https://doi.org/10.18800/dys.202402.016

FECHA DE RECEPCIÓN: 12/08/2024
FECHA DE APROBACIÓN: 24/09/2024

Gobernanza y Reglamento de Inteligencia Artificial desde la primera óptica de OpenAI

Governance and regulation of Artificial Intelligence from the first perspective of OpenAI

Diego Fierro Rodríguez[1]
Letrado de la Administración de Justicia del Ministerio de Justicia de España.
Codirector de la *Revista Acta Judicial*

Resumen:
El Reglamento de Inteligencia Artificial de la Unión Europea, que entrará en vigor en agosto de 2024, introduce un marco regulatorio integral para la Inteligencia Artificial en Europa, centrado en la seguridad y la confianza. Esta legislación clasifica los sistemas de Inteligencia Artificial en función de su riesgo, estableciendo requisitos específicos para cada categoría, con un enfoque particular en los sistemas de alto riesgo y las prácticas inaceptables. El Reglamento prohíbe ciertas prácticas de Inteligencia Artificial y establece estrictas obligaciones para los sistemas considerados de alto riesgo. Los proveedores y responsables de despliegue deben cumplir con requisitos específicos, y la legislación también tiene una aplicación extraterritorial que afecta a las organizaciones fuera de la Unión Europea. La preparación para el cumplimiento implica la clasificación de los sistemas de Inteligencia Artificial y la consulta con asesores legales especializados.

Abstract:
The European Union Artificial Intelligence Act, set to come into force in August 2024, establishes a comprehensive regulatory framework for artificial intelligence in Europe, focusing on safety and trust. This legislation categorizes Artificial Intelligence systems by risk level, imposing specific requirements for each category, particularly for high-risk systems and unacceptable practices. The Act bans certain Artificial Intelligence practices and mandates rigorous obligations for high-risk Artificial Intelligence systems. Providers and deployers of Artificial Intelligence systems must adhere to these requirements, and the Act's extraterritorial reach affects organizations outside the EU. Preparing for compliance involves classifying Artificial Intelligence systems and consulting with legal experts.

1 Licenciado en Derecho por la Universidad de Málaga (España) y desde 2021 es letrado de la Administración de Justicia ingresado por oposición. En febrero de 2024, fue designado titular del Juzgado de Primera Instancia e Instrucción nº6 de Estepona, tras haber ocupado previamente la misma posición en el Juzgado de Primera Instancia e Instrucción nº1 de Berja desde enero de 2022 hasta febrero de 2024, donde también dirigió el Servicio Común de Actos de Comunicación y Embargos y actuó como secretario de la Junta Electoral de Zona durante tres procesos electorales. Además de su labor procesal, Ha participado como docente en cursos especializados del Instituto Andaluz de Administración Pública y es un colaborador activo en prensa digital, con publicaciones en medios especializados en Derecho. Desde principios de 2024, es codirector de la *Revista Acta Judicial*. Cuenta con una formación complementaria, con Diplomas de Experto Universitario en responsabilidad civil, el ejercicio de la función jurisdiccional en el orden civil y el ejercicio de la función jurisdiccional en el orden penal, todos ellos obtenidos en la Universidad Nacional de Educación a Distancia (España). Su producción académica y profesional está disponible en diversas plataformas digitales, como *Economist & Jurist*, *Legaltoday*, *Law&Trends*, el *Blog jurídico de Sepín* y Dialnet.

Palabras clave:
Reglamento de Inteligencia Artificial, Reglamento de Inteligencia Artificial de la Unión Europea, regulación de Inteligencia Artificial, sistemas de alto riesgo, prácticas inaceptables, proveedores de Inteligencia Artificial, responsables de despliegue de Inteligencia Artificial, aplicación extraterritorial, cumplimiento normativo, seguridad de Inteligencia Artificial.

Keywords
EU Artificial Intelligence Act, artificial intelligence regulation, high-risk Artificial Intelligence systems, unacceptable Artificial Intelligence practices, Artificial Intelligence providers, Artificial Intelligence deployers, extraterritorial application, regulatory compliance, Artificial Intelligence safety.

1. Introducción

La Inteligencia Artificial ha emergido como un factor transformador en la sociedad moderna, trayendo consigo la promesa de mejorar la eficiencia, optimizar procesos y proporcionar soluciones innovadoras a problemas complejos. Sin embargo, el poder y el alcance de la Inteligencia Artificial también han suscitado preocupaciones significativas en torno a su impacto en los derechos fundamentales, la privacidad, la seguridad y la equidad. En este contexto, se vuelve imperativo establecer un conjunto de normas que regulen de manera efectiva el desarrollo y uso de la Inteligencia Artificial, garantizando que sus beneficios sean accesibles para todos y que sus riesgos sean mitigados de manera proporcional[2].

El establecimiento de un marco regulador para la Inteligencia Artificial debe basarse en un enfoque de gestión de riesgos claramente definido[3]. Este enfoque reconoce que no todos los sistemas de Inteligencia Artificial presentan el mismo nivel de riesgo y, por lo tanto, no deben estar sujetos a las mismas normas y requisitos. Al igual que en otros campos tecnológicos, la regulación de la Inteligencia Artificial debe ser flexible y adaptativa, capaz de abordar la diversidad y complejidad de los sistemas de Inteligencia Artificial y su impacto potencial en diferentes contextos.

La primera consideración en la regulación de la Inteligencia Artificial es la identificación de prácticas que deben ser prohibidas por completo. Existen ciertos usos de la Inteligencia Artificial que, debido a su potencial para causar daños significativos o irreversibles, no son aceptables bajo ninguna circunstancia[4].

Uno de los desafíos más apremiantes en la regulación de la Inteligencia Artificial es la definición de los requisitos específicos para los sistemas de alto riesgo. Los sistemas de Inteligencia Artificial que se utilizan en contextos sensibles, como la justicia, la salud, la seguridad pública o el empleo, tienen un potencial significativo para afectar la vida de las personas. Por esta razón, es necesario que estos sistemas estén sujetos a requisitos estrictos que aseguren su fiabilidad, seguridad y equidad[5].

Los sistemas de Inteligencia Artificial de alto riesgo también deben cumplir con obligaciones de transparencia que permitan a los usuarios y a las personas afectadas comprender cómo funcionan estos sistemas y cómo se toman las decisiones automatizadas. La transparencia es una directriz fundamental en la regulación de la Inteligencia Artificial, ya que permite a los individuos tomar decisiones informadas sobre su interacción con estos sistemas y, cuando sea necesario, cuestionar las decisiones que puedan afectarles[6].

Además de los requisitos técnicos y operativos, es crucial que los sistemas de Inteligencia Artificial de alto riesgo se desarrollen y utilicen de manera que respeten los derechos fundamentales de las

2 El Considerando 146 del Reglamento de Inteligencia Artificial establece que, dado el reducido tamaño de algunas empresas, es necesario aplicar un enfoque proporcional respecto a los costes relacionados con la innovación. En este contexto, se permite que las microempresas puedan cumplir una de las obligaciones más onerosas, como la implementación de un sistema de gestión de calidad, de manera simplificada. Esta medida busca aliviar la carga administrativa y financiera que tales requisitos suponen para estas empresas, sin comprometer los niveles de protección ni la obligación de cumplir con los estándares exigidos para los sistemas de IA de alto riesgo. Asimismo, se menciona que la Comisión tiene la responsabilidad de elaborar directrices que definan los elementos específicos que las microempresas deben cumplir dentro de este esquema simplificado del sistema de gestión de calidad. Esta guía proporcionará claridad y ayudará a las microempresas a cumplir con sus obligaciones de manera más eficiente.

3 Un enfoque de gestión de riesgos permite diferenciar entre los sistemas de Inteligencia Artificial de bajo riesgo, que pueden operar con una supervisión mínima, y aquellos de alto riesgo, que requieren controles más estrictos y una vigilancia constante, como se podrá comprobar en páginas siguientes.

4 Los mismos pueden incluir, por ejemplo, sistemas de Inteligencia Artificial que manipulan el comportamiento humano de manera indebida, violan los derechos fundamentales o perpetúan la discriminación. La prohibición de estas prácticas es esencial para proteger a la sociedad de los peligros inherentes a la Inteligencia Artificial mal utilizada y para garantizar que el desarrollo de esta tecnología se realice dentro de límites éticos y jurídicos claros.

5 Ello incluye la necesidad de realizar evaluaciones de impacto antes de su despliegue, establecer mecanismos de supervisión continua y adoptar medidas correctivas en caso de que se identifiquen problemas o riesgos.

6 Ello es especialmente importante en contextos donde las decisiones automatizadas pueden tener consecuencias significativas, como en la contratación de personal, la concesión de créditos, la toma de decisiones judiciales o el diagnóstico médico.

personas(López de Mántaras, 2018). Ello implica no solo garantizar la protección de la privacidad y la seguridad de los datos, sino también prevenir la discriminación y promover la equidad en todas las etapas del ciclo de vida de la Inteligencia Artificial. Los desarrolladores y operadores de sistemas de Inteligencia Artificial deben ser conscientes de los sesgos que pueden surgir en los algoritmos y tomar medidas proactivas para mitigarlos. La equidad en la Inteligencia Artificial no es solo una cuestión de justicia social, sino también un imperativo legal y ético que debe guiar el desarrollo y uso de estas tecnologías.

La implementación de normas y regulaciones para la Inteligencia Artificial también debe ir acompañada de un esfuerzo continuo por parte de los gobiernos, las empresas y la sociedad civil para educar y capacitar a las personas sobre el uso y las implicaciones de la Inteligencia Artificial. La alfabetización en Inteligencia Artificial es fundamental para asegurar que todos los sectores de la sociedad puedan beneficiarse de estas tecnologías de manera equitativa y que las personas estén equipadas para enfrentar los desafíos que puedan surgir en un mundo cada vez más impulsado por la Inteligencia Artificial(Jiménez, 2024).

Además de la alfabetización en Inteligencia Artificial, es esencial fomentar una cultura de responsabilidad y ética en el desarrollo y uso de estas tecnologías[7]. Los desarrolladores, operadores y usuarios de sistemas de Inteligencia Artificial deben ser conscientes de las implicaciones éticas de sus decisiones y estar comprometidos con el desarrollo de una Inteligencia Artificial que respete los derechos humanos y promueva el bienestar social. Ello requiere un compromiso continuo con la formación ética, así como la adopción de principios éticos en todas las etapas del desarrollo y despliegue de la Inteligencia Artificial.

Otro aspecto crucial en la regulación de la Inteligencia Artificial es la supervisión y el cumplimiento de las normas establecidas. Por lo cual, los marcos regulatorios para la Inteligencia Artificial deben incluir mecanismos eficaces de supervisión y aplicación que aseguren que las normas se respeten y que los infractores sean sancionados de manera adecuada[8].

La supervisión efectiva también requiere la cooperación internacional, dado que la Inteligencia Artificial es una tecnología global y sus impactos trascienden las fronteras nacionales. Los gobiernos y las organizaciones internacionales deben colaborar para desarrollar estándares y normas comunes que puedan ser adoptados a nivel global, asegurando que la regulación de la Inteligencia Artificial sea coherente y eficaz en todos los contextos[9].

Un enfoque basado en el riesgo para la regulación de la Inteligencia Artificial también debe ser dinámico y adaptable, capaz de evolucionar a medida que la tecnología avanza y que surgen nuevos desafíos. La Inteligencia Artificial es una tecnología en rápida evolución, y los marcos regulatorios deben ser lo suficientemente flexibles para adaptarse a los cambios en el panorama tecnológico y social. Ello puede incluir la revisión periódica de las normas existentes, la actualización de los requisitos técnicos y la incorporación de nuevas tecnologías y enfoques en la regulación de la Inteligencia Artificial.

También, es importante que la regulación de la Inteligencia Artificial se base en una sólida comprensión de la tecnología y sus implicaciones. Los responsables de la formulación de políticas y los reguladores deben trabajar en estrecha colaboración con expertos en Inteligencia Artificial, científicos de datos, eticistas y otros actores relevantes para asegurar que las normas sean técnicas y éticamente sólidas. Ello incluye la necesidad de una investigación continua en el campo de la Inteligencia Artificial para comprender mejor los riesgos y oportunidades asociados con estas tecnologías y para desarrollar enfoques de regulación basados en la evidencia (Salazar García, 2023).

La regulación de la Inteligencia Artificial también debe ser inclusiva, involucrando a todas las partes interesadas en el proceso de toma de decisiones. Ello incluye no solo a los desarrolladores y operadores de Inteligencia Artificial, sino también a los usuarios, las comunidades afectadas, la sociedad civil, las organizaciones de derechos humanos y otros actores relevantes. La inclusión de una amplia gama de perspectivas es fundamental para garantizar que la regulación de la Inteligencia Artificial sea justa, equitativa y representativa de los intereses de todos los sectores de la sociedad.

El 30 de julio, OpenAI presentó su "Primera aproximación al Reglamento de Inteligencia Artificial", un documento que aborda de manera preliminar las implicaciones del Reglamento de Inteligencia Artificial de la Unión Europea[10]. Este marco regulatorio representa un paso significativo

7 Precisamente, debe establecerse una vía para poder limitar y marcar los contornos de lo que es correcto con la Inteligencia Artificial (González Alvarado, 2024)...

8 Ello puede incluir la creación de organismos de supervisión independientes con la autoridad para investigar y sancionar violaciones, así como la implementación de auditorías periódicas y la obligación de informar sobre el cumplimiento de las normas Martínez Rodríguez, 2023).

9 Esta cooperación internacional es especialmente importante para abordar los desafíos que surgen en áreas como la seguridad cibernética, la privacidad de los datos y la protección de los derechos humanos en un entorno digital globalizado.

10 Así se hará referencia al Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se

en la gobernanza del desarrollo, implementación y uso de la Inteligencia Artificial en el territorio europeo.

Desde una perspectiva jurídica, el Reglamento de Inteligencia Artificial busca equilibrar la promoción de la adopción de tecnologías de Inteligencia Artificial fiables y seguras con la protección de los derechos fundamentales, la salud y la seguridad de los ciudadanos europeos. Precisamente, OpenAI ya ha mostrado parte de sus cartas desarrollando su primera visión y anotando algunos aspectos a remarcar en cuanto a la nueva norma que le afectan a las empresas del sector.

2. Contexto y objetivos del Reglamento de Inteligencia Artificial de la Unión Europea

La Inteligencia Artificial se ha convertido en una de las tecnologías más transformadoras de nuestra era, y su impacto en los sectores económicos, sociales y medioambientales es tan amplio como profundo. Este conjunto de tecnologías en constante evolución está revolucionando múltiples aspectos de la vida humana y tiene el potencial de generar beneficios sin precedentes en diversas áreas clave para el desarrollo sostenible y el bienestar global, aunque también numerosos peligros (Álvarez Cantalapiedra, 2023).

Desde una perspectiva económica, la Inteligencia Artificial está redefiniendo la competitividad empresarial a través de su capacidad para optimizar procesos, mejorar la eficiencia y crear nuevas oportunidades de mercado (Espinosa Proa , 2024). En sectores como la manufactura, la Inteligencia Artificial permite la automatización avanzada de líneas de producción, la gestión inteligente de la cadena de suministro y la personalización masiva de productos, lo que a su vez mejora la productividad y reduce los costos operativos. Las empresas que adoptan la Inteligencia Artificial no solo logran una ventaja competitiva significativa, sino que también abren nuevas fronteras en la innovación de productos y servicios. Esta capacidad para innovar y adaptarse a los cambios del mercado es vital en un mundo donde la rapidez y la flexibilidad son fundamentales para el éxito empresarial, aunque también es necesario atender a los peligros que ello conlleva (Tourpe, 2023).

En el ámbito medioambiental, la Inteligencia Artificial puede acabar jugando un papel crucial en la lucha contra el cambio climático y en la promoción de la sostenibilidad. Las tecnologías basadas en Inteligencia Artificial se pueden utilizar para mejorar la predicción del clima, optimizar el uso de los recursos naturales y reducir las emisiones de carbono. Por ejemplo, en el sector energético, el aprovechamiento de algoritmos permite la gestión inteligente de redes eléctricas, lo que facilita la integración de fuentes de energía renovable y reduce la dependencia de combustibles fósiles. Asimismo, la Inteligencia Artificial se emplea en la agricultura para monitorizar cultivos, predecir rendimientos y gestionar el uso del agua y los fertilizantes de manera

más eficiente, lo que no solo mejora la productividad agrícola, sino que también minimiza el impacto ambiental. Mientras que, en la gestión de infraestructuras, la utilización de algoritmos contribuye a optimizar el mantenimiento de edificios y carreteras, lo que prolonga su vida útil y reduce la necesidad de nuevas construcciones, con el consiguiente ahorro de recursos naturales y reducción de residuos.

El impacto social de la Inteligencia Artificial es igualmente significativo. En el ámbito de la salud, por ejemplo, el uso de algoritmos está transformando la medicina personalizada, permitiendo diagnósticos más precisos y tratamientos adaptados a las necesidades individuales de los pacientes. Los sistemas de Inteligencia Artificial pueden analizar grandes volúmenes de datos médicos para identificar patrones que serían imposibles de detectar para los humanos, lo que mejora la detección temprana de enfermedades y la eficacia de las intervenciones médicas. Además, la Inteligencia Artificial está facilitando el acceso a la atención médica en regiones remotas o desfavorecidas a través de la telemedicina y los sistemas de diagnóstico remoto. Esto no solo mejora la calidad de vida de las personas, sino que también contribuye a la equidad en el acceso a servicios de salud.

En el sector educativo, la Inteligencia Artificial está revolucionando la forma en que se imparte la educación y se realiza la formación. Los sistemas de tutoría inteligente basados en algoritmos pueden adaptarse a las necesidades de aprendizaje de cada estudiante, proporcionando un enfoque personalizado que mejora la retención de conocimientos y el rendimiento académico. También, la Inteligencia Artificial permite la creación de contenidos educativos interactivos y adaptativos, que pueden ajustarse en tiempo real en función del progreso del estudiante[11].

establecen normas armonizadas en materia de Inteligencia Artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), que se halla en el «DOUE» núm. 1689, de 12 de julio de 2024, páginas 1 a 144.

11 Ello no solo beneficia a los estudiantes, sino que también facilita el trabajo de los educadores al proporcionarles herramientas más eficaces para evaluar y apoyar a sus alumnos. En el ámbito de la formación profesional, la utilidad de los algoritmos está desempeñando un papel fundamental en la capacitación de la fuerza laboral para las nuevas demandas del mercado, ofreciendo programas de aprendizaje automatizado y personalizado que preparan a los trabajadores para las competencias del futuro. (Lizarazu Gutiérrez, 2024).

El uso de la Inteligencia Artificial también está teniendo un impacto profundo en la cultura, el deporte y los medios de comunicación. En el ámbito cultural, la Inteligencia Artificial está siendo utilizada para la conservación y restauración de obras de arte, la creación de nuevas formas de expresión artística y la preservación de la herencia cultural. En el deporte, los algoritmos se utilizan para analizar el rendimiento de los atletas, optimizar las estrategias de juego y mejorar la experiencia de los aficionados a través de análisis en tiempo real y la personalización de contenidos. En los medios de comunicación, la Inteligencia Artificial está transformando la producción y distribución de contenidos, permitiendo la creación de noticias personalizadas y la automatización de procesos editoriales, lo que está cambiando radicalmente la forma en que consumimos información y entretenimiento.

En la esfera pública, la Inteligencia Artificial está mejorando la eficiencia y la eficacia de los servicios públicos. Los sistemas de algoritmos se están utilizando para optimizar la gestión del tráfico, mejorar la seguridad pública y facilitar la administración de justicia[12]. En la seguridad, la Inteligencia Artificial permite la detección y prevención de delitos a través del análisis de patrones y comportamientos, lo que ayuda a las fuerzas del orden a tomar decisiones más informadas y a responder de manera más efectiva a las amenazas. En la justicia, la Inteligencia Artificial está siendo utilizada para analizar grandes volúmenes de datos legales, lo que facilita la toma de decisiones judiciales y mejora la transparencia y la coherencia en la aplicación de la ley.Incluso, en la gestión de recursos y energía, la Inteligencia Artificial está ayudando a las ciudades a convertirse en "*smart cities*", donde los recursos se gestionan de manera más eficiente y se mejoran los servicios a los ciudadanos, desde la recolección de basura hasta la gestión del agua y la energía.

La personalización de soluciones digitales es otro ámbito en el que la Inteligencia Artificial está marcando una diferencia significativa. En cuanto, los sistemas de Inteligencia Artificial pueden analizar grandes volúmenes de datos para ofrecer soluciones personalizadas a las necesidades específicas de individuos y organizaciones. Esto es especialmente importante en el contexto de la atención médica, donde los algoritmos permiten la creación de planes de tratamiento personalizados que tienen en cuenta el historial médico, el perfil genético y las preferencias individuales del paciente. En el sector educativo, la personalización impulsada por Inteligencia Artificial permite a los estudiantes aprender a su propio ritmo y de la manera que mejor se adapte a sus necesidades, lo que mejora los resultados de aprendizaje y reduce la tasa de abandono escolar.

Por otro lado, en el ámbito empresarial, la personalización también juega un papel crucial en la mejora de la experiencia del cliente. Los sistemas de Inteligencia Artificial pueden analizar los comportamientos y preferencias de los consumidores para ofrecer productos y servicios que se ajusten mejor a sus necesidades y deseos. Esto no solo mejora la satisfacción del cliente, sino que también aumenta la lealtad a la marca y las ventas. Es más, la Inteligencia Artificial permite a las empresas optimizar sus estrategias de marketing y ventas, identificando las mejores oportunidades de negocio y personalizando las campañas publicitarias para alcanzar a los clientes adecuados en el momento adecuado.

La capacidad de la Inteligencia Artificial para optimizar la asignación de recursos es particularmente relevante en sectores como el transporte y la logística, donde la eficiencia es clave. Y es que, los sistemas algorítmicos pueden analizar datos en tiempo real para optimizar las rutas de transporte, gestionar el tráfico y mejorar la eficiencia de las cadenas de suministro. Esto no solo reduce los costos operativos, sino que también disminuye las emisiones de gases contaminantes y mejora la puntualidad en la entrega de bienes y servicios. En el sector energético, la Inteligencia Artificial permite la optimización de la distribución de electricidad, asegurando que la energía se utilice de la manera más eficiente posible y minimizando las pérdidas.

El transporte es otro sector en el que la Inteligencia Artificial está teniendo un impacto transformador. Los sistemas de conducción autónoma, impulsados por Inteligencia Artificial, están cambiando la forma en que nos movemos, mejorando la seguridad vial, reduciendo el tráfico y disminuyendo las emisiones de carbono. Puesto que, la programación algorítmica está siendo utilizada para gestionar de manera más eficiente el transporte público, optimizando las rutas y horarios para satisfacer mejor las necesidades de los pasajeros. En el futuro, se espera que la Inteligencia Artificial juegue un papel aún más importante en la creación de sistemas de transporte más sostenibles y eficientes, que contribuyan a la reducción de la congestión urbana y al desarrollo de ciudades más habitables.

El Reglamento de Inteligencia Artificial de la Unión Europea, que ha entrado vigor y aplicación en agosto de 2024 con algunos matices[13], es el primer intento integral y efectivo de regular la Inteligencia Artificial

12 En este campo, se ha revelado el grave peligro derivado de los sesgos algorítmicos. (López Martínez, 2022).

13 Debe tenerse presente las reglas sobre vigencia y aplicación del artículo 113 del Reglamento de Inteligencia Artificial. El Reglamento entrará en vigor veinte días después de su publicación en el Diario Oficial de la Unión Europea, pero su aplicación será gradual,

a nivel supranacional. Se centra en la seguridad y la confianza, fijando un marco normativo que clasifica los sistemas de Inteligencia Artificial según su nivel de riesgo y asigna obligaciones específicas a los desarrolladores y usuarios de estos sistemas. La norma distingue entre sistemas de riesgo inaceptable, alto riesgo y riesgo limitado o mínimo, estableciendo requisitos específicos para cada categoría[14].

La legislación tiene como objetivo principal mitigar los riesgos asociados con la Inteligencia Artificial, promoviendo al mismo tiempo su innovación y desarrollo seguro. Para lograrlo, se introducen requisitos rigurosos de transparencia[15], gobernanza de datos[16], gestión de riesgos[17] y supervisión continua[18]. Además, se presta especial atención a los sistemas de Inteligencia Artificial de uso general (en adelante, IAUG), que incluyen modelos como los

comenzando completamente el 2 de agosto de 2026. Antes de esa fecha, algunas disposiciones se implementarán en fases: los capítulos I y II serán aplicables a partir del 2 de febrero de 2025, seguidos por otras secciones el 2 de agosto de 2025, y algunas obligaciones específicas no entrarán en vigor hasta el 2 de agosto de 2027. Este Reglamento será obligatorio y aplicable directamente en todos los Estados miembros de la Unión Europea desde su adopción en Bruselas el 13 de junio de 2024.

14 El Considerando 51 del Reglamento de Inteligencia Artificial aclara que el hecho de que un sistema de IA sea catalogado como de alto riesgo según este reglamento no implica automáticamente que el producto en el que se integre como componente de seguridad, o el propio sistema de IA, sea considerado de "alto riesgo" bajo la normativa armonizada de la Unión Europea aplicable al producto. Esta distinción es particularmente relevante en relación con los Reglamentos (UE) 2017/745 y (UE) 2017/746, los cuales contemplan un proceso de evaluación de conformidad por parte de terceros para productos clasificados como de riesgo medio y alto. Este enfoque asegura que la evaluación de los riesgos se ajuste a los criterios específicos de cada normativa, garantizando la correcta aplicación de las disposiciones en función de las características particulares del producto o sistema.

15 El artículo 13.1 del Reglamento de Inteligencia Artificial dispone que los sistemas de IA clasificados como de alto riesgo deben ser diseñados y desarrollados de manera que se garantice un nivel adecuado de transparencia. Esto es fundamental para que quienes los implementen puedan interpretar y utilizar correctamente los resultados generados. Además, el grado de transparencia debe ser suficiente para que tanto el proveedor como el responsable del despliegue cumplan con las obligaciones que se especifican en la sección 3 del reglamento, asegurando un uso responsable y conforme a la normativa aplicable.

16 El artículo 10.2 del Reglamento de Inteligencia Artificial es muy claro. Los conjuntos de datos utilizados en los sistemas de inteligencia artificial de alto riesgo deben gestionarse mediante prácticas rigurosas de gobernanza y gestión de datos, asegurando su adecuación para el propósito del sistema. Estas prácticas incluyen la toma de decisiones sobre el diseño, la recogida de datos, su origen, y, en el caso de datos personales, su propósito inicial. Además, se deben llevar a cabo operaciones de tratamiento de datos, como su anotación, etiquetado, y depuración. En este sentido, resulta esencial formular supuestos sobre lo que los datos miden y representan, evaluar la disponibilidad y calidad de los datos, y examinar posibles sesgos que puedan afectar la salud, seguridad, derechos fundamentales, o provocar discriminación. Finalmente, se deben implementar medidas para prevenir y mitigar estos sesgos y detectar cualquier deficiencia en los datos que impida cumplir con las normativas, tomando las acciones necesarias para corregirlas.

17 El artículo 9 del Reglamento de Inteligencia Artificial determina que la gestión de riesgos para sistemas de IA de alto riesgo debe ser un proceso continuo y cíclico a lo largo de todo el ciclo de vida del sistema. Este proceso incluye la identificación y evaluación de riesgos potenciales para la salud, la seguridad y los derechos fundamentales, así como la previsión de posibles usos indebidos. En función de estos análisis, se deben adoptar medidas específicas para mitigar o eliminar los riesgos detectados, considerando el contexto y los conocimientos sobre el uso del sistema. Las pruebas de los sistemas, realizadas en diferentes fases del desarrollo, son esenciales para asegurar que el sistema funcione según su propósito y cumpla con los requisitos regulatorios, prestando especial atención a los colectivos vulnerables, como los menores. Asimismo, el Considerando 65 del Reglamento refuerza que este proceso de gestión de riesgos debe ser iterativo y ejecutado a lo largo de toda la vida útil del sistema de IA de alto riesgo. Debe enfocarse en detectar y mitigar los riesgos significativos para la salud, la seguridad y los derechos fundamentales, y ser revisado y actualizado periódicamente para garantizar su eficacia. Es crucial que todas las decisiones y acciones importantes sean justificadas y documentadas adecuadamente. Los proveedores deben identificar y mitigar tanto los riesgos conocidos como los previsibles, considerando el estado actual de la técnica en IA. La participación de expertos y partes interesadas externas puede ser necesaria para asegurar la adecuación de las medidas adoptadas. Además, se debe tener en cuenta el uso indebido razonablemente previsible, que aunque no esté explícitamente cubierto por la finalidad prevista o las instrucciones de uso, puede surgir de comportamientos humanos previsibles. Las instrucciones del sistema deben advertir sobre cualquier circunstancia conocida o previsible que pueda generar riesgos. Aunque el Reglamento no exige que se realicen entrenamientos adicionales específicos para abordar usos indebidos previsibles, se alienta a los proveedores a considerar tales medidas cuando sean necesarias para mejorar la seguridad y la eficacia del sistema.

18 El artículo 14 del Reglamento de Inteligencia Artificial establece que los sistemas de IA de alto riesgo deben ser diseñados y desarrollados para permitir una supervisión humana efectiva, incorporando herramientas de interfaz humano-máquina adecuadas. La finalidad de esta supervisión es mitigar los riesgos para la salud, la seguridad y los derechos fundamentales, tanto en el uso previsto del sistema como en casos de uso indebido razonablemente previsible. Las medidas de supervisión deben ser proporcionales a los riesgos, al grado de autonomía del sistema y al contexto de uso, y pueden incluir herramientas integradas o procedimientos a seguir por el responsable del despliegue. Estas medidas deben permitir a los supervisores entender las capacidades y limitaciones del sistema, monitorear su funcionamiento, identificar problemas y evitar una confianza excesiva en los resultados generados, conocida como "sesgo de automatización". Además, los supervisores deben estar capacitados para interpretar los resultados, tomar decisiones sobre el uso del sistema y, cuando sea necesario, intervenir o detener el sistema de manera segura. En el caso de sistemas de alto riesgo que identifican personas, las decisiones basadas en esta identificación deben ser revisadas por al menos dos personas competentes, excepto en situaciones excepcionales previstas por la ley, como el control migratorio o fronterizo, donde la doble verificación podría considerarse desproporcionada. Precisamente, el Considerando 73 del Reglamento aclara que los sistemas de IA de alto riesgo deben estar diseñados para permitir la supervisión humana continua, asegurando que se usen de acuerdo con su propósito y que se aborden sus repercusiones a lo largo de su ciclo de vida. El proveedor del sistema debe definir las medidas de supervisión humana adecuadas antes de la comercialización o puesta en servicio del sistema, garantizando que el sistema tenga limitaciones operativas incorporadas y que los supervisores humanos cuenten con las competencias, formación y autoridad necesarias. También es crucial que los sistemas incluyan mecanismos para guiar e informar a los supervisores sobre cuándo intervenir y cómo hacerlo para evitar riesgos. En el caso de sistemas de identificación biométrica, donde los errores pueden tener consecuencias graves, se requiere una supervisión humana reforzada, exigiendo que al menos dos personas verifiquen y confirmen la identificación por separado. Este requisito no debe causar cargas ni retrasos innecesarios y puede ser registrado automáticamente en los registros del sistema. Sin embargo, en áreas como el cumplimiento del Derecho, migración, control fronterizo y asilo, este requisito puede no aplicarse si su aplicación se considera desproporcionada según el Derecho nacional o de la Unión.

desarrollados por OpenAI. En este sentido, resalta poderosamente el Considerando 27 del Reglamento de Inteligencia Artificial.

Aunque el enfoque basado en el riesgo constituye el fundamento de un conjunto de normas vinculantes eficaces y proporcionadas, resulta esencial tener en cuenta las Directrices éticas para una IA fiable de 2019, elaboradas por el Grupo de expertos de alto nivel sobre IA creado por la Comisión. En estas directrices, se desarrollaron siete principios éticos no vinculantes cuyo objetivo es garantizar la fiabilidad y el carácter ético de la Inteligencia Artificial. Estos principios abordan cuestiones clave como la intervención y supervisión humana, la solidez técnica y la seguridad, la gestión adecuada de la privacidad y los datos, así como la transparencia, la promoción de la diversidad, la no discriminación y la equidad.

Cabe resaltar que, los principios también destacan la importancia del bienestar social y ambiental y la rendición de cuentas. Aunque estas directrices no imponen obligaciones legales, complementan las disposiciones del Reglamento y otros actos jurídicos de la Unión, contribuyendo al diseño de una IA coherente, fiable y centrada en las personas, alineada con los valores fundamentales de la Unión Europea y la Carta de los Derechos Fundamentales.

El principio de "acción y supervisión humanas" implica que los sistemas de IA respeten la dignidad y la autonomía personal, permitiendo que los humanos puedan controlarlos y supervisarlos adecuadamente. La "solidez técnica y seguridad" exige que los sistemas de IA sean robustos frente a fallos y resistentes a intentos de manipulación maliciosa, minimizando así los posibles daños no deseados.

En cuanto a la "gestión de la privacidad y de los datos", el desarrollo y uso de los sistemas de IA debe cumplir con las normas de protección de datos, asegurando que se mantengan altos estándares de calidad e integridad en los datos tratados. El principio de "transparencia" demanda que los sistemas de IA sean trazables y explicables, informando claramente tanto a los responsables de su implementación como a las personas afectadas acerca de sus capacidades, limitaciones y los derechos que les asisten.

La "diversidad, no discriminación y equidad" promueve la inclusión de una amplia variedad de agentes y asegura la igualdad de acceso, evitando cualquier sesgo o efecto discriminatorio prohibido por la legislación nacional o de la Unión. Por último, el "bienestar social y ambiental" subraya que los sistemas de IA deben ser sostenibles y respetuosos con el medio ambiente, contribuyendo al beneficio de todos los seres humanos y evaluando sus efectos a largo plazo sobre la sociedad, la democracia y el entorno.

Estos principios éticos no solo deben inspirar el diseño y uso de modelos de IA, sino también guiar la elaboración de códigos de conducta conforme al Reglamento. Se anima a la industria, al mundo académico, a la sociedad civil y a las organizaciones de normalización a considerar estos principios en el desarrollo de estándares y mejores prácticas voluntarias.

El desarrollo y la implementación de sistemas de Inteligencia Artificial están transformando de manera significativa el panorama tecnológico y social global. A medida que estos sistemas se integran más profundamente en diversas facetas de la vida cotidiana, se hace evidente la necesidad de establecer un conjunto de normas que no solo regulen su funcionamiento, sino que también garanticen su concordancia con principios éticos y derechos fundamentales[19].

El enfoque basado en el riesgo para la regulación de la Inteligencia Artificial busca equilibrar la innovación con la protección de los derechos individuales y colectivos[20]. Este enfoque se fundamenta en la idea de que no todos los sistemas de Inteligencia Artificial presentan el mismo nivel de riesgo y, por tanto, no deben estar sujetos a las mismas normas. Los sistemas de alto riesgo, aquellos cuya implementación puede tener un impacto significativo en los derechos fundamentales, la seguridad o el bienestar de las personas, deben estar sujetos a requisitos más estrictos[21].

En el marco de este enfoque, es imperativo prohibir ciertas prácticas de Inteligencia Artificial que se consideran inaceptables bajo cualquier circunstancia[22]. La prohibición de estas prácticas no solo responde a la necesidad de proteger los derechos fundamentales, sino también a la

19 En este sentido, es crucial que cualquier marco regulador se base en un enfoque de gestión de riesgos claramente definido y proporcionado, adaptando las normas al nivel de riesgo que cada sistema de Inteligencia Artificial pueda representar.

20 El Considerando 2 del Reglamento de Inteligencia Artificial establece que su aplicación debe alinearse con los valores fundamentales de la Unión Europea, tal como se recogen en la Carta. Ello tiene como objetivo proteger a las personas físicas, las empresas, la democracia, el Estado de Derecho y el medio ambiente, al tiempo que fomenta la innovación, el empleo y refuerza el liderazgo de la Unión en la adopción de una inteligencia artificial fiable.

21 Estos requisitos incluyen, entre otros, la evaluación exhaustiva antes de su despliegue, el control continuo de su funcionamiento, y la implementación de salvaguardias que permitan mitigar posibles daños.

22 Es fundamental erradicar prácticas que impliquen el uso de sistemas de inteligencia artificial que manipulen de manera indebida el comportamiento humano o que generen discriminación injusta, para proteger a la sociedad de sus riesgos. El Considerando 46 del Reglamento de Inteligencia Artificial señala que la comercialización, puesta en servicio o uso de sistemas de IA de alto riesgo en

obligación de mantener la confianza del público en las tecnologías emergentes.

El artículo 5 del Reglamento de Inteligencia Artificial recoge una serie de restricciones rigurosas en relación con el uso y la comercialización de sistemas de Inteligencia Artificial que se consideran perjudiciales o potencialmente peligrosos para la sociedad y los individuos. Por ello, este artículo enfatiza la prohibición de prácticas que empleen Inteligencia Artificial para manipular o influir en el comportamiento de las personas de manera sutil y subliminal, trascendiendo su conciencia. Este tipo de técnicas, que pueden ser deliberadamente engañosas, tienen el objetivo o el efecto de alterar significativamente la capacidad de una persona para tomar decisiones informadas, llevándola a actuar de una manera que, en condiciones normales, no hubiera elegido. El uso de estas técnicas, que puede causar daños considerables, es considerado inaceptable y queda estrictamente prohibido.

De hecho, se prohíbe el uso de sistemas de Inteligencia Artificial que exploten las vulnerabilidades de personas o grupos específicos, ya sea debido a su edad, discapacidad, situación social o económica. Esta explotación, con el fin de modificar sustancialmente el comportamiento de dichos individuos o colectivos, podría resultar en daños significativos para ellos o para otros, y por lo tanto, no está permitida. Los sistemas de Inteligencia Artificial diseñados para evaluar o clasificar a personas basándose en su comportamiento social o características personales durante un periodo determinado también están prohibidos si tales evaluaciones resultan en un trato injustificado o desproporcionado hacia las personas o colectivos afectados. Esto incluye situaciones en las que la puntuación ciudadana resultante de estas evaluaciones conduzca a un trato desfavorable en contextos distintos a aquellos en los que se recopilaron los datos originalmente.

Asimismo, el citado precepto prohíbe el uso de sistemas de Inteligencia Artificial para predecir la probabilidad de que una persona cometa un delito, basándose únicamente en la elaboración de perfiles o en la evaluación de sus características de personalidad. Por tanto, esta restricción es importante para evitar decisiones prejuiciosas y discriminatorias que puedan surgir de la aplicación automatizada de perfiles. Sin embargo, esta prohibición no se extiende a los sistemas de Inteligencia Artificial que apoyan la valoración humana en investigaciones delictivas basadas en hechos objetivos y verificables.

El precepto también aborda la prohibición del uso de Inteligencia Artificial para la creación o ampliación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes de internet o de circuitos cerrados de televisión, una práctica que atenta contra la privacidad y los derechos de los individuos. De igual manera, queda prohibido el uso de sistemas de Inteligencia Artificial para inferir emociones en lugares de trabajo y centros educativos, salvo que se justifique por motivos médicos o de seguridad, y el uso de sistemas de categorización biométrica que clasifiquen a las personas en función de datos biométricos sensibles, como raza, opiniones políticas, orientación sexual, entre otros.

En cuanto a la identificación biométrica remota "en tiempo real" en espacios públicos, esta práctica está prohibida a menos que sea estrictamente necesaria para cumplir con fines específicos relacionados con la seguridad pública, como la búsqueda de víctimas de delitos graves o la prevención de amenazas inminentes a la vida o seguridad de las personas. Incluso en estos casos, el uso de estos sistemas debe estar acompañado de estrictas garantías y condiciones proporcionales, como la limitación temporal, geográfica y personal, y requiere una autorización previa de una autoridad judicial o administrativa independiente.

Si se presenta una situación de urgencia, se puede permitir el uso temporal de estos sistemas sin la autorización previa, pero dicha autorización debe ser solicitada sin demora. En cualquier caso, si se rechaza la autorización, el uso debe cesar inmediatamente y todos los datos generados deben ser eliminados de forma permanente. Además, cualquier uso de sistemas de identificación biométrica en espacios públicos debe ser notificado a las autoridades pertinentes, y los estados miembros deben establecer normativas detalladas sobre la solicitud y supervisión de estas autorizaciones.

Los Estados miembros están obligados a informar a la Comisión Europea sobre el uso de estos sistemas

la Unión Europea debe estar condicionada al cumplimiento de ciertos requisitos obligatorios. Estos requisitos buscan garantizar que dichos sistemas no representen riesgos inaceptables para los intereses públicos fundamentales, reconocidos y protegidos por el Derecho de la Unión. Según el marco legislativo establecido, y conforme a lo señalado en la "Guía azul" sobre la aplicación de las normas europeas de 2022, es común que más de un acto jurídico de armonización de la Unión, como los Reglamentos (UE) 2017/745 y (UE) 2017/746 o la Directiva 2006/42/CE, se aplique a un producto. En este sentido, un producto solo puede ser comercializado si cumple con toda la legislación de armonización aplicable. Para evitar cargas administrativas y costos innecesarios, los proveedores de productos que integren sistemas de IA de alto riesgo deben adoptar decisiones operativas flexibles que aseguren la conformidad de estos productos con los requisitos establecidos tanto en este Reglamento como en la legislación de armonización pertinente. La clasificación de un sistema de IA como "de alto riesgo" debe restringirse a aquellos que puedan tener un impacto considerable en la salud, la seguridad o los derechos fundamentales de los ciudadanos de la Unión, minimizando así posibles barreras al comercio internacional.

y la Comisión publicará informes anuales basados en los datos agregados de los estados miembros. Finalmente, este precepto no afecta otras prohibiciones existentes bajo el Derecho de la Unión Europea en relación con prácticas de Inteligencia Artificial, asegurando una capa adicional de protección para los derechos fundamentales de los individuos en el contexto del avance tecnológico.

Además de las prohibiciones, es esencial definir de manera clara los requisitos que deben cumplir los sistemas de Inteligencia Artificial de alto riesgo[23]. Estos requisitos deben ser diseñados para garantizar que tales sistemas operen dentro de un marco que minimice los riesgos y maximice los beneficios sociales[24].

La transparencia es especialmente relevante en contextos donde la Inteligencia Artificial interactúa directamente con los individuos, como en el ámbito de la salud, la justicia o el empleo[25]. En tales casos, es fundamental que las personas sean conscientes de que están interactuando con un sistema automatizado y que comprendan sus derechos en relación con esta interacción[26].

En cuanto a la ética y los principios fundamentales que deben guiar el desarrollo y el uso de la Inteligencia Artificial, las *Directrices éticas para una Inteligencia Artificial fiable*, elaboradas en 2019 por el Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial de la Comisión Europea, ofrecen un marco valioso (Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, 2019). Aunque estas directrices no son jurídicamente vinculantes, proporcionan una base sólida para el desarrollo de una Inteligencia Artificial que respete la dignidad humana y los valores fundamentales de la Unión Europea. Entre los principios destacados en estas directrices se encuentran la acción y supervisión humanas, la solidez técnica y la seguridad, la gestión de la privacidad y los datos, la transparencia, la diversidad, la no discriminación y la equidad, el bienestar social y ambiental, y la rendición de cuentas[27].

La acción y supervisión humanas son esenciales para garantizar que los sistemas de Inteligencia Artificial se utilicen como herramientas al servicio de las personas y no como mecanismos que socaven su autonomía o dignidad[28]. La supervisión humana permite mantener un control efectivo sobre los sistemas de Inteligencia Artificial, asegurando que sus decisiones puedan ser revisadas y corregidas si es necesario[29].

La solidez técnica y la seguridad son igualmente cruciales[30]. Por ello, los sistemas de Inteligencia Artificial deben ser diseñados y desarrollados de manera que sean robustos ante posibles fallos y resilientes frente a intentos de manipulación maliciosa. La integridad del sistema es fundamental para evitar usos indebidos y minimizar los daños potenciales que puedan derivarse de su operación.

23 Véase el artículo 6.2 del Reglamento de Inteligencia Artificial en relación con el Anexo III. Los sistemas de Inteligencia Artificial considerados de alto riesgo, según lo establecido en el artículo 6.2, abarcan una amplia gama de aplicaciones en diferentes sectores clave. En el ámbito de la biometría, se incluyen sistemas de identificación biométrica remota, excluyendo aquellos destinados únicamente a la verificación de identidad de una persona. También se consideran de alto riesgo los sistemas que utilizan la Inteligencia Artificial para categorización biométrica basada en atributos sensibles o protegidos, así como aquellos diseñados para el reconocimiento de emociones. En infraestructuras críticas, los sistemas de Inteligencia Artificial que actúan como componentes de seguridad en la gestión de infraestructuras digitales, transporte, y servicios esenciales como agua y electricidad, también están incluidos. En el sector educativo, los sistemas que determinan el acceso a centros educativos, evalúan el aprendizaje o monitorean el comportamiento en exámenes se consideran de alto riesgo. En el ámbito laboral, se incluyen sistemas de Inteligencia Artificial utilizados para la contratación, gestión de empleados y evaluación del desempeño. Además, se consideran de alto riesgo los sistemas que evalúan la admisibilidad a servicios esenciales, como asistencia pública, calificación crediticia, o que son utilizados en la evaluación de riesgos y fijación de precios en seguros. Los sistemas de Inteligencia Artificial utilizados en la garantía del cumplimiento del Derecho, como los destinados a evaluar el riesgo de delitos o verificar pruebas, también están bajo esta categoría. En el contexto de la migración y el control fronterizo, los sistemas que evalúan riesgos de seguridad o ayudan en la gestión de solicitudes de asilo y visados se clasifican como de alto riesgo. Finalmente, en la administración de justicia y procesos democráticos, los sistemas de Inteligencia Artificial que asisten a autoridades judiciales o que influyen en elecciones también están incluidos. Estos sistemas requieren un alto nivel de supervisión y regulación debido a su potencial impacto significativo en derechos fundamentales, seguridad y procesos democráticos.

24 Por ejemplo, la transparencia y la explicabilidad son aspectos cruciales para asegurar que los sistemas de Inteligencia Artificial puedan ser comprendidos y supervisados por seres humanos. Ello implica que los operadores de estos sistemas deben ser capaces de explicar cómo funcionan y cómo se toman las decisiones automatizadas, de manera que los usuarios y las personas afectadas puedan comprender el proceso y, en caso necesario, cuestionarlo.

25 Precisamente, se puede hablar, en estos casos, de sistemas de alto riesgo o, al menos, de sistemas que pueden llegar a alcanzarlo.

26 Los operadores de sistemas de Inteligencia Artificial, por tanto, tienen la obligación de proporcionar información clara y accesible que permita a los usuarios ejercer sus derechos de manera efectiva.

27 En este sentido, debe volverse al Considerando 27 del Reglamento de Inteligencia Artificial.

28 Ello ha de ponerse en relación con la supervisión humana en el sentido reseñado por el Considerando 27 del Reglamento de Inteligencia Artificial: "De acuerdo con las directrices del Grupo independiente de expertos de alto nivel sobre IA, por «acción y supervisión humanas» se entiende que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por seres humanos".

29 Ello es particularmente importante en áreas sensibles como la administración de justicia, donde la falta de control humano podría llevar a decisiones automatizadas que afecten negativamente a los derechos fundamentales.

30 El Considerando 75 del Reglamento de Inteligencia Artificial ha de tenerse en consideración en lo que concierne a los aspectos de seguridad.

Ello requiere que los desarrolladores y operadores implementen medidas de seguridad avanzadas que protejan tanto el sistema como los datos que maneja.

La gestión de la privacidad y de los datos es otro pilar fundamental en el desarrollo de la Inteligencia Artificial[31]. Los sistemas de Inteligencia Artificial deben manejar los datos de los usuarios con el mayor respeto por la privacidad y la protección de datos, cumpliendo con las normas vigentes como el Reglamento General de Protección de Datos de la Unión Europea[32].

Debe tenerse presente que la transparencia en los sistemas de Inteligencia Artificial va más allá de la simple explicabilidad de su uso[33]. Implica también que los operadores sean claros acerca de las capacidades y limitaciones del sistema, y que los usuarios comprendan las posibles implicaciones de interactuar con una Inteligencia Artificial. Es por ello, la transparencia es clave para la confianza del público en estas tecnologías y es fundamental para asegurar que los sistemas de Inteligencia Artificial se utilicen de manera responsable[34].

La diversidad, no discriminación y equidad son principios que deben guiar todo el ciclo de vida de los sistemas de Inteligencia Artificial, desde su concepción hasta su implementación[35]. Es crucial que estos sistemas sean diseñados para promover la inclusión y evitar la perpetuación de sesgos que puedan resultar en discriminación. Los desarrolladores de Inteligencia Artificial tienen la responsabilidad de asegurarse de que sus sistemas no reproduzcan ni amplifiquen las desigualdades existentes, sino que contribuyan a una sociedad más justa y equitativa.

El bienestar social y ambiental debe ser un objetivo central en el desarrollo de la Inteligencia Artificial[36]. Ello significa que los sistemas de Inteligencia Artificial deben ser diseñados no solo para ser eficientes y efectivos, sino también para tener un impacto positivo en la sociedad y el medio ambiente[37].

Por último, la rendición de cuentas es un principio que debe estar presente en todas las fases del desarrollo y uso de los sistemas de Inteligencia Artificial. Los desarrolladores, operadores y usuarios de Inteligencia Artificial deben ser responsables de las decisiones y acciones que tomen en relación con estas tecnologías (Tamarit, 2024). Ello incluye la obligación de corregir cualquier daño causado por el uso de la Inteligencia Artificial y de tomar medidas para evitar que dichos daños se repitan en el futuro[38].

El Reglamento de Inteligencia Artificial de la Unión Europea es una respuesta directa a las crecientes preocupaciones sobre el impacto de la Inteligencia Artificial en la sociedad. En un contexto donde la Inteligencia Artificial está cada vez más presente en diversas áreas de la vida cotidiana, desde la medicina hasta el transporte y la educación, la Unión Europea ha decidido tomar una postura proactiva en su regulación. El objetivo no es solo proteger a los ciudadanos de posibles abusos y riesgos, sino también fomentar un entorno en el que la Inteligencia Artificial pueda desarrollarse de manera ética y responsable (Martín Ramallal, P., Micaletto Belda, J. P., & Polo Serrano, 2023). Este enfoque se alinea con las políticas de la Unión Europea en otras áreas tecnológicas, donde la seguridad y los derechos fundamentales son prioridades innegociables.

La estructura del Reglamento se basa en una clasificación de riesgos que permite adaptar las obligaciones y requisitos a la naturaleza y el impacto potencial de cada sistema de Inteligencia

31 El Considerando 10 del Reglamento de Inteligencia Artificial es muy preciso al respecto.

32 Ello implica no solo garantizar que los datos sean tratados de manera segura, sino también que se utilicen únicamente para los fines para los que fueron recolectados, y que los usuarios tengan control sobre su información personal.

33 Más bien, habría que incluir al elemento de la explicabilidad el factor de la trazabilidad del algoritmo y la posibilidad de poder entender los sesgos que puedan incidir.

34 La transparencia en los sistemas de Inteligencia Artificial es un concepto que va más allá de la mera explicación técnica de su funcionamiento. No solo se trata de aclarar cómo operan estos sistemas, sino también de proporcionar a los operadores y usuarios una comprensión integral de sus capacidades y limitaciones. La transparencia requiere que los desarrolladores y proveedores de Inteligencia Artificial sean claros y específicos sobre lo que sus sistemas pueden y no pueden hacer, y sobre los contextos en los que estos sistemas podrían no funcionar como se espera. Además, implica que los usuarios estén informados sobre las posibles implicaciones y efectos de interactuar con tecnologías de Inteligencia Artificial. Esta apertura y claridad son esenciales para fomentar la confianza pública en estas tecnologías y para garantizar que se empleen de manera ética y responsable. En última instancia, la transparencia contribuye a que los sistemas de Inteligencia Artificial sean utilizados de manera que respete los principios de responsabilidad y equidad, ayudando a mitigar riesgos y a promover una integración segura y beneficiosa en la sociedad.

35 Claramente, se debe diferenciar la programación propiamente dicha de la aplicación efectiva de los algoritmos.

36 En este sentido, se puede llegar a hablar de la función social de la Inteligencia Artificial.

37 Es necesario evaluar y mitigar los posibles efectos a largo plazo de la Inteligencia Artificial en la sociedad, incluyendo su impacto en el empleo, la privacidad, la seguridad y el medio ambiente. La sostenibilidad debe estar en el centro de cualquier estrategia de desarrollo de Inteligencia Artificial, asegurando que estas tecnologías beneficien a todos los seres humanos y no solo a unos pocos.

38 Por ende, la regulación de la Inteligencia Artificial debe ser integral y basada en un enfoque de riesgo que garantice la protección de los derechos fundamentales mientras se fomenta la innovación. Resulta esencial que los sistemas de Inteligencia Artificial se desarrollen y utilicen dentro de un marco ético que respete la dignidad humana, promueva la justicia social y ambiental, y asegure la transparencia y la rendición de cuentas. Solo así se puede garantizar que la Inteligencia Artificial se convierta en una herramienta al servicio del bienestar humano y no en una fuente de nuevos riesgos y desigualdades.

Artificial. Este enfoque diferenciado es crucial, ya que no todos los sistemas de Inteligencia Artificial presentan el mismo nivel de riesgo[39].

3. Prohibiciones y regulaciones de alto riesgo

El Reglamento de Inteligencia Artificial prohíbe explícitamente ciertas prácticas que se consideran inaceptables debido a los riesgos significativos que plantean para los derechos individuales[40]. Estas prácticas incluyen el uso de técnicas subliminales y manipulativas que pueden distorsionar el comportamiento humano y afectar la toma de decisiones informada, la explotación de vulnerabilidades inherentes a ciertas condiciones personales como la edad o la discapacidad, y el uso de sistemas de categorización biométrica que infieren atributos sensibles sin el debido consentimiento y propósito legal[41].

Aunado a ello, se prohíben los sistemas de puntuación social que clasifiquen a las personas basándose en su comportamiento social o características personales, así como la evaluación de riesgos de conducta delictiva basada únicamente en perfiles y rasgos de personalidad[42]. La compilación de bases de datos de reconocimiento facial a partir de imágenes recogidas de manera indiscriminada también está vetada, así como la inferencia de emociones en contextos laborales o educativos, y el uso de identificación biométrica remota en tiempo real en espacios públicos, salvo excepciones estrictamente reguladas.

Estas prohibiciones reflejan una preocupación profunda por las implicaciones éticas y sociales de la Inteligencia Artificial. El uso de técnicas manipulativas y subliminales es especialmente problemático porque puede socavar la autonomía y la capacidad de decisión de los individuos[43].

El veto a los sistemas de puntuación social y la evaluación de riesgos basados en perfiles responde a preocupaciones similares. La idea de que una persona pueda ser juzgada y clasificada en función de su comportamiento social o características personales plantea serias cuestiones de equidad y justicia. En una sociedad democrática, la igualdad de oportunidades y el respeto por la privacidad son principios fundamentales que no deben ser comprometidos por el uso de la tecnología. De manera similar, la compilación indiscriminada de datos biométricos y la inferencia de emociones en ciertos contextos pueden llevar a abusos significativos y deben ser estrictamente reguladas.

4. Obligaciones para sistemas de alto riesgo

Los sistemas de Inteligencia Artificial categorizados como de alto riesgo, debido a su potencial para afectar significativamente la salud, la seguridad o los derechos fundamentales de las personas, están sujetos a una serie de obligaciones estrictas. Estos sistemas incluyen aquellos que son componentes de seguridad de productos sujetos a otras normas de la Unión Europea y aplicaciones específicas como la evaluación de elegibilidad para educación, empleo, asistencia pública y servicios financieros (Olcoz Basarte, 2024).

Las obligaciones para estos sistemas de alto riesgo incluyen la implementación de un sistema de gestión de riesgos que evalúe continuamente los riesgos y estrategias de mitigación a lo largo de todo el ciclo de vida del sistema. Además, se requiere una gobernanza exhaustiva de datos, incluyendo pruebas y evaluaciones para detectar y mitigar sesgos. La documentación técnica detallada debe estar preparada antes de que el sistema se comercialice, y se exige una monitorización continuo post- implementación.

El artículo 16 del Reglamento de Inteligencia Artificial establece una serie de obligaciones específicas para los proveedores de sistemas algorítmicos clasificados como de alto riesgo. Estas obligaciones están diseñadas para asegurar que estos sistemas cumplan con los requisitos técnicos y de calidad necesarios para su correcto funcionamiento y su conformidad con la normativa vigente.

En primer lugar, los proveedores deben garantizar que sus sistemas de Inteligencia Artificial de alto riesgo cumplan con los requisitos definidos en la sección correspondiente del reglamento. Además,

39 Por ejemplo, una aplicación de Inteligencia Artificial en la atención médica puede tener implicaciones mucho más serias que una aplicación en entretenimiento. Al distinguir entre diferentes niveles de riesgo, la Unión Europea pretende asegurar que los recursos regulatorios se enfoquen en los aspectos más críticos, sin sofocar la innovación en áreas de menor riesgo.

40 Véase el artículo 5 del Reglamento de Inteligencia Artificial, analizado anteriormente.

41 En este sentido, tienen una gran relevancia los patrones oscuros, que inducen a las personas a comportamientos concretos a partir del aprovechamiento de condicionamientos habituales. El Considerando 29 del Reglamento de Inteligencia Artificial llega a pronunciarse en conexión con este tema. (Ponce Solé, 2023). Igualmente, es de interés lo manifestado en Martínez Rolán, L. X. (2020). "Diseños oscuros en el desarrollo web. Cuando el usuario no es tan libre de elegir una navegación". En D. Caldevilla Domínguez (Coord.), *Unidos por la comunicación: Libro de Actas del Congreso Internacional Latina de Comunicación Social 2020*, pp. 200-215, p. 204. (¿Esta cita es válida? No hay contenido citado aparentemente)

42 En este sentido, se busca evitar que se vulnere el principio de culpabilidad y de responsabilidad penal por el hecho a partir de perfiles programados que, lamentablemente, pueden sufrir una fuerte incidencia por los sesgos algorítimicos.

43 Precisamente, en un contexto donde las decisiones se basan cada vez más en datos y algoritmos, es esencial garantizar que estas decisiones se tomen de manera informada y libre de coerción. La explotación de vulnerabilidades personales también es una cuestión crítica, ya que puede llevar a situaciones de abuso y discriminación, especialmente en poblaciones vulnerables.

deben proporcionar información clara sobre su identidad y datos de contacto en el propio sistema, en el embalaje o en la documentación asociada, según sea posible. La documentación debe incluir el nombre comercial o marca registrada y la dirección de contacto del proveedor.

Es fundamental que los proveedores cuenten con un sistema de gestión de la calidad que esté alineado con los requisitos establecidos en el artículo 17 del reglamento. Este sistema debe registrar las políticas, procedimientos e instrucciones necesarias para asegurar que los sistemas de Inteligencia Artificial de alto riesgo cumplan con los estándares de calidad requeridos. Entre otros aspectos, el sistema de gestión debe incluir una estrategia para cumplir con la normativa, técnicas y procedimientos para el diseño, desarrollo y control de calidad, y procedimientos para la evaluación y validación del sistema en diferentes etapas.

Los proveedores también están obligados a conservar la documentación técnica y de calidad durante un período de diez años desde la introducción en el mercado o la puesta en servicio del sistema. Esta documentación debe estar disponible para las autoridades nacionales competentes y debe incluir los documentos técnicos, las decisiones de los organismos notificados, y la declaración UE de conformidad.

En relación con los archivos de registro generados automáticamente por los sistemas de Inteligencia Artificial de alto riesgo, los proveedores deben conservar estos archivos por un período adecuado, que no debe ser menor a seis meses, a menos que la legislación aplicable disponga lo contrario. Los proveedores que sean entidades financieras deben mantener estos archivos de acuerdo con los requisitos específicos de la normativa en materia de servicios financieros.

En caso de que un sistema de Inteligencia Artificial de alto riesgo no cumpla con la normativa, el proveedor debe adoptar medidas correctivas inmediatas, que pueden incluir la retirada del mercado, desactivación o recuperación del sistema. También deben informar a los distribuidores y otras partes relevantes sobre cualquier medida correctiva adoptada.

Los proveedores tienen la obligación de cooperar con las autoridades competentes proporcionando toda la información y documentación necesarias para demostrar la conformidad del sistema de Inteligencia Artificial con los requisitos del reglamento. Esta información debe estar disponible en una lengua que las autoridades puedan entender y, cuando se solicite, los proveedores deben permitir el acceso a los archivos de registro generados automáticamente por el sistema.

Estas obligaciones reflejan un enfoque meticuloso y riguroso para garantizar que los sistemas de alto riesgo sean seguros y fiables. La gestión continua de riesgos es esencial porque los riesgos asociados con la Inteligencia Artificial pueden evolucionar con el tiempo[44]. Un sistema que es seguro hoy puede no serlo mañana, especialmente a medida que cambian las condiciones de su uso o se descubren nuevas vulnerabilidades[45].

La gobernanza de datos también es un componente clave, ya que los datos son el núcleo de cualquier sistema de Inteligencia Artificial. La calidad, integridad y equidad de los datos utilizados para entrenar y operar estos sistemas pueden tener un impacto directo en su desempeño y en los resultados que producen. Las pruebas y evaluaciones regulares para detectar y mitigar sesgos son esenciales para garantizar que los sistemas sean justos y no discriminen a ningún grupo de personas. Además, la preparación de documentación técnica detallada y el monitoreo post-implementación aseguran que haya transparencia y responsabilidad en todo el ciclo de vida del sistema.

5. Requisitos para los modelos de inteligencia artificial de propósito general (iaug)

Los proveedores de modelos IAUG, como OpenAI, enfrentan requisitos adicionales debido a la versatilidad y el amplio uso potencial de estos sistemas. Se requiere desarrollar y proporcionar documentación técnica detallada del modelo a la Oficina de Inteligencia Artificial de la Unión Europea bajo demanda. También deben crear documentación específica para los responsables de despliegue que utilicen el modelo IAUG para desarrollar sus propios sistemas de Inteligencia Artificial. Asimismo, deben implementar políticas para asegurar el cumplimiento de la ley de derechos de autor de la Unión Europea y proporcionar un resumen del contenido utilizado para entrenar los modelos IAUG.

Para los modelos IAUG con capacidades de alto impacto, considerados por presentar "riesgos sistémicos", se deben realizar evaluaciones exhaustivas para identificar y mitigar estos riesgos. Además, es obligatorio notificar a la Comisión de la Unión Europea sobre los modelos que cumplan con los criterios de alto riesgo, monitorear y reportar incidentes graves, e implementar medidas de ciberseguridad adecuadas para proteger tanto el modelo como su infraestructura física.

44 Es lógico que ello pueda suceder, pues el avance de los sistemas algorítmicos se está produciendo a un ritmo vertiginoso.

45 Por lo tanto, la capacidad de evaluar y mitigar riesgos de manera continua es fundamental para mantener la seguridad y la confianza en estos sistemas.

Estos requisitos reflejan la preocupación por el potencial impacto amplio y profundo de los modelos IAUG. Dada su naturaleza general y su capacidad para ser adaptados a una variedad de aplicaciones, los modelos IAUG pueden tener efectos sistémicos que van más allá de los usos individuales. Por lo tanto, es crucial que los proveedores de estos modelos tomen medidas proactivas para gestionar y mitigar los riesgos asociados[46].

Las políticas de cumplimiento de derechos de autor también son importantes, ya que los modelos IAUG a menudo se entrenan con grandes cantidades de datos que pueden incluir contenido protegido por derechos de autor. Asegurar el cumplimiento de la ley de derechos de autor es fundamental para proteger los intereses de los creadores de contenido y evitar posibles conflictos jurídicos. Las evaluaciones de riesgos sistémicos y las notificaciones a la Comisión de la Unión Europea ayudan a garantizar que los riesgos se gestionen de manera adecuada y que las autoridades reguladoras estén al tanto de los desarrollos importantes. Finalmente, las medidas de ciberseguridad son cruciales para proteger la integridad y seguridad de los modelos IAUG y su infraestructura.

6. Implicaciones para proveedores y responsables de despliegue

El Reglamento de Inteligencia Artificial distingue claramente entre proveedores y responsables de despliegue de sistemas de Inteligencia Artificial. Los proveedores, como OpenAI, son entidades que desarrollan o ponen en el mercado sistemas de Inteligencia Artificial o modelos IAUG bajo su propio nombre o marca. Los responsables de despliegue son aquellas entidades que utilizan estos sistemas o modelos en sus propias aplicaciones. Sin embargo, un responsable de despliegue puede convertirse en proveedor si integra un modelo de Inteligencia Artificial en su propio sistema de Inteligencia Artificial, utiliza su propia marca o modifica el sistema de maneras no previstas por el proveedor original[47].

La distinción refleja la complejidad y la diversidad del ecosistema de Inteligencia Artificial. Los proveedores de Inteligencia Artificial son responsables de desarrollar y poner en el mercado sistemas que cumplan con los requisitos regulatorios y sean seguros y efectivos. Sin embargo, los responsables de despliegue también tienen un papel crucial, ya que son ellos quienes finalmente utilizan estos sistemas en aplicaciones prácticas. Al modificar o reconfigurar sistemas de Inteligencia Artificial, los responsables de despliegue pueden introducir nuevos riesgos y desafíos que deben ser gestionados de manera adecuada.

Las obligaciones de los proveedores incluyen el desarrollo de sistemas que cumplan con los estándares regulatorios y la implementación de medidas de seguridad y gestión de riesgos. Ello incluye la preparación de documentación técnica detallada y la realización de pruebas y evaluaciones para asegurar que los sistemas sean seguros y efectivos. Por otro lado, los responsables de despliegue deben asegurarse de que utilizan estos sistemas de manera responsable y conforme a las regulaciones aplicables. Ello incluye la implementación de políticas y procedimientos para gestionar los riesgos asociados y asegurar que cualquier modificación se realice de manera segura y conforme a los requisitos regulatorios.

7. Aplicación extraterritorial del reglamento de Inteligencia Artificial

El Reglamento de Inteligencia Artificial tiene una aplicación extraterritorial amplia, lo que significa que organizaciones fuera de la Unión Europea también deberán cumplir con sus disposiciones si operan en el mercado europeo o si sus sistemas de Inteligencia Artificial afectan a ciudadanos europeos[48]. Además, si el resultado producido por un sistema de Inteligencia Artificial es utilizado dentro de la Unión Europea, independientemente de la ubicación del proveedor o responsable de despliegue, también se deberá cumplir con el instrumento.

El Considerando 22 del Reglamento de Inteligencia Artificial aborda un aspecto crucial relacionado con la aplicación del reglamento en contextos internacionales. Según este considerando, el alcance del reglamento se extiende más allá de los sistemas de IA que se introducen, se ponen en servicio o se utilizan directamente dentro de la Unión Europea.

En particular, señala que ciertos sistemas de IA deben cumplir con las disposiciones del reglamento incluso si no están físicamente presentes en el mercado de la Unión. Ello se da, por ejemplo, cuando un operador de la Unión Europea celebra un contrato con un proveedor ubicado en un tercer país para la prestación de servicios asociados a un

46 La documentación técnica detallada y la transparencia en el contenido utilizado para entrenar estos modelos son esenciales para garantizar que los usuarios comprendan sus capacidades y limitaciones.

47 Esta diferenciación es crucial, ya que la mayoría de las obligaciones bajo el Reglamento recaen sobre los proveedores. No obstante, los responsables de despliegue también deben cumplir con ciertas obligaciones, especialmente si modifican o reconfiguran los sistemas de Inteligencia Artificial.

48 Por ejemplo, si un proveedor pone un sistema de Inteligencia Artificial o un modelo IAUG en el mercado de la Unión Europea, o si los responsables de despliegue de estos sistemas tienen su sede en la Unión Europea o están ubicados en la Unión Europea, estarán sujetos a la norma.

sistema de IA considerado de alto riesgo. En estos casos, aunque el sistema de IA no esté disponible en el mercado europeo, puede procesar datos que han sido recopilados legalmente en la Unión y transferidos a través de fronteras. El sistema en el tercer país podría generar resultados que luego se envían a la Unión, lo que implica que los efectos del sistema de IA afectan a la Unión, y por ende, el reglamento debe aplicarse para garantizar que no se eluda su cumplimiento.

El reglamento busca prevenir la elusión y asegurar la protección efectiva de las personas en la Unión Europea. Para ello, se extiende la aplicación del reglamento a los proveedores y responsables del despliegue de sistemas de IA establecidos en terceros países, siempre que los resultados generados por estos sistemas sean utilizados en la Unión. Este enfoque asegura que las normativas de la Unión no sean eludidas a través de la externalización o la localización de actividades en jurisdicciones externas. Sin embargo, hay excepciones contempladas para las autoridades públicas de terceros países y organizaciones internacionales que operan bajo acuerdos internacionales de cooperación con la Unión Europea.

Estos acuerdos deben ofrecer garantías adecuadas para la protección de los derechos y libertades fundamentales. Esta excepción se aplica principalmente a actividades relacionadas con la cooperación policial y judicial, donde los acuerdos internacionales permiten una mayor flexibilidad en cuanto a la aplicación del reglamento, siempre que se mantenga un nivel adecuado de protección de datos.

Para asegurar el cumplimiento del reglamento, los acuerdos internacionales deben ser revisados periódicamente y ajustados si es necesario para alinearse con los requisitos del reglamento de la Unión. Las autoridades nacionales y las instituciones de la Unión que reciben y utilizan los resultados generados por sistemas de IA de terceros países deben garantizar que su uso cumpla con la normativa europea. Este enfoque no solo refuerza la protección de los derechos y libertades fundamentales dentro de la Unión, sino que también establece un marco claro para la cooperación internacional en la gestión de riesgos asociados con la IA.

Esta aplicación extraterritorial refleja la intención de la Unión Europea de proteger a sus ciudadanos y su mercado interno de los riesgos asociados con la Inteligencia Artificial, independientemente de dónde se desarrollen o desplieguen estos sistemas[49]. Por lo tanto, es esencial que estas entidades cumplan con las regulaciones de la Unión Europea para asegurar que los sistemas de Inteligencia Artificial sean seguros y fiables.

La aplicación extraterritorial también plantea desafíos para las empresas que operan a nivel global. Estas empresas deben asegurarse de que sus sistemas de Inteligencia Artificial cumplan con las regulaciones de la Unión Europea, incluso si no están ubicadas en Europa. Ello puede implicar la implementación de políticas y procedimientos adicionales para asegurar el cumplimiento y la colaboración con las autoridades reguladoras de la Unión Europea[50]. En última instancia, la aplicación extraterritorial del Reglamento de Inteligencia Artificial refleja el compromiso de la Unión Europea con la protección de sus ciudadanos y su mercado interno, y la necesidad de una gobernanza global de la Inteligencia Artificial que aborde los riesgos y desafíos asociados.

8. Reflexiones finales sobre los desafíos y la preparación para el cumplimiento

Para aquellas organizaciones que buscan cumplir con el Reglamento de Inteligencia Artificial de la Unión Europea, el primer y más crucial paso consiste en realizar un análisis exhaustivo de todos los sistemas de Inteligencia Artificial que actualmente están en uso dentro de la entidad. Este análisis implica un proceso detallado de clasificación de cada uno de estos sistemas, evaluando su nivel de riesgo en base a las categorías definidas por la norma europea. Es importante destacar que este proceso de clasificación no es meramente un ejercicio administrativo, sino un paso esencial para asegurar que la organización opere dentro del marco regulatorio establecido. Este marco ha sido diseñado específicamente para garantizar que la implementación de la Inteligencia Artificial se

49 Precisamente, en un mundo cada vez más interconectado, los sistemas de Inteligencia Artificial desarrollados fuera de la Unión Europea pueden tener un impacto significativo en el mercado europeo y en la vida de los ciudadanos europeos.

50 La aplicación extraterritorial de las normativas de la Unión Europea presenta desafíos significativos para las empresas que operan globalmente. A pesar de no estar físicamente ubicadas en Europa, estas empresas deben garantizar que sus sistemas de Inteligencia Artificial cumplan con las regulaciones europeas, como el Reglamento General de Protección de Datos y el Reglamento de Inteligencia Artificial. Este cumplimiento puede requerir la implementación de políticas y procedimientos específicos para adherirse a los estándares europeos, que a menudo incluyen medidas rigurosas de protección de datos, transparencia en el uso de la Inteligencia Artificial y mecanismos de supervisión. Las empresas deberán establecer procesos para monitorear y ajustar sus prácticas en conformidad con las normativas, así como colaborar estrechamente con las autoridades reguladoras de la Unión Europea. Esta colaboración puede incluir la designación de representantes dentro de la Unión Europea para facilitar la comunicación y resolver cualquier problema regulatorio que surja. La necesidad de cumplir con estas regulaciones extraterritoriales no solo incrementa la complejidad operativa y los costos de cumplimiento para las empresas globales, sino que también destaca la importancia de tener un enfoque proactivo en la gestión de la conformidad internacional.

realice de manera segura y ética, minimizando los riesgos potenciales asociados con su uso.

Una parte fundamental de este proceso es la identificación precisa del rol que la organización juega en relación con estos sistemas de Inteligencia Artificial. Las organizaciones deben determinar si son proveedores de tecnología o si están directamente involucradas en el despliegue de los sistemas. Esta distinción es crítica, ya que cada rol conlleva obligaciones legales específicas que deben ser comprendidas y cumplidas rigurosamente. Los proveedores de tecnología, por ejemplo, tienen la responsabilidad de asegurarse de que los sistemas que desarrollan y suministran cumplen con los estándares de seguridad y ética estipulados por la norma. Por otro lado, los responsables del despliegue deben garantizar que estos sistemas se utilicen de manera correcta y segura en la práctica, conforme a las directrices establecidas.

Dado que estos temas pueden ser complejos y que la norma es extensa y detallada, es altamente recomendable que las organizaciones consulten con asesores legales que tengan experiencia en tecnología y en la regulación de la Inteligencia Artificial. Estos expertos pueden proporcionar la orientación necesaria para interpretar correctamente las obligaciones legales y para implementar las medidas necesarias que aseguren el cumplimiento de la norma. Ello no solo ayudará a las organizaciones a evitar posibles sanciones, sino que también contribuirá a construir un marco de confianza y transparencia en el uso de la Inteligencia Artificial, lo que es fundamental para su adopción exitosa en la sociedad.

Del análisis de lo anterior, se puede inferir que el Reglamento de Inteligencia Artificial de la Unión Europea no es simplemente una norma más entre tantas otras, sino un marco regulatorio robusto y extremadamente detallado que ha sido diseñado con el objetivo específico de mitigar los riesgos inherentes al uso de la Inteligencia Artificial. Este reglamento no solo busca limitar los posibles daños o riesgos, sino que también pretende fomentar un entorno en el que la Inteligencia Artificial pueda desarrollarse de manera segura, ética y sostenible, permitiendo que su adopción se realice con plena confianza por parte de todas las industrias y sectores de la sociedad.

Las obligaciones impuestas tanto a los proveedores de tecnología como a los responsables del despliegue de sistemas de Inteligencia Artificial son significativas, especialmente en aquellos casos donde los sistemas son clasificados como de alto riesgo. Estos sistemas, por su naturaleza, requieren una atención y preparación adicional por parte de las organizaciones, que deben adaptarse cuidadosamente para cumplir con los estándares y requisitos establecidos por la norma. La preparación y la adaptación no solo implican cambios técnicos en los sistemas, sino también una transformación en las prácticas empresariales y en la cultura organizacional, que debe alinearse con los principios éticos y de seguridad promovidos por la norma.

Además, la colaboración con las autoridades reguladoras será un elemento esencial en todo este proceso. No se trata únicamente de cumplir con las normas de manera pasiva, sino de participar activamente en un diálogo continuo con las autoridades para asegurar que los sistemas de Inteligencia Artificial no solo cumplan con los requisitos legales, sino que también se utilicen de manera que aporten beneficios tangibles y reales a la sociedad en general. Este cumplimiento estricto de las normas será clave para asegurar que la Inteligencia Artificial se utilice de manera segura y responsable, contribuyendo al bienestar general de la sociedad y respetando los valores fundamentales que guían la convivencia en el marco de la Unión Europea.

Al reflexionar sobre el futuro que nos depara la Inteligencia Artificial, es evidente que esta tecnología tiene el potencial de transformar radicalmente diversos aspectos de nuestra vida diaria, desde la forma en que trabajamos hasta cómo interactuamos socialmente y cómo se toman decisiones a gran escala. La Inteligencia Artificial promete mejoras significativas en eficiencia y productividad, abriendo nuevas oportunidades en campos como la medicina, la educación, el transporte, y muchos otros. Sin embargo, junto con estas promesas, también surgen desafíos éticos y sociales importantes que debemos enfrentar. El riesgo de sesgos en los algoritmos, la posibilidad de una mayor vigilancia, y la potencial pérdida de empleos son solo algunas de las preocupaciones que acompañan a este avance tecnológico.

Por lo tanto, es esencial que el desarrollo y la implementación de la Inteligencia Artificial se realicen con una perspectiva ética y responsable. La norma de la Unión Europea en este sentido es un paso importante hacia la creación de un entorno en el que la Inteligencia Artificial pueda prosperar, pero siempre dentro de un marco que proteja los derechos fundamentales y asegure que los beneficios de esta tecnología se distribuyan de manera equitativa en toda la sociedad. El futuro de la Inteligencia Artificial dependerá en gran medida de nuestra capacidad para equilibrar el entusiasmo por la innovación con la prudencia necesaria para gestionar los riesgos asociados. Con un enfoque adecuado, la Inteligencia Artificial no solo podrá mejorar nuestras vidas, sino también contribuir a la construcción de una sociedad más justa, inclusiva y sostenible.

LISTA DE REFERENCIAS

Álvarez Cantalapiedra, S. (2023). "Luces, sombras y riesgos de la inteligencia artificial".

Papeles de relaciones ecosociales y cambio global, Nº. 164, pp. 5-12.

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías (2019). *Directrices* éticas *para una IA fiable*. Oficina de Publicaciones, 2019. Recuperado de https://data.europa.eu/doi/10.2759/14078.

Espinosa Proa, S. (2024). "Del hechizo de la Tecnociencia: Inteligencia artificial y finitud". En

A. González Padilla (Coord.), *Inteligencia Artificial, Ética y Tecnofilosofía: Ensayos sobre sesgos algorítmicos, crisis ecosocial, transhumanismo y otros disruptivos*, pp. 227- 248.

González Alvarado, N. (2024). "El papel de la ética en el campo de la inteligencia artificial". En

A. González Padilla (Coord.), *Inteligencia Artificial, Ética y Tecnofilosofía: Ensayos sobre sesgos algorítmicos, crisis ecosocial, transhumanismo y otros disruptivos*, pp. 113- 122.

Jiménez, J. S. (2024). "Desafíos éticos y legales de la inteligencia artificial en la sociedad actual". En A. González Padilla (Coord.), *Inteligencia Artificial, Ética y Tecnofilosofía: Ensayos sobre sesgos algorítmicos, crisis ecosocial, transhumanismo y otros disruptivos*, pp. 123-134.

Lizarazu Gutiérrez, C. V. (2024). "La preeminencia de la creatividad humana: La regla de la no conmutatividad colaborativa entre Inteligencia Humana + IA". En A. González Padilla (Coord.), *Inteligencia Artificial,* Ética *y Tecnofilosofía: Ensayos sobre sesgos algorítmicos, crisis ecosocial, transhumanismo y otros disruptivos*, pp. 145-160.

López de Mántaras, R. (2018). "Hacia la inteligencia artificial: progresos, retos y riesgos".

Mètode: Revista de difusión de la Investigación, Nº. 99, pp. 44-51.

López Martínez, R. (2022). "Riesgos de la aplicación de la inteligencia artificial en la administración de justicia". En S. Calaza López & M. Llorente Sánchez-Arjona (Dirs.), *Inteligencia artificial legal y administración de justicia*, pp. 555-565.

Martín Ramallal, P., Micaletto Belda, J. P., & Polo Serrano, D. (2023). "Inteligencia artificial en los metaversos. Riesgos y oportunidades desde una perspectiva ética». En V. Guarinos

Galán & M. Blanco Pérez (Coords.), *Universos distópicos y manipulación en la comunicación contemporánea: del periodismo a las series pasando por la política*, pp. 536-553.

Martínez Rodríguez, O. M. (2023). "Inteligencia artificial: riesgos y desafíos de su regulación".

Actualidad administrativa, Nº 12, pp. 37-45.

Martínez Rolán, L. X. (2020). "Diseños oscuros en el desarrollo web. Cuando el usuario no es tan libre de elegir una navegación". En D. Caldevilla Domínguez (Coord.), *Unidos por la comunicación: Libro de Actas del Congreso Internacional Latina de Comunicación Social 2020*, pp. 200-215.

Olcoz Basarte, I. (2024). "Infinito introspectivo: Reflexiones sobre la inteligencia artificial general y los límites de la computación a través de intuiciones sobre los infinitos". En A. González Padilla (Coord.), *Inteligencia Artificial, Ética y Tecnofilosofía: Ensayos sobre sesgos algorítmicos, crisis ecosocial, transhumanismo y otros disruptivos*, pp. 71-84.

Ponce Solé, J. (2023). "Derecho, nudging digital y manipulación: patrones oscuros, inteligencia artificial y derecho a una buena administración". *Anuario de la Red Eurolatinoamericana de Buen Gobierno y Buena Administración*, Nº. 3, pp. 45-59.

Salazar García, I. (2023). "Inteligencia artificial, retos, riesgos y oportunidades". En T. Vázquez-Barrio & I. Salazar García (Coords.), *Inteligencia artificial, periodismo y democracia*, pp. 45-72.

Tamarit, F. (2024). "Ventajas y riesgos del uso de la inteligencia artificial". *Revista Methodo: Investigación Aplicada a las Ciencias Biológicas*, Vol. 9, Nº. 2, pp. 1-3.

Tourpe, H. (2023). "Promesas y riesgos de la inteligencia artificial: la inteligencia artificial generativa promete desatar una ola de creatividad y productividad, pero con importantes interrogantes para la humanidad". *Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y del Banco Mundial*, Vol. 60, Nº. 4, pp. 76-89.