en cinco unidades clave: regulación y cumplimiento, seguridad, excelencia, relaciones internacionales e innovación, lo que le permitirá abordar los múltiples desafíos de la IA y asegurar una implementación eficaz de las normativas a nivel europeo e internacional.

8.4. Comité Europeo de IA

El Comité Europeo de Inteligencia Artificial está compuesto por representantes de alto nivel de las autoridades nacionales de supervisión de cada Estado miembro, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Este órgano tiene como función principal proporcionar asesoramiento experto e independiente a la Comisión Europea en cuestiones relacionadas con la inteligencia artificial (IA). Establecido en junio de 2018, el comité adopta un enfoque multidisciplinario, compuesto por 52 miembros de áreas como la tecnología, la ética, el derecho y las ciencias sociales, lo que le permite abordar de forma integral los desafíos regulatorios que presenta la IA.

Sus funciones incluyen asistir tanto a la Comisión como a los Estados miembros en la implementación efectiva del RIA, garantizando una aplicación uniforme y armonizada en toda la Unión Europea. Emitirá recomendaciones y dictámenes sobre sistemas de IA de alto riesgo y otros aspectos clave para asegurar una interpretación coherente de las normativas en los distintos Estados miembros. Además, el Comité desempeñará un papel esencial en el apoyo a las iniciativas de normalización de la IA, colaborando con organismos europeos encargados de establecer estándares técnicos y regulatorios, asegurando que el desarrollo de la IA en Europa se ajuste a principios que equilibran la innovación con la protección de los derechos fundamentales.

En cumplimiento del artículo 65 del RIA, el Comité también asesorará a la Comisión Europea, a la Oficina Europea de IA y a los Estados miembros en la correcta aplicación del reglamento, con un enfoque especial en los modelos de IA de propósito general (GPAI), según lo establecido en el artículo 66.c. El reglamento prevé diversas obligaciones de información, notificación y

consulta entre la Oficina Europea de IA, las autoridades nacionales de vigilancia del mercado y el Comité, conforme a los artículos 75.2 y 90.2 del RIA.

Este marco de cooperación asegura que las normativas sobre IA se implementen de manera coordinada y eficaz, evitando discrepancias en la interpretación de las regulaciones, y garantizando que el desarrollo de la IA en Europa siga un enfoque ético y robusto, alineado con los objetivos de la Unión Europea.

8.5. Otros órganos

El Foro Consultivo estará compuesto por una representación equitativa de diversas partes interesadas, incluidas la industria, empresas emergentes, pymes, organizaciones de la sociedad civil y representantes del ámbito académico. Su principal función será proporcionar asesoramiento especializado y conocimiento técnico tanto al Comité Europeo de Inteligencia Artificial como a la Comisión Europea. Los miembros del Foro serán seleccionados por el propio Comité, asegurando una representación diversa y equilibrada de los sectores implicados en el desarrollo y regulación de la inteligencia artificial.

La Comisión Científica de Expertos Independientes tendrá un papel fundamental en la implementación y supervisión del cumplimiento del RIA, con un enfoque particular en los modelos y sistemas de inteligencia artificial de propósito general (GPAI). Este grupo ofrecerá apoyo técnico especializado para la evaluación y control de estos sistemas, garantizando que cumplan con las normativas del reglamento. Además, será clave en el asesoramiento a la Oficina Europea de IA y a las autoridades nacionales de vigilancia del mercado, contribuyendo a una aplicación uniforme y efectiva del reglamento en toda la Unión Europea.

Establecida bajo el artículo 68 del RIA, la Comisión de expertos también tendrá la facultad de emitir alertas cualificadas a la Oficina de IA, especialmente en casos de riesgos sistémicos asociados con los modelos GPAI. Su labor se centrará en respaldar las actividades de supervisión, evaluación e investigación estipuladas por el reglamento, colaborando con las autoridades competentes de los Estados miembros para garantizar que los sistemas de IA operen dentro de los parámetros de seguridad y ética establecidos.

Este grupo de expertos no solo contribuirá a armonizar la implementación de las normativas en toda la Unión, sino que también ofrecerá orientación técnica para mitigar los riesgos relacionados con los modelos de IA de alto impacto. Los Estados miembros podrán recurrir a esta Comisión para

obtener asesoramiento especializado, asegurando una respuesta eficaz y coherente a los desafíos de la IA en Europa.

8.6. Las autoridades públicas de los Estados miembros de la UE

Cada Estado miembro de la Unión Europea está obligado a designar al menos una autoridad de vigilancia del mercado y una autoridad notificante para supervisar la aplicación del RIA, con la excepción de los modelos de IA de propósito general (GPAI), cuya supervisión exclusiva corresponde a la Oficina Europea de IA (art. 70.1 del RIA). La autoridad de vigilancia del mercado tiene la responsabilidad principal de asegurar el cumplimiento del reglamento a nivel nacional, mientras que la autoridad notificante se encarga de las evaluaciones de conformidad de los sistemas de IA.

Las autoridades de vigilancia del mercado cuentan con amplias competencias en supervisión, investigación y ejecución, en concordancia con el art. 74 del RIA y el art. 14 del Reglamento (UE) 2019/1020, que regula la vigilancia del mercado y la conformidad de productos. Estas facultades incluyen la capacidad de requerir información a proveedores, desarrolladores e importadores para evaluar el cumplimiento de los sistemas de IA, incluyendo el acceso al código fuente de sistemas de alto riesgo bajo ciertas condiciones. Asimismo, pueden exigir la adopción de medidas correctivas en caso de incumplimiento. Si estas medidas no son suficientes, las autoridades tienen la potestad de imponer restricciones o prohibir la comercialización de un sistema de IA.

Los Estados miembros están obligados a legislar sobre sanciones y medidas coercitivas en el marco del RIA. Estas sanciones pueden incluir multas, advertencias y otras medidas no pecuniarias que garanticen la correcta aplicación del reglamento.

En España, la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) es la entidad encargada de la supervisión en este ámbito, aunque aún se requiere una ley que regule el régimen sancionador y las medidas coercitivas aplicables conforme al RIA.

9. RELACIÓN CON OTRAS NORMATIVAS

9.1. Reglamento General de Protección de Datos

El RIA se integra con el Reglamento General de Protección de Datos (RGPD) para crear un marco normativo específico que aborde la gestión de

riesgos y la protección de datos en el contexto de la inteligencia artificial. La relación entre ambos reglamentos se articula en torno a dos principios fundamentales.

El primero es la compatibilidad normativa. Las disposiciones del Reglamento de IA están diseñadas para alinearse completamente con las obligaciones del RGPD, garantizando que ambas normativas se complementen sin generar conflictos. Esto asegura que las regulaciones de IA refuercen los estándares de protección de datos ya establecidos, sin contradecir los principios del RGPD.

El segundo principio es la protección integral. Se busca una defensa exhaustiva de los derechos de los ciudadanos en todas las dimensiones relacionadas con el uso de la inteligencia artificial y el tratamiento de datos personales. Esto significa que tanto las garantías del RGPD como las del Reglamento de IA se aplican de manera conjunta, preservando la privacidad, la seguridad y los derechos fundamentales en todos los procesos que involucran la IA.

9.2. Relación con la Directiva de Seguridad de Productos

El RIA se integra con el Reglamento General de Protección de Datos (RGPD) para crear un marco normativo específico que aborde la gestión de riesgos y la protección de datos en el contexto de la inteligencia artificial. La relación entre ambos reglamentos se articula en torno a dos principios fundamentales:

El primero es la compatibilidad normativa. Las disposiciones del Reglamento de IA están diseñadas para alinearse completamente con las obligaciones del RGPD, garantizando que ambas normativas se complementen sin generar conflictos. Esto asegura que las regulaciones de IA refuercen los estándares de protección de datos ya establecidos, sin contradecir los principios del RGPD.

El segundo principio es la protección integral. Se busca una defensa exhaustiva de los derechos de los ciudadanos en todas las dimensiones relacionadas con el uso de la inteligencia artificial y el tratamiento de datos personales. Esto significa que tanto las garantías del RGPD como las del Reglamento de IA se aplican de manera conjunta, preservando la privacidad, la seguridad y los derechos fundamentales en todos los procesos que involucran la IA.

9.3. Protección del Consumidor en el Contexto de la IA

El RIA tiene un impacto significativo en el derecho de consumo, centrado en la protección de los consumidores frente a los riesgos asociados con el uso de sistemas de inteligencia artificial. Uno de sus principales objetivos es proteger a los consumidores de daños derivados del uso indebido o incorrecto de la IA en productos y servicios. Un aspecto clave es la obligación de proporcionar a los consumidores información clara y comprensible sobre su interacción con sistemas de IA, garantizando que sepan si están interactuando con una máquina o sistema automatizado. Esto refuerza la transparencia y la claridad en el uso de la IA.

Asimismo, el reglamento impone la necesidad de obtener el consentimiento informado de los consumidores antes de utilizar sus datos en un sistema de IA. Este consentimiento debe asegurar que los consumidores comprendan de manera plena cómo se utilizarán sus datos y las posibles consecuencias de su tratamiento, promoviendo una mayor transparencia en la gestión de la información personal.

El reglamento también garantiza el derecho de los consumidores a no ser sometidos a decisiones automatizadas que puedan tener efectos jurídicos o afectarlos significativamente. Este derecho, en línea con el Reglamento General de Protección de Datos (RGPD), impide que los consumidores se vean perjudicados por decisiones basadas únicamente en procesamiento automatizado, incluida la elaboración de perfiles. Estas disposiciones buscan asegurar que la IA se utilice de manera ética y responsable, protegiendo a los consumidores de los posibles efectos adversos de la automatización y el procesamiento de datos, y garantizando que se respeten sus derechos fundamentales.

10. INNOVACIÓN

El RIA de la Unión Europea no solo establece prohibiciones y obligaciones, sino que también tiene como objetivo promover la innovación y el desarrollo tecnológico en el ámbito de la IA. Este enfoque busca equilibrar la seguridad y el cumplimiento normativo con el impulso al progreso y la competitividad, en particular para pymes y startups. El RIA crea un marco jurídico que garantiza tanto la seguridad como la innovación en el desarrollo de sistemas de IA. Para fomentar un entorno favorable, introduce medidas como los sandboxes regulatorios, que permiten a los desarrolladores experimentar bajo supervisión regulatoria, asegurando el cumplimiento de las normativas y reduciendo barreras técnicas y costos regulatorios.

ESTUDIOS

Las nuevas tecnologías han irrumpido en todos los ámbitos de la vida y lo hacen en constante evolución. Esta imparable evolución provoca el planteamiento de nuevos conflictos, retos y oportunidades frente a las que el Derecho debe reaccionar. Así, está teniendo lugar un torrente de nuevas regulaciones y propuestas regulatorias para adaptar los clásicos paradigmas del Derecho privado a esta nueva realidad, que exige de profesionales en la materia de una constante labor de actualización. En este sentido, la obra contribuye, no solo a esta necesaria labor de actualización, mediante el análisis de diversas de estas normas de recentísima aprobación y proposición (MiCA, DSA, DMA, propuestas regulatorias en materia de IA, garantías y productos defectuosos, etc.), sino también al fomento del juicio crítico respecto a la oportunidad de estas regulaciones. Asimismo, la obra ofrece diversas propuestas de utilidades y provechos que el propio Derecho puede extraer de la aplicación de estas nuevas tecnologías. En fin, la obra contiene un estudio multisectorial de las últimas normas aprobadas y propuestas en materia de nuevas tecnologías, con un enfoque marcadamente crítico, así como el análisis de distintas implementaciones de las nuevas tecnologías que permitirían alcanzar una mejor aplicación y ejecución del propio Derecho.

El precio de esta obra incluye la publicación en formato DÚO sin coste adicional (papel + libro electrónico)

ACCEDE A LA VERSIÓN ELECTRÓNICA SIGUIENDO LAS INDICACIONES DEL INTERIOR DEL LIBRO

ISBN: 978-84-1163-866-1