FACULTAD DE DERECHO

REGULACIÓN EUROPEA DE LA INTELIGENCIA ARITIFICIAL

Autor: Carmen Cañete García-Ferrer

5º E-3 A (Derecho y ADE)

Departamento de Mercantil

Tutor: Ignacio Ramos Villar

Madrid

Abril 2024

Resumen

La revolución de la inteligencia artificial en la última década ha transformado radicalmente diversos sectores, evidenciando un crecimiento exponencial y una naturaleza innovadora que plantean tanto oportunidades como desafíos significativos.

Ante este panorama, la necesidad de una regulación adecuada se hace imperativa para asegurar que el desarrollo de la IA se alinee con los principios de protección de los derechos y libertades fundamentales. El Reglamento de Inteligencia Artificial, aprobado por el Parlamento Europeo el 13 de marzo de 2024, emerge como respuesta a esta necesidad, estableciendo un marco normativo integral y ordenado para guiar el avance de la IA en Europa.

Este marco legislativo intenta equilibrar la innovación con la salvaguarda de los derechos individuales, abarcando desde la clasificación de los sistemas de IA según su nivel de riesgo—categorizando sistemas prohibidos, de alto riesgo y de uso general—hasta la implementación de requisitos y obligaciones específicas para su desarrollo y operación. Se enfatiza la importancia de un seguimiento y adaptación continuos del marco normativo frente a las innovaciones tecnológicas, para proteger el interés público sin frenar el progreso tecnológico.

La regulación europea se contrasta con enfoques internacionales, como los de China y Estados Unidos, destacando las singularidades de la perspectiva europea. Este análisis subraya la relevancia de una regulación proactiva y crucial para el futuro de la IA, asegurando que su desarrollo se alinee con los valores y necesidades sociales, económicas y éticas de nuestra era.

Palabras clave: Inteligencia Artificial, Unión Europea, Reglamento de la Inteligencia Artificial, riesgo, protección.

Abstract

The artificial intelligence revolution over the last decade has radically transformed various sectors, demonstrating exponential growth and an innovative nature that presents both significant opportunities and challenges.

In this context, the need for appropriate regulation becomes imperative to ensure that the development of AI is aligned with the principles of protecting fundamental rights and freedoms. The European Parliament adopted the Artificial Intelligence Regulation on 13 March 2024 as a response to the need for a comprehensive and orderly regulatory framework to guide the advancement of AI in Europe.

This legislative framework seeks to balance innovation with the safeguarding of individual rights. It categorizes AI systems based on their level of risk, including prohibited, high-risk, and general-purpose systems. The framework also includes specific requirements and obligations for the development and operation of these systems. The importance of continuous monitoring and adaptation of the regulatory framework in the face of technological innovations is emphasized, to protect the public interest without slowing down technological progress.

European regulation is contrasted with international approaches, such as those of China and the United States, highlighting the singularities of the European perspective. This analysis highlights the importance of proactive and essential regulation for the future of AI, ensuring that its development aligns with the social, economic, and ethical values and needs of our time.

Key words: Artificial Intelligence, European Union, AI Act, risk, protection.

LISTADO DE ABREVIATURAS

Art.	Artículo
Arts.	Artículos
AI	Algoritmos Inteligentes
BD	Big Data
DMA	Reglamento de Mercados Digitales
DGA	Ley de Gobernanza de Datos
DSA	Ley de servicios Digitales
EM	Estados Miembros
EE. UU	Estados Unidos
FLOP	Operaciones de punto flotante
HPC	*High-Performance Computing*
IA	Inteligencia Artificial
I+D	Investigación y Desarrollo
MFP	Marco Financiero Plurianual
ODS	Objetivos de Desarrollo Sostenible
PE	Parlamento Europeo
PI	Propiedad Intelectual
RGDP	Reglamento General de Protección de Datos
RIA	Reglamento de Inteligencia Artificial
MFP	Marco Financiero Plurianual
TFG	Trabajo de Fin de Grado
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea

ÍNDICE

I. INTRODUCCIÓN

CAPÍTULO I. CUESTIONES PRELIMINARES

La Inteligencia Artificial (en adelante, IA), ha supuesto un impacto en todos los campos profesionales, como resalta el Fondo Monetario Internacional, la IA afecta a casi un 40% del empleo mundial[1]. Como consecuencia, existe una necesidad de regulación a nivel internacional y español. Por ello, la Unión Europea propuso en abril de 2021 un primer marco regulador mediante la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadoras en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021.

Esta propuesta se ha ido perfeccionando y el 13 de marzo de 2024 el Parlamento Europeo aprobó el Reglamento de Inteligencia Artificial (en adelante, RIA) mediante la Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021)0206 – C9-0146/2021 –2021/0106(COD)).

La regulación jurídica de la IA ha supuesto un reto jurídico y la UE es la primera en ofrecer una regulación integral y ordenada. La razón principal para la falta de regulación a nivel internacional es que, aunque algunas tecnologías existen desde hace más de 50 años, los avances más importantes, de la mano del Big Data se han acometido en los últimos años[2].

A lo largo de este Trabajo de Fin de Grado analizaremos el RIA, que tiene como objetivo proteger los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad ambiental frente a la nueva disciplina científica que como define la Real Academia Española, "se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico".

[1] Georgieva, K. "La economía mundial transformada por la inteligencia artificial ha de beneficiar a la humanidad". *IMF Blog*, 16 de enero de 2024 (disponible en imf./ai-global-economy-benefits; última consulta 9/04/2024)

[2] MARTÍN LÓPEZ, J. (enero 2023). Inteligencia artificial y transparencia. Monografías. Inteligencia artificial y comprobación tributaria: transparencia y no discriminación. Editorial Aranzadi S.A.U

CAPÍTULO II. METODOLOGÍA Y ESTRUCTURA

En el ámbito del derecho, la IA representa un desafío normativo y conceptual de primer orden; por lo que este Trabajo de Fin de Grado se centra en las complejidades jurídicas que la IA impone. La estructura de este trabajo se divide en tres segmentos que, en conjunto, buscan ofrecer una visión comprensiva sobre cómo su actual regulación.

Siguiendo una metodología deductiva, el TFG comienza con el concepto de IA y su evolución histórica hasta llegar a su comprensión actual. Esta sección no solo establece el marco teórico necesario para el análisis subsiguiente, sino que también contextualiza la importancia de la IA en el tejido social y económico actual.

Posteriormente, el foco se desplaza hacia el estudio riguroso del Reglamento de Inteligencia Artificial (RIA), aprobado por el Parlamento Europeo. Este análisis abarca desde el ámbito de aplicación del reglamento, hasta su sistema de clasificación de riesgos, pasando por las medidas de apoyo a la innovación, su estructura de gobernanza y las posibles sanciones en caso de incumplimiento.

El último tramo del TFG se dedica a explorar las implicaciones que el RIA tendrá en el futuro. A través de esta sección, se pretende revelar cómo esta enfrenta una problemática respecto a su ámbito de aplicación, efectos en las responsabilidades empresariales y el sector laboral; y por último sus repercusiones éticas.

Para abordar con en profundo estos temas, la metodología empleada combina distintos métodos de investigación jurídica. Desde la perspectiva de derecho positivo, se han revisado las disposiciones legales sobre la IA en España, en especial, la normativa a nivel europeo. Complementando metodológico conceptualista, al estudiar obras doctrinales que ilustran la necesidad de una regulación pronta y precisa.

Asimismo, se ha recurrido a ponencias especializadas sobre la materia, como la que tuvo lugar el pasado mes de febrero, con el título “El futuro de la regulación de la inteligencia artificial en la

UE: El riesgo como elemento clave de responsabilidad", impartida por Juan Pedro Díaz Senés, investigador predoctoral de la URJC especializado en Derecho Digital y organizada por AJAMadrid.

Así como la titulada "Coyuntura sector bancario: Tendencias globales y sector bancario" de D. José Luis de Mora, que ocupa el puesto de CEO de Santander Consumer Finance y que tuvo lugar en la Universidad Pontificia de Comillas en el mes de enero. Estas fuentes han ayudado a situar el debate sobre la IA en un contexto más amplio y globalizado, de la mano de expertas en la materia.

El derecho comparado también juega un papel esencial en este estudio, permitiendo situar la regulación de la IA en España dentro de un marco más amplio, facilitando así la comprensión de cómo diferentes jurisdicciones abordan los retos similares, en concreto estudiamos la regulación china y estadounidense en materia de IA.

En conclusión, este TFG se adentra en la complejidad jurídica que la IA representa y propone una reflexión sobre el futuro de la regulación en este ámbito, destacando la necesidad de adaptar el marco normativo a las rápidas innovaciones. La combinación de análisis legislativo, doctrina especializada y derecho comparado conforma una metodología robusta y coherente, capaz de ofrecer respuestas a algunas de las preguntas que la IA plantea al derecho contemporáneo.

II. REGULACIÓN EUROPEA

CAPÍTULO I. LA INTELIGENCIA ARTIFICIAL

La IA es un concepto difícil de definir, dada su naturaleza heterogénea y su constante evolución, o como expresa BUJOSA VADELL, es el mejor ejemplo de *work in progress*, del que todavía no sabemos bien adónde nos va a llevar[3]. Por ello, el Parlamento Europeo ha acogido un término amplio que expone en su página web, "la IA es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear"[4].

Los sistemas de IA, como expone el considerando 12 del RIA, poseen una capacidad única de inferencia, lo que les permite generar predicciones, recomendaciones o decisiones. Esta capacidad se logra mediante técnicas de aprendizaje automático, que permiten a los sistemas aprender y alcanzar objetivos específicos basados en conocimiento y lógica, que infieren a partir de información codificada. La inferencia en IA va más allá del simple procesamiento de datos, facilitando el aprendizaje avanzado, el razonamiento y la creación de modelos, lo que significa que estos sistemas pueden tener un impacto significativo en el mundo físico y virtual.

Este nivel de autonomía les permite operar con un margen de independencia de las acciones humanas, lo que incluye la capacidad de ejecutar sin intervención directa. BEATRIZ BELANDO GARÍN en su obra "La inteligencia artificial en la supervisión del mercado de valores"[5], destaca los riesgos asociados con el uso de algoritmos en la toma de decisiones, subrayando la necesidad de no reemplazar el juicio humano, especialmente en lo que respecta a la iniciación de procedimientos de inspección o sanción la discriminación.

Como consecuencia de esta evolución de la IA, la línea entre la realidad y la simulación cada vez es más borrosa. Jason Rohrer ha desarrollado un sistema llamado *Project December* que permite

[3] BUJOSA VADELL, L.M., (enero 2022). La gran incógnita de la inteligencia artificial, Editorial Aranzadi, S.A.U.
[4] Parlamento Europeo, "¿Qué es la inteligencia artificial y cómo se usa?", *Nota de Prensa Parlamento Europeo*, 8 de septiembre de 2020. (disponible en europarl.europa.eu/ia-y-como-se-usa; última consulta 7/04/2024).
[5] BELANDO GARÍN, B. (2022). La inteligencia artificial en la supervisión del mercado de valores. Revista de Derecho del Sistema Financiero num 4/2022, Editorial Aranzadi S.A.U.

tener conversaciones de texto con cualquier persona, incluso simulando con aquellas ya fallecidas[6]. MARÍA SUÁREZ PLIEGO, socia de Derecho Mercantil en el despacho de Andersen, realiza un análisis sobre el impacto de esta tecnología en propiedad intelectual titulado "Impacto de las tecnologías de Inteligencia Artificial generativa y los derechos de propiedad intelectual: necesidad de establecer una estrategia"[7], el cual aborda el desafío que representa la IA, especialmente la IA generativa, para los derechos de propiedad intelectual (en adelante, PI).

Se destaca cómo estas tecnologías, capaces de generar nuevas obras sin intervención humana, plantean cuestiones críticas sobre la titularidad de los derechos sobre las obras generadas y cómo gestionar sus infracciones. Es clave identificar la titularidad de los derechos de explotación y abordar la infracción de derechos de PI por el uso de obras preexistentes en el entrenamiento de IA. Se sugiere aumentar el grado de intervención humana y la importancia de los datos y material protegido utilizados, así como sus fuentes.

A modo de ejemplo, el usuario llamado "Ghostwriter977" creó con IA y publicó una canción de Drake con The Weekend llamada "Heart on my Sleeve"[8], la cual obtuvo 625.000 reproducciones en Spotify, 275.000 en YouTube, 15 millones en TikTok y más de 20 millones en Twitter.

Dado el alcance que tiene, se requiere un estudio y regulación para minimizar el impacto negativo. MARÍA TERESA MARTÍNEZ en su estudio "Claves del impacto de la protección de datos en la sostenibilidad"[9], subraya como actualmente se está dando un tsunami regulatorio en Derecho Digital, con regulaciones como el Reglamento de Mercados Digitales (DMA), la Ley de servicios Digitales (DSA), la Ley de Gobernanza de Datos (DGA), la Ley de datos (DA) y el objeto de estudio de este TFG, la propuesta de Reglamento de Inteligencia Artificial (RIA).

[6] Mance, H. "A chatbot that imitates the death. Is it a good idea?", *Financial Times*, 12 de febrero de 2024 (disponible en https://www.ft.com/content/ , última consulta 10/04/2024)
[7] SUÁREZ, M. (2024). Impacto de las tecnologías de la IA generativa y los derechos de propiedad intelectual: necesidad de establecer una estrategia. Actualidad Jurídica Aranzadi num. 1005/2024, Editorial Aranzadi S.A.U.
[8] Savage, M. "El éxito viral de una canción creada por inteligencia artificial con las voces de Drake y The Weekend", *BBC*, 17 de abril de 2023 (disponible en https://www.bbc.com/mundo/ , última consulta 10/04/2024)
[9] MARTÍNEZ, M.T. (2023). Claves del impacto de la protección de datos en la sostenibilidad. Actualidad Jurídica Aranzadi num 998/2023 parte comentario. Editorial Aranzadi, S.A.U., Cizur menor.

CAPÍTULO II. EVOLUCIÓN HISTÓRICA

La UE es pionera en la regulación de la IA. Desde muy temprano, y de forma coherente con los principios de buena gobernanza y fomente de un mercado único armonizado, la UE ha velado por una regulación de las nuevas tecnologías.

El compromiso regulatorio de la UE refleja la preocupación por garantizar aquellos derechos que considera fundamentales. Uno de ellos es el derecho a la protección de los datos personales contenido en el art. 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, así como en el art. 16.1 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE).

Este derecho es de gran importancia y por ello, en 2016 la UE aprobó el Reglamento (UE) 2016/679 (LCEur 2016, 605) del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), que posteriormente se adaptó a nuestro ordenamiento jurídico, a través de la Ley Orgánica 3/2018 de 5 de diciembre (RCL 2018, 1629), de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). El uso de la IA sin una regulación apropiada puede suponer una amenaza para la protección de los datos de carácter personal[10].

La exposición de motivos de este reglamento, no se aleja mucho de la realidad actual cuando expone que se crea el RGDP con motivo de la evolución tecnológica y la globalización que han aumentado de manera significativa. Además, añade que la tecnología ha transformado la economía y la vida social y concluye que las personas físicas deben tener el control de sus propios datos personales y en consecuencia, se debe reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

Este reglamento, bastante reciente, contiene algunos principios que no siempre resultan sencillos de conciliar con la IA. Por ejemplo, la adopción de criterios de transparencia sobre los modelos y

[10] GONZÁLEZ RUIZ, F.J. (2019). Inteligencia artificial: implicaciones en materia de protección de datos, Actualidad Jurídica Aranzadi, Editorial Aranzadi S.A.U.

algoritmos puede colisionar con los derechos de propiedad intelectual y de competencia[11]. Por otra parte, la aplicación de principios generales recogidos en el reglamento, como la minimización de datos y protección de datos por defectos, pueden entrar en conflicto con la forma de actuar de la IA. Además, el RGPD otorga el derecho a no ser objeto de una decisión que haya sido automatizada y que produzca efectos jurídicos en él o le afecte de manera significativa.

Un año más tarde, en 2017, el Consejo Europeo, con la colaboración de un Comité de Expertos de Intermediarios en Internet (MSI-NET), desarrolló un estudio sobre el impacto que tendrían las técnicas automatizadas de datos – especialmente los algoritmos – en los derechos humanos. Este estudio es conocido como *Algorythms and Human Rights*.

En este estudio se atienden algunas preocupaciones como la supresión de la libertad de expresión, la tendencia a la discriminación de las IA, el menoscabo del derecho a las elecciones libres, el peligro de no alcanzar juicios justos y con garantías procesales como consecuencia de algoritmos capaces de predecir individuos con mayor disposición a delinquir. Es sonado el caso de la policía de Estados Unidos que hacía uso de un sistema de IA llamado *PredPol*, para predecir los crímenes que pueden cometerse, desde el tipo de delito, hasta su lugar y fecha[12].

Esta IA reproduce hábitos policiales y, por tanto, prima que se patrulle por determinadas zonas durante más tiempo e intensidad. Esto ha provocado que se descubran más delitos y estos delitos estén relacionados con algunas minorías que retroalimentan el sistema que está sesgado y atenta contra los derechos humanos[13]. Otro ejemplo de discriminación de las IA nos lo ofrece VELIZ en relación con el uso de la IA en la contratación. Se expone el caso de Amazon que discriminó a las mujeres frente a los hombres, no porque los hombres fueran mejores candidatos sino porque la base de datos del historial de contratación que le habían introducido a la IA reflejaba que Amazon había preferido contratar a hombres en los años anteriores[14].

---

[11] SUÁREZ, M. (2024). *Op. cit.*
[12] Navarrete, F., "PredPol: Inteligencia Artificial, Algoritmos y Predicción de Crímenes", *Métodos Avanzados de Investigación 1*, de 23 de mayo de 2021 (disponible en metodos/predpol-crimenes , última consulta 10/04/2024)
[13] MARTÍN DIZ, F. (enero 2022). La eclosión de la inteligencia artificial en el ámbito jurídico, Editorial Aranzadi S.A.U.
[14] VELIZ, C., "Inteligencia artificial: ¿proceso o retroceso?" (Tribuna). Suplemento Retina, *El País*. 14 de junio de 2019

El otro gran pilar es la pérdida de la privacidad y falta de protección de datos. MARÍA TERESA BENDITO CAÑIZARES aborda la crucial necesidad de una regulación ética en el espacio digital europeo, para crear un entorno digital europeo ético, transparente y responsable, en su obra "Estadio intermedio de reflexión para una futura regulación de la ética en el espacio digital europeo: los principios de transparencia y accountability"[15].

Resalta la dificultad de aplicar la normativa existente a la terminología dinámica y en constante cambio de la IA, el big data (BD) y los algoritmos inteligentes (AI). Resalta los principios de transparencia y responsabilidad en el tratamiento de datos personales, no solo como una rendición de cuentas, si no como un derecho a la explicación de la lógica detrás de los algoritmos.

También en 2017, varios Estados Miembros pactaron colaborar para desarrollar infraestructuras de informática de alto rendimiento y así fortalecer la posición europea en el mercado mundial. Este pacto dio lugar al Reglamento (UE) 2018/1488 por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea, más conocida como EuroHPC (*High-Performance Computing*). La informática de alto rendimiento es una rama informática que realiza tareas científicas y de ingeniería tan complejas que no es posible realizar los cálculos con ordenadores de uso general[16].

El plan de la declaración se articulaba en tres pilares: (i) la construcción de una infraestructura de supercomputación de clase mundial, (ii) El desarrollo de tecnologías y aplicaciones de HPC innovadoras y (iii) el fomento de la adopción de HPC en la economía y en la sociedad. La UE consideró que esta declaración era importante para derribar los obstáculos virtuales que existían entre los 28, en aquel momento, Estados Miembros y promover la libre circulación. Para materializar esta propuesta, se previó una considerable inversión para crear una red de

[15] BENDITO CAÑIZARES, M.T., (2021). Estadio intermedio de reflexión para una futura regulación de la ética en el espacio digital europeo: los principios de transparencia y accountability. Revista Aranzadi de Derecho y Nuevas Tecnologías num. 55/2021, Editorial Aranzadi S.A.U.

[16] Comisión Europea, "La información de alto rendimiento y la iniciativa EuroHPC", *Nota Informativa Comisión Europea*, 11 de enero de 2018 (disponible en https://ec.europa.eu/commission/presscorner/detail/es/MEMO_18_3)

computadoras de alto rendimiento, centros de datos de última generación y tecnologías que mejoraran la eficiencia y rendimiento de los sistemas HPC.

En 2018, la UE dio un paso más en esta evolución, mediante la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027. En este plan, el PE y el Consejo se enfocaron en las inversiones estratégicas para el apoyo a la investigación y la innovación, centrándose en el tratamiento de datos, la ciberseguridad y la IA.

Este programa dotaba parte del presupuesto del marco financiero plurianual (MFP) para los cinco objetivos contenidos en el programa Europa Digital que eran: (i) la informática de alto rendimiento, (ii) la inteligencia artificial, (iii) la ciberseguridad y confianza, (iv) las competencias digitales avanzadas y (v) el despliegue o mejor uso de las capacidades digitales y de interoperabilidad.

En relación a la IA, el art. 5 contiene las siguientes propuestas:

a) "Intensificar y reforzar las capacidades básicas de inteligencia artificial en la Unión, incluidos los recursos de datos y las bibliotecas de algoritmos de conformidad con la legislación sobre protección de datos;
b) Hacer accesibles dichas capacidades a todas las empresas y administraciones públicas[17];
c) Reforzar y poner en red las instalaciones de ensayo y experimentación de inteligencia artificial existentes en los Estados miembros".

El 7 de diciembre 2018, la Comisión Europea realizó una comunicación al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre un plan coordinado sobre Inteligencia Artificial[18]. El objetivo principal de este comunicado era

[17] ARIZA COLMENAREJO, Mª J. (2022). Decisiones basadas en inteligencia artificial y el objeto de la impugnación. Inteligencia artificial y administración de justicia, Editorial Aranzadi S.A.U.
[18] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan Coordinado sobre la inteligencia artificial, 7 de diciembre de 2018. COM (2018) 795.

establecer un marco ético y legal sólido, así como buscar la competitividad y la innovación frente a otras potencias mundiales.

El reto al que se enfrentó la Comisión en 2018 y con la que nos seguimos encontrando actualmente en la regulación de la IA, fue encontrar un equilibrio entre la seguridad y la protección de los ciudadanos frente al impulso en la inversión y desarrollo. La Comisión comunicaba que era necesario crear unos mínimos legales comunes a todos los EM para poder lograr un mercado único digital, como ya había anunciado el año anterior en la Declaración EuroHPC.

Además, la Comisión, consciente del impacto ético que puede llegar a tener la IA propuso un marco que sirviera para guiar en la creación de estas nuevas tecnologías y que reflejara los valores europeos como la transparencia, la responsabilidad o la equidad. Asimismo, conscientes de la capacidad de integración de las tecnologías, la Comisión promovió la educación y la formación continua en habilidades digitales, creando másteres y doctorados en IA para evitar que los conocedores de esta materia migraran a centros de tecnología e innovación como es Silicon Valley.

A modo de colofón, la Comisión propuso, con el fin de materializar la propuesta, crear un Grupo de Expertos en IA para asesorar sobre cuestiones éticas y legales y constituir el Observatorio Europeo de la IA con el fin de monitorear y analizar el progreso en este ámbito.

En 2019 la Comisión siguió avanzando, mediante una nueva comunicación[19] con el objetivo de generar confianza en la IA centrada en el ser humano. El 8 de abril de 2019 se emitió el comunicado donde la Comisión Europea completa y amplía las propuestas presentadas en el Plan Coordinado sobre IA de 2018. En este nuevo comunicado se fijaron directrices más detalladas enfocadas a garantizar que el desarrollo y despliegue de las IA se realice de manera ética y respetando los derechos fundamentales y valores consagrados en la normativa europea.

[19] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Generar confianza en la inteligencia artificial centrada en el ser humano, 8 de abril de 2019. COM (2019) 168.

La privacidad y dignidad de las personas eran el foco principal del comunicado, por lo que iban de la mano con medidas para garantizar la transparencia y la responsabilidad en el diseño y uso de los sistemas de IA. Además, como indica el título de la comunicación, se pretende generar confianza en la IA y esto se consigue reforzando la educación digital[20] y creando mecanismos de evaluación y certificación de conformidad con la ética.

El 19 de febrero de 2020, unas semanas antes de que la pandemia de Covid-19 paralizara las actividades corrientes de las instituciones de la UE, se desarrolló el Libro Blanco sobre la IA- un enfoque europeo orientado a la excelencia y la confianza[21]. Los Libros Blancos de la Comisión son documentos con propuestas de acciones de la UE para un campo de actuación específico. Tienen como propósito iniciar un debate con el público, las partes interesadas, el Parlamento Europeo y el Consejo, para lograr un consenso político.

El Libro Blanco trajo nuevas aportaciones y reforzó algunas de las existentes, entre ellas, podemos mencionar: (i) la creación de un mercado único digital; (ii) el fomento de la inversión en investigación y desarrollo, para posicionar a Europa como líder mundial; (iii) el establecimiento de estándares éticos y de seguridad para los sistemas de IA; (iv) la promoción de la colaboración internacional, con el fin de garantizar la coherencia y eficacia de las políticas.

Como antecedente inmediato del RIA encontramos la propuesta de reglamento del Parlamento Europeo y del Consejo, del 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión. El 6 de diciembre de 2022, el Consejo adoptó por unanimidad la propuesta y el 14 de junio de 2023, el PE confirmó su posición con una votación plenaria. Entre junio y octubre de 2023 tuvieron lugar diálogos políticos tripartitos donde se alcanzaron acuerdos sobre partes menos controvertidas de la propuesta y sobre las disposiciones de medidas de apoyo a la innovación y los sistemas de IA como de alto riesgo. En el siguiente apartado, procedemos a analizar el RIA en profundidad.

[20] PLAZA PENADÉS, J. (2019). Protección y cuestiones legales de la inteligencia artificial. Formación e-learning. Curso de especialización en Know-How, propiedad intelectual en el mercado único digital. Editorial Aranzadi, S.A.U.
[21] Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, 19 de febrero de 2020 COM (2020) 65.

CAPÍTULO III. Reglamento de Inteligencia Artificial 5662/2024

La Ley de Inteligencia Artificial fue aprobada por el Parlamento Europeo el 13 de marzo de 2024[22] con 523 votos a favor, 46 en contra y 49 abstenciones. El Reglamento aún debe pasar por una verificación final de aspectos jurídicos y lingüísticos antes de su aprobación definitiva, que se espera ocurra antes del término de la legislatura de 2024, mediante un proceso conocido como el procedimiento de corrección de errores. Además, debe recibir la aprobación formal del Consejo[23].

1. ENTRADA EN VIGOR

Conforme al art. 113 RIA, este entrará en vigor veinte días después de su publicación en el Diario Oficial de la Unión Europea, iniciando un periodo de dos años para su plena aplicación. No obstante, el Reglamento prevé algunas excepciones que ajustan este calendario para ciertos capítulos y disposiciones.

En primer lugar, las disposiciones generales y las limitaciones a las prácticas prohibidas de IA (Capítulos I y II) entrarán en efecto seis meses tras la entrada en vigor del Reglamento.

Asimismo, se establece un plazo de un año desde la entrada en vigor para la aplicación de las normativas relacionadas con las autoridades notificantes y los organismos notificados de los sistemas de IA de alto riesgo (Capítulo III, Sección 4), los modelos de IA de uso general (Capítulo V), el marco de gobernanza (Capítulo VII), y el régimen sancionador (Capítulo XII), con la excepción del artículo 101, que detalla las multas para proveedores de modelos de IA de uso general.

[22] Parlamento Europeo, "La Eurocámara aprueba una ley histórica para regular la inteligencia artificial", *Nota de Prensa Parlamento Europeo*, 13 de marzo de 2024 (disponible en europarl.europa.eu/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial , última consulta 10/04/2024)
[23] Álvarez, P. (27 de diciembre de 2023). Avance histórico hacia el Reglamento de IA: se alcanza un acuerdo provisional. Blog de Propiedad Intelectual y Tecnologías de Cuatrecasas. (Disponible en cuatrecasas/propiedad-intelectual/historico-reglamento-ia-acuerdo-provisional, última consulta 10/04/2024)

Por último, las reglas de clasificación de los sistemas de IA de alto riesgo (Artículo 6.1), junto con el resto de las obligaciones estipuladas en el Reglamento, se implementarán a los 36 meses después de su efectiva entrada en vigor.

2. ÁMBITO DE APLICACIÓN

Este Reglamento aplica de manera indiscriminada a todos los proveedores de sistemas de IA, sin importar si tienen su base en la Unión Europea o en países externos a ella, así como los responsables de despliegue de sistemas de IA que estén establecidos dentro de la Unión.

Un sistema de IA puede manejar datos recogidos de manera legítima en la UE y enviados al exterior, entregando posteriormente sus resultados al contratista europeo sin que dicho sistema haya entrado en el espacio económico europeo. Con el objetivo de evitar la evasión de las normativas, el artículo 2 RIA amplía su alcance para incluir a los proveedores y operadores de sistemas de IA localizados fuera de la UE, condicionado a que la información procesada por estos sistemas se destine a ser utilizada dentro de la Unión.

Más adelante, pasa a excluir de su ámbito de aplicación a las entidades gubernamentales de países fuera de la UE y a organizaciones internacionales que operen en el marco de acuerdos internacionales o de cooperación con la UE o sus EM, para fines de cooperación policial y judicial, siempre que dichos terceros países u organizaciones aseguren una protección adecuada de los derechos y libertades individuales. Esto puede extenderse a las entidades a las que estos países terceros deleguen tareas específicas en apoyo a dicha cooperación. (Considerando 22 del RIA).

También excluyen a cualquier entidad, ya sea público o privado, que opere con fines militares, de defensa o de seguridad nacional. Esta exclusión se apoya en el artículo 4.2 del TUE y en las particularidades de las políticas de defensa de los Estados miembros y la UE en su conjunto, las cuales están regidas por el Derecho internacional público (Considerando 24 del RIA).

Sin embargo, si dichos sistemas de IA se emplean temporal o permanentemente para propósitos distintos a los militares o de seguridad nacional, como usos civiles, humanitarios, o de seguridad

pública, entonces sí entrarían en el ámbito de aplicación de este Reglamento. Del mismo modo, si el sistema de IA es de naturaleza mixta, es decir ofrece usos excluidos (militares, de defensa o de seguridad nacional) y no excluidos, deben sujetarse a este Reglamento.
Por último, excluye de su alcance a los sistemas y modelos de IA desarrollados y utilizados exclusivamente para la investigación y desarrollo científicos. Esta decisión se toma con el objetivo de promover la innovación y preservar la libertad en el ámbito científico, evitando obstaculizar las actividades de investigación y desarrollo (I+D). (Considerando 25)

No obstante, se establece claramente que esta exclusión no libera a dichos sistemas de cumplir con el Reglamento una vez que entran en el mercado o comienzan a ser utilizados fuera de un contexto de I+D. La intención es asegurar un equilibrio entre el fomento de la innovación en IA y la adherencia a los estándares regulatorios una vez que los productos de I+D se ofrecen al público o se implementan. (Considerando 26).

3. SISTEMA DE RIESGOS

El Reglamento se estructura en torno a la noción de riesgo, prohibiendo ciertas prácticas de IA consideradas peligrosas o éticamente inaceptables. Impone reglas estrictas para aquellos sistemas de IA identificados como de alto riesgo, garantizando su seguridad y conformidad ética. Mientras que, para el resto de los sistemas, exige medidas de transparencia y responsabilidad, equilibrando la promoción de la innovación con la protección del bienestar público.

Por tanto, la normativa se organiza en tres categorías claras: i) Sistemas de IA Prohibidos; ii) Sistemas de IA de Alto Riesgo; y iii) Sistemas de IA de Uso General.

En abril de 2019, el Grupo Independiente de Expertos de Alto Nivel sobre IA desarrolló "Directrices Éticas para una IA Fiable"[24], donde fijaba siete principios clave para una IA coherente y centrada en el ser humano. Estos principios han servido de marco general para la clasificación de riesgo: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y

[24] Grupo Independiente de Expertos de Alto Nivel sobre IA, "Directrices Éticas para una IA Fiable", Comisión Europea, 8 de abril de 2019 (disponible en digital-strategy.eu/ethics-guidelines-trustworthy-ai, última consulta 7/04/2024)

de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental y la rendición de cuentas.

3.1 Sistemas de IA Prohibidos

En el art. 5 RIA, establece la prohibición de ocho sistemas de IA que representan riesgos inaceptables. Busca evitar el uso de la IA como vehículo para prácticas de manipulación, explotación y control social contrarias a los principios de dignidad humana, libertad, igualdad, democracia y Estado de Derecho (Considerando 28).

Añadiendo una cláusula residual, en el apartado 8 del mismo artículo, donde se amplían las prohibiciones a cualquier práctica de IA que infrinja las leyes existentes de la Unión Europea, asegurando una cobertura integral.

3.1.1 Prohibición de técnicas subliminales, manipuladoras o engañosas en IA.

En su primer apartado, prohíbe de manera específica todo tipo de sistemas de IA que hagan uso de técnicas subliminales, manipuladoras o engañosas, cuyo fin o resultado sea cambiar sustancialmente cómo actúa una persona o un grupo, afectando seriamente su habilidad para tomar decisiones conscientes y provocando decisiones que de otra forma no se tomarían.

En su última parte, recalca la importancia de que este tipo de prácticas resulten en daño real o potencial para el usuario del sistema, para otras personas o para grupos. Enfatizando que el impacto debe ser de tal magnitud que cause o pueda causar perjuicios considerables.

3.1.2 Prohibición de IA que Explotan Vulnerabilidades Sociales

Más adelante, en su apartado b), específicamente veta los sistemas de IA diseñados para explotar vulnerabilidades específicas de individuos o grupos, por razón de su edad, discapacidad, o su condición social o económica.

El objetivo o consecuencia de estas prácticas debe ser la alteración sustancial del comportamiento de dichas personas, de tal forma que pueda causar, o sea probable que cause, daños significativos para a esas personas o terceros.

3.1.3 Prohibición de IA para Puntuación de la Ciudadanía

Se establece la prohibición de sistemas de IA destinados a evaluar o clasificar a individuos o grupos según su comportamiento social, características personales o rasgos de personalidad, ya sean explícitos, deducidos o predichos, durante un período determinado.

Esta medida busca evitar que las evaluaciones resultantes, conocidas como puntuaciones de ciudadanía, desemboquen en escenarios adversos como: i) el uso indebido de datos para perjudicar a individuos o grupos fuera del contexto original de recolección de datos, y ii) acciones desmedidas o injustas hacia personas o grupos, no acordes a su comportamiento o la severidad de este.

3.1.4 Prohibición de IA para Predicción de Delitos mediante Perfilado Personal

Se prohíben los sistemas de IA destinados a evaluar el riesgo de que individuos cometan delitos o predecir su probabilidad, fundamentándose exclusivamente en la creación de perfiles personales o en el análisis de sus rasgos y características de personalidad.

Sin embargo, se permite una excepción a esta regla. Dichos sistemas pueden emplearse para asistir en la evaluación de la implicación de una persona en actos delictivos, siempre que dicha evaluación esté basada en datos objetivos y verificables que estén directamente relacionados con la actividad criminal en cuestión.

3.1.5 Prohibición de IA para la Extracción Masiva de Reconocimiento Facial

Se establece la prohibición sistemas de IA destinados a generar o expandir bases de datos de reconocimiento facial a través de la recolección indiscriminada de imágenes faciales desde internet o sistemas de videovigilancia.

3.1.6 Prohibición de IA para el Reconocimiento de Emociones

Prohibición de sistemas de IA diseñados para deducir las emociones de las personas en lugares de trabajo y centros educativos, salvo en casos justificados donde el sistema se instale o introduzca por razones médicas o de seguridad. El art. 3.39 RIA define un Sistema de Reconocimiento de Emociones, como aquel "*destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos*".

Siendo los datos biométricos, según el apartado 34 del mismo artículo: "*los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos*".

El Considerando 18 del RIA aclara qué se entiende por emociones o intenciones, especificando ejemplos como ira, sorpresa, timidez, entusiasmo y vergüenza. Del mismo modo, excluye estados físicos tales como el dolor o la fatiga, siendo relevante, por ejemplo, en sistemas destinados a detectar fatiga en pilotos o conductores para prevenir accidentes.

Asimismo, se excluye la simple detección de expresiones, gestos o movimientos evidentes, a menos que estos se empleen para inferir emociones. Esto incluye expresiones faciales básicas, como sonrisas o ceños fruncidos; gestos corporales, como movimientos de manos, brazos o cabeza; o modulaciones en la voz, tales como elevar el tono o susurrar, siempre que dichas señales se utilicen para deducir emociones.

3.1.7 Prohibición de Sistemas de IA de Categorización Biométrica

Se prohíben sistemas de IA de categorización biométrica, los cuales están definidos en el art. 3.40 RIA como: "*un sistema de IA destinado a incluir a las personas físicas en categorías específicas*

en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas."

La práctica prohibida implica hacer uso de estos sistemas con el fin de deducir o predecir características personales de los individuos como su etnicidad, creencias políticas, afiliación sindical, creencias religiosas o filosóficas, su vida u orientación sexual.

No obstante, esta prohibición no aplica a la clasificación o el etiquetado de información biométrica obtenida legalmente, ni al manejo de dicha información en contextos de aplicación de la ley, como pueden ser operaciones policiales o de seguridad.

3.1.8 Prohibición de Sistemas de Identificación Biométrica Remota en Tiempo Real

Por último, se establece una prohibición específica para los sistemas de IA de identificación biométrica remota en tiempo real en lugares públicos. Es crucial destacar el término "tiempo real" para diferenciarlo de la identificación en diferido, que se tratará más adelante y no está sujeta a la misma restricción.

El artículo 3.41 RIA nos define en términos generales un Sistema de Identificación Biométrica Remota como "*un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia*".

Más adelante, en su apartado 42 se aclara que se entiende por identificación en "tiempo real", indicando que la captura, comparación e identificación de los datos ocurren "*sin una demora significativa"*. Por lo que engloba no solo la identificación instantánea, sino también las identificaciones que presenten retrasos mínimos.

a. Excepción a la prohibición general

No obstante, esta prohibición no es absoluta y el apartado 5.1.h) RIA habilita el uso de estos sistemas bajo ciertas circunstancias justificadas por tres objetivos principales. Estos representan

situaciones de urgencia que requieren actuación directa para salvaguardar la seguridad y el bienestar público.

El Reglamento establece los siguientes tres objetivos específicos: i) identificación de víctimas de secuestro, trata o explotación sexual, ii) la prevención de amenazas significativas e inminentes a la vida o seguridad, y iii) la localización o identificación de sospechosos de infracciones penales graves para su investigación, enjuiciamiento o ejecución de sanciones penales.

b. Requisitos para aplicar la excepción

i. Análisis de la situación y sus implicaciones

El uso de las excepciones debe ser limitado, destinándose exclusivamente a la verificación de la identidad del sujeto específico en cuestión. Es esencial considerar factores como el contexto que motiva la potencial aplicación de esta excepción, enfocándose en la gravedad, probabilidad e impacto del perjuicio que podría ocurrir si el sistema no se empleara.

Igualmente, es crucial evaluar las implicaciones que el uso del sistema tendría sobre los derechos y libertades de los individuos afectados, prestando especial atención a la gravedad, la probabilidad y el alcance de estas consecuencias.

ii. Autorización previa

Se exige que la autoridad nacional competente, ya sea judicial o administrativa, autorice el uso del sistema tras la realización de una evaluación de impacto en los derechos fundamentales, y la posterior inscripción del sistema en la base de datos de la UE, de acuerdo con el artículo 49 RIA.

Sin embargo, en situaciones de emergencia que requieran una acción inmediata, será posible activar estos sistemas sin autorización previa, siempre y cuando se solicite dentro de las siguientes 24 horas. Si la autorización acaba siendo denegada, el uso del sistema se deberá detener de inmediato y eliminar los datos recopilados.

Bajo las mismas circunstancias, se podrá activar el sistema antes de su registro en la base de datos de la UE, siempre y cuando se efectué tan pronto como sea posible sin retrasos innecesarios.

La autorización solo se concederá si se demuestra, mediante evidencia objetiva, que el uso del sistema es necesario y proporcionado para los objetivos específicos, delimitando de forma clara la duración, área geográfica y personas afectadas.

iii. Notificación a la autoridad de vigilancia y a la autoridad de protección de datos

Para aplicar esta excepción, es necesario notificar tanto a la autoridad de vigilancia del mercado como a la autoridad nacional de protección de datos. Estas autoridades, a su vez, están obligadas a informar a la Comisión mediante informes anuales sobre el uso autorizado.

Los Estados miembros pueden fijar condiciones específicas para autorizar estos usos, las cuales deben estar claramente detalladas en sus respectivas legislaciones nacionales. Este marco normativo debe abordar el trámite de solicitud, autorizaciones, uso, forma de supervisión y notificación correspondiente. Además, es requisito que los Estados miembros comuniquen a la Comisión las normativas adoptadas en un plazo no mayor a 30 días después de su aprobación.

iv. Garantías adicionales

Además, se requiere que cualquier uso de estos sistemas esté respaldado por las garantías y condiciones necesarios, conforme a la legislación nacional que regula dicha utilización, especialmente en términos de restricciones temporales, geográficas y de los individuos objetivo.

v. Participación de la Comisión Europea

La Comisión Europea proporcionará un formato estándar para recoger y analizar la cantidad de autorizaciones solicitadas y concedidas, tanto por parte de entidades judiciales como administrativas independientes, y los resultados de dichas solicitudes.

Anualmente, la Comisión difundirá informes sobre la implementación y el impacto de estos sistemas, garantizando que estos informes preserven la confidencialidad de cualquier dato operativo sensible vinculado a operaciones de seguridad.

3.2 Sistemas de IA de Alto Riesgo

Se define un marco de sistemas de IA catalogados como de alto riesgo, los cuales están sujetos a una serie de requisitos y obligaciones esenciales para su incorporación al mercado de la UE. Inicialmente, se establecen dos criterios fundamentales que, de ser cumplidos, clasifican automáticamente a un sistema de IA como de alto riesgo. Adicionalmente, se identifican ocho sectores específicos que, debido a su sensibilidad o relevancia estratégica, requieren que los sistemas de IA empleados sean considerados de alto riesgo.

3.2.1 Dos requisitos generales

El artículo 6 RIA define los sistemas de IA de alto riesgo como aquellos que reúnan dos características cumulativas. El primero es que el sistema sea un producto de seguridad o un componente de estos, regulado por las normativas de armonización de la UE. El segundo, es que, además, requiera una evaluación de conformidad por parte de un organismo independiente antes de su lanzamiento al mercado o su puesta en funcionamiento.

3.2.2 Ocho ámbitos clave con sistemas de IA de alto riesgo

Por otro lado, también se considerarán sistemas de IA de alto riesgo aquellos que pertenezcan a cualquiera de los ocho ámbitos fijados en el Anexo III del Reglamento. Estos son:

a. Biometría

El uso de la biometría se admite en tres categorías específicas, sujetas a la legislación de la UE y nacional. Primero, se autoriza el uso de sistemas de identificación biométrica remota, exceptuando aquellos sistemas de IA que se utilizan exclusivamente para verificar la identidad de una persona, confirmando que es quien dice ser. En segundo lugar, se permiten clasificar individuos según atributos sensibles o protegidos. Por último, se admite los sistemas de IA utilizados para el reconocimiento de emociones.

Es importante destacar que estos tres tipos de sistemas pasan a estar permitidos bajo la consideración de "alto riesgo", en tanto en cuanto no cumplen con los requisitos previstos del artículo 5 RIA. De cumplir con dichas estipulaciones, automáticamente serían clasificados como sistemas prohibidos.

b. Infraestructuras críticas

Engloba todos los sistemas de IA utilizados como elementos de seguridad en la administración y operación de "*infraestructuras digitales críticas*", así como en los sistemas de tráfico de vehículos o en la provisión de servicios de agua, gas, calefacción y electricidad.

c. Educación y formación profesional

Dentro de este ámbito, identificamos cuatro categorías de sistemas de alto riesgo. En primer lugar, se encuentran los sistemas diseñados para decidir sobre la admisión de individuos a instituciones educativas y de formación profesional en cualquier nivel.

En segundo lugar, se incluyen los sistemas de evaluación de desempeño educativo, particularmente aquellos utilizados para orientar y optimizar el proceso de aprendizaje. La tercera categoría abarca sistemas de IA destinados a determinar el nivel educativo que podría recibir un individuo, basándose en su acceso a unas instituciones educativas o de formación profesional u otras.

Por último, se clasifican como de alto riesgo aquellos sistemas empleados para supervisar y detectar comportamientos indebidos de estudiantes durante los exámenes.

d. Empleo, gestión de los trabajadores y acceso al autoempleo

En esta área se identifican dos categorías de sistemas con consideración de alto riesgo. La primera engloba a aquellos sistemas de IA diseñados para facilitar la contratación o selección de candidatos, incluyendo actividades como la publicación de vacantes laborales, el análisis y filtrado de candidaturas, y la evaluación de los postulantes.

La segunda categoría comprende sistemas de IA orientados a influir en decisiones relacionadas con las condiciones laborales, ascensos, o terminaciones de contratos, basados en análisis de comportamientos, cualidades o atributos personales para la asignación de responsabilidades. Estos sistemas también se utilizan para supervisar y valorar el rendimiento y actitudes de los trabajadores en el contexto de sus relaciones laborales

e. Acceso a servicios y prestaciones esenciales

En este apartado, enfocado en asegurar la igualdad de acceso para todos los ciudadanos a servicios esenciales, identificamos cuatro tipos de sistemas de IA de alto riesgo. Primero, aquellos sistemas utilizados por las autoridades públicas para determinar la elegibilidad de individuos al acceso a servicios esenciales o para administrar su concesión, modificación o suspensión.

En segundo lugar, se encuentran los sistemas empleados para evaluar la solvencia financiera de individuos o determinar su calificación crediticia, con la excepción de aquellos sistemas destinados a la detección de fraudes financieros. En tercer lugar, aquellos específicamente diseñados para la evaluación de riesgos y el establecimiento de tarifas en seguros de vida y salud.

Por último, los sistemas destinados a valorar y clasificar llamadas de emergencia, coordinar y priorizar el despliegue de servicios de respuesta inmediata, como policía, bomberos y asistencia médica, incluyendo el triaje de pacientes en situaciones de emergencia sanitaria.

f. Aplicación de la ley

Se identifican cinco categorías de sistemas de alto riesgo en el contexto de la aplicación de la ley. Estos incluyen sistemas desarrollados para predecir la posibilidad de que una persona se convierta en víctima de delitos, evaluar la credibilidad de las evidencias, y crear perfiles detallados de individuos durante investigaciones o procesos judiciales.

También se consideran de alto riesgo los polígrafos o sistemas similares. Por último, aquellos sistemas destinados a calcular la probabilidad de que una persona cometa un delito o reincida. Esto

abarca desde la creación de perfiles hasta la evaluación de rasgos de personalidad o el análisis de comportamientos delictivos previos, ya sea de individuos específicos o de grupos.

g. Migración, asilo y gestión del control fronterizo

Las autoridades están autorizadas a emplear determinados sistemas de IA para optimizar la gestión de estos procesos tan complejos, en el contexto de la migración, el asilo y el control fronterizo.

Se autoriza el uso de tecnologías como los polígrafos, así como sistemas para evaluar riesgos específicos, tales como amenazas a la seguridad, problemas de salud o situaciones de migración irregular, presentados por individuos que intentan entrar o que ya han ingresado al territorio de un Estado miembro.

Además, se faculta el uso de sistemas de IA para analizar solicitudes de asilo, visados o permisos de residencia, determinando su elegibilidad según los criterios establecidos, incluida la valoración de la veracidad de las evidencias presentadas.

Finalmente, se contemplan sistemas enfocados en la detección, reconocimiento o identificación de personas, con la excepción de aquellos utilizados exclusivamente para la verificación de documentos de viaje, en cuyo caso tendrán la consideración de IA de riesgo limitado.

h. Administración de justicia y procesos democráticos

Por último, la administración de justicia se encuentra dentro de los ocho ámbitos donde el legislador ha querido calificar dos tipos de sistemas como de alto riesgo. La primera categoría incluye sistemas diseñados para asistir a las autoridades judiciales en la investigación y análisis de hechos y leyes, así como en la adecuada aplicación legal a casos específicos.

La segunda categoría comprende aquellos sistemas capaces de influenciar el resultado de elecciones o referéndums, o el comportamiento de votantes en tales eventos. No obstante, se excluyen de esta clasificación aquellos sistemas cuyos resultados no impactan directamente a los

individuos, como las herramientas destinadas a la organización, optimización o planificación de campañas políticas desde un enfoque administrativo o logístico.

3.2.3 Excepciones a la Clasificación de Alto Riesgo

Un sistema de IA no se clasificará como de alto riesgo si no supone un peligro significativo para la salud, la seguridad o los derechos fundamentales de las personas, y en particular si no tiene un impacto sustancial en la toma de decisiones.

Esta excepción se aplica si se cumple al menos una de las siguientes condiciones: primero, el sistema de IA está diseñado para ejecutar una tarea procedimental específica y limitada; segundo, si el sistema tiene el objetivo de mejorar los resultados de operaciones humanas ya existentes; tercero, si se emplea para detectar patrones de decisión o desviaciones, sin suplantar o alterar juicios humanos anteriores, asegurando siempre la existencia de un control humano adecuado.

Finalmente, se aplica si el sistema de IA se destina a tareas preparatorias para evaluaciones relevantes relacionadas con los ocho ámbitos descritos anteriormente del anexo III. No obstante, es importante recalcar que, independientemente de estas excepciones, cualquier sistema de IA se considerará automáticamente de alto riesgo si se utiliza para crear perfiles detallados de personas.

3.2.4 Requisitos de los sistemas de alto riesgo

De acuerdo con el art. 8 RIA, los sistemas de alto riesgo deben satisfacer una serie de condiciones específicas para su lanzamiento y comercialización, según su finalidad y conforme al conocimiento técnico actual en IA y tecnologías afines.

a. Sistema de gestión de riesgos.

El art. 9 RIA establece la obligatoriedad para los proveedores de crear, implementar y mantener un sistema de gestión de riesgos a lo largo de todo su ciclo de vida. Debe ser un proceso continuo que incluya la identificación y evaluación de riesgos potenciales, tanto en el uso previsto como en

un mal uso razonablemente previsible, así como el análisis de datos recopilados tras el lanzamiento.

Los proveedores deben tomar medidas adecuadas para mitigar o eliminar los riesgos detectados. Estos esfuerzos se deben realizar con la asistencia de los responsables de despliegue, los cuales deben tener conocimiento técnico, experiencia y formación sobre el uso previsto para el sistema de IA.

Además, se requiere que los sistemas de IA se sometan a pruebas exhaustivas para asegurar su funcionamiento conforme a la finalidad prevista antes de su lanzamiento al mercado, incluyendo, cuando sea necesario, pruebas en condiciones reales.

b. Datos y gobernanza de datos.

El artículo 10 RIA subraya la importancia de la gestión y gobernanza de datos en sistemas de alto riesgo. Establece criterios para asegurar que los conjuntos de datos de entrenamiento, validación y prueba sean de alta calidad y representativos, con el objetivo de minimizar errores y sesgos. Destaca la necesidad de prácticas rigurosas de gestión de datos para prevenir la discriminación, incluyendo el análisis y corrección de sesgos potenciales.

Los datos deben ser suficientemente representativos, tomando en cuenta las propiedades estadísticas necesarias y las características específicas del entorno donde se utilizará el sistema de IA. En circunstancias excepcionales, se permite el uso de categorías de datos personales para corregir sesgos, siempre y cuando se respeten los derechos y libertades fundamentales.

c. Documentación técnica.

El artículo 11 RIA exige a los proveedores de sistemas de IA de alto riesgo elaborar y actualizar continuamente una documentación técnica que evidencie la conformidad con los requisitos, antes de su introducción al mercado o puesta en servicio; para su posterior evaluación por autoridades.

Dicha documentación, detallada en el Anexo IV, debe abarcar todos los aspectos críticos del sistema, desde su elementos y proceso de desarrollo y supervisión, hasta su sistema gestión de riesgos. La Comisión se reserva el derecho de actualizar dicho anexo para adaptarse a los avances tecnológicos y asegurar una evaluación adecuada de los sistemas.

Se ofrece un formato simplificado para pymes y startups, facilitado por un formulario específico de la Comisión. Para sistemas vinculados a productos bajo regulación de armonización de la UE, la documentación deberá ser unificada, incluyendo tanto los requisitos de IA como los específicos del producto.

d. Conservación de registros.

El artículo 12 RIA estipula la obligación de que los sistemas de alto riesgo incorporen la capacidad de generar registros automáticos de eventos, llamado "archivos de registro", a lo largo de su ciclo de vida, con el objetivo de asegurar un adecuado nivel de trazabilidad. Estos registros buscan facilitar identificar situaciones de riesgo, apoyar la vigilancia pos-comercialización y monitorear el desempeño del sistema.

En el caso particular de sistemas de IA dedicados a reconocimientos biométricos, se exige que los archivos de registro capturen información detallada sobre cada uso del sistema, incluyendo las fechas y horas de operación, las bases de datos contra las que se comparan los datos de entrada, los datos específicos que generaron coincidencias y la identificación del personal que verifica estos resultados.

e. Transparencia y comunicación de información a los responsables del despliegue.

El artículo 13 RIA establece las directrices de transparencia y comunicación de información para los sistemas de IA de alto riesgo. Establece que estos sistemas deben ser transparentes para facilitar su correcta interpretación y uso por parte de los responsables del despliegue.

Requiere que los sistemas incluyan instrucciones de uso claras y comprensibles que describan sus características, funcionamiento, y requisitos técnicos, junto con información sobre los niveles de precisión, solidez, ciberseguridad, y posibles riesgos.

Es fundamental que estas instrucciones detallen los procesos de entrenamiento, validación y prueba, así como cualquier cambio relevante desde la evaluación de conformidad inicial. Adicionalmente, deben orientar sobre la supervisión humana, los recursos necesarios para su operación, y las prácticas de mantenimiento para asegurar su funcionamiento óptimo, proporcionando una base sólida para su uso seguro y eficaz.

f. Vigilancia humana.

Como último requisito, el artículo 14 RIA obliga a los sistemas de IA de alto riesgo a ser diseñados para permitir una supervisión efectiva por seres humanos, lo que implica incluir en los sistemas herramientas de interfaz adecuadas.

Esta disposición busca minimizar riesgos para la salud, la seguridad, y otros derechos fundamentales. Las medidas de vigilancia deben ser proporcionales a los riegos, al nivel de autonomía y al contexto de uso del sistema.

Estas medidas permitirán a los supervisores entender y monitorear el sistema, interpretar correctamente su información de salida, y tomar decisiones informadas sobre su uso, incluida la capacidad de intervenir o detener el sistema de manera segura.

En particular, los sistemas de identificación biométrica remota requieren la verificación por al menos dos personas competentes, antes de actuar en base a la identificación generada por el sistema, con excepciones en casos donde aplicar este requisito sería desproporcionado.

3.3 Sistemas de IA de Uso General

En el último puesto de esta clasificación por riesgo, nos encontramos con los modelos de IA de uso general desarrollado en el Capítulo V del RIA. Introduce un marco general para su clasificación y obligaciones, en especial, cuando estos modelos presentan un riesgo sistémico.

A diferencia de los sistemas con mayor riesgo, estos modelos se consideran de riesgo limitado, sujetos a directrices menos estrictas, cuyo objetivo principal se centra en fomentar la transparencia y prevenir cualquier forma de engaño.

3.3.1 Clasificación como modelos con riesgo sistémico

De acuerdo con el artículo 51 RIA, se clasificará un modelo de IA de uso general como poseedor de un riesgo sistémico si demuestra tener capacidades de gran impacto, ya sea mediante evaluación técnica directa o a través de una resolución de la Comisión. Esta última puede actuar por iniciativa propia o en base a una alerta cualificada del Grupo de Expertos Científicos.

Para determinar si un modelo posee "capacidades de gran impacto", se recurrirá a metodologías y herramientas especializadas, como son indicadores y parámetros específicos. Además, se fija un criterio cuantitativo para esta clasificación, donde se establece que cualquier modelo que requiera más de 10^25 operaciones de punto flotante (FLOP) para su entrenamiento automáticamente se considerará de "gran impacto".

Además, la Comisión tiene la facultad de ajustar estos umbrales, permitiendo adaptaciones según la evolución tecnológica, como avances algorítmicos o mejoras en la eficiencia del hardware. Este enfoque flexible garantiza que la clasificación de los modelos de IA como de riesgo sistémico permanezca relevante y actualizada con el progreso tecnológico.

3.3.2 Procedimiento

El artículo 52 RIA describe el procedimiento para abordar los modelos con riesgos sistémicos. En todo caso, se exige al proveedor notificar a la Comisión si su modelo cumple con los criterios de "gran impacto" definidos anteriormente, a más tardar dos semanas desde alcanzar dicho umbral.

Adicionalmente, un proveedor puede argumentar que su modelo, a pesar de cumplir con los criterios de gran impacto, no constituye un riesgo sistémico debido a sus características únicas. La Comisión tendrá la facultad para desestimarlo si considera las pruebas insuficientes.

Los proveedores cuyos modelos hayan sido designados como de riesgo sistémico tienen el derecho a solicitar una reevaluación de esta clasificación, como máximo una vez cada seis meses. Dicha solicitud debe fundamentarse en razones objetivos y novedosas que no estuvieran disponibles en el momento de la decisión inicial.

Finalmente, la Comisión se compromete a mantener y publicar una lista actualizada de modelos de IA de uso general con riesgo sistémico, sin desproteger los derechos de propiedad intelectual e industrial, y la confidencialidad de la información empresarial.

3.3.3 Obligaciones de los proveedores de modelos de IA de uso general

El artículo 53 del Reglamento impone una serie de obligaciones a los proveedores, enfocadas en asegurar la transparencia, la seguridad y el cumplimiento normativo. Este enfoque subraya la importancia de la cooperación entre los proveedores de IA y las autoridades reguladoras, con el objetivo de asegurar prácticas éticas y seguras en el desarrollo y uso de la IA.

Se obliga a los proveedores a crear y actualizar continuamente una documentación técnica detallada de cada modelo, que debe ser accesible a la Oficina de IA y las autoridades competentes. Esta documentación debe incluir información detallada sobre el entrenamiento, las pruebas realizadas y los resultados de evaluación.

Asimismo, los proveedores deben proveer información relevante y actualizada a otros proveedores que planeen integrar dichos modelos en sus sistemas de IA. Esta obligación busca garantizar que los integradores de modelos puedan comprender las capacidades y limitaciones de los modelos de IA de uso general; sin olvidar la protección a los derechos de propiedad intelectual e industrial.

Además, se espera que los proveedores elaboren y difundan públicamente resúmenes detallados del contenido usado en el entrenamiento de los modelos, siguiendo las directrices de la Oficina de IA, promoviendo así la transparencia en las prácticas de entrenamiento.

Por último, toda información recopilada, incluyendo secretos comerciales y otra información sensible, será manejada bajo estrictas medidas de confidencialidad, asegurando que las prácticas y divulgación de modelos de IA de uso general se realicen de manera responsable y segura.

a. Adhesión a un Código de Buenas prácticas

La adhesión a códigos de buenas prácticas, según el artículo 53.4, permite a los proveedores de modelos de IA de uso general demostrar su cumplimiento regulatorio, hasta que se apruebe una normativa armonizada. Esta disposición permite el uso de códigos de buenas prácticas como evidencia de cumplimiento y, en su ausencia, exige a los proveedores demostrar a la Comisión la implementación de alternativas suficientes.

El artículo 56 delinea el proceso de desarrollo de estos códigos, promoviendo un enfoque colaborativo que involucra a la Oficina de IA, el Comité, autoridades nacionales, sociedad civil, y representantes de la industria y del ámbito académico.

Este esfuerzo conjunto tiene como objetivo asegurar una implementación efectiva del Reglamento, abordando temas clave como la actualización de la información sobre los modelos de IA, la gestión de riesgos sistémicos y la seguridad cibernética.

Para garantizar la efectividad de los códigos, se establecerán objetivos claros y específicos, como indicadores de rendimiento, que reflejen las variadas capacidades y tamaños de los participantes.

La Oficina de IA, con el apoyo del Comité, se encargará de supervisar el progreso y la implementación de estos compromisos, evaluando su impacto.

La Comisión, a través de actos de ejecución, puede conceder a estos códigos un estatus de validez general, incentivando así la adhesión por parte de los proveedores y su adaptación continua a las evoluciones tecnológicas y de mercado.

3.3.4 Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico.

El artículo 55 establece responsabilidades adicionales para los proveedores de modelos de IA de uso general clasificados como de riesgo sistémico. Estas responsabilidades complementan las obligaciones generales aplicables a todos los modelos de IA de uso general, subrayando la importancia de la precaución y mitigación de riesgos en su manejo.

En primer lugar, se exige a estos proveedores llevar a cabo evaluaciones detalladas de los modelos mediante protocolos y herramientas que reflejen los últimos avances tecnológicos, incluyendo pruebas de simulación para identificar y disminuir cualquier riesgo inherente al modelo.

Además, estos proveedores deben mantener un registro diligente y notificar sin demoras cualquier incidente grave a la Oficina de IA y, cuando sea aplicable, a las autoridades nacionales competentes, proporcionando también detalles sobre medidas correctivas potenciales.

Asimismo, es fundamental que evalúen y mitiguen cualquier riesgo potencial que pueda emerger del desarrollo, comercialización o uso de estos modelos, identificando y abordando las causas que lo originen. Por último, tendrán la obligación de establecer un nivel apropiado de protección de ciberseguridad para el modelo y su infraestructura física, asegurando así su integridad y seguridad.

4. MEDIDAS DE APOYO A LA INNOVACIÓN

La Unión Europea, reconociendo la crucial importancia de la innovación en IA para su competitividad global, ha instituido medidas específicas para promover el desarrollo responsable

y seguro de estas tecnologías. A través del Capítulo VI, se establece un marco para el apoyo activo a la innovación, centrando esfuerzos en la creación de espacios controlados de pruebas para IA.

4.1 Espacios Controlados de Prueba para IA

De conformidad con el artículo 57, los Estados miembros están obligados a implementar, al menos, un espacio de pruebas nacional dentro de los dos años posteriores a la entrada en vigor del reglamento. La UE busca proporcionar un entorno seguro y regulado para el desarrollo, la experimentación y la validación de nuevos sistemas de IA antes de su introducción en el mercado.

Estos espacios pueden ser establecidos individualmente o en colaboración con otros Estados, siempre contando con el soporte técnico y asesoramiento de la Comisión. Gracias a ello, los proveedores podrán probar sus sistemas bajo supervisión regulatoria, identificando y mitigando riesgos potenciales.

4.1.1 Características y Beneficios

Estos espacios representan ecosistemas innovadores donde los riesgos relacionados con los derechos fundamentales, la salud y la seguridad son evaluados cuidadosamente, y las estrategias de mitigación, verificadas.

Al participar en estos entornos, los proveedores de tecnología obtienen orientación crucial sobre cómo alinear sus desarrollos con las normativas vigentes, beneficiándose de la producción de informes de salida que acreditan la conformidad de sus sistemas con el reglamento.

Respetando las normas de confidencialidad y con el consentimiento del proveedor, la Comisión y el Comité podrán revisar dichos informes de salida, y en acuerdo mutuo hacerse públicos. La Comisión se encargará de crear una plataforma que sirva como punto de encuentro entre los diversos actores, ofreciendo un acceso directo a información valiosa.

Finalmente, como objetivos clave de estos espacios se encuentra mejorar la seguridad jurídica, apoyar el intercambio de mejores prácticas, fomentar la innovación y la competitividad, facilitar

el acceso al mercado de sistemas de IA, especialmente para pymes, y promover el aprendizaje regulatorio basado en evidencia.

4.1.2 Directrices y Gestión

Para asegurar una implementación armoniosa y evitar la fragmentación, en el artículo 58 se prevé la emisión de actos de ejecución, por parte de la Comisión, que detallen principios unificados sobre aspectos como la admisibilidad, la participación y las condiciones en los espacios de pruebas.

Este enfoque busca garantizar igualdad de acceso para todos los proveedores, fomentando en especial la inclusión de pymes mediante la simplificación de los trámites administrativos. Además, se limitará el tiempo de participación en estos espacios según la complejidad del proyecto, permitiendo extensiones por parte de la autoridad competente.

Se busca promocionar la seguridad jurídica, el intercambio de mejores prácticas y el fortalecimiento de la competitividad. Las autoridades nacionales competentes deberán garantizar la cooperación adecuada y proporcionar informes anuales sobre el progreso y resultados de estos espacios de pruebas a la Oficina de IA y al Comité de IA, promoviendo así la transparencia.

4.2 Tratamiento de Datos en Espacios de Prueba

El artículo 59 introduce directrices claras para el tratamiento de datos personales dentro de estos espacios, enfatizando la importancia de mantener estos datos en un entorno seguro, aislado y bajo estricto control. Esto garantiza que solo el personal autorizado pueda acceder a la información, y asegura la protección y eliminación de los datos, una vez que se finalice su uso o expire el plazo de conservación estipulado. También se establecen obligaciones de transparencia, como la publicación de una síntesis del proyecto de IA y sus objetivos.

4.3 Pruebas de sistemas de IA de alto riesgo en condiciones reales

Conforme al artículo 60, se permite a los proveedores de sistemas de IA de alto riesgo la oportunidad de realizar pruebas en condiciones reales. Para ello, es imprescindible adherirse a un conjunto de criterios estrictos, que incluyen la elaboración y aprobación de un plan de pruebas por parte de la autoridad de vigilancia, la obligatoriedad de registro en la base de datos de la UE, y la exigencia de que el proveedor tenga una presencia legal en la UE.

Además, se deben tomar medidas para proteger a los participantes vulnerables, garantizar su consentimiento informado, y supervisar meticulosamente el desarrollo de las pruebas. Las pruebas están temporalmente limitadas a un máximo de seis meses, con la posibilidad de una única prórroga.

Es obligatorio informar a las autoridades sobre cualquier incidente significativo durante las pruebas. Además, los participantes tienen el derecho de retirarse del proceso en cualquier momento, solicitando la eliminación de sus datos personales. Los proveedores asumen total responsabilidad por cualquier daño resultante de estas pruebas.

5. GOBERNANZA

El Capítulo VII RIA se dedica íntegramente a establecer un sistema de gobernanza, diseñado para garantizar una aplicación eficaz y un monitoreo continuo y evaluación de las mismas. Este marco es crucial para abordar los retos de la IA, promoviendo un equilibrio entre la innovación tecnológica y la protección de los derechos de los ciudadanos y la seguridad pública.

Para alcanzar estos objetivos, el reglamento instituye varias entidades clave, como eje central, se encuentra la Oficina de la IA, el Comité Europeo de IA (en adelante, el "Comité"), y el Foro Consultivo. Adicionalmente, el Grupo de Expertos Científicos Independientes provee asesoramiento técnico esencial para adaptarse a la evolución tecnológica, mientras que las Autoridades Nacionales Competentes aseguran la adherencia a las normas en el ámbito local.

5.1 Oficina de la IA

La Oficina Europea de Inteligencia Artificial, creada por la Comisión el 24 de enero de 2024 mediante la decisión C/2024/1459[25]. Esta entidad se incrusta en la estructura de la Dirección General de Redes de Comunicación, Contenido y Tecnologías, desempeñando un rol crucial en la implementación y supervisión de la inteligencia artificial en la UE.

Las responsabilidades clave incluyen, pero no se limitan a, el apoyo a la aplicación del RIA mediante el desarrollo de herramientas y metodologías para evaluar los modelos de IA y supervisar su cumplimiento normativo, tal como se establece en el artículo 3 de la Decisión.

Además, esta Oficina fomenta la colaboración con jugadores clave, desde expertos académicos y desarrolladores de IA, hasta otras Direcciones Generales, servicios de la Comisión, y órganos de la UE, para promover el uso seguro y efectivo de la tecnología – arts. 3 y 4 de la Decisión.

Asimismo, es responsable de realizar evaluaciones y revisiones regulares del reglamento de IA y coordinar la gobernanza efectiva del ecosistema de IA. La cooperación internacional, un pilar definido en el artículo 7 de la Decisión, destaca el compromiso de la Oficina con la promoción global de una IA fiable y el liderazgo en establecer normativas responsables[26].

Los recursos para sus las operaciones y el personal están asegurados a través del Programa Europa Digital -artículo 8 de la Decisión. La Oficina también juega un papel indispensable en la organización de actividades relacionadas con el Comité de IA, desde la planificación de reuniones hasta la preparación de agendas, para alinearlas con los objetivos estratégicos - artículo 65 RIA.

Por último, se encargan de la creación de códigos de buenas prácticas – art. 50.7 RIA, y la adopción de medidas para monitorear el cumplimiento de los proveedores con el reglamento, subrayando así su papel esencial en la supervisión y el cumplimiento normativo - artículo 89 RIA.

[25] Decisión de la Comisión de 24 de enero de 2024 por la que se crea la Oficina Europea de Inteligencia Artificial (C/2024/1459).
[26] Agustinoy, A. (30 de enero de 2024). Nueva Oficina Europea de IA. Blog de Propiedad Intelectual y Tecnologías de Cuatrecasas. (Disponible en: cuatrecasas.com/propiedad-intelectual/oficina-ia, última consulta 10/04/2024)

5.2 Comité Europeo de IA

El Reglamento en su artículo 65 RIA establece la creación del Comité Europeo de Inteligencia Artificial, con la obligación de mantener la objetividad e imparcialidad en todas sus operaciones.

5.2.1 Estructura del Comité

El Comité estará compuesto por un representante de cada Estado miembro y cuenta también con la participación del Supervisor Europeo de Protección de Datos en calidad de observador. La Oficina de IA asistirá a las reuniones, aunque sin derecho a voto. Según la relevancia de los asuntos tratados, el Comité tiene la facultad de convocar a autoridades adicionales, entidades u otros especialistas.

Los representantes de los Estados miembros son designados por un período de tres años, con la posibilidad de una única renovación. Deben poseer las competencias y poderes necesarios para contribuir efectivamente al Comité, actuar como puntos de contacto principales y promover la coordinación entre las autoridades nacionales competentes.

El Comité determinará su Reglamento Interno mediante una mayoría de dos tercios, definiendo los criterios de selección, duración de los mandatos, roles de la presidencia, procedimientos de votación y la estructura de sus actividades y subgrupos.

Se establecerán dos subgrupos permanentes con el objetivo de fomentar la colaboración e intercambio entre las autoridades de control del mercado y para abordar cuestiones específicas. Además, se podrán constituir subgrupos adicionales, ya sean temporales o permanentes, para examinar asuntos concretos.

5.2.2 Funciones del Comité

El Comité desempeña un papel esencial en el asesoramiento y apoyo tanto a la Comisión como a los Estados miembros, asegurando una implementación uniforme y efectiva del reglamento. Es por ello, que el Reglamento en su artículo 66 detalla numerosas funciones para este fin.

Entre sus responsabilidades, el Comité está debe fomentar la coordinación entre autoridades nacionales, apoyar actividades conjuntas de vigilancia del mercado y difundir conocimientos técnicos y reglamentarios, así como mejores prácticas entre los Estados miembros.

Su labor asesoría abarca la correcta aplicación del reglamento y la emisión de recomendaciones y opiniones en temas clave para la adecuada ejecución del mismo, que incluyen desde códigos de conducta y la revisión del reglamento hasta especificaciones técnicas y tendencias en IA.

Además, el Comité deberá promover activamente la alfabetización en IA, sensibilizando y educando al público sobre las implicaciones de la IA, y trabajar en el desarrollo de un entendimiento mutuo y criterios comunes entre las partes interesadas.

Por otro lado, se encargará de facilitar el avance técnico y organizacional necesario para aplicar el reglamento, impulsando espacios de pruebas controlados y aportando en la creación de guías de orientación y estrategias de cooperación internacional en IA.

Finalmente, el Comité proporcionará asesoramiento especializado a la Comisión en asuntos internacionales relacionados con la IA. También tendrá la responsabilidad de proporcionar dictámenes sobre alertas específicas vinculadas a modelos de IA de uso general. Esta función garantiza que la Comisión reciba información crítica permitiéndole adoptar medidas proactivas para proteger el bienestar público en el dinámico campo de la IA.

5.3 Foro consultivo

Conforme al artículo 67 RIA, se creará un foro consultivo dedicado a brindar asesoramiento especializado y apoyo técnico tanto al Comité Europeo de IA como a la Comisión Europea, facilitando así la ejecución de sus funciones regulatorias.

Este foro estará compuesto de manera equilibrada por representantes de diversos sectores, incluidos la industria, startups, pymes, sociedad civil y academia, asegurando un balance entre intereses comerciales y no comerciales.

La Comisión será la encargada de nombrar a los miembros del foro por un término de dos años, extensible hasta un máximo de cuatro. Se elegirá a dos copresidentes, solo renovables por una vez. Como miembros permanentes del Foro nos encontramos con la Agencia de la UE de para la Ciberseguridad, el Comité Europeo de Normalización, el Comité Europeo de Normalización Electrotécnica y el Instituto Europeo de Normas de Telecomunicaciones.

El foro establecerá su propio reglamento interno y se reunirá semestralmente y podrá formar subgrupos para abordar temas específicos. Anualmente, elaborará un informe de sus actividades, disponible públicamente, y podrá emitir dictámenes y recomendaciones a solicitud del Comité o de la Comisión.

5.4 Grupo de expertos científicos independientes

De acuerdo con el artículo 68 RIA, la Comisión formará un grupo de expertos científicos dedicado a fortalecer el cumplimiento normativo del reglamento. Este grupo estará compuesto por expertos seleccionados por sus profundos conocimientos en IA, garantizando su independencia de cualquier proveedor de sistemas de IA y su capacidad para actuar con objetividad y precisión.

Las principales funciones del grupo incluyen asesorar y apoyar a la Oficina de IA en la aplicación y cumplimiento del reglamento, especialmente en lo relativo a sistemas y modelos de IA de uso general. Esto abarca desde alertar sobre posibles riesgos sistémicos hasta contribuir al desarrollo de herramientas de evaluación y clasificación de riesgos.

El grupo también colaborará en la supervisión del mercado y en el fomento de la vigilancia transfronteriza, asegurando en todo momento su imparcialidad, confidencialidad y objetividad en sus funciones.

Los expertos cumplirán sus roles sin influencia externa, y sus declaraciones de intereses serán públicas para garantizar la transparencia. La designación por parte de la Comisión, a través de un acto de ejecución, especificará los procedimientos y condiciones bajo los cuales el grupo podrá emitir alertas y requerir el apoyo de la Oficina de IA en sus labores.

Por último, de acuerdo con el artículo 69 RIA, los Estados miembros tienen la facultad de solicitar la asistencia del grupo de expertos científicos para reforzar sus acciones de cumplimiento normativo. La contribución financiera por parte de los Estados para esta asesoría será establecida a través de un acto de ejecución por la Comisión, al momento de formar el grupo. Este acto definirá un modelo de tasas basado en la eficiencia de costos y el aseguramiento de un acceso justo para todos.

La Comisión se compromete a proporcionar a los Estados miembros acceso expedito a estos expertos, coordinando eficazmente el apoyo entre las infraestructuras de prueba de IA y los expertos, para optimizar recursos y maximizar el beneficio de su intervención.

La Comisión garantizará un acceso ágil de los Estados miembros a estos expertos, asegurando una coordinación efectiva entre las actividades de soporte de IA y el asesoramiento experto, con el objetivo de aprovechar al máximo los recursos disponibles y potenciar el valor agregado de estas colaboraciones.

5.5 Autoridades nacionales competentes

El artículo 70 RIA cierra el esquema de gobernanza, estableciendo cómo cada Estado miembro debe designar sus autoridades nacionales competentes, así como las responsabilidades que estas asumirán. Debiendo comunicar a la Comisión la identidad de estos.

Cada Estado deberá nombrar, como mínimo, una autoridad notificante y una autoridad de vigilancia del mercado, las cuales operarán de manera independiente y objetiva para asegurar la adherencia al reglamento. Estas autoridades deberán hacer accesible su contacto al público dentro del año posterior a la vigencia del Reglamento.

Los Estados asegurarán que estas entidades cuenten con los recursos necesarios, incluyendo personal cualificado en IA y ciencias de datos, para cumplir con sus funciones eficazmente. Además, deberán de implementar medidas de ciberseguridad y mantener la confidencialidad.

Se requerirá que los Estados miembros envíen informes bienales a la Comisión sobre los recursos de las autoridades, los cuales serán evaluados por el Comité para emitir recomendaciones según sea necesario. La Comisión promoverá el intercambio de experiencias entre las autoridades para fomentar el avance conjunto.

Por último, las autoridades proporcionarán orientación y asesoramiento, especialmente dirigida a pymes. El Supervisor Europeo de Protección de Datos actuará como la autoridad supervisora de las actividades de instituciones, órganos y organismos de la UE en el marco de este reglamento.

6. VIGILANCIA Y CUMPLIMIENTO

El Capítulo IX del reglamento busca asegurar que los sistemas de IA mantengan un cumplimiento constante con las regulaciones, adaptándose a cualquier cambio en sus riesgos inherentes y garantizando la seguridad y los derechos fundamentales de los usuarios.

6.1 Vigilancia pos-comercialización

La vigilancia pos-comercialización es una obligación clave para los proveedores de sistemas de IA de alto riesgo, establecida en el artículo 72 RIA. Este mandato exige la implementación de un sistema que documente y analice datos sobre el funcionamiento de estos sistemas a lo largo de su ciclo de vida. Este seguimiento busca asegurar que los sistemas mantengan un cumplimiento constante con las regulaciones, adaptándose a cualquier cambio en sus riesgos inherentes.

Dentro de este marco, se contempla la creación de un plan detallado de vigilancia pos-comercialización, que debe ser parte de la documentación técnica del sistema. La Comisión tiene

la responsabilidad de desarrollar un modelo estándar para este plan, como guía sobre los elementos clave, al menos seis meses antes de la entrada en vigor del Reglamento.

En el caso de sistemas que ya están sujetos a normativas específicas de la UE, los proveedores tienen la opción de alinear sus prácticas de vigilancia pos-comercialización existentes con los requisitos del nuevo Reglamento. Esto asegurar un nivel de protección equivalente, evitando duplicaciones y minimizando cargas adicionales.

6.2 Notificación de incidentes graves

El artículo 73 RIA detalla el procedimiento obligatorio para que los proveedores de sistemas de IA de alto riesgo notifiquen incidentes graves a las autoridades de vigilancia del mercado. Esta notificación debe hacerse tan pronto como se conozca el incidente o se sospeche de un vínculo causal con el sistema de IA, siguiendo plazos específicos según la gravedad del incidente.

Los proveedores deben investigar el incidente, evaluar los riesgos y tomar medidas correctoras, cooperando con las autoridades sin alterar el sistema de manera que afecte la evaluación del incidente. Del mismo modo, la autoridad de vigilancia del mercado deberá actuar conforme al reglamento para evitar la reincidencia.

6.3 Ejecución

La Sección 3 del Reglamento establece procedimientos detallados para la ejecución efectiva del mismo, centrándose en la vigilancia del mercado, la asistencia mutua entre Estados miembros, la supervisión de pruebas en condiciones reales, y el tratamiento del incumplimiento tanto formal como sustancial de los sistemas de IA.

El artículo 74 RIA recalca que el Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA, lo que incluye el deber de las autoridades de vigilancia del mercado de informar a la Comisión y a las autoridades competentes sobre cualquier actividad relevante sobre las prácticas prohibidas.

Para los sistemas de IA de alto riesgo asociados a productos específicos, se designan autoridades específicas de vigilancia del mercado, permitiendo la coordinación con las autoridades sectoriales pertinentes.

Los artículos 77 y 78 RIA destacan el papel de las autoridades nacionales competentes, otorgándoles poderes para solicitar y acceder a la documentación necesaria para el cumplimiento de sus mandatos, y enfatizando la importancia de mantener la confidencialidad de la información obtenida durante dicha vigilancia.

El procedimiento aplicable a los sistemas de IA clasificados erróneamente como no de alto riesgo se detalla en el artículo 80 RIA, proporcionando un mecanismo para que las autoridades de vigilancia del mercado evalúen y exijan la conformidad con los requisitos del reglamento, aplicando multas en caso de clasificación errónea intencional.

El artículo 81 RIA introduce un procedimiento de salvaguardia a nivel de la Unión, permitiendo a la Comisión evaluar y decidir sobre la justificación de las medidas adoptadas por los Estados miembros en caso de objeciones, asegurando una aplicación coherente de todos los EM.

Los sistemas de IA que, a pesar de cumplir con el reglamento, presenten riesgos para la salud, la seguridad o los derechos fundamentales de las personas son abordados en el artículo 82 RIA, estableciendo la obligación de los proveedores de adoptar medidas correctoras adecuadas.

En casos de incumplimiento formal, como la incorrecta colocación del marcado CE[27] o la falta de registro adecuado, el artículo 83 RIA detalla las medidas que las autoridades de vigilancia del mercado deben exigir a los proveedores para rectificar tales incumplimientos.

Finalmente, el artículo 84 RIA señala la designación por parte de la Comisión de estructuras de apoyo a los ensayos de IA de la Unión para proporcionar asesoramiento técnico o científico independiente, facilitando así la aplicación efectiva del reglamento y el avance hacia una IA segura y confiable dentro de la Unión Europea.

[27] *Conformité Européenne*: marca de la UE que demuestra que el fabricante cumple con requisitos de seguridad.

6.4 Vías de recurso

Más allá de las opciones administrativas o judiciales disponibles en cada EM, el reglamento especifica tres mecanismos de vías de recurso que contribuyen a reforzar una buena ejecución. En primer lugar, el art. 85 RIA otorga a cualquier persona física o jurídica la capacidad de presentar reclamaciones motivadas ante la autoridad de vigilancia del mercado competente.

Por otro lado, el artículo 86 RIA establece el derecho de los individuos a recibir explicaciones detalladas sobre las decisiones tomadas en base a sistemas de IA de alto riesgo que les afecten directamente, especialmente si dichas decisiones tienen un impacto adverso en su salud, seguridad o derechos fundamentales. Este derecho excluye a sistemas de IA de infraestructuras críticas, asegurando así un balance entre la seguridad operacional y la transparencia.

Finalmente, el artículo 87 RIA crea un marco para la denuncia de infracciones del reglamento y para la protección de aquellos que denuncien tales violaciones. Este mecanismo redirige el procedimiento de denuncia a la normativa perteneciente en la Directiva UE 2019/1937, proporcionando así un enfoque consistente y seguro.

Estas medidas, refuerzan la transparencia y responsabilidad en la implementación y uso de sistemas de IA, ofreciendo canales para la protección y defensa de los derechos en el ámbito digital.

7. SANCIONES

El Capítulo XII está dedicado a establecer un régimen integral de sanciones, diseñado para asegurar el cumplimiento de sus disposiciones por parte de los operadores de sistemas de IA. Este régimen no solo incluye sanciones económicas sino también advertencias y otras medidas correctivas no pecuniarias, estableciendo un marco que busca ser efectivo, proporcional y disuasorio. De manera especial, se considera la situación de las pymes y startups, ajustando las sanciones para no comprometer su sostenibilidad económica.

7.1 Marco General de Sanciones

Según lo estipulado en el artículo 99 RIA, los Estados miembros son los encargados de definir las sanciones aplicables, las cuales deben ser comunicadas a la Comisión y actualizarse ante cualquier cambio. La estructura de sanciones distingue entre diversas categorías de infracciones, aplicando el principio de menor sanción en el caso de las pymes para fomentar su crecimiento.

El artículo 5 RIA detalla las infracciones más graves, siendo aquellas que contravienen las prohibiciones de los sistemas de IA prohibidos. Pueden conllevar multas de hasta 35 millones de euros o el 7% del volumen de negocios anual del infractor, aplicando la cifra que resulte mayor.

Por otro lado, infracciones relacionadas con el incumplimiento de obligaciones específicas por parte de proveedores, importadores, distribuidores, entre otros, pueden acarrear multas de hasta 15 millones de euros o hasta el 3% del volumen de negocios mundial.

Además, la presentación de información inexacta, incompleta o engañosa a las autoridades competentes se sancionará con multas de hasta 7.5 millones de euros o hasta el 1% del volumen de negocios mundial.

La imposición de sanciones tendrá en cuenta múltiples factores, entre los que se encuentra la naturaleza y gravedad de la infracción, número de personas afectadas, la reincidencia, la cooperación del infractor con las autoridades, la intencionalidad o negligencia, y cualquier otro factor agravante o atenuante relevante.

Los Estados tienen la facultad de imponer multas a autoridades y organismos públicos; y de determinar el órgano jurisdiccional u otro organismo competente para imponer las multas. Finalmente, los Estados miembros están obligados a informar anualmente a la Comisión sobre las sanciones impuestas y los procedimientos judiciales relacionados.

7.2 Multas Administrativas a Entidades de la UE

El artículo 100 RIA introduce un sistema de sanciones específicamente dirigido a las instituciones, órganos y organismos de la UE que contravengan las normas establecidas. Este mecanismo, bajo la dirección del Supervisor Europeo de Protección de Datos, aplica multas administrativas en función de diversos factores, tales como la severidad, duración de la infracción, el impacto en los afectados, las medidas correctivas implementadas, y el nivel de cooperación con las autoridades.

Se han establecido límites máximos para estas sanciones, hasta 1.5 millones de euros para violaciones de las prohibiciones de sistemas de IA prohibidos del artículo 5 y hasta 750 mil euros para el incumplimiento de cualquier otra obligación.

Fundamentalmente, antes de la imposición de cualquier sanción, se asegura el derecho de audiencia de las entidades implicadas, protegiendo sus derechos de defensa y basando las decisiones en elementos debidamente discutidos.

Cabe destacar, que el apartado 6 del mismo artículo, se establece que los fondos obtenidos a través de estas multas se integrarán al presupuesto general de la UE, sin que ello impida la operatividad de las entidades sancionadas.

Además, el Supervisor Europeo de Protección de Datos se compromete a informar anualmente a la Comisión sobre las multas administrativas aplicadas y sobre cualquier acción legal pertinente, fomentando así la transparencia y la responsabilidad en el cumplimiento del reglamento.

7.3 Multas a Proveedores de Modelos de IA de Uso General

Por último, el artículo 101 RIA establece un régimen de sanciones específico para los proveedores de modelos de IA de uso general. La Comisión tiene autoridad para imponer multas de hasta el 3% del volumen de negocios mundial total del último ejercicio financiero, o 15 millones de euros, si esta cantidad es mayor.

Las causas de estas sanciones exigen que el incumplimiento haya sido deliberado o por negligencia, de cuatro tipos: las disposiciones del reglamento; la falta de respuesta a solicitudes de información o la provisión de datos inexactos o engañoso; el incumplimiento de medidas requeridas; o la denegación de acceso a la Comisión a los modelos de IA para evaluación.

La determinación de la sanción económica tomará en consideración varios factores, incluyendo la seriedad, gravedad y persistencia de la infracción, siempre bajo los principios de proporcionalidad y adecuación. Asimismo, se tendrán en cuenta los compromisos asumidos por los proveedores, así como su adhesión a los códigos de buenas prácticas.

Antes de imponer cualquier sanción, la Comisión garantizará el derecho de audiencia al proveedor implicado, proporcionando una oportunidad para que este pueda exponer su caso. Se informará sobre las sanciones impuestas al Comité, y el Tribunal de Justicia de la Unión Europea tendrá autoridad completa para revisar, anular o incrementar las decisiones de la Comisión, pudiendo modificar su importe según considere pertinente.

III. IMPLICACIONES DEL NUEVO REGLAMENTO DE IA

Si bien este nuevo reglamento aún no ha sido implementado formalmente, pendiente de correcciones finales y de la aprobación formal por parte del Consejo, es pertinente adelantar un análisis sobre las potenciales repercusiones que este marco normativo tendrá tanto dentro de la Unión Europea como en el escenario global.

Iniciamos con un estudio comparativo de la regulación de la IA, examinando las estrategias adoptadas por otras grandes potencias como China y Estados Unidos, para así entender de forma diversificada las distintas metodologías con las que cada región enfrenta los desafíos y oportunidades de la IA. Posteriormente, profundizamos en las consecuencias comerciales y éticas que se derivarán de la implementación del RIA.

CAPÍTULO I. OTRAS REGULACIONES MUNDIALES

Este análisis comparativo resalta las divergencias en el enfoque regulatorio entre China y Estados Unidos, con China centrando sus esfuerzos en el control del sector privado y Estados Unidos buscando promover la innovación responsable. La comparación subraya la importancia de un marco ético y de seguridad en el uso gubernamental de la IA[28].

1. CHINA

El Gobierno Chino fue una de las pioneras en regular la IA. En julio de 2023[29] emitió una serie de directivas que entraron el vigor el 15 de agosto de ese mismo año, donde destacan una Ley General de IA y una regulación específica para la IA generativa.

[28] Padín, A., "Así se está regulando la IA en la UE, EE.UU. y la OCDE: el difícil equilibrio entre seguridad y fomento de la innovación", *Garrigues Digital*, 23 de febrero de 2024 (Disponible en: garrigues.com/regulando-ia-ue-eeuu-dificil-equilibrio-seguridad-fomento, última consulta 10/04/2024)

[29] Cyberspace Administration of China, "Medidas provisionales para la gestión de los servicios de inteligencia artificial generados", *China Information Network*, 13 de julio de 2023 (disponible en http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm)

La Ley de IA se compone de 73 artículos y establece definiciones, ámbitos de aplicación y principios para el desarrollo de IA centrados en la seguridad, transparencia, responsabilidad, y la promoción del bienestar humano.
Entre sus artículos, introduce un sistema de listas negativas y un *sandbox* regulatorio para experimentación, junto con mecanismos de aplicación y sanciones significativas por incumplimientos[30].

Al igual que la regulación europea, esta nueva ley china contempla disposiciones extraterritoriales en cuanto su ámbito de aplicación. A priori limita la regulación a toda la investigación, desarrollo, suministro y uso de IA dentro de la República Popular de China. No obstante, más adelante en su artículo 2 establece su aplicación extraterritorial:

> "Las actividades relacionadas con (…) de la IA realizadas fuera del territorio de la RPC que afecten o puedan afectar a la seguridad nacional, los intereses públicos o los derechos e intereses legítimos de personas u organizaciones de la RPC, están sujetas a esta ley"

Entre las múltiples obligaciones que se imponen a los sistemas de IA, incluye evitar cualquier tipo de discriminación, aglomeración que contrarie la competencia desleal, respetar los derechos de propiedad intelectual, no poner en peligro la salud física y mental, el honor, la privacidad y la información personal de los ciudadanos. En su artículo 4.1 establece:

> "Adherirse a los valores fundamentales del socialismo, y no incitar a la subversión del poder estatal, derrocar el sistema socialista, poner en peligro la seguridad y los intereses nacionales, dañar la imagen del país, incitar a la secesión del país, socavar la unidad nacional y la estabilidad social, promover el terrorismo, el extremismo, el odio nacional, la discriminación étnica, la violencia, Pornografía obscena, información falsa y dañina y otros contenidos prohibidos por leyes y reglamentos administrativos"

[30] Fernández, C., "China aprueba una regulación de la inteligencia artificial y de la inteligencia artificial generativa", *DiarioLaLey*, 31 de agosto de 2023 (disponible en https://diariolaley.laleynext.es/dll/2023/09/01/china-aprueba-una-regulacion-de-la-inteligencia-artificial-y-de-la-inteligencia-artificial-generativa , última consulta 10/04/2024)

Por otro lado, la regulación sobre IA generativa, emitida por la Administración del Ciberespacio de China, busca promover el desarrollo responsable de la IA generativa, proteger la seguridad nacional y los intereses públicos, y los derechos de los ciudadanos. Incluye directrices sobre el contenido generado, la gestión de datos de entrenamiento, y la seguridad y protección de datos personales, con énfasis en la transparencia y la prevención de abusos.

Ambas normativas representan un enfoque detallado y estructurado hacia la regulación de la IA en China, marcando un equilibrio entre la promoción de la innovación y la protección de la sociedad y los valores estatales.

JUAN PEDRO DÍAZ SENÉS en su ponencia de febrero 2024, "El futuro de la regulación de la inteligencia artificial en la UE: El riesgo como elemento clave de responsabilidad", explicó como la gran diferencia de la regulación China, frente a la europea y estadounidense, es que esta no contiene obligaciones para el propio Gobierno, solo contempla imposiciones para el sector privado.

2. ESTADOS UNIDOS

Estados Unidos también ha tomado pasos significativos para asegurar que la innovación en IA se realice de manera responsable y segura. Reconociendo tanto las oportunidades como los desafíos que la IA presenta, el presidente Joe Biden promulgó una orden ejecutiva el 30 de octubre de 2023[31], estableciendo un marco de políticas para guiar el desarrollo y uso de la IA en el país.

La orden ejecutiva introduce una serie de requerimientos y estándares destinados a asegurar la seguridad y fiabilidad de los sistemas de IA, especialmente aquellos que representan un riesgo grave para la seguridad nacional, económica, o de salud[32]. Este conjunto de medidas abarca desde la exigencia de transparencia hasta el desarrollo de un marco legal para materiales peligrosos,

[31] White House Government, "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence", *Briefing Room of the White House*, 30 de octubre de 2023 (disponible en, whitehouse.gov/president-biden-issues-executive-order-artificial-intelligence última consulta el 10/04/2024)
[32] Dougal, D. y Ostrowski, J "What's in Biden's Executive Order on Artificial Intelligence?", *LawFare*, 3 de enero de 2024 (disponible en lawfaremedia/biden-executive-order-on-artificial-intelligence , última consulta el 10/04/2024)

pasando por la implementación de estándares pre-lanzamiento, la autenticación de contenidos y la creación de un programa de ciberseguridad robusto.

Una de las piedras angulares de esta iniciativa es la exigencia de transparencia, que obliga a los desarrolladores de IA a compartir con el gobierno los resultados de todas las pruebas de seguridad realizadas. En consonancia con este principio, se establece la obligación de desarrollar estándares y herramientas pre-lanzamiento que garanticen la seguridad y fiabilidad de la IA, enfocándose en mitigar riesgos específicos como los químicos, biológicos, nucleares y de ciberseguridad.

Además, se desarrolla un marco legal robusto diseñado para prevenir la creación de materiales biológicos peligrosos por parte de sistemas de IA. También se establecen normas para detectar contenidos generados por IA y autenticar los contenidos oficiales, abordando directamente los riesgos asociados con la desinformación y la manipulación de contenido. Por otro lado, se implementa un programa de ciberseguridad destinado a detectar y corregir vulnerabilidades en software crítico, reforzando la infraestructura digital contra ataques y fallos de seguridad.

La orden ejecutiva pone un énfasis particular en la protección de la privacidad de los ciudadanos y el fomento de la equidad y los derechos civiles[33]. Se prioriza el desarrollo y uso de técnicas que preserven la privacidad, con el apoyo de la Fundación Nacional de Ciencia de EE.UU., y se refuerzan las tecnologías que protegen la intimidad, como las herramientas criptográficas.

En términos de equidad, la orden ejecutiva provee directrices claras a los desarrolladores de IA para evitar el uso de algoritmos que puedan exacerbar la discriminación. Para proteger y beneficiar a consumidores, pacientes y estudiantes, la orden ejecutiva enfatiza la necesidad de explorar y desarrollar herramientas de IA que mejoren la educación y la atención sanitaria. Esto incluye desde aplicaciones educativas diseñadas para asistir a profesores en la personalización del aprendizaje, hasta el avance en el uso de la IA para el desarrollo de medicamentos asequibles.

[33] Neill, B., Hallmark, J. D., Jackson, R. J., & Diasio, D., "Key takeaways from the Biden administration executive order on AI", *EY*, 31 de octubre de 2023 (disponible en https://www.ey.com/en_us/public-policy/key-takeaways-from-the-biden-administration-executive-order-on-ai , última consulta 10/04/2023)

La promoción de la innovación y la competitividad ocupa un lugar central en la orden ejecutiva, a través del establecimiento de proyectos piloto y la expansión de subvenciones en áreas críticas como la salud y el cambio climático. Esto se complementa con iniciativas para atraer talento extranjero altamente cualificado y fomentar un ecosistema de IA abierto y competitivo, bajo la supervisión de entidades como la Comisión Federal del Comercio.

A nivel internacional, la orden busca fortalecer el liderazgo de Estados Unidos mediante la ampliación de compromisos bilaterales y multilaterales. Finalmente, se hace hincapié en garantizar un uso responsable y eficaz de la IA por parte del gobierno, estableciendo directrices claras para su implementación y procurando que los organismos públicos puedan adquirir y utilizar productos de IA de manera más eficiente y económica.

Destaca la importancia de establecer altos estándares éticos y de seguridad en el uso gubernamental de la IA, ilustrado por el perjuicio causado por el algortimo MiDAS en Michigan, que acusó erróneamente a más de 34,000 personas de fraude de desempleo entre 2013 y 2015, lo que desembocó en la destrucción de su crédito, bancarrota y pérdida de hogares.

A pesar de la publicación de múltiples documentos por parte de la administración Biden, que subrayan la necesidad de regulaciones claras y estándares para el uso gubernamental de la IA, la ciencia para evaluar la fiabilidad, la equidad y la seguridad de los sistemas de IA todavía está en sus etapas iniciales. La creación del Instituto de Seguridad de la IA por parte del Instituto Nacional de Estándares y Tecnología (NIST) es un paso positivo, aunque se enfrenta al desafío de obtener financiamiento significativo para cumplir con sus objetivos.

Resaltan la necesidad de herramientas más estandarizados para evaluar los sistemas. El éxito de los esfuerzos de regulación dependerá de la capacidad de traducir principios de alto nivel en criterios de evaluación tangibles, un desafío que el Instituto de Seguridad de la IA podría ayudar a superar si recibe unos fondos suficientes.

CAPÍTULO II. FUTURO DE LA IA TRAS EL RIA

ANNA JARQUES en su análisis "El futuro Reglamento Europeo de Inteligencia Artificial"[34] destaca la posición de liderazgo de la UE en la regulación de la IA, buscando equilibrar las oportunidades que ofrece la tecnología con la necesidad de prevenir riesgos y abusos, asegurando que el desarrollo y uso de sistemas de IA se alinee con los principios y derechos fundamentales.

1. DIFICULTADES EN SU ÁMBITO DE APLICACIÓN

Según AURELIO LÓPEZ-TARUELLA MARTÍNEZ, en su análisis "El Futuro Reglamento de Inteligencia Artificial y las Relaciones con Terceros Estados"[35], se centra en las complejidades del artículo 2.1 RIA, el cual determina el ámbito de aplicación del Reglamento. Este ámbito no solo destaca por su posible aplicación extraterritorial, sino también por su triple vertiente entre los operadores económicos, las autoridades competentes o los tribunales de justicia.

Para los operadores económicos, que incluyen distribuidores, usuarios, proveedores, importadores y sistemas de IA, prevalece una notable incertidumbre sobre a quiénes exactamente se aplica el Reglamento, dado que inicialmente parece dirigirse solo a aquellos proveedores y usuarios con actividades estrechamente vinculadas a la UE. Además, se subraya la carga significativa que supondrá cumplir con los diversos requisitos que el RIA impone según el nivel de riesgo, especialmente para las startups y pequeñas empresas.

Las autoridades enfrentan el reto de disponer de los recursos y conocimientos técnicos necesarios para supervisar la implementación del reglamento, especialmente en tecnologías emergentes. El RIA establece que cada Estado miembro debe designar una autoridad nacional competente, pero persiste la duda sobre cómo se manejarán aquellos casos con elementos de hecho vinculados a varios Estados miembros, cuestionando qué autoridad tendría jurisdicción en estas situaciones.

[34] JARQUES, A. (2023). El futuro Reglamento Europeo de Inteligencia Artificial. Actualidad Jurídica Aranzadi num. 1003/2023, Editorial Aranzadi S.A.U.
[35] LÓPEZ-TARUELLA MARTÍNEZ, A., "El Futuro Reglamento de Inteligencia Artificial y las Relaciones con Terceros Estados", *Revista Electrónica de Estudios Internacionales*, vol. 45, 2023, página 10.

En cuanto a los tribunales de justicia, se presentan grandes dificultades en la interpretación y aplicación del RIA. LÓPEZ-TARUELLA considera el RIA como una "ley policía", en línea con el artículo 9.1 del Reglamento de Roma[36]:

> "Una ley de policía es una disposición cuya observancia un país considera esencial para la salvaguardia de sus intereses públicos, tales como su organización política, social o económica, hasta el punto de exigir su aplicación a toda situación comprendida dentro de su ámbito de aplicación, cualquiera que fuese la ley aplicable al contrato según el presente Reglamento".

Esto implica, de acuerdo con el artículo 9.2 del mismo Reglamento, que el RIA tendría preferencia de aplicación con respecto a las leyes nacionales.

Por otro lado, la extraterritorialidad[37] que busca implementar el RIA, tiene el objetivo de establecer obligaciones para aquellos proveedores que, si bien no tienen presencia física dentro de la UE, sus actividades tienen un impacto significativo en los ciudadanos o en los mercados europeos. Esta medida se justifica debido a la naturaleza transfronteriza de los servicios de IA y la necesidad de garantizar los objetivos perseguidos, lo que a su vez conlleva retos considerables para su ejecución efectiva.

En esencia, el reglamento se aplica a empresas que, estando radicadas en terceros estados, mantienen una relación suficiente con el mercado europeo. Sin embargo, es precisamente en este punto donde surgen debates, dado que los parámetros para determinar el grado de conexión requerido con el mercado europeo no están claramente establecidos. Será tarea de los tribunales establecer los criterios que definirán la suficiencia de este vínculo, consolidando así el umbral de conexión necesario para que el reglamento sea aplicable.

[36] Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I) (Diario Oficial de la Unión Europea núm. 177, de 4 de julio de 2008).
[37] LÓPEZ-TARUELLA MARTÍNEZ, A,. Página 12.

Uno de los aspectos críticos señalados por LÓPEZ-TARUELLA es la implementación de sanciones a entidades basadas en terceros países. Este desafío subraya la necesidad de establecer mecanismos eficaces que aseguren el cumplimiento de las sanciones impuestas, lo cual requiere no solo una coordinación internacional robusta sino también un marco legal que facilite la ejecución de estas medidas más allá de las fronteras de la UE.

2. IMPACTO EN EL SECTOR LABORAL

JAVIER ERCILLA GARCÍA en "Transparencia en la Inteligencia Artificial: explorando la necesidad de acceso al código fuente por parte de los Comités de Empresa"[38] discute la importancia de la transparencia en la implementación de algoritmos y sistemas de IA en el entorno laboral, centrándose en la necesidad de que los comités de empresa accedan al código fuente.

Otorga importancia a los comités de empresa, los cuales pueden desempeñar un papel vital en promover la transparencia algorítmica, estableciendo protocolos para la revisión regular de estos sistemas. Además, propone la implementación de enfoques de "caja negra", "caja blanca" y "constructivo" para analizar y diseñar sistemas de IA con aplicabilidad desde el inicio.

La transparencia es crucial cuando la IA se usa para tareas como asignar trabajos o evaluar el desempeño de los empleados. Los errores en la programación pueden llevar a resultados injustos, por lo que una rigurosa regulación resulta imperativa para fomentar mayor transparencia, legibilidad y aplicabilidad en la IA[39].

En la misma línea, IVÁN ANTONIO RODRÍGUEZ CARDO discute en su obra la incidencia de los algoritmos en la relación laboral, llamada “Decisiones automatizadas y discriminación algorítmica en la relación laboral: ¿hacia un Derecho del Trabajo de dos velocidades?”[40], centrándose en cómo

[38] ERCILLA GARCÍA, J. (2023). Transparencia en la Inteligencia Artificial: explorando la necesidad de acceso al código fuente por parte de los Comités de Empresa.
[39] VILLAGRASA ALCAIDE, C. (2022). El derecho de propiedad intelectual y la protección de datos personales frente al derecho de transparencia de los algoritmos. Grandes Tratados. Discriminación algorítimica en el ámbito laboral: perspectiva de género e intervención. Editorial Aranzadi S.A.U
[40] RODRÍGUEZ CARDO, I. A. (2022). Decisiones automatizadas y discriminación algorítmica en la relación laboral: ¿hacia un Derecho del Trabajo de dos velocidades?, Revista Española de Derecho del Trabajo num. 253/2022, Editorial Aranzadi, S.A.U.

estos pueden influir en decisiones críticas como la selección de trabajadores, asignación de tareas, evaluación del rendimiento, y terminación de contratos.

Destaca que los fundamentos de estos algoritmos a menudo no son transparentes y carecen de control humano, lo que ha generado preocupaciones sobre la responsabilidad y la justicia de estas decisiones automatizadas.

Si bien el RIA no sigue esta específica estructura, si parece abordar la mayoría de los retos presentados el ámbito laboral. Dentro de su sistema de clasificación, en los sistemas considerados como de alto riesgo, se especifican ocho sectores a tener en cuenta, por su especial sensibilidad en la salvaguarda de derechos fundamentales. Uno de estos es el empleo, gestión de los trabajadores y acceso al autoempleo.

Se imponen altas obligaciones a dos tipos de sistemas de IA que presentan riesgos considerables en el ámbito laboral. Entre las obligaciones destacan los altos niveles de transparencia, vigilancia humana, implementación de un sistema de gestión de riesgos, y obligaciones en la forma de obtención, gobernanza y conservación de los datos obtenido.

Estos sistemas de IA de alto riesgo incluyen aquellos diseñados para facilitar la contratación o selección de candidatos, con actividades como la publicación de vacantes laborales, el filtrado de candidaturas, y la evaluación de los postulantes. Del mismo modo, incluye sistemas orientados a influir en decisiones laborales, ascensos, o terminaciones de contratos, basados en análisis de comportamientos, cualidades o atributos personales para la asignación de responsabilidades.

Todas las compañías que implementaban este tipo de sistemas en su departamento de recursos humanos se verán obligados a adaptar sus modelos a las obligaciones y requisitos exigidos en el RIA, lo que *a priori* debería mitigar las grandes discriminaciones dadas en este sector.

3. IMPLICACIONES ÉTICAS DE LA IA

El RIA representa un avance significativo en la regulación de las tecnologías de IA, estableciendo un marco normativo detallado y proactivo para guiar su desarrollo y aplicación dentro de la UE. Se centra en la protección de los derechos fundamentales, la promoción de la innovación y la definición de un enfoque basado en el riesgo para la clasificación de los sistemas de IA.

Aunque el RIA no logra mitigar completamente todos los riesgos asociados con esta tecnología, introduce innovaciones regulatorias y éticas notables. Destaca especialmente la clasificación basada en el riesgo, que resuelve grandes problemáticas sobre ciertas prácticas y sistemas de IA que suscitaban gran preocupación por sus implicaciones en derechos fundamentales, como la privacidad o la autonomía personal, estableciendo su prohibición directa.

Respecto con otras prácticas consideradas de alto riesgo, se establecen estrcitos requisitos como la imposición de vigilancia humana, lo cual limita de la autonomía de IA. Esta medida aborda en gran medida las preocupaciones planteadas por BERNARDO DEL ROSAL BLASCO en su comentario "¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial? "[41].

Al requerir una constante vigilancia y monitoreo humano, el RIA clarifica las fronteras de la responsabilidad y la culpabilidad en situaciones de perjuicio, asegurando así un marco de seguridad y confiabilidad en la interacción entre humanos y sistemas de IA.

A pesar de estos avances, el RIA enfrentan varios desafíos y áreas de incertidumbre que podrían impactar su eficacia y aplicabilidad en el futuro. La rápida evolución tecnológica de la IA desafía la capacidad del marco regulatorio para mantenerse actualizado, lo que requerirá un esfuerzo coordinado y continuo de todas las entidades de gobernanza para adaptar y refinar las regulaciones de manera efectiva.

[41] ROSAL BLASCO, B. (2023). ¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial? Revista Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance num 2/2023, Editorial Aranzadi, S.A.U.

Además, asegurar una interpretación y aplicación coherentes del RIA en todos los Estados Miembros emerge como un desafío crítico, esencial para prevenir discrepancias normativas que puedan fragmentar el mercado único digital.

Simultáneamente, es imprescindible encontrar un equilibrio prudente entre la protección contra los riesgos inherentes a la IA y la promoción de un clima de innovación. Una regulación excesivamente restrictiva podría inhibir el desarrollo y la aplicación de la IA, limitando su potencial para enriquecer el bienestar social y económico.

En este contexto, la discusión propuesta por FRANCISCA RAMÓN FERNÁNDEZ en su obra "Nuevos retos de la inteligencia artificial: ética y responsabilidad"[42], adquiere relevancia al sugerir la viabilidad y las implicaciones de conferir personalidad jurídica a robots y sistemas de IA.

Este enfoque significativamente más arriesgado al planteado por el RIA, provoca un intenso debate tanto ético y económico respecto a cómo las responsabilidades asociadas a la creación y operación de sistemas de IA podrían empezar a transferirse a las propias entidades tecnológicas. Aunque el RIA actual no incorpora este mecanismo, la propuesta subraya la importancia de explorar soluciones creativas y proactivas para abordar las limitaciones y posibles fallas del marco normativo vigente, manteniendo abierta la posibilidad de adaptaciones futuras que respondan de manera efectiva a los desafíos emergentes en el campo de la inteligencia artificial.

El RIA representa un paso significativo hacia una regulación ética y efectiva de la IA. Sin embargo, el futuro de la IA y su regulación requieren una reflexión continua, adaptación y diálogo internacional para asegurar que la tecnología avance de manera que beneficie a la sociedad en su conjunto[43].

[42] RAMÓN FERNÁNDEZ, F. (2022). Nuevos retos de la inteligencia artificial: ética y responsabilidad. Monografía de Revista Aranzadi de Derecho y Nuevas Tecnologías. Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación. Editorial Aranzadi S.A.U.

[43] ESTUPIÑÁN CÁCERES, R., FONTICIELLA HERNÁNDEZ, B. (2022). Big data e inteligencia artificial ¿nuevas herramientas para un cambio de modelo en la contratación con consumidores frente a cláusulas abusivas?, Revista de Derecho Bancario y Bursátil num. 168/2022, Editorial Aranzadi, S.A.U.

IV. CONCLUSIONES

Primera conclusión – El nuevo Reglamento sobre Inteligencia Artificial Europeo representa un avance significativo en el mundo digital.

La adopción del RIA por parte de la Unión Europea marca un hito histórico en la regulación de esta tecnología. Introduce un sistema de clasificación de riesgos detallado para los sistemas de IA y estableciendo prohibiciones claras contra aquellas prácticas que comprometen de manera significativa los derechos y libertades fundamentales.

Aborda directamente los riesgos inherentes a la IA, estableciendo una categoría específica para aquellos sistemas de IA considerados de alto riesgo. Estos sistemas se permiten bajo la condición de que cumplan con rigurosos requisitos, como una supervisión humana efectiva, y unos elevados estándares de transparencia, gestión de datos y gobernanza.

Mediante esta normativa, la Unión Europea traza un camino innovador hacia el logro de un delicado equilibrio, impulsa una innovación responsable al tiempo que asegura la protección integral de sus ciudadanos. Este enfoque dual no solo refuerza la confianza pública en los sistemas de IA, sino que también establece un modelo regulatorio ejemplar a nivel mundial.

Segunda conclusión – La Unión Europea aboga por la protección de derechos fundamentales frente al impulso de la innovación.

En la dicotomía entre la protección de los derechos fundamentales y la promoción de la innovación, la Unión Europea ha optado por un enfoque prudente con la implementación del RIA. Esta postura más conservadora, prioriza limitar de prácticas de IA que presenten riesgos potenciales, subrayando la primacía de la protección de derechos sobre el impulso desenfrenado hacia la novedad tecnológica.

Aunque el reglamento dedica un capítulo completo para el fomento de la innovación, en particular a través de espacios de prueba regulados, es evidente que el modelo regulatorio europeo pone un énfasis particular en la prevención del uso indebido de la IA.

Esta decisión puede representar una desventaja competitiva respecto a potencias tecnológicas como China y Estados Unidos, que han optado por marcos regulatorios más permisivos, acelerando así su avance en el desarrollo y despliegue de innovaciones en IA.

No obstante, este modelo conservador de la UE refleja un compromiso firme con la seguridad, la privacidad y la defensa de los derechos civiles, por encima de una carrera desmedida por el liderazgo tecnológico. Esta decisión refleja un reconocimiento de que la verdadera innovación requiere no solo avances tecnológicos, sino también un marco ético sólido que garantice el bienestar y la protección de todos los ciudadanos.

Tercera conclusión – El RIA solo es el primer paso, quedan grandes retos pendientes.

El RIA constituye un avance significativo en la regulación tecnológica, enfrentando el desafío de adaptarse a la rápida evolución de la IA. Sin embargo, aún quedan muchos desafíos y áreas por desarrollar. Uno de los retos más significativos es la adaptación continua del marco regulatorio a la evolución tecnológica rápida e impredecible de la IA, asegurando que las regulaciones permanezcan relevantes y efectivas.

Además, la implementación uniforme y coherente del RIA a través de los Estados miembros de la UE es crucial para evitar la fragmentación del mercado digital europeo y garantizar que las normas se apliquen efectivamente en toda la Unión.

Otro reto importante es encontrar el equilibrio adecuado entre la regulación y el fomento de la innovación, para que Europa no quede rezagada en el desarrollo tecnológico global. Por último, la cooperación internacional y el diálogo entre bloques y países serán esenciales para enfrentar los desafíos globales que presenta la IA, desde cuestiones éticas hasta impactos sociales, para promover estándares y prácticas que reflejen los valores y principios europeos a nivel mundial.

V. BIBLIOGRAFÍA

- **LEGISLACIÓN**

Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I) (Diario Oficial de la Unión Europea núm. 177, de 4 de julio de 2008).

Reglamento (UE) 2018/1488 del Consejo, de 28 de septiembre de 2018, por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea.

Reglamento (UE) de Inteligencia Artificial, mediante la Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD). P9_TA (2024)0138.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Ley Orgánica 3/2018 de 5 de diciembre (RCL 2018, 1629), de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027, de 6 de junio de 2018. 2018/0227(COD).

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021. 2021/0106(COD).

Decisión de la Comisión, de 24 de enero de 2024, por la que se crea la Oficina Europea de Inteligencia Artificial (C/2024/1459).

Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, 19 de febrero de 2020 COM (2020) 65.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan Coordinado sobre la inteligencia artificial, 7 de diciembre de 2018. COM (2018) 795.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Generar confianza en la inteligencia artificial centrada en el ser humano, 8 de abril de 2019. COM (2019) 168

- **OBRAS DOCTRINALES**

ARIZA COLMENAREJO, Mª J. (2022). Decisiones basadas en inteligencia artificial y el objeto de la impugnación. Inteligencia artificial y administración de justicia, Editorial Aranzadi S.A.U.

BELANDO GARÍN, B. (2022). La inteligencia artificial en la supervisión del mercado de valores. Revista de Derecho del Sistema Financiero num 4/2022, Editorial Aranzadi S.A.U.

BENDITO CAÑIZARES, M.T., (2021). Estadio intermedio de reflexión para una futura regulación de la ética en el espacio digital europeo: los principios de transparencia y accountability. Revista Aranzadi de Derecho y Nuevas Tecnologías num. 55/2021, Editorial Aranzadi S.A.U.

BUJOSA VADELL, L.M., (enero 2022). La gran incógnita de la inteligencia artificial, Editorial Aranzadi, S.A.U.

ERCILLA GARCÍA, J. (2023). Transparencia en la Inteligencia Artificial: explorando la necesidad de acceso al código fuente por parte de los Comités de Empresa.

ESTUPIÑÁN CÁCERES, R., FONTICIELLA HERNÁNDEZ, B. (2022). Big data e inteligencia artificial ¿nuevas herramientas para un cambio de modelo en la contratación con consumidores frente a cláusulas abusivas?, Revista de Derecho Bancario y Bursátil num. 168/2022, Editorial Aranzadi, S.A.U.

GONZÁLEZ RUIZ, F.J. (2019). Inteligencia artificial: implicaciones en materia de protección de datos, Actualidad Jurídica Aranzadi, Editorial Aranzadi S.A.U.

JARQUES, A. (2023). El futuro Reglamento Europeo de Inteligencia Artificial. Actualidad Jurídica Aranzadi num. 1003/2023, Editorial Aranzadi S.A.U.

LÓPEZ-TARUELLA MARTÍNEZ, A., "El Futuro Reglamento de Inteligencia Artificial y las Relaciones con Terceros Estados", *Revista Electrónica de Estudios Internacionales*, vol. 45, 2023.

MARTÍN DIZ, F. (enero 2022). La eclosión de la inteligencia artificial en el ámbito jurídico, Editorial Aranzadi S.A.U.

MARTÍN LÓPEZ, J. (enero 2023). Inteligencia artificial y transparencia. Monografías. Inteligencia artificial y comprobación tributaria: transparencia y no discriminación. Editorial Aranzadi S.A.U

MARTÍNEZ, M.T. (2023). Claves del impacto de la protección de datos en la sostenibilidad. Actualidad Jurídica Aranzadi num 998/2023 parte comentario. Editorial Aranzadi, S.A.U., Cizur menor.

PLAZA PENADÉS, J. (2019). Protección y cuestiones legales de la inteligencia artificial. Formación e-learning. Curso de especialización en Know-How, propiedad intelectual en el mercado único digital. Editorial Aranzadi, S.A.U.

RAMÓN FERNÁNDEZ, F. (2022). Nuevos retos de la inteligencia artificial: ética y responsabilidad. Monografía de Revista Aranzadi de Derecho y Nuevas Tecnologías. Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación. Editorial Aranzadi S.A.U.

RODRÍGUEZ CARDO, I. A. (2022). Decisiones automatizadas y discriminación algorítmica en la relación laboral: ¿hacia un Derecho del Trabajo de dos velocidades?, Revista Española de Derecho del Trabajo num. 253/2022, Editorial Aranzadi, S.A.U.

ROSAL BLASCO, B. (2023). ¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial? Revista Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance num 2/2023, Editorial Aranzadi, S.A.U.

SUÁREZ, M. (2024). Impacto de las tecnologías de la IA generativa y los derechos de propiedad intelectual: necesidad de establecer una estrategia. Actualidad Jurídica Aranzadi num. 1005/2024, Editorial Aranzadi S.A.U.

VELIZ, C., "Inteligencia artificial: ¿proceso o retroceso?" (Tribuna). Suplemento Retina, *El País*. 14 de junio de 2019

VILLAGRASA ALCAIDE, C. (2022). El derecho de propiedad intelectual y la protección de datos personales frente al derecho de transparencia de los algoritmos. Grandes Tratados. Discriminación algorítimica en el ámbito laboral: perspectiva de género e intervención. Editorial Aranzadi S.A.U

- **RECURSOS DE INTERNET**

Comisión Europea, "La información de alto rendimiento y la iniciativa EuroHPC", Nota Informativa Comisión Europea, 11 de enero de 2018 (disponible en https://ec.europa.eu/commission/presscorner/detail/es/MEMO_18_3)

Dougal, D. y Ostrowski, J “What’s in Biden’s Executive Order on Artificial Intelligence?”, LawFare, 3 de enero de 2024 (disponible en lawfaremedia/biden-executive-order-on-artificial-intelligence , última consulta el 10/04/2024)

White House Government, “Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence”, Briefing Room of the White House, 30 de octubre de 2023 (disponible en whitehouse.gov/president-biden-issues-executive-order-artificial-intelligence última consulta el 10/04/2024).

Fernández, C., “China aprueba una regulación de la inteligencia artificial y de la inteligencia artificial generativa”, DiarioLaLey, 31 de agosto de 2023 (disponible en https://diariolaley.laleynext.es/dll/2023/09/01/china-aprueba-una-regulacion-de-la-inteligencia-artificial-y-de-la-inteligencia-artificial-generativa , última consulta 10/04/2024)

Grupo Independiente de Expertos de Alto Nivel sobre IA, “Directrices Éticas para una IA Fiable”, Comisión Europea, 8 de abril de 2019 (disponible en digital-strategy.eu/ethics-guidelines-trustworthy-ai, última consulta 7/04/2024)

Georgieva, K. “La economía mundial transformada por la inteligencia artificial ha de beneficiar a la humanidad”. IMF Blog, 16 de enero de 2024 (disponible en imf.org/ai-global-economy-benefits-humanity; última consulta 9/04/2024)