Universidad de Valladolid

Facultad de **Derecho**

Grado en **Derecho y Administración y Dirección de Empresas**

Título del Trabajo Fin de Grado:

REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL.

Presentado por:

Lucas Nanclares Martínez

Tutelado por:

Antonio Calonge Velázquez

Valladolid, 15 de mayo de 2025

Tabla de contenido

RESUMEN

La inteligencia artificial (IA) es una tecnología emergente que ha transformado profundamente diversos sectores, tanto públicos como privados, generando expectativas extraordinarias de desarrollo económico y social. Sin embargo, su rápida evolución y adopción plantean desafíos significativos, especialmente en términos de dilemas éticos y jurídicos. La Unión Europea (UE) ha adoptado un enfoque distintivo para abordar estos desafíos, centrado en la creación de un marco regulatorio armonizado que garantice la seguridad jurídica y esté fundamentado en los valores europeos, incluyendo la preservación de los derechos fundamentales.

El enfoque europeo busca equilibrar el impulso al desarrollo y la implementación de la IA con la necesidad de establecer controles y normas que prevengan abusos y mitiguen riesgos. Este enfoque ha sido formalizado a través de varias iniciativas y documentos clave, como el Libro Blanco sobre la IA y la Propuesta de Reglamento sobre normas armonizadas en IA, conocidos colectivamente como la "Ley de Inteligencia Artificial". Estos documentos no solo delinean las bases para un ecosistema de excelencia y confianza, sino que también reflejan el compromiso de la UE con un desarrollo de la IA que sea seguro, ético y respetuoso de los derechos humanos.

En el presente trabajo, se analizarán las características principales del enfoque europeo hacia la IA, así como la ambiciosa propuesta regulatoria aprobada el 14 de marzo de 2024. Este análisis permitirá comprender cómo la UE busca posicionarse como líder en la regulación de la IA, estableciendo estándares que podrían sentar las bases para el desarrollo de legislaciones similares a nivel global, pese a los desafíos competitivos que esto pueda implicar para el desarrollo europeo en comparación con otras regiones del mundo donde las regulaciones son bastante menos estrictas.

Abstract

Artificial intelligence (AI) is an emerging technology that has profoundly transformed various sectors, both public and private, generating extraordinary expectations for economic and social development. However, its rapid evolution and adoption pose significant challenges, especially in terms of ethical and legal dilemmas. The European Union (EU) has adopted a distinctive approach to address these challenges, focusing on the creation of a harmonised regulatory framework that ensures legal certainty and is grounded in European values, including the preservation of fundamental rights.

The European approach seeks to balance the drive for AI development and implementation with the need to establish controls and standards that prevent abuses and mitigate risks. This approach has been formalised through several key initiatives and documents, such as the White Paper on AI and the Proposal for a Regulation on harmonised rules on AI, collectively known as the 'Artificial Intelligence Act'. These documents not only outline the foundations for an ecosystem of excellence and trust, but also reflect the EU's commitment to AI development that is safe, ethical and respectful of human rights.

This paper will analyse the main features of the European approach to AI, as well as the ambitious regulatory proposal adopted on 14 March 2024. This analysis will provide insight into how the EU seeks to position itself as a leader in AI regulation, setting standards that could lay the groundwork for the development of similar legislation globally, despite the competitive challenges this may imply for European development compared to other regions of the world where regulations are considerably less stringent.

Keywords

Reglamento Europeo, Inteligencia Artificial, Protección de Datos, Regulación Tecnológica, Privacidad.

European Act, Artificial Intelligence, Data Protection, Technology Regulation, Privacy.

MARCO CONCEPTUAL

Definición Inteligencia Artificial

Debido a que nos encontramos ante una idea compleja en constante desarrollo y de alcance multifacético, los expertos en la materia no han llegado a un consenso a la hora de aportar una definición única y concreta que abarque todas las vertientes y enfoques que constituye el campo de la Inteligencia Artificial (en adelante IA).

Uno de los padres de la IA (y el responsable de acuñar y promover el término para definir ese nuevo concepto), el profesor de Stanford John McCarthy, lo definió como "la ciencia y la ingeniería de crear máquinas inteligentes"[1], durante la Conferencia de Dartmouth de 1956; es la réplica de la inteligencia humana en máquinas haciéndolas capaces de realizar acciones complejas e incluso predecir un resultado.

Para Marvin Minsky, otro gran contribuyente en el desarrollo de este nuevo campo, la IA se entendía también de una forma similar, como "la ciencia dedicada a lograr que las máquinas realizaran tareas que, si fueran hechas por humanos, requerirían inteligencia"[2]. Minsky veía el cerebro como una máquina cuyas funciones podían ser estudiadas y replicadas por un ordenador para conseguir resultados complejos.

En un contexto más reciente, la Comisión Europea se refirió a ella en 2018: "*La inteligencia artificial (IA) se refiere a sistemas que muestran un comportamiento inteligente al analizar su entorno y tomar acciones, con cierto grado de autonomía, para lograr objetivos específicos.*"[3] Esta definición destaca la capacidad de los sistemas de IA para operar de manera autónoma y realizar tareas específicas basadas en el análisis de datos de su entorno.

Mientras que otros, como el Instituto de Investigación Conjunta de la UE, enfatizan más en la capacidad de observación y aprendizaje y toma de

[1] Manning, C. (2020) *Artificial Intelligence Definitions.* Stanford University..P. 1

[2] Fajardo de Andara, C (2021) *Marvin Lee Minsky: pionero en la investigación de la inteligencia artificial.* Universidad Nacional Experimental Politécnica Antonio José de Sucre, Venezuela. P. 44

[3] Plan coordinado sobre la inteligencia artificial, Comunicación de la Comisión Europea COM (2018).

decisiones basadas en la experiencia previa adquirida, por lo que nos dan el siguiente significado:

"*La IA es un término genérico que se refiere a cualquier máquina o algoritmo capaz de observar su entorno, aprender y, basándose en el conocimiento y la experiencia adquiridos, tomar acciones inteligentes o proponer decisiones.*"[4]

La idea general que podemos extraer de las definiciones que existen tanto dentro del ámbito académico como del político es que la IA es una rama de la informática dedicada a la creación de sistemas capaces de realizar tareas que, si fueran realizadas por seres humanos, requerirían pensamientos complejos e inteligentes.

Estas tareas descritas pueden incluir el razonamiento, el aprendizaje, la percepción, la toma de decisiones y la interacción con el entorno.

Evolución de la Inteligencia Artificial

Los fundamentos teóricos que empiezan a sentar las bases en este nuevo campo de investigación se empiezan a desarrollar de una forma más directa a partir de los años cincuenta del siglo pasado, con el matemático Alan Turing como primer exponente principal. En su ensayo "*Computing Machinery and Intelligence*"[5] Turing explora las capacidades de las máquinas digitales, describiendo cómo podrían ser programadas para aprender y adaptarse y a la misma vez plantea respuestas a las objeciones que puedan ser planteadas desde distintos puntos de vista sobre la idea de que estas máquinas puedan pensar.

[4] Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C.(2018) *Artificial intelligence - a european perspective*. Luxemburg. P.18

[5] Turing, A. (1950) *Computing Machinery and Intelligence*. Oxford University Press

En 1956 se considera el nacimiento oficial de la IA como campo de estudio en la ya mencionada Conferencia de Dartmouth, en la cual se invitó a un pequeño grupo de investigadores de diversas disciplinas (incluyendo matemáticas, psicología, ingeniería y ciencias de la computación) con el objetivo de investigar cómo hacer que las máquinas usen el lenguaje, formen conceptos y resuelvan problemas similares a los humanos. Aunque no se lograron avances inmediatos revolucionarios durante la conferencia misma, las ideas y la visión compartida por los participantes sentaron las bases para décadas de investigación y desarrollo en IA.

Durante los años sesenta y principios de los setenta, hubo un gran optimismo sobre las capacidades y el progreso de la IA, los investigadores y defensores hicieron promesas esperanzadoras sobre el rápido avance hacia máquinas verdaderamente inteligentes. Sin embargo, las limitaciones tecnológicas de la época, especialmente en términos de poder de procesamiento y memoria, impidieron que estos avances se materializaran rápidamente.

El campo de la IA volvió a coger ritmo en la década de los noventa con avances en el aprendizaje automático y el procesamiento del lenguaje natural. La mejora en el poder de procesamiento de las computadoras y la disponibilidad de grandes cantidades de datos (*Big Data*) también contribuyeron a este renacimiento.

El principio del siglo XXI estuvo marcado por el crecimiento explosivo de Internet, que generó una cantidad sin precedentes de datos, impulsando aún más el desarrollo de algoritmos de aprendizaje automático. Este periodo también vio un aumento en el uso comercial de la IA, especialmente dentro del comercio electrónico y los sistemas de recomendación. Plataformas como Amazon y Netflix utilizaron algoritmos para personalizar la experiencia del usuario, destacando la necesidad de marcos legales adecuados para proteger los derechos de los consumidores y asegurar la equidad en los sistemas automatizados.

Con el perfeccionamiento de los "*smartphones*", comenzó el auge del aprendizaje profundo (*Deep Learning*), con innovaciones clave en algoritmos y modelos que han impactado significativamente el panorama legal. Las *Generative Adversarial Networks*[6] (GANs) y los modelos de transformadores, como BERT y GPT-3, revolucionaron el procesamiento del lenguaje natural y la generación de datos. Estas tecnologías plantearon nuevos desafíos legales, incluyendo la protección contra el uso indebido de IA para crear contenidos falsos (*deepfakes*), la propiedad intelectual de contenidos generados por IA y la transparencia en la toma de decisiones automatizadas.

Las aplicaciones prácticas de la IA se expandieron rápidamente, integrándose en la vida diaria a través de asistentes virtuales de fácil acceso como Siri, Alexa o Google Assistant, en la esfera industrial, la automatización de procesos y la robótica progresaron significativamente

Estos avances subrayaron la necesidad de marcos regulatorios hasta ahora poco desarrollados para asegurar la seguridad, la ética y la responsabilidad en el uso de IA, particularmente en aplicaciones críticas como la conducción autónoma.

En la presente década, la IA enfrenta desafíos éticos y legales cruciales, el sesgo algorítmico es una de las preocupaciones centrales, ya que puede llevar a decisiones discriminatorias; otro gran problema es dilucidar quién tiene la responsabilidad en el uso de la IA, las leyes deben definir quién es responsable de los errores de estos sistemas. La transparencia y explicabilidad de los modelos de IA son cruciales para decisiones justas, especialmente en sectores críticos como la salud y la justicia.

Muchos gobiernos a lo largo del mundo están desarrollando hoy en día regulaciones para el uso seguro y ético de la IA, estos marcos regulatorios deberán adaptarse a los avances tecnológicos, promoviendo tanto la

[6] De la Torre, J. (2023) *Redes generativas adversarias (GAN) Fundamentos teóricos y aplicaciones*. Universitat Oberta de Catalunya. P.2

innovación como el desarrollo responsable de los mismos para lograr un futuro libre de riesgos para las personas.

CONTEXTO JURÍDICO EN LA UNIÓN EUROPEA

En marzo de 2018, la Comisión Europea empezó a establecer un grupo de trabajo sobre IA para recopilar aportes de expertos y reunir a un amplio abanico de partes interesadas en el tema. Este Grupo de Expertos sería el encargado de elaborar una propuesta sobre la ética en la IA, basándose en la declaración del Grupo Europeo de Ética en Ciencia y Nuevas Tecnologías y de presentar antes de fin de año las directrices para el desarrollo y uso ético de la IA, teniendo en cuenta los derechos fundamentales de la UE para aplicarlos al tratar temas como la equidad, seguridad, transparencia, el futuro del trabajo y el impacto en dichos derechos fundamentales, incluyendo la privacidad, protección de datos personales, dignidad, protección del consumidor y no discriminación.

Los cincuenta y dos expertos nombrados en junio de 2018 constituyeron el nuevo Grupo de Alto Nivel en Inteligencia Artificial, planteando recomendaciones sobre cómo abordar los desafíos y oportunidades a mediano y largo plazo relacionados con la IA. Estas recomendaciones contribuirían al desarrollo de políticas, la evaluación legislativa y la creación de una estrategia digital para la próxima generación de europeos.

El resultado de las investigaciones de estos expertos se plasmó en el documento “Directrices éticas para una IA fiable” entregado a la Comisión en abril de 2019. El objetivo principal por el que trabajaron fue para lograr promover una IA fiable y para ello enumeraron una serie de aspectos que debería tener una IA para ser denominada como tal:

- Componentes y requisitos que debe tener una IA fiable:
    - Legalidad: Cumplimiento de todas las leyes y regulaciones aplicables.

        - Los sistemas de IA deben operar dentro de un marco jurídico que garantice el respeto de todas las leyes y reglamentos vigentes. Esto incluye leyes europeas, nacionales e internacionales que abordan aspectos como la protección de datos, la no discriminación, la responsabilidad por productos defectuosos y la seguridad y salud en el trabajo, entre otros.

    - Ética: Respeto a principios y valores éticos, como la dignidad humana, autonomía, equidad y explicabilidad.
        - **Dignidad Humana**: Los sistemas de IA deben respetar y proteger la integridad física y mental de las personas, su identidad personal y cultural, y sus necesidades esenciales, no pueden tratar a las personas como objetos de manipulación o control.

        - **Libertad Individual**: La IA debe permitir que las personas tomen decisiones libres e informadas sin coacción ni manipulación, incluyendo la protección contra la vigilancia injustificada.

        - **Democracia, Justicia y Estado de Derecho**: Se deben apoyar los procesos democráticos y respetar el pluralismo de valores y las elecciones individuales, se busca luchar contra el socavamiento de los sistemas democráticos y las garantías procesales.

        - **Igualdad, No Discriminación y Solidaridad**: La IA debe garantizar una distribución justa de beneficios y costes, evitando sesgos injustos y asegurando la representación de grupos vulnerables, promoviendo la igualdad de oportunidades.

        - **Derechos de los Ciudadanos**: Se busca la mejora de la eficiencia y alcance del gobierno en la prestación de bienes y servicios públicos, respetando los derechos de los ciudadanos a la participación y a una buena administración.

    - Robustez: Seguridad técnica y prevención de daños accidentales.
        - **Seguridad Técnica**: Una IA debe resistir a ataques y fallos, con medidas de protección adecuadas para evitar usos malintencionados. Debe incluir salvaguardias y planes de contingencia.

        - **Prevención de Daños**: Los sistemas de IA deben ser seguros para los usuarios y para el entorno en el que operan, debiendo incluir mecanismos de supervisión humana para evitar efectos adversos.

        - **Robustez Social***:* Se tiene que considerar el contexto y el entorno en el que opera, asegurando que no pueda causar daños sociales ni culturales, promoviendo el bienestar social y la sostenibilidad ambiental.

Estos requisitos deben ser aplicados a lo largo de todo el ciclo de vida de los sistemas de IA, desde su diseño y desarrollo hasta su implementación y uso en la sociedad. Además, se deben considerar tanto métodos técnicos como no técnicos para garantizar el cumplimiento de los mismos, fomentando de esta manera la investigación y la innovación para mejorar la ansiada fiabilidad. De

igual forma, estas directrices tendrían que ser revisadas regularmente para adaptarse a la evolución tecnológica y social de la Unión.

El siguiente gran paso hacia la consecución de una legislación europea sobre la IA se dio en febrero de 2020, con la presentación del Libro Blanco sobre la Inteligencia Artificial[7]. En este documento se buscaba seguir con el objetivo marcado por los Expertos de una IA basada en la excelencia (con medidas para armonizar esfuerzos a nivel regional, nacional y europeo, movilizando recursos para la investigación y la innovación) y la confianza (con un marco normativo para garantizar que la IA cumpla con las normas de la UE, especialmente en derechos fundamentales y protección del consumidor) y ha sido fundamental para el desarrollo del futuro Reglamento, promoviendo la adopción de la IA y abordando sus riesgos desde una perspectiva garantista.

En este documento se expone la situación de como la IA está en desarrollo permanente de manera muy veloz y tiene el potencial de mejorar significativamente varios aspectos de nuestro día a día, como la atención sanitaria, la agricultura, el cambio climático, la producción industrial y la seguridad. Sin embargo, también presenta riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación y la invasión de la privacidad.

Dentro de la UE se necesitaba un enfoque común para promover esta IA y enfrentar sus desafíos, basado en la Estrategia Europea para la IA[8] recogida a lo largo de estos últimos años, por lo que la Comisión Europea se comprometió a avanzar científicamente, mantener el liderazgo tecnológico y garantizar que las nuevas tecnologías beneficien a todos los europeos respetando sus derechos.

[7] Libro Blanco sobre la inteligencia artificial - *Un enfoque europeo orientado a la excelencia y la confianza* COM(2020)

[8] *Plan coordinado sobre la inteligencia artificial* COM (2018)

Para ello se propone la creación de centros de excelencia y pruebas, redes de universidades y centros de educación superior, y el apoyo a las PYMES para que puedan acceder y utilizar esta nueva tecnología.

Además, se puntualiza la importancia de atraer inversiones significativas en este campo, con el objetivo de alcanzar una inversión total anual de más de 20.000 millones de euros durante la próxima década.

Otro de los puntos clave que desarrolla este Libro Blanco son los riesgos asociados a la IA, en el que se analiza si la legislación actual a nivel europeo puede hacer frente a los nuevos problemas que surjan durante los años venideros, si es necesario adaptarla o crear una nueva. Los riesgos a los que se enfrentan se clasifican dentro de tres categorías principales: derechos fundamentales, seguridad y responsabilidad civil.

- Riesgos para los Derechos Fundamentales: La IA tiene el potencial de afectar varios derechos fundamentales, lo cual puede ocurrir de diversas maneras:

    - **Protección de Datos Personales y Privacidad**: Como gracias al desarrollo de las nuevas IAs estas pueden procesar grandes cantidades de datos personales, pueden llegar a ocurrir violaciones de la privacidad. La opacidad en la toma de decisiones ("efecto caja negra[9]") puede dificultar la supervisión y el control de cómo se utilizan estos datos. Además, existe el riesgo de que los datos sean “desanonimizados”, revelando información personal sin el consentimiento del propio individuo.

    - **No Discriminación**: La IA puede perpetuar o incluso amplificar sesgos existentes si los datos de entrenamiento están sesgados. Esto puede resultar en discriminación basada en género, raza, origen étnico, religión, discapacidad, edad u orientación sexual.

[9] : Giró Gràcia, X., & Sancho-Gil, J. M. (2021) *La Inteligencia Artificial en la educación: Big data, cajas negras y solucionismo tecnológico*. Seminar.net, 17(2). https://doi.org/10.7577/seminar.4281. P 133-135

Por ejemplo, los algoritmos de IA utilizados en la contratación de personal o en la concesión de créditos pueden discriminar injustamente contra ciertos grupos si no se diseñan y supervisan adecuadamente.

- **Libertad de Expresión y Reunión**: Aquellas IAs que filtran o moderan contenido en plataformas digitales pueden limitar la libertad de expresión si no son gestionados de manera transparente[10] y equitativa. Además, la vigilancia masiva habilitada por estos sistemas puede restringir la libertad de reunión y la privacidad de las comunicaciones.

- **Dignidad Humana**: Si se utiliza esta tecnología en contextos como el reconocimiento facial o los sistemas de monitoreo puede llegar a invadir la privacidad personal y socavar la dignidad humana, por lo tanto, una automatización de decisiones críticas sin supervisión humana adecuada también puede llevar a tratamientos contrarios al derecho.

- Riesgos para la Seguridad: Los productos y servicios basados en IA pueden presentar nuevos riesgos de seguridad, tanto materiales como inmateriales:

  - **Seguridad Física**: Cuando se integra la IA en productos físicos, como vehículos autónomos, se corre peligro de accidentes si funcionan incorrectamente. Por poner un ejemplo, un error en la tecnología de reconocimiento de objetos puede llevar a un mal funcionamiento del vehículo y provocar accidentes graves.

  - **Ciberseguridad**: Debido a su especial vulnerabilidad a ataques cibernéticos que pueden comprometer su funcionamiento, la manipulación de datos de entrenamiento o la introducción de

[10] June Orenga (2022) *Impactos del uso de las nuevas tecnologías digitales en la libertad de expresión*. Institut de Drets Humans de Catalunya. P. 26

malwares dañinos pueden causar fallos en los sistemas, lo que puede tener consecuencias desastrosas para empresas y usuarios.

- **Actualizaciones y Aprendizaje Automático**: Los sistemas de IA que aprenden y se actualizan continuamente pueden introducir nuevos riesgos a lo largo de su ciclo de vida.

  Las actualizaciones de software pueden cambiar la funcionalidad del sistema, añadiendo escollos que no estaban presentes en el momento de su lanzamiento al mercado y de los que el consumidor no estaba al tanto.

- Riesgos para la Responsabilidad Civil: La asignación de responsabilidad en caso de daños causados por sistemas de IA es compleja y plantea varios desafíos:

  - **Dificultad para atribuir responsabilidad**: La opacidad y la autonomía de los sistemas pueden dificultar la identificación de quién es responsable en caso de que ocurran fallos o daños (esto incluye a desarrolladores, operadores y fabricantes). Por continuar con el ejemplo de un vehículo autónomo que causa un accidente, puede ser difícil determinar si la responsabilidad recae en el fabricante del vehículo, el proveedor del software o el operador del vehículo[11].

  - **Pruebas y Compensaciones**: Las personas afectadas por daños causados IA pueden enfrentar dificultades para acceder a las pruebas necesarias para demostrar la responsabilidad y obtener compensaciones, hay una necesidad de demostrar un defecto en

[11] Bustamante Donas ,J. (2022) *Diilemas éticos de los vehículos autónomos: responsabilidad ética, análisis de riesgo y toma de decisiones* Universidad Complutense de Madrid. P.296

el sistema de IA, el daño causado y la posible conexión ocurrida en el caso particular.

A lo largo del Libro Blanco se proponen varias adaptaciones legales para abordar dichos riesgos asociados siendo estas adaptaciones cruciales para garantizar que el marco regulador sea adecuado y efectivo frente a los desafíos y oportunidades que se presentan.

Por ejemplo, esta falta de transparencia que puede recogerse en el proceso de toma de decisiones de los algoritmos resulta en una dificultad a la hora de detectar y demostrar infracciones legislativas, especialmente las disposiciones legales que protegen los derechos fundamentales imputan responsabilidades y permiten reclamar indemnizaciones.

Los usuarios también deberán ser informados sobre las opciones disponibles para controlar el funcionamiento del sistema, incluyendo mecanismos para intervenir en el proceso de decisión y poder proporcionar retroalimentación sobre su desempeño.

Siguiendo dentro del ámbito de la responsabilidad civil, se requiere una revisión minuciosa para garantizar que las normativas sean claras y precisas, permitiendo así que las leyes se apliquen de manera eficiente y justa. Esto implica una actualización y posible reestructuración de las leyes existentes para abordar cualquier ambigüedad o laguna legal, asegurando así que los responsables sean debidamente identificados y que las víctimas reciban la compensación adecuada.

Otro apunte que destacar dentro de la clasificación que hace este Libro Blanco sobre los riesgos (y que deja su desarrollo para el posterior Reglamento) es en lo relativo a los riesgos elevados. Estos se determinan en función de dos criterios: los sectores de alto riesgo, como salud, transporte y energía, y el uso específico de la IA dentro de estos sectores, considerando el impacto potencial.

Para mitigar estos riesgos, se proponen varios requisitos obligatorios para sistemas de IA denominados de alto riesgo: transparencia y claridad de los algoritmos, supervisión humana, solidez y seguridad de los sistemas, y protección de datos personales.

Además, se sugiere la implementación de procedimientos de certificación y auditoría para asegurar el cumplimiento continuo de estos requisitos.

La vigilancia del mercado es otra medida crucial, permitiendo monitorear el desempeño de los sistemas de IA y tomar acciones correctivas cuando sea necesario. La cooperación entre los Estados miembros y las instituciones de la UE es esencial para una implementación coherente y efectiva de las regulaciones, con el objetivo de promover un entorno seguro y ético para el desarrollo de la IA en Europa.

A la misma vez que se publicaba el Libro Blanco, se inició un proceso de consultas públicas en línea que se extendió hasta junio de 2020, con el objetivo principal de recabar las opiniones tanto de la ciudadanía como de otros expertos o empresas de la materia sobre las propuestas recogidas en el documento.

A nivel general, la Comisión pudo comprobar que existía un consenso en Europa sobre la necesidad de establecer una serie de medidas regulatorias en este sector. Los encuestados consideraban que sí que existían vacíos significativos tanto en el derecho europeo como en el de cada país que requerían el desarrollo de nuevas leyes para poder adaptarse a esta nueva tecnología.

También hubo partes interesadas que advirtieron sobre el peligro de sobrerregular este nuevo mercado, abogando por medidas más laxas y neutrales, para evitar posibles imposiciones que pudieran ser demasiado complejas y de esta forma entregar este sector tecnológico a otros países (como Estados Unidos[12]) en los que fuera más fácil desarrollar una empresa de un ámbito de tan rápidos avances como es la IA.

Todo este trabajo a lo largo de los años empezaba a dar sus primeros resultados tangibles con la *Propuesta de Reglamento para establecer normas armonizadas en materia de Inteligencia Artificial* en abril de 2021, en la que se recogían los estudios previos y se instaba a la UE a tomar el liderazgo mundial en este nuevo sector tecnológico.

Tras unos años de continuos debates sobre el contenido, que estuvo varias veces a punto de dinamitar (por discrepancias principalmente a cerca de las IAs generativas como CHAT GPT o DALL-E y sobre los sistemas de vigilancia biométrica) este Reglamento fue aprobado por el Parlamento Europeo el 13 de marzo de 2024 con 523 votos a favor, 46 en contra y 49 abstenciones.

Unos meses más tarde, el 21 de mayo de 2024, el Consejo Europeo certificó el texto definitivo, poniendo el broche final a todo el trabajo realizado en el que han participado activamente cuarenta y seis Estados miembros del Consejo de Europa, la Unión Europea y once Estados no miembros, así como representantes del sector privado, la sociedad civil y el mundo académico.

La aprobación de este Reglamento en Europa es un hito que nos coloca a la vanguardia mundial en regulación tecnológica. Al ser los primeros en implementar una legislación de este tipo, estamos estableciendo estándares globales para el uso responsable y ético de la IA.

[12] Kearns, J. "AI's Reverberations across finance". *FINANCE & DEVELOPMENT* Diciembre 2023. P.40-41

Este Reglamento no solo protege nuestros derechos y privacidad, sino que también garantiza que la tecnología se desarrolle de manera segura y transparente conforme a nuestros altos estándares.

Además, al fomentar la confianza pública en la IA, se debería impulsar la innovación y el crecimiento económico en diversas industrias, asegurando que Europa siga siendo un líder en el mercado global de tecnología.

REGLAMENTO DE LA INTELIGENCIA ARTIFICIAL

Estructura

Como primer paso en el análisis del contenido de este Reglamento, vamos a examinar la estructura sobre la cual la cual está desarrollado:

- Capítulo I: **Disposiciones Generales** (art. 1-4)

  Define principalmente el objetivo y el ámbito de aplicación del Reglamento, así como diversas definiciones del campo de la IA que se utilizarán a lo largo del mismo, estableciendo el marco general para la regulación de la IA en la UE.

- Capítulo II: **Prácticas de Inteligencia Artificial Prohibidas** (art.5)

  Detalla las prácticas de IA que están prohibidas debido a los riesgos inaceptables que plantean para la seguridad, los derechos fundamentales y otros valores de la Unión Europea.

- Capítulo III: **Sistemas de IA de Alto Riesgo** (art 6-49)

  Se centra en la clasificación, evaluación de conformidad y requisitos de transparencia para estos sistemas. Un sistema de IA se considera de alto

riesgo si está destinado a ser utilizado como componente de seguridad de productos regulados por la UE o si influye significativamente en decisiones críticas en áreas como la biometría, infraestructuras críticas, educación, empleo y justicia. Los proveedores deben someter estos sistemas a una evaluación de conformidad por organismos independientes y cumplir con requisitos estrictos de transparencia, precisión y ciberseguridad.

- Capítulo IV: **Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA** (art.50)

Especifica los requisitos de transparencia que deben cumplir todos los sistemas de IA, conforme a su nivel de riesgo, para garantizar que los usuarios estén informados sobre su funcionamiento

- Capítulo V: **Modelos de IA de uso general** (art.51-56)

En este Capítulo se explica como un modelo de IA de uso general se clasificará como "de riesgo sistémico" si posee capacidades de gran impacto, evaluadas con herramientas técnicas adecuadas, o si la Comisión Europea así lo decide, así de como deben actuar los proveedores en el desarrollo de estos.

- Capítulo VI: **Medidas de apoyo a la innovación** (art. 57-63)

Establece la creación de espacios controlados de pruebas para la IA a nivel nacional con el fin de fomentar la innovación y facilitar su desarrollo antes de su introducción en el mercado, junto con cómo garantizar los recursos necesarios para tal fin. Además, también regula el tratamiento de datos personales para el desarrollo de sistemas de IA en beneficio del interés público en estos espacios, siempre que se cumplan ciertas condiciones de seguridad y protección de derechos fundamentales.

- Capítulo VII: **Gobernanza** (art.64-70)

Despliega las funciones de la Oficina de IA, encargada de desarrollar las capacidades y conocimientos especializados de la Unión en IA y crea el Comité Europeo de Inteligencia Artificial, compuesto por un representante de cada Estado miembro y otras entidades relevantes, que se encargará de asesorar y asistir a la Comisión y a los Estados miembros para una aplicación coherente y eficaz del Reglamento.

- Capítulo VIII: **Base de datos de la UE para sistemas de IA de alto riesgo** (art.71)

En este breve Capítulo se trata la creación y mantenimiento de una base de datos de la UE para sistemas de IA de alto riesgo. La Comisión, en colaboración con los Estados miembros, será responsable de esta base de datos, la cual incluirá información detallada sobre estos sistemas.

- Capítulo IX: **Vigilancia poscomercialización, intercambio de información, vigilancia del mercado** (art.72-94)

Aquí se muestra cómo los proveedores deben implementar y mantener un sistema de vigilancia poscomercialización para recopilar, documentar y analizar datos relevantes sobre el desempeño de sus sistemas de IA a lo largo de su vida útil, además de notificar cualquier incidente grave a las autoridades competentes. También se describen los procedimientos de cooperación y asistencia mutua entre las autoridades nacionales y la Comisión para garantizar la conformidad y abordar los riesgos asociados a estos sistemas. Se incluyen medidas específicas para la gestión de riesgos, la protección de datos y la confidencialidad de la información.

- Capítulo X: **Códigos de conducta y directrices** (art. 95 y 96)

Fomenta la creación y adopción de códigos de conducta voluntarios para los sistemas de IA y como estos deben alinearse con los principios y requisitos del Reglamento. También explica el papel de Comisión Europea y el Comité Europeo de Inteligencia Artificial dentro de la emisión de

Directrices para ayudar a los desarrolladores y usuarios a cumplir con las normas establecidas.

- Capítulo XI: **Delegación de poderes y procedimiento de Comité** (art 97-99)

Otorga a la Comisión Europea la autoridad para adoptar actos delegados que complementen o modifiquen ciertos aspectos no esenciales del Reglamento. Además, establece un procedimiento de comité para garantizar la supervisión adecuada y la participación de los Estados miembros en el desarrollo y la implementación de estos actos delegados.

- Capítulo XII: **Sanciones** (art. 100 y 101)

Describe los procedimientos para la imposición de sanciones en caso de incumplimiento del Reglamento y los mecanismos de recurso disponibles para las partes afectadas.

- Capítulo XIII: **Disposiciones Finales** (art. 102-113)

Proporciona disposiciones transitorias para la implementación gradual del reglamento y las fechas de entrada en vigor, facilitando una transición ordenada y efectiva a las nuevas normas establecidas, además de establecer modificaciones a otros actos legislativos de la UE.

- **Anexos**

Los siete anexos proporcionan detalles específicos y técnicos para apoyar la implementación y el cumplimiento del Reglamento, esenciales para garantizar la claridad y la uniformidad en la aplicación de este, proporcionando un marco detallado para la clasificación, evaluación y vigilancia de los sistemas de IA en la UE.

Finalidad

El objetivo que se marca este Reglamento en su Capítulo I sigue la estela de los documentos ya analizados, lograr fortalecer el mercado interno mediante el establecimiento de un marco legal homogéneo que regule el desarrollo, la puesta en marcha y el uso de los sistemas de IA.

Esta IA debe estar centrada en las personas, fomentando la innovación y asegurando la protección de la salud, la seguridad y los derechos fundamentales recogidos en nuestro ordenamiento, logrando facilitar de esta manera la circulación de bienes y servicios que utilizan esta tecnología, intentando evitar las restricciones innecesarias.

Se aboga por un marco jurídico uniforme para evitar la fragmentación del mercado único, en virtud del desarrollo del art 114 del Tratado de Funcionamiento de la Unión Europea[13] (en adelante TFUE) que se utiliza frecuentemente como base legal para armonizar las normativas nacionales que afectan al mercado interior, asegurando así la libre circulación de bienes, servicios, capitales y personas dentro de la UE.

Antes de la consumación del Reglamento, algunos Estados miembros habían comenzado a desarrollar sus propias normativas nacionales sobre IA, lo que podría haber llevado a un mosaico de regulaciones divergente por lo que esta fragmentación habría dificultado la libre circulación de sistemas y productos basados en IA dentro de la UE.

[13] Art 114.1 TFUE (…) *se adoptarán las medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior.*

Además, al proporcionar un marco regulador claro y armonizado, se reduce la incertidumbre y los costos de cumplimiento, con el consecuente aumento de seguridad para empresas e individuos, priorizando garantizar la protección para promover una IA segura y que tenga la plena confianza de nuestros conciudadanos europeos.

Otra parte fundamental de estas disposiciones es la protección de los datos personales, que viene en sintonía con lo dispuesto en el artículo 16 del TFUE, en el cual se garantiza la protección de este derecho de los individuos[14].

La regulación incluye medidas específicas en diversos Capítulos (III, IV, VI y VII) para asegurar que los sistemas de IA manejen los datos personales de manera segura y responsable, previniendo cualquier forma de mal uso o violación de la privacidad de los individuos (Capítulo IX), que desarrollaremos más adelante.

Esto no solo abarca la recopilación y el almacenamiento de datos, sino también cómo se procesan y utilizan para tomar decisiones automatizadas. Además, el Reglamento asegura que estos sistemas sean transparentes y explicables, de manera que los usuarios puedan entender cómo se toman las decisiones y puedan cuestionarlas si es necesario

Afrontar la enseñanza de esta nueva tecnología

Antes de pasar a analizar los puntos clave del Reglamento, cabe destacar la importancia que la Comisión otorga a la "alfabetización" (como recoge el art 4.) sobre la IA para que todos los actores implicados comprendan sus capacidades y limitaciones. Esto no solo se refiere a la comprensión técnica de los sistemas de IA, sino también a la conciencia de sus implicaciones éticas, legales y sociales

[14] Art 16.1 TFUE: *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

Se aboga por la educación y la sensibilización sobre los beneficios y riesgos de la IA, ya que el conocimiento y la comprensión adecuados de estas tecnologías son cruciales para su adopción segura y efectiva. Se promoverá proporcionar formación específica tanto a los desarrolladores como a los usuarios de sistemas de IA, incluyendo profesionales en diversos sectores y el público en general.

Por este motivo se podría apoyar del Reglamento 2018/1724[15] que defiende la creación de la pasarela digital única para proporcionar acceso fácil y seguro a información, procedimientos administrativos y servicios de asistencia en toda la Unión.

Este Portal Digital Único puede servir como una plataforma centralizada para proporcionar acceso a recursos educativos sobre IA, incluyendo materiales didácticos, guías, tutoriales y cursos en línea que cubran aspectos técnicos y humanos de la IA además de facilitar la realización de procedimientos administrativos en línea.

El objetivo es que todos los involucrados entiendan cómo funcionan estas tecnologías, cuáles son sus implicaciones éticas y legales, y cómo pueden influir en la vida cotidiana y en la sociedad como conjunto.

Para lograr esto, el Reglamento insta también a la colaboración entre la Comisión Europea, los Estados Miembros y diversas partes interesadas (como la industria, las organizaciones académicas y la sociedad civil) para desarrollar códigos de conducta voluntarios y herramientas educativas.

Estas iniciativas ayudarán a garantizar que el uso de la IA sea responsable y provechoso para todos, sembrando al mismo tiempo la innovación y el crecimiento económico

Ámbito de aplicación

[15] Reglamento 2018/1724 del Parlamento Europeo y del Consejo del 2 de octubre de 2018 *relativa a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas.*

Aplicación a terceras partes

El Reglamento se va a aplicar a todos los proveedores y responsables del despliegue de sistemas de IA que operen dentro de la UE con independencia de si están establecidos en la UE o en terceros países. Este enfoque extraterritorial se alinea con otros marcos regulatorios de la UE, como el Reglamento General de Protección de Datos (en adelante, RGPD), que también tiene una aplicación extraterritorial similar a la recogida en este art. 2.

Lo que se busca con esto es evitar la desintegración del mercado y garantizar una competencia equitativa, asegurando que todos los operadores cumplan con los mismos estándares, sin importar su origen geográfico y así no poner trabas legislativas adicionales a las entidades europeas, con la consecuente desventaja competitiva que esto supondría.

Además, este Reglamento también se destina a los sistemas de IA que, aunque desarrollados y operados fuera de la UE, generen efectos significativos dentro de la Unión. Por ejemplo, si un sistema de IA desarrollado en un tercer país trata datos de ciudadanos europeos o influye en decisiones que afectan a personas en la UE, estará sujeto a las disposiciones recogidas dentro de este.

Exclusiones específicas

Por otra parte, en este Reglamento se hace una mención explícita sobre la exclusión de los sistemas de IA destinados a fines militares, de defensa y de seguridad nacional, pues esta exclusión respeta el principio de subsidiariedad y permite a los Estados miembros mantener control sobre sus propias políticas de seguridad y defensa por la naturaleza específica y las necesidades operativas de estos sectores.

Las actividades de defensa y seguridad nacional son responsabilidad exclusiva de los Estados miembros (art 4.2 del del Tratado de la Unión Europea (TUE)), y requieren un marco regulador distinto, adaptado a sus particularidades.

Y aunque la UE tiene una Política Común de Seguridad y Defensa, esta no equivale a una transferencia de competencias legislativas en materia de defensa a la UE.

Según los Artículos 42 y 43 del TUE, la PCSD es intergubernamental, lo que significa que las decisiones se toman por unanimidad en el Consejo de la UE y no pueden imponerse a los Estados miembros. La UE puede coordinar y apoyar acciones comunes, pero no legislar de manera obligatoria en este ámbito.

Sin embargo, si un sistema de IA inicialmente desarrollado para fines militares o de seguridad es utilizado para aplicaciones civiles o comerciales, entonces podría entrar en el ámbito de aplicación del Reglamento.

Para esto, dicho sistema debe cumplir con todas las disposiciones pertinentes recogidas en este documento para garantizar la seguridad y los derechos fundamentales en su nueva área.

Si se lograra conseguir una regulación conjunta a nivel de la Unión en este aspecto, podría ayudar a prevenir una carrera armamentista, que desembocaría en la proliferación de armas autónomas y sistemas militares basados en IA sin las debidas salvaguardias. Un compromiso europeo puede establecer estándares y límites claros para el desarrollo y despliegue de tales tecnologías, promoviendo su uso responsable y ético[16].

Investigación y desarrollo

También está recogida la importancia de la investigación y el desarrollo (I+D) en la evolución de la IA y establece exenciones específicas para facilitar la

[16] Ruiz Vigevano, M. (2021) “Inteligencia artificial aplicable a los conflictos armados: límites jurídicos y éticos”. *ARBOR Ciencia, Pensamiento y Cultura 197* (800) P.4

innovación. Los sistemas que sean desarrollados y puestos en servicio únicamente con fines de I+D estarán exentos de las disposiciones que se disponen en este reglamento hasta que se comercialicen o se utilicen fuera del ámbito de la investigación.

Con esta exención se pretende apoyar la investigación científica y la innovación tecnológica, permitiendo a los desarrolladores experimentar y probar nuevas tecnologías sin las trabas totales de la regulación para poder crear así un entorno en el que las empresas pueden invertir en el desarrollo de nuevas tecnologías de IA con la confianza de que sus productos cumplirán con las normas europeas.

En este aspecto, se podría seguir la Directiva Europea de Ensayos Clínicos[17] en la que se establece los principios y requisitos para la realización de ensayos clínicos en medicamentos para uso humano dentro de la Unión Europea.

Aunque esta Directiva se enfoca principalmente en el ámbito de la investigación médica, sus principios pueden aplicarse de manera análoga a la investigación y desarrollo de la IA por diversos motivos.

Como uno de los objetivos principales de esta directiva es proteger la seguridad, los derechos y el bienestar de los participantes en ensayos clínicos, en el contexto de la I+D en IA implicaría obtener el consentimiento informado de las personas cuyos datos se utilizarán, realizar las diversas evaluaciones necesarias, y establecer comités de ética para supervisar los proyectos.

La directiva también requiere que los ensayos clínicos sean aprobados por autoridades competentes antes de su inicio. Este principio puede trasladarse a este nuevo ámbito, donde los proyectos deben obtener la aprobación

[17] Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, *relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano*.

regulatoria y estar sujetos a monitoreo continuo para asegurar el cumplimiento de las normativas dispuestas.

La protección de datos y la privacidad son igualmente esenciales tanto en los ensayos clínicos como en la investigación de IA por lo que los proyectos de I+D en IA deben cumplir con el RGPD, utilizando técnicas de pseudonimización y anonimización para proteger la privacidad de los participantes de igual manera que los ensayos clínicos de medicamentos.

Esto es particularmente importante en un mercado global competitivo, donde la capacidad de innovar de manera segura y ética puede proporcionar una ventaja significativa y aportar una diferenciación clave en calidad frente a productos desarrollados en otros países.

Sin embargo, una vez que un sistema de IA se comercializa o se utiliza de manera general, deberá cumplir con los requisitos que se recogen aquí. Esto garantiza que los estándares de seguridad y protección de derechos fundamentales se apliquen una vez que estén listos para el mercado o el uso público.

Cooperación internacional

Pero, como bien es sabido, la IA tiene un impacto global y, por lo tanto, su gobernanza no puede limitarse a las fronteras europeas, de esta forma la cooperación internacional es crucial para abordar los desafíos globales, establecer estándares comunes y garantizar que la IA se utilice de manera ética y segura en todo el mundo.

Esta colaboración entre países y organizaciones internacionales puede facilitar el intercambio de conocimientos, la armonización de regulaciones y la gestión de riesgos transfronterizos.

Para lograr una cooperación internacional efectiva, la Unión Europea debe participar activamente en diversos foros y organizaciones internacionales que se ocupan de la IA, existiendo multitud de iniciativas en las que puede tomar parte y liderar la conversación aportando su experiencia, como pueden ser la ONU (a través de organismos como UNESCO o la UIT), la OCDE, el Foro Económico Mundial, …

Dentro de esta colaboración internacional, se hace hincapié en los ámbitos de la policía y la justicia. Las autoridades de terceros países y las organizaciones internacionales que actúan en el marco de acuerdos de cooperación con la UE pueden estar exentas del Reglamento, siempre y cuando dichos acuerdos ofrezcan garantías suficientes para la protección de los derechos y libertades para los altos estándares europeos.

La UE puede establecer acuerdos bilaterales específicos con países líderes en IA, como Estados Unidos, Japón, Canadá y Corea del Sur, y dentro de estos acuerdos pueden incluir proyectos de investigación conjuntos, intercambios de expertos y la creación de centros de excelencia en IA.

De la misma forma, Europa puede promover acuerdos multilaterales en el marco de organizaciones regionales, como la Unión Africana, la ASEAN y la CELAC. La idea es que estos acuerdos estén más enfocados en la transferencia de tecnología, el desarrollo de capacidades y la creación de marcos regulatorios comunes, proporcionando asistencia técnica y recursos a los países en desarrollo.

Con esto se busca evitar que dicha cooperación pueda llegar a comprometer nuestros niveles de seguridad acordados evitando los riesgos transfronterizos, estableciendo protocolos de ciberseguridad comunes, compartiendo información sobre amenazas y vulnerabilidades, y desarrollando capacidades conjuntas de respuesta rápida ante incidentes.

Esto incluye la creación de centros de respuesta a incidentes cibernéticos que operen de manera coordinada a nivel internacional, permitiendo una respuesta rápida y eficaz a ataques cibernéticos que involucren sistemas de IA.

También se marca como objetivo el trabajar con otros países para armonizar las regulaciones de protección de datos, garantizando que se apliquen principios comunes como el consentimiento informado, la minimización de datos y la transparencia en el uso de datos personales.

Esto podría lograrse a través de la firma de acuerdos que reconozcan la equivalencia de las normativas de protección de datos entre la UE y otros países; consecuentemente, la UE puede promover la adopción de tecnologías de mejora de la privacidad, como el cifrado de datos en estos lugares, para perseguir una mejora en el "*know-how*" a nivel global.

El fin último que persigue toda esta colaboración es que las autoridades de los Estados miembros y las instituciones de la UE sigan siendo responsables de garantizar que cualquier uso de información o tecnología de IA en el marco de estos acuerdos sea conforme con el derecho de la Unión.

Normas y obligaciones generales del Reglamento

El Reglamento que estamos estudiando establece una serie de normas y obligaciones generales que buscan asegurar un uso seguro, transparente y ético de los sistemas de IA que vienen a ser una continuación de los conceptos desarrollados en los documentos analizados previamente en este trabajo, como las Directrices éticas para una IA fiable o el Libro Blanco para la Inteligencia Artificial.

Una de las normas más fundamentales del Reglamento es la regulación exhaustiva de ciertas prácticas de IA que se consideran inadmisibles debido a

los altos riesgos que presentan para los derechos y libertades de las personas como pueden ser:

- **Manipulación Subliminal**: Está prohibido el uso de IA que manipule el comportamiento humano de manera inconsciente, utilizando estímulos que las personas no pueden percibir.

  Este tipo de manipulación puede alterar significativamente el comportamiento de una persona sin su consentimiento, lo cual es inaceptable desde el punto de vista ético y legal.

- **Explotación de Vulnerabilidades**: Los sistemas de IA no pueden ser utilizados para explotar las vulnerabilidades de grupos específicos de personas, como pueden ser los niños, personas con discapacidades o personas en situaciones socioeconómicas precarias.

  Se tiene en consideración que estos grupos son especialmente susceptibles a ser manipulados o explotados por lo que el Reglamento busca protegerlos explícitamente de cualquier abuso de la tecnología a la que puedan ser expuestos

- **Puntajes Sociales**: Uno de los mayores temores es el uso de estas nuevas tecnologías automáticas para evaluar o clasificar a las personas en función de su comportamiento social o características personales de manera que pueda resultar en una discriminación o exclusión social.

  Estos puntajes pueden tener consecuencias graves para las oportunidades y el bienestar de las personas y su uso por lo tanto está estrictamente regulado.

Es necesaria una mención aparte sobre el quebradero de cabeza que ha supuesto la regulación de los sistemas de reconocimiento biométrico para los legisladores.

El reconocimiento biométrico[18] se refiere al uso de tecnologías que analizan características físicas únicas de las personas, como el rostro, las huellas dactilares, el iris o la voz, para identificarlas o verificar su identidad. Cuando se aplica en tiempo real, estas tecnologías pueden capturar y analizar datos biométricos en directo, comparándolos con bases de datos preexistentes para identificar individuos de manera instantánea.

Las preocupaciones clave sobre su uso en tiempo real incluyen la intrusión en la privacidad y la vigilancia masiva debido a que estos sistemas pueden invadir significativamente la privacidad de las personas al capturar y analizar estos datos sin su consentimiento, rastreando y monitoreando sus movimientos y actividades en espacios públicos.

La vigilancia masiva, donde grandes poblaciones son monitoreadas continuamente, genera un riesgo significativo de abuso y uso indebido de los datos recolectados, creando un ambiente de control y desconfianza que afecta la libertad y los derechos individuales.

Además, los sistemas de reconocimiento biométrico pueden cometer errores, identificando incorrectamente a personas inocentes como sospechosas, lo que puede resultar en detenciones injustas y violaciones de los derechos fundamentales.

De igual manera, los algoritmos de reconocimiento biométrico también pueden estar sesgados, resultando en tasas de error más altas para ciertos grupos demográficos, como minorías étnicas o mujeres.

Una de las principales inquietudes para los expertos es que estos sesgos perpetúan la discriminación y la injusticia, reforzando desigualdades existentes en la sociedad que pueden ser aprovechadas por las personas en el poder.

[18] Art 4.14 del Reglamento (UE) 2016/679. Art 3.18 del Reglamento (UE) 2018/1725, y Art 3.13, de la Directiva (UE) 2016/680

Debido a todo este nerviosismo generado a cerca de la violación de nuestra privacidad y la posible vigilancia perpetua por parte del Estado que podría producirse[19], el uso de estos sistemas de reconocimiento biométrico en tiempo real en espacios públicos se prohíbe, salvo en las circunstancias excepcionales recogidas en el artículo 5.1.h.

Estas circunstancias excepcionales en las que se permite el uso incluyen la búsqueda de personas desaparecidas, la prevención de amenazas terroristas inminentes o la identificación de sospechosos de delitos graves, y aún en estos casos, el uso debe ser autorizado por una autoridad judicial o independiente competente.

Por lo tanto, para cualquier uso autorizado de sistemas de reconocimiento biométrico en tiempo real, deben existir mecanismos de transparencia y supervisión.

El principio de proporcionalidad es un pilar fundamental del derecho europeo, pues exige que cualquier medida que restrinja los derechos fundamentales debe ser adecuada, necesaria y proporcionada en relación con los objetivos legítimos que se persiguen.

La prohibición del uso de sistemas de reconocimiento biométrico en tiempo real en espacios públicos con fines de aplicación de la ley se justifica por la falta de dicha proporcionalidad entre los beneficios y los riesgos asociados.

Aunque estas tecnologías pueden ser útiles en ciertos contextos mencionados, (búsqueda de personas desaparecidas o la prevención de delitos graves) su uso generalizado no es proporcional a la intrusión significativa en los derechos de privacidad y el potencial de abuso y discriminación.

[19] Cotino Hueso, L. (2023). “Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal”. *El Cronista del Estado Social y Democrático de Derecho Nº100.* P.71

Este enfoque restrictivo nos sirve como precedente para la futura innovación en este ámbito de la IA tan importante, por lo que que a medida que la tecnología de reconocimiento biométrico evolucione, es probable que las normativas también se adapten para abordar los nuevos desafíos y oportunidades desde esta perspectiva, reflejando el firme compromiso con la protección de la privacidad y los derechos fundamentales.

En este punto volvemos a retomar lo mencionado anteriormente como “sistemas de alto riesgo”, que la UE considera que deberían estar sujetos a una serie de requisitos más estrictos para certificar que tales sistemas sean seguros, transparentes y respetuosos con nuestros derechos como ciudadanos.

Una de las piedras angulares del Reglamento es la obligación de implementar un sistema robusto para la gestión de riesgos, por lo que las entidades proveedoras de sistemas de IA de “alto riesgo” deben establecer procedimientos para identificar, analizar y mitigar los riesgos potenciales asociados con el uso de sus sistemas.

Esto incluye no solo los riesgos técnicos, sino también aquellos relacionados con la privacidad, la seguridad y otros derechos fundamentales de los usuarios. Dicha gestión no debe un proceso estático; debe ser continuo y adaptativo, permitiendo actualizaciones y mejoras a medida que se desarrollen nuevas amenazas o se detecten vulnerabilidades en su uso diario.

Por lo tanto, antes de que cualquier sistema de IA de alto riesgo pueda ser comercializado o puesto en funcionamiento, debe pasar por una evaluación de conformidad rigurosa.

Este proceso de evaluación está diseñado para garantizar que el sistema cumple con todas las normativas técnicas y legales pertinentes y puede incluir

una serie de pruebas detalladas, auditorías y revisiones exhaustivas de la documentación técnica proporcionada por los desarrolladores del sistema.

Estos mismos desarrolladores también van a tener que mantener registros detallados sobre el diseño, desarrollo y funcionamiento del sistema debiendo incluir información sobre los algoritmos utilizados, los datos de entrenamiento, las pruebas realizadas y las medidas adoptadas para mitigar los riesgos.

La documentación técnica debe incluir detalles sobre todas las etapas del desarrollo del sistema en cuestión, desde el diseño inicial hasta la implementación final, permitiendo una revisión completa del proceso de desarrollo y ayudando a identificar cualquier problema potencial.

De la misma forma, debe ser actualizada regularmente para reflejar cualquier cambio o mejora en el sistema, asegurando que siempre haya un examen preciso y actualizado del funcionamiento del sistema pues los proveedores y operadores de IA deben mantener registros detallados sobre el uso del sistema y las decisiones tomadas por él, como por ejemplo las circunstancias en las que se utilizaron y los resultados obtenidos.

Además, se prevé implementar mecanismos para recibir y revisar la retroalimentación de los usuarios y otras partes interesadas sobre el desempeño de la IA en estos sistemas especialmente peligrosos.

También se debe cerciorar que estos sistemas sean comprensibles tanto para los usuarios como para las autoridades reguladoras, proporcionando información clara sobre cómo funciona el sistema, qué datos utiliza, y cómo toma sus decisiones; esta explicabilidad permite a los usuarios comprender las bases de las decisiones tomadas por la IA y facilita la supervisión humana.

Una mayor implicación respecto a la supervisión humana implica que debe haber mecanismos en lugar para que los operadores humanos puedan intervenir, monitorear y, si es necesario, corregir las acciones del sistema, siendo vital para prevenir errores y garantizar que los sistemas de IA actúen de manera ética y conforme a las normativas.

Los sistemas de alto riesgo deben estar configurados para que los humanos puedan tomar el control en situaciones críticas, minimizando el riesgo de que las decisiones automatizadas causen daños irreparables, teniendo también que mantener registros detallados sobre el uso del sistema, incluyendo datos sobre las decisiones tomadas por la IA, las circunstancias en las que se utilizaron y los resultados obtenidos.

La conservación de estos registros es esencial para la trazabilidad y para evaluar el impacto del sistema en los usuarios, facilitando la investigación de incidentes y la resolución de disputas, asegurando que siempre haya un listado claro y verificable de las operaciones dadas.

Por lo tanto, la gestión de estos datos es un aspecto crítico de las obligaciones de transparencia, ya que los datos son la base sobre la cual funciona la IA.

Las empresas tienen un papel fundamental a la hora de garantizar que el procesamiento de datos cumpla con las leyes de protección de datos y respeten la privacidad de los individuos, implementando medidas técnicas necesarias para proteger los datos contra el acceso no autorizado y el uso indebido.

Para los casos en que se requiera el consentimiento de los usuarios para la recopilación y el procesamiento de sus datos, estas deben asegurarse de que el consentimiento sea informado y voluntario.

Estos requisitos específicos establecidos en el Reglamento son esenciales para garantizar que estos sistemas se utilicen de manera segura, ética y transparente para el beneficio del pueblo europeo.

Además, este principio desarrollado de responsabilidad proactiva es un concepto clave en la normativa europea y establece que las organizaciones no solo deben cumplir con las normativas, sino que también deben poder demostrar dicho cumplimiento de manera activa y continua.

Con esto no solo se conseguirá minimizar los riesgos asociados, sino que también promoverán la confianza y la responsabilidad en el desarrollo y uso de estas tecnologías avanzadas, este enfoque integral asegura que la IA pueda ser una fuerza positiva en la sociedad, beneficiando a todos mientras se mitigan los posibles desafíos.

Supervisión y Cumplimiento

A lo largo de todo el Reglamento se va estructurando un marco robusto para la supervisión y el cumplimiento, asegurando que los sistemas se desarrollen, implementen y utilicen de manera segura conforme a la normativa.

Con este enfoque integral se busca proteger los derechos de los ciudadanos y fomentar la confianza pública en estas tecnologías avanzadas, incluyendo una variedad de medidas y mecanismos que abarcan desde la evaluación inicial de conformidad hasta la supervisión continua y las medidas correctivas en caso de incumplimiento.

Uno de los componentes fundamentales dispuestos en este sistema de supervisión es el desarrollo de autoridades competentes y organismos independientes encargados de monitorear el cumplimiento de lo dispuesto, como diversos mandos de vigilancia del mercado y la recientemente creada

para este fin “Oficina Europea de la IA”[20] (organismo regulador creado por la Comisión Europea, dependiente de la Dirección general de Redes de Comunicación, Contenidos y Tecnología de la Comisión Europea), que van a desempeñar un papel fundamental para mantener y proteger el orden imperante.

Estas entidades tienen la responsabilidad de investigar denuncias, supervisar la implementación de las IA y asegurar que el cumplimiento todas las normas y requisitos establecidos.

De igual manera, también tienen el poder de imponer sanciones y medidas correctivas en caso de incumplimiento, asegurando así que las empresas y los proveedores sean responsables tanto económicos como penales de sus acciones.

Desde un punto de vista jurídico, el fundamento para la actuación de estas autoridades se encuentra recogido en el Reglamento 2019/1020[21] sobre vigilancia del mercado y conformidad de productos, que establece un marco general para la supervisión del mercado en la UE.

La aplicación de este Reglamento refuerza la capacidad de las autoridades de vigilancia del mercado al proporcionarles herramientas legales para realizar sus funciones de manera efectiva.

Estas herramientas incluyen la potestad de realizar inspecciones in situ, solicitar documentación técnica y datos relacionados con la conformidad de los sistemas de IA, y aplicar sanciones en caso de incumplimiento. Estos poderes se aplican directamente a los sistemas de IA, permitiendo a las autoridades evaluar si los sistemas cumplen con los requisitos de seguridad y protección establecidos en el Reglamento de IA.

[20] Decisión de la Comisión Europa del 24 de enero de 2024 de establecer la Oficina Europea de Inteligencia Artificial.

[21] Reglamento 2019/1020 del Parlamento Europeo y del Consejo de 20 de junio de 2019 *relativo a la vigilancia del mercado y la conformidad de los productos*

Además, se establecen mecanismos de cooperación y coordinación entre las autoridades de vigilancia del mercado de los distintos Estados miembros, siendo esto particularmente relevante para la supervisión de estos sistemas, dado el carácter transnacional de esta nueva tecnología.

Las autoridades deben compartir información sobre los productos que no cumplen con las normativas y coordinar sus acciones para retirar del mercado aquellos sistemas de IA que representen un riesgo para la seguridad o que no cumplan con los requisitos legales. Esta cooperación es fundamental para asegurar un enfoque armonizado y eficaz en la supervisión del mercado de la IA en toda la Unión Europea.

También implica la necesidad de una formación y capacitación adecuadas para las autoridades de vigilancia del mercado pues dado el carácter técnico y complejo de la IA, las autoridades deben estar bien equipadas con conocimientos especializados para evaluar la conformidad y detectar posibles incumplimientos.

Esto incluye la capacidad de entender y analizar algoritmos, modelos de IA y datos técnicos, así como la implementación de evaluaciones de impacto relativas a los derechos fundamentales.

Régimen sancionador

Se establece un régimen de sanciones administrativas en el Capítulo XII que incluye la imposición de multas para asegurar el cumplimiento de lo recogido en el Reglamento.

Estas multas están basadas en varios principios jurídicos fundamentales como son el principio de proporcionalidad (las sanciones deben ser proporcionales a la gravedad de la infracción y al daño potencial o real causado, asegurando que las multas no sean excesivas, pero suficientemente disuasorias),

efectividad (las multas deben ser efectivas para garantizar el cumplimiento de las normativas; esto significa que deben ser lo suficientemente altas para disuadir a los infractores potenciales y asegurar que las empresas cumplan con las obligaciones acordadas) y equidad (al imponer multas, las autoridades deben considerar todas las circunstancias pertinentes del caso, incluyendo la naturaleza, gravedad y duración de la infracción, las medidas de mitigación adoptadas por el infractor, y su grado de cooperación con las autoridades).

Este régimen sancionador tiene como función garantizar el cumplimiento del Reglamento y proteger los derechos y la seguridad de los ciudadanos europeos.

Se entienden las multas como una herramienta clave para disuadir a los proveedores y responsables del despliegue de sistemas de IA de incumplir las normativas. La base legal para estas sanciones se encuentra en el artículo 99 del Reglamento, que detalla las infracciones y las correspondientes sanciones administrativas según el tipo de infracción cometida.

- **Violación de Prohibiciones de Prácticas de IA**: Las infracciones más graves son aquellas relacionadas con la violación de las prohibiciones de ciertas prácticas de IA consideradas inaceptables, que han sido explicadas previamente, como la utilización de la IA en sistemas que empleen técnicas subliminales para manipular el comportamiento de las personas, la explotación de vulnerabilidades de grupos específicos (por ejemplo, niños o personas con discapacidades) o el uso de sistemas de IA para la puntuación social por parte de autoridades públicas que pueda llevar a un trato injusto o discriminatorio.

  Las violaciones de las prohibiciones establecidas en el artículo 5 pueden resultar en multas administrativas de hasta 35 millones de euros o, si el infractor es una empresa, hasta el 7% del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cifra es superior.

Estas multas están diseñadas para ser suficientemente disuasorias, reflejando la gravedad de las infracciones y su potencial impacto negativo en los derechos fundamentales y la seguridad de los ciudadanos.

- **Incumplimiento de Requisitos de Conformidad y Obligaciones**: Este tipo de infracción abarca una variedad de obligaciones específicas establecidas en el Reglamento, incluyendo los relativos a los requisitos para proveedores de sistemas de IA de Alto Riesgo, las obligaciones de vigilancia post-comercialización y respecto a la transparencia e información proporcionada al usuario.

  El incumplimiento de estos requisitos y obligaciones está sujeto a multas de hasta 15 millones de euros o el 3% del volumen de negocios mundial total del infractor, si esta cuantía fuese superior. Este nivel de sanción refleja la importancia de cumplir con los requisitos esenciales de seguridad en el desarrollo y despliegue de sistemas de IA.

- **Proporcionar información incorrecta o engañosa**: Proporcionar información incorrecta, incompleta o engañosa a las autoridades nacionales competentes o a los organismos notificados constituye otra categoría de infracción.
  Esto puede incluir la falsificación de documentos o datos en la evaluación de conformidad, la ocultación de fallos o riesgos asociados con el sistema de IA o el suministro de datos erróneos durante auditorías o inspecciones.

  Las multas contempladas pueden llegar hasta los 7.5 millones de euros o el 1% del volumen de negocios mundial total del infractor, si esta cuantía fuese superior. Estas sanciones aseguran que los operadores actúen con integridad y transparencia en todas las interacciones con las autoridades de supervisión en un contexto de lucha creciente contra la desinformación, presente cada vez más en el debate político.

De la misma forma, para lograr un procedimiento imparcial, la defensa puede valerse de distintos medios para protegerse de decisiones injustas.

Para empezar, tiene derecho al acceso de su expediente. El operador debe tener acceso a todos los documentos y pruebas que la autoridad tiene en su poder y que son relevantes para el caso, asegurando de esta manera poder preparar una defensa informada y completa, permitiéndole conocer en detalle las alegaciones y las pruebas presentadas en su contra.

También tiene el derecho de ser oído, que incluye la posibilidad de hacer alegaciones por escrito y de participar en una audiencia oral. Durante esta audiencia, el acusado puede estar representado por un abogado y presentar pruebas adicionales, llamar a testigos y cuestionar las pruebas presentadas por la autoridad.

Además, la decisión que tome la autoridad debe ser motivada, proporcionando una explicación detallada de las razones por las que se ha tomado la decisión, incluyendo una evaluación de las pruebas y de los argumentos presentados por la defensa.

Una decisión motivada es crucial para asegurar la transparencia y la rendición de cuentas en este proceso administrativo, permitiendo a la defensa entender la base legal y factual de la decisión y evaluar si se ha cometido alguna irregularidad o error en el procedimiento.

En última instancia, se tiene el derecho de recurrir la decisión de imposición de sanciones ante un órgano judicial independiente, en este caso al Tribunal de Justicia de la Unión Europea. Este derecho de recurso es esencial para asegurar que la decisión administrativa sea revisada de manera imparcial y objetiva.

El recurso puede basarse en diversas razones, como errores en la aplicación del Reglamento, la valoración incorrecta de las pruebas, o la desproporcionalidad de la sanción impuesta, este derecho a recurrir es un componente vital del proceso, ya que proporciona una vía para corregir posibles injusticias o errores administrativos.

Una forma en la que la UE puede complementar este régimen sancionador sería con la aplicación de mecanismos de mediación y el arbitraje. Estas herramientas permiten resolver conflictos de manera rápida, menos costosa y menos confrontacional que los procedimientos judiciales tradicionales.

La base legal para su implementación se encuentra en el principio de eficiencia procesal, la Directiva 2008/52/CE sobre Mediación[22] y el Reglamento 2019/1150 sobre Transparencia y Equidad[23].

Mientras que la mediación es un proceso voluntario y confidencial facilitado por un mediador neutral, el arbitraje es más formal y termina en una decisión vinculante emitida por un árbitro.

La UE podría establecer centros especializados de mediación y arbitraje para IA, con expertos en derecho y tecnología de IA, ofreciendo servicios específicos para abordar las disputas en este ámbito.

Entre las ventajas claves de estos procesos se incluyen la rapidez y eficiencia, menores costos, flexibilidad y confidencialidad, pero para implementar estos mecanismos de manera efectiva, se deberían seguir desarrollando normas y procedimientos uniformes a nivel de la UE, capacitar y acreditar mediadores y árbitros especializados en IA, y ofrecer incentivos para su uso, como la reducción de sanciones o asistencia financiera.

[22] Directiva 2008/52/CE del Parlamento Europeo y del Consejo, de 21 de mayo de 2008, *sobre ciertos aspectos de la mediación en asuntos civiles y mercantiles*.

[23] Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, *sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.*

Entrada en vigor y aplicación del Reglamento

El proceso de entrada en vigor y aplicación de un Reglamento europeo es fundamental para asegurar que las nuevas normativas sean implementadas de manera efectiva y conforme al marco legal establecido y se encuentra recogido en el Capítulo XIiI.

Conforme a lo estipulado en el art. 113, entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea, lo que es estándar en la legislación europea y proporciona un período suficiente para que las partes interesadas tomen conocimiento del nuevo marco regulatorio.

Además, la aplicación de las disposiciones del Reglamento es escalonada, permitiendo diferentes fechas de inicio para diversas obligaciones, facilitando así una transición gradual.

Se establece un período transitorio de dos años desde su entrada en vigor para la aplicación general de sus disposiciones, durante el cual se anima a los proveedores de sistemas de IA de alto riesgo a cumplir voluntariamente con las obligaciones pertinentes.

Esta disposición busca facilitar la adaptación de los operadores a las nuevas normativas, permitiéndoles adquirir experiencia en el cumplimiento antes de que sea de obligatorio cumplimiento.

Sin embargo, algunas disposiciones relacionadas con la prohibición de ciertos usos de la IA, debido a los riesgos inaceptables que representan, se aplicarán seis meses después de su entrada en vigor, con el objetivo de proteger los derechos fundamentales y la seguridad pública de manera más inmediata.

También nos encontramos con que este Reglamento produce modificaciones legales a textos anteriores para introducir cambios significativos, incorporando especificaciones relacionadas con la IA.

Por ejemplo, se introduce un nuevo párrafo en el artículo 4.3 del Reglamento n.º 300/2008[24], que trata sobre la seguridad en la aviación civil, en el que se incluye especificaciones técnicas y procedimientos relacionados con sistemas de IA en los equipos de seguridad.

Otro punto modificado por este Reglamento es el artículo 17.5 del Reglamento n.º 167/2013[25], que trata sobre la homologación de vehículos agrícolas y forestales. Esta reforma añade sistemas de IA como componentes de seguridad que deben cumplir con detalles técnicos.

Estas modificaciones se fundamentan en las competencias conferidas por el TFUE, especialmente en lo que respecta a la armonización de normativas técnicas para asegurar el funcionamiento del mercado interior (el ya mencionado artículo 114).

La incorporación de estos sistemas de IA en los Reglamentos responde a la necesidad de actualizar y armonizar las normativas técnicas conforme a los avances tecnológicos, buscando asegurar la coherencia normativa dentro del marco legal europeo, evitando la desintegración de nuestro mercado interior.

Al actualizar los requisitos técnicos y procedimientos, las modificaciones proporcionan claridad y seguridad jurídica para todos los agentes que operan dentro de la UE, siendo esta actualización esencial para mantener la relevancia y eficacia de las normativas técnicas en un contexto de rápida evolución en todos los aspectos.

[24] Reglamento nº 300/2008 del Parlamento Europeo y del Consejo de 11 de marzo de 2008 *sobre normas comunes para la seguridad de la aviación civil*

[25] Reglamento nº 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013*, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos.*

La coherencia normativa también facilita la libre circulación de bienes y servicios dentro de la UE, uno de los principios fundamentales del mercado único europeo.

CONCLUSIONES

Primera. Valoración del modelo regulador europeo de IA

El análisis del Reglamento Europeo sobre Inteligencia Artificial pone de manifiesto un esfuerzo monumental por parte de la Unión Europea para establecer un marco regulatorio que no solo permita el desarrollo y la implementación de la IA, sino que también proteja los valores fundamentales y derechos de sus ciudadanos.

La adopción de este Reglamento, el primero de su tipo a nivel mundial, destaca el compromiso de la UE con una regulación proactiva y equilibrada que aspire a convertir a Europa en un líder en el campo de la IA segura y ética.

Desde un punto de vista jurídico, este Reglamento establece una serie de medidas que son esenciales para abordar los riesgos inherentes de esta nueva tecnología. La clasificación de los sistemas de IA según su nivel de riesgo y la introducción de requisitos estrictos para aquellos considerados de alto riesgo son pasos fundamentales para asegurar que la IA se despliegue de manera responsable.

Estos requisitos incluyen la necesidad de evaluaciones de conformidad, la obligación de mantener documentación técnica exhaustiva y la implementación de mecanismos de supervisión humana, siendo crucial para prevenir abusos y garantizar la seguridad y protección de los derechos de las personas.

La prohibición de prácticas de IA consideradas inaceptables, como la manipulación subliminal y la explotación de vulnerabilidades de grupos específicos, refleja un compromiso firme con la ética y los valores europeos.

En particular, la regulación del uso de sistemas de reconocimiento biométrico en tiempo real en espacios públicos subraya la importancia de proteger la privacidad y evitar la vigilancia masiva, estableciendo un precedente importante para futuras legislaciones.

Segunda. Desafíos y proyección futura del marco normativo

En términos de futuro legislativo, el camino hacia una regulación efectiva de la IA está lleno de desafíos y oportunidades. La tecnología de IA evoluciona a un ritmo vertiginoso, lo que requiere que el marco regulatorio sea dinámico y adaptable. La UE deberá estar preparada para actualizar y modificar su legislación a medida que surjan nuevos desarrollos tecnológicos y desafíos éticos.

En este contexto, es probable que veamos un enfoque cada vez más granular y específico en áreas como la transparencia algorítmica, la mitigación de sesgos y la rendición de cuentas en decisiones automatizadas.

La cooperación internacional será otro pilar fundamental en la evolución legislativa de la IA. La naturaleza global de la IA implica que los marcos regulatorios nacionales y regionales deben alinearse y colaborar para abordar los desafíos transfronterizos de manera efectiva.

La UE tiene la oportunidad de liderar estos esfuerzos, promoviendo la creación de estándares internacionales que aseguren un uso seguro y ético de la IA en todo el mundo. Esta colaboración no solo puede facilitar la armonización de las regulaciones, sino que también puede fomentar la innovación y la competitividad global.

El papel de la educación y la sensibilización sobre la IA también será crucial en el futuro legislativo. Es esencial que tanto los desarrolladores como los usuarios comprendan las capacidades y limitaciones de la IA, así como sus implicaciones éticas y legales.

La promoción de una "alfabetización digital" en IA contribuirá a un uso más informado y responsable de esta tecnología, fortaleciendo la confianza pública y facilitando la adopción de normativas cada vez más sofisticadas y adecuadas a la realidad tecnológica.

En resumen, el Reglamento Europeo sobre Inteligencia Artificial es un paso significativo hacia la creación de un marco regulador que no solo fomenta la innovación, sino que también protege los derechos fundamentales y la seguridad de los ciudadanos.

El futuro legislativo de la IA en la UE será un proceso continuo de adaptación y refinamiento, en respuesta a los avances tecnológicos y a los nuevos desafíos éticos y sociales que surjan. Con un enfoque basado en la cooperación internacional, la educación y la adaptabilidad, la UE está bien posicionada para liderar el camino hacia un uso seguro, ético y beneficioso de IA en todo el mundo.

BIBLIOGRAFÍA

- **Bustamante Donas, J.** (2022). *Dilemas éticos de los vehículos autónomos: responsabilidad ética, análisis de riesgo y toma de decisiones*. Universidad Complutense de Madrid.
- **Craglia, M.** (Ed.), Annoni, A., Benczur, P., Bertoldi, P., Delipetrev, P., De Prato, G., Feijoo, C. (2018). *Artificial intelligence - a european perspective*. Luxemburg.
- **Cotino Hueso, L.** (2023). *Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal*. El Cronista del Estado Social y Democrático de Derecho, Nº100.
- **De la Torre, J.** (2023). *Redes generativas adversarias (GAN) Fundamentos teóricos y aplicaciones*. Universitat Oberta de Catalunya.
- **Fajardo de Andara, C.** (2021). *Marvin Lee Minsky: pionero en la investigación de la inteligencia artificial*. Universidad Nacional Experimental Politécnica Antonio José de Sucre, Venezuela.
- **Giró Gràcia, X., & Sancho-Gil, J. M.** (2021). *La Inteligencia Artificial en la educación: Big data, cajas negras y solucionismo tecnológico*. Seminar.net.
- **Kearns, J.** (2023). *AI's Reverberations across finance*. FINANCE & DEVELOPMENT, diciembre 2023.
- **Manning, C.** (2020). *Artificial Intelligence Definitions*. Stanford University.
- **Orenga, J.** (2022). *Impactos del uso de las nuevas tecnologías digitales en la libertad de expresión*. Institut de Drets Humans de Catalunya.

- **Ruiz Vigevano, M.** (2021). *Inteligencia artificial aplicable a los conflictos armados: límites jurídicos y éticos*. ARBOR Ciencia, Pensamiento y Cultura, 197.

OTROS DOCUMENTOS

- *Libro Blanco sobre la inteligencia artificial - Un enfoque europeo orientado a la excelencia y la confianza.*