POSICIONAMIENTO AMETIC SOBRE

AI ACT

JULIO DE 2023

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

aniversario 50 1973 - 2023

CONTENIDO

RESUMEN EJECUTIVO

La Inteligencia Artificial ha experimentado un gran desarrollo en las últimas décadas, gracias a la mejora de las comunicaciones y del avance de la computación, que ha permitido crear ordenadores más potentes y capaces de procesar grandes cantidades de datos. Algunos campos que se han beneficiado de la IA son el aprendizaje automático, las redes neuronales, el procesamiento del lenguaje natural o la visión artificial.

Sin embargo, la IA también plantea una serie de desafíos y riesgos para la sociedad, como la seguridad, la transparencia, la privacidad, la ética o los derechos fundamentales de las personas. Por ello, se hace necesario establecer un marco legal común que regule el uso de la IA y garantice su confianza y responsabilidad para lograr una IA más humana.

Es por ello por lo que AMETIC, como patronal del sector de la industria digital en España, presenta este documento de análisis de la propuesta del Reglamento con las aportaciones y experiencias de nuestros asociados que representan a toda la cadena de valor de la industria digital, e identifica propuestas de mejora y recomendaciones específicas para abordar los impactos sectoriales. Este documento está estructurado en torno a 5 apartados:

1. Introducción, orígenes de la inteligencia artificial y fundamentos para la creación de la AI Act, así como una descripción preliminar de la misma.
2. Visión general de la AI Act.
3. Análisis e impacto de la AI Act en la industria y el sector tecnológico desde la perspectiva del sector digital.
4. Exposición de los principios generales que guían la posición de AMETIC sobre la AI Act, identificación de oportunidades y desafíos para las empresas del sector, así como propuestas y recomendaciones.
5. Análisis desde un aspecto ético, social y humanista de la propuesta de regulación

De entre sus primeros análisis, AMETIC valora muy positivamente los esfuerzos de la UE para implementar un enfoque efectivo basado en el riesgo para la regulación de la IA que proteja los derechos civiles y al mismo tiempo permita la innovación continua y la aplicación práctica de esta importante tecnología. Al igual que otras tecnologías, la mayoría de los riesgos asociados con la IA, además de encontrarse en los sistemas de IA (transparencia y explicabilidad de los modelos, frecuencia del reentrenamiento de estos o sesgo en los datos), se localiza en la aplicación de la tecnología y en casos de uso específicos.

Sin duda, la IA se utilizará para abordar algunos de los mayores desafíos a los que se enfrenta la sociedad, desde la seguridad alimentaria, detección temprana y tratamientos preventivos en enfermedades, el cambio climático y la seguridad energética hasta la seguridad de la cadena de suministro. Por lo tanto, los requisitos deben orientarse a garantizar las salvaguardas apropiadas sin limitar involuntariamente los usos que no suponen un riesgo y que posiblemente mejoren la calidad de vida.

Siendo conscientes del trabajo que queda por delante, desde AMETIC ofrecemos algunas sugerencias para la mejora de las realidades del ecosistema de la IA en la actualidad y en el futuro, y otras recomendaciones específicas para abordar los

impactos sectoriales, todas ellas cumpliendo con la legislación vigente, respetando los derechos a la intimidad en el ámbito laboral que en España se encuentra regulada por diversas leyes, como el Reglamento General para la Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD) y el Estatuto de Trabajadores, unidos a los derechos y libertades recogidas en la Constitución Española:

- **Rechazar la propuesta del Parlamento de prohibir la inferencia de emociones en el lugar de trabajo y evitar la manipulación de las emociones con fines que atenten contra los derechos de privacidad, intimidad y laborales**. En cualquier caso, muchos usos de la IA en el lugar de trabajo caerán en la categoría de alto riesgo, Anexo III.

- **Apoyar la propuesta del Consejo que excluye de la definición de "alto riesgo" los sistemas de IA cuyo resultado es "puramente accesorio".** Además, apoyar la propuesta del Parlamento que limita la clasificación de alto riesgo a la IA que impone un riesgo significativo de daño a la salud, la seguridad y los derechos fundamentales. El "daño significativo" debe especificarse de manera que se centre en los riesgos materiales adversos.

- **La legislación de la GPAI debe consistir en requisitos personalizados y técnicamente factibles basados en estándares existentes y principios interoperables como los de la OCDE.** Apoyar la propuesta del Consejo de que los implementadores deben tener la oportunidad de aclarar en las instrucciones de uso que una GPAI no debe implementarse en áreas de alto riesgo, considerando situaciones en las que el desarrollador tiene el control total del despliegue. El desarrollador de GPAI debe tener la obligación de apoyar al implementador de GPAI para garantizar el cumplimiento cuando sea necesario (similar a los mecanismos del Reglamento General de Protección de Datos en el Art. 28).

- **Los Modelos Fundacionales (FM) no deben considerarse en general de alto riesgo.** En caso de que las instituciones de la UE en trílogo acuerden imponer obligaciones a los FM, estas deben ser proporcionadas, técnicamente factibles y alineadas con legislación europea y con estándares internacionales y principios de interoperabilidad como los acordados en la OCDE. Se deberían considerar los mecanismos existentes sobre extracción de texto y datos incluidos en la Directiva de derechos de autor de la UE y la jurisprudencia, como motores de búsqueda e índices. Esto evitaría sobrecargar las negociaciones específicas de la AI. Se debería garantizar la transparencia respecto al origen de las fuentes sobre las que se ha entrenado.

- Para garantizar la claridad legal**, las obligaciones deben dirigirse principalmente al actor mejor ubicado para cumplir con los requisitos**. Esto incluiría el reconocimiento por parte del desarrollador del uso de su IA en un sistema de alto riesgo, las obligaciones específicas de las que sería responsable el desarrollador y la obligación del desarrollador de ayudar con las solicitudes de una autoridad nacional. Este mecanismo no se aplicaría en situaciones en las que el desarrollador de GPAI haya aclarado en las instrucciones de uso que la GPAI no debe utilizarse en un caso de uso de alto riesgo (ver más arriba las sugerencias sobre GPAI). Este enfoque equilibrado inspirado en el Reglamento General de Protección de Datos garantizaría el cumplimiento por parte del implementador habilitado por el desarrollador. Además, se deben aclarar las terminologías, particularmente entre los desarrolladores de IA (es decir, aquellos que ponen a disposición IA, modelos preentrenados y similares), implementadores (es decir, aquellos que implementan un sistema de IA o que implementan el caso de uso para usuarios finales) y usuarios finales (es decir, consumidores o aquellos que usan IA para uso personal). Deben aclararse las responsabilidades por las

obligaciones, en particular con respecto a los sistemas de IA de alto riesgo. Tanto el Consejo como el Parlamento incluyen propuestas útiles en este contexto que deberían especificarse más detalladamente.

Como recomendaciones, destacar:

- **Definir correctamente qué es IA**, del ámbito de la AI Act, previo consenso con el sector tecnológico que invierte, produce y ayuda a su despliegue.
- **Definir correctamente la cadena de valor de la IA y las responsabilidades de cada parte**, consensuándola con el sector tecnológico. Clarificar las responsabilidades en toda la cadena de valor de la IA. Cuando proceda, el Reglamento de IA debería aportar una mayor flexibilidad, garantizando la libertad de las partes para asignar responsabilidades a través de obligaciones contractuales.
- **Garantizar la armonización del Reglamento con legislación ya vigente**, para evitar la duplicación de procedimientos y simplificar el cumplimiento de la normativa en muchos sectores en los que Europa es hoy líder, y debe seguir siendo competitiva.
- **Designar un punto de contacto centralizado en cada Estado** y articular un sólido mecanismo de coordinación para garantizar una aplicación y un cumplimiento coherente.
- **Gestionar lo más posible los procesos de evaluación y cumplimiento** basándolos en procesos de autoevaluación responsable, que optimicen el cumplimiento en tiempo y costes. En particular, ha de evitarse que el proceso de cumplimiento en Europa se convierta en un negocio que encarezca innecesariamente toda actividad en IA haciendo que Europa pierda competitividad, así como la necesidad de re-certificar o re-evaluar sistemas o modelos cada vez que haya que reentrenarlos o recalibrarlos.
- **Utilizar los Sandboxes para testar el impacto potencial de la regulación en las empresas** y ayudarles también a prepararse para su cumplimiento. Los Estados miembros deben comprometerse a la creación de Sandboxes de escala europea. Sería deseable articular mecanismos de apoyo a las empresas en función de métricas como su tamaño o nivel de facturación, así como a agentes de desarrollo tecnológico e innovación en IA aplicada sobre retos económicos y sociales, que facilite la entrada y desarrollo de proyectos sobre los Sandbox regulatorios para garantizar el *level playing field*, la competencia y la innovación.
- **IA ética y confiable**: es necesario explicitar en forma de valor en el mercado las propuestas de valor basadas en IA que cumple cuatro principios básicos de toda IA ética y confiable: (1) IA que genera resultados justos, (2) transparente y explicable en cuanto a sus decisiones o prescripciones, (3) al servicio de las personas y (4) que garantice los máximos niveles de privacidad y seguridad desde el diseño.
- **La AI Act establece que los desarrolladores de IA basada en fuente abierta**, open source, no están sujetos a la regulación. Sin embargo, esta exención solo se aplica cuando los componentes no se comercializan o utilizan por un proveedor como parte de un sistema de IA de alto riesgo. Los desarrolladores no estarán obligados a cumplir los requisitos incluso si el tercero utiliza sus modelos de código abierto, pero si el tercero construye un nuevo producto por encima del componente de código abierto, estará obligado a certificarse. Será sin duda necesario ver en la práctica cómo estas excepciones y obligaciones se despliegan sin que afecten al valor que supone para la industria digital el impulso de ecosistemas de fuente abierta y su posterior traducción en productos de alto valor añadido basados en IA.

- **Implantar y desarrollar nuevos marcos de seguridad.** Aplicar y desarrollar nuevos marcos de seguridad de la IA dirigidos por los gobiernos. Para esta acción se considera oportuno aprovechar los éxitos y las buenas ideas de otros. En este caso, existe una importante oportunidad de aprovechar el trabajo realizado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST).
- **Requerir a los operadores de infraestructuras críticas que incorporen "frenos de seguridad" eficaces** para que los sistemas de IA puedan controlar el funcionamiento de estas.
- **Definir la clase de sistema de IA de alto riesgo que controlan las infraestructuras críticas** y que garanticen las medidas de seguridad como parte de un enfoque integral de la gestión del sistema.
- **Los sistemas de IA que controlan el funcionamiento de infraestructuras críticas designadas se desplegarían únicamente en centros de datos de IA autorizados** que garanticen una segunda capa de protección para aplicar estos frenos de seguridad, garantizando así un control humano.
- **Desarrollar un marco jurídico y normativo más amplio basado en la arquitectura tecnológica de la IA.**
- **Promover la transparencia y garantizar el acceso académico y público a la IA.**
- **Promover la colaboración público-privada para utilizar la IA como herramienta eficaz para abordar los inevitables retos sociales** que conllevan las nuevas tecnologías. Definición de grupos de interés externos para la mejora de la implementación de la AI Act.
- **Favorecer la formación y capacitación sobre IA** y/o acceso a documentación que facilite el entendimiento y/o cumplimiento de la AI ACT.

1. INTRODUCCIÓN

AMETIC es la asociación representante del sector de la industria digital en España, agrupa a empresas e instituciones líderes en transformación digital. AMETIC tiene como misión impulsar el desarrollo de una industria digital y tecnológica robusta e innovadora que contribuya a la competitividad y el crecimiento sostenible de nuestro país.

El objetivo de este documento es presentar la posición de AMETIC sobre la propuesta de regulación de la Inteligencia Artificial (AI Act) presentada por la Comisión Europea el 21 de abril de 2021. Esta propuesta pretende introducir un marco común de normas y principios legales para la Inteligencia Artificial, basado en un enfoque de riesgo y en el respeto a los valores y derechos fundamentales de la Unión Europea.

Este documento se basa en el análisis del texto de la propuesta de regulación y en las aportaciones y experiencias de los asociados de AMETIC, que representan a toda la cadena de valor de la industria digital. También, se tiene en cuenta el contexto y el proceso legislativo de la AI Act, así como las opiniones y recomendaciones de otras organizaciones empresariales y tecnológicas a nivel nacional, europeo e internacional.

El documento se estructura tras un breve resumen ejecutivo en 5 apartados:

1. Introducción, orígenes de la inteligencia artificial y fundamentos para la creación de la AI Act, así como una descripción preliminar de la misma.
2. Visión general de la AI Act.
3. Análisis e impacto de la AI Act en la industria y el sector tecnológico desde la perspectiva del sector digital.
4. Exposición de los principios generales que guían la posición de AMETIC sobre la AI Act, identificación de oportunidades y desafíos para las empresas del sector, así como propuestas y recomendaciones del sector
5. Análisis desde un aspecto ético y social de la propuesta de regulación

Contexto y antecedentes de la AI Act

Adoptando la definición de la OCDE[1] sobre la Inteligencia Artificial (IA), es un sistema basado en una máquina que puede, para un conjunto determinado de objetivos definidos por humanos, hacer predicciones, recomendaciones o decisiones que influyan en entornos reales o virtuales. Los sistemas de IA están diseñados para operar con diferentes niveles de autonomía.

La IA puede realizar tareas que antes solo podían delegarse en un humano, como el aprendizaje, la percepción, la organización de la memoria y el razonamiento crítico.

La Inteligencia Artificial ha experimentado un gran desarrollo en las últimas décadas, gracias al avance de la informática, que ha permitido crear ordenadores más potentes y capaces de procesar grandes cantidades de datos. Algunos campos que se han beneficiado de la IA son el aprendizaje automático, las redes neuronales, el procesamiento del lenguaje natural o la visión artificial.

Sin embargo, la IA también plantea una serie de desafíos y riesgos para la sociedad, como la seguridad, la transparencia, la privacidad, la ética o los derechos fundamentales de las personas. Por ello, se hace necesario establecer un marco legal común que regule el uso de la IA y garantice su confianza y responsabilidad.

[1] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Los inicios de la IA

El concepto de Inteligencia Artificial se acuñó por primera vez en la conferencia de Dartmouth en 1956, donde se reunieron varios científicos para discutir sobre el potencial de las máquinas para simular procesos cognitivos humanos. Uno de esos científicos fue John McCarthy, quien definió la IA como "la construcción de programas informáticos que se dedican a tareas que actualmente son realizadas de forma más satisfactoria por los seres humanos porque requieren procesos mentales de alto nivel".

A partir de aquí, y hasta los años 80, la IA pasó por varias etapas de auge y declive, según los avances y las limitaciones que se encontraba la tecnología en cada momento.

En los años 1990 y 2000, la IA experimentó un nuevo impulso gracias al aumento de la potencia computacional, el acceso a internet y la disponibilidad de grandes volúmenes de datos.

Finalmente, en estas primeras décadas del siglo XXI, la Inteligencia Artificial ha alcanzado niveles sin precedentes, en cuanto a sofisticación y rendimiento, gracias al uso de técnicas como el aprendizaje profundo (deep learning), que consiste en entrenar redes neuronales con múltiples capas ocultas para resolver problemas complejos. Algunos ejemplos famosos de su uso son el programa AlphaGo, que venció al campeón mundial del juego Go, Lee Sedol, el sistema Watson que ganó el concurso Jeopardy, o el generador de texto GPT que puede producir textos coherentes y verosímiles a partir de una entrada dada.

La AI Act

Ante este panorama tan dinámico y diverso de la Inteligencia Artificial, la Unión Europea decidió elaborar un nuevo Reglamento destinado a regular algunos aspectos sobre su uso. La nueva norma (popularmente conocida como “AI Act”), presentada en abril de 2021, fue aprobada por el Parlamento Europeo en una votación celebrada el 14 de junio de 2023. Momento a partir del cual se ha iniciado la fase de negociación entre el Parlamento, el Consejo y la Comisión Europea en los llamados trílogos, con el objetivo de dar vigencia y validez legal a la normativa antes de 2026.

La AI Act tiene como objetivo establecer un marco legal común para garantizar la seguridad, la transparencia y el respeto a los derechos fundamentales de las personas que interactúan con los sistemas de IA. Se basa en los principios éticos definidos por el Grupo Europeo sobre Ética en Ciencia y Nuevas Tecnologías (EGE) y por las Directrices sobre Ética en Inteligencia Artificial elaboradas por un grupo independiente de expertos designado por la Comisión Europea.

La AI Act prevé la creación de un **Comité Europeo de Inteligencia Artificial** que se encargará de asesorar y apoyar a la Comisión Europea en la aplicación del Reglamento. El Comité estará formado por representantes de los Estados miembro y de las partes interesadas (como la sociedad civil, la industria o el mundo académico).

La AI Act también establece un sistema de **supervisión y control** basado en la cooperación entre las autoridades nacionales y la Comisión Europea. El sistema incluye mecanismos para verificar el cumplimiento de los requisitos, sancionar las infracciones y retirar del mercado los sistemas que supongan un riesgo inaceptable.

La importancia de la AI Act

La AI Act es una norma pionera a nivel mundial que pretende regular el uso de la Inteligencia Artificial en la Unión Europea. La norma tiene una gran importancia tanto para los ciudadanos como para las empresas que desarrollan o utilizan sistemas de IA.

Para los ciudadanos, la AI Act supone una garantía de que sus derechos fundamentales serán respetados y protegidos cuando interactúen con sistemas de IA. También ofrece información y transparencia sobre el funcionamiento y el propósito de los sistemas de IA, así como mecanismos para ejercer su control y supervisión. Adicionalmente, busca fomentar la confianza y la aceptación social de la Inteligencia Artificial como una tecnología beneficiosa para la sociedad.

Para las empresas, la AI Act supone una oportunidad para impulsar la innovación y la competitividad en el ámbito de la Inteligencia Artificial. Les ofrece un marco legal claro y armonizado para desarrollar y comercializar sus productos y servicios de IA en todo el mercado único europeo. También, les incentiva a adoptar buenas prácticas y estándares éticos que mejoren la calidad y la seguridad de sus sistemas de IA. Asimismo, busca promover el liderazgo y la excelencia europeos en el campo de la Inteligencia Artificial como una tecnología estratégica para el futuro.

2. VISIÓN GENERAL DE LA AI ACT

Resumen de los principales puntos de la AI Act

La AI Act sigue un planteamiento basado en riesgo, con el objetivo de crear un marco jurídico para todos los Estados Miembros que sea uniforme y horizontal. Para ello, establece el ámbito de aplicación y el objeto del Reglamento, definiendo los sistemas de IA, las prácticas que se consideran prohibidas y las distintas clasificaciones de riesgo y sus requisitos. Además, de fomentar la inversión y la innovación en IA, mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y seguridad.

Para el logro de dichos objetivos, la AI Act se ha basado en la siguiente estructura. Primero, en el Título I define su objeto y ámbito de aplicación, las cuales abarcan la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA. Además, para lograr una mayor seguridad jurídica, se establecen las definiciones específicas utilizadas en el Reglamento, entre ellas, principalmente, la de los "sistemas de IA", definición que pretende ser lo más tecnológicamente neutra posible y resistir a la rápida evolución tecnológica que hay en el mercado. También se proporciona una definición clara de las principales figuras en la cadena de valor de la IA, tales como los proveedores y los usuarios de sistemas de IA.

Tras este Título I, el Reglamento trata los Sistemas de IA de Uso General y, las prácticas de IA prohibidas. Así, en el Título II se abarcan todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la Unión. Entre otros usos, se prohíbe el uso de sistemas de IA que exploten las vulnerabilidades de un grupo específico de personas debido a su situación social o económica, la identificación biométrica remota, con ciertas excepciones, y el denominado social scoring.

Posteriormente, en el Título III, se definen y se clasifican las tipologías de IA de Alto Riesgo, los requisitos que deben tener, las obligaciones de los proveedores de estos Sistemas de IA y la evaluación que se debe de llevar a cabo para dichos sistemas. Así, en concordancia con el enfoque basado en riesgo, los sistemas de IA de alto riesgo están permitidos en el mercado europeo siempre que cumplan determinados requisitos obligatorios y sean sometidos a una evaluación de conformidad "ex ante".

La AI Act procede, en su Título IV, a determinar las obligaciones de transparencia de los proveedores y usuarios de determinados sistemas de IA por los riesgos concretos que estos acarrean. Por ejemplo, cuando una persona interactúe con un sistema de IA y sus emociones o características sean reconocidas por medios automatizados, es necesario que sea informada sobre esta condición o si un sistema de IA se utiliza para generar o manipular imágenes, audios o vídeos que a simple vista parezcan contenido auténtico, debe ser obligatorio informar de que dicho contenido se ha generado por medios automatizados.

Por otro lado, el Reglamento tiene varias previsiones y medidas dirigidas a crear un marco jurídico más favorable a la innovación y a promover el aprendizaje normativo. En particular, se promueven los espacios aislados de regulación de la IA, los denominados Sandbox regulatorios, que tienen por objeto establecer un entorno controlado para el desarrollo, prueba y validación de sistemas innovadores de IA.

Finalmente, AI Act crea un marco para la elaboración de códigos de conducta, cuyo objetivo es fomentar que los proveedores de sistemas de IA que no son necesariamente

de alto riesgo cumplan de manera voluntaria los requisitos que son obligatorios para los sistemas de IA de alto riesgo.

Alcance y aplicabilidad de la regulación propuesta

La AI Act adopta un enfoque basado en la valoración de riesgo, es decir, establece requisitos distintos para los sistemas de IA según el nivel de impacto que puedan tener en la sociedad. Así, pues, la AI Act clasifica los sistemas de IA en cuatro categorías:

1. Sistemas **inaceptables**. Son aquellos que suponen una amenaza clara para la seguridad, los derechos fundamentales o los valores democráticos.

2. Sistemas **de alto riesgo.** Son aquellos que pueden afectar a aspectos esenciales como la salud, la seguridad o los derechos fundamentales. Estos sistemas están sujetos a requisitos estrictos por parte de la AI Act.

3. Sistemas **de riesgo limitado**. Son aquellos que pueden implicar algún tipo de interferencia con los derechos fundamentales.

4. Sistemas **de riesgo mínimo**. Son aquellos que tienen un impacto insignificante en los derechos fundamentales.

Los requisitos que deben cumplir los sistemas **de alto riesgo** son:

- Realizar una evaluación previa del riesgo antes de ponerlos en el mercado.
- Implementar medidas adecuadas para garantizar su calidad, seguridad y robustez.
- Garantizar un alto nivel de transparencia sobre su funcionamiento, propósito y limitaciones.
- Facilitar información clara e inteligible a sus usuarios finales.
- Asegurar una supervisión humana efectiva sobre su uso.
- Implementar mecanismos adecuados para registrar su funcionamiento, corregir sus errores y permitir su auditoría.
- Respetar las normas sobre protección de datos personales y privacidad.
- Cooperar con las autoridades competentes para garantizar el cumplimiento de la AI Act.

Los requisitos que deben cumplir los sistemas **de riesgo limitado** son:

- Informar a los usuarios finales de que están interactuando con un sistema de IA y no con un humano.
- Revelar el uso de técnicas de generación o manipulación de contenido y advertir de su posible falta de autenticidad.

Los requisitos que deben cumplir los sistemas **inaceptables** son:

- No se pueden desarrollar, ni proporcionar o utilizar bajo ninguna circunstancia.

Adicional a los requisitos referenciados entendemos que deberían cumplir otros aspectos que permitan tener conocimiento de la situacion tales como:

- Facilitar información clara e inteligible a sus usuarios finales.
- Implementar mecanismos adecuados para registrar su funcionamiento, corregir sus errores y permitir su auditoría.
- Informar a los usuarios finales de que están interactuando con un sistema de IA y no con un humano.
- Revelar el uso de técnicas de generación o manipulación de contenido y advertir de su posible falta de autenticidad.

3. ANÁLISIS E IMPACTO DE LA AI ACT EN LA INDUSTRIA Y EL SECTOR TECNOLÓGICO

Evaluación de los aspectos positivos de la regulación

La AI Act introduce en el proyecto de regulación múltiples aspectos positivos a destacar:

- Dirección y ambición: al redactar AI Act e integrar nuestras normas y valores en la arquitectura y la infraestructura de nuestra tecnología, la UE proporciona una dirección y conduce al mundo hacia un destino significativo y ambicioso. De alguna forma nos encontramos ante una ambición similar el RGPD, que ahora se ha convertido en el estándar internacional de privacidad, protección de datos y soberanía de datos.

- Toda Europa, todas las industrias: AI Act establece normas horizontales para el desarrollo, comercialización y uso de productos, servicios y sistemas basados en IA para todo el territorio de la UE. El proyecto de Reglamento establece un núcleo de normas de Inteligencia Artificial aplicables a todas las industrias. La Ley de IA de la UE introduce un sofisticado «marco de seguridad de los productos» construido en torno a un conjunto de cuatro categorías de riesgo, suficientemente concreto y certero en relación a los retos presentes y futuros de la IA.

- Protección a la innovación: AI Act tiene por objeto evitar que las normas socaven la innovación, evitando en la medida de lo posible obstáculos al crecimiento de un ecosistema de IA propio en Europa. Esto se garantiza mediante la introducción de varias herramientas de flexibilización y excepciones, incluida la aplicación de Sandbox regulatorios que permitan espacios de experimentación a instituciones de investigación, empresas innovadoras y startups. Así pues, el concepto de Sandbox regulatorio busca equilibrar los intereses divergentes, incluidos los ligados con valores europeos, económicos y sociales. Eso significa que sin duda durante su etapa de negociación se harán concesiones, pero es de esperar que el mecanismo de Sandbox regulatorio impida que la propuesta quede plagada de compromisos inviables.

- Impulso a una IA confiable: la IA responsable y confiable requiere la conciencia de todas las partes involucradas. La manera en que diseñamos nuestra tecnología está dando forma al futuro de nuestra sociedad. En esta visión los valores democráticos y los derechos fundamentales desempeñan un papel fundamental. La AI Act introduce herramientas indispensables para facilitar una IA confiable mediante procesos de sensibilización, evaluaciones del impacto y la conformidad de la IA, el impulso de mejores prácticas y códigos de conducta. Estas herramientas serían empleadas por equipos multidisciplinares, que las utilizarían para supervisar, validar y evaluar los sistemas de IA. Las nuevas normas europeas derivadas de la AI Act cambiarán para siempre la forma en que se genera valor con la IA, estableciendo la necesidad de modelos y técnicas fiables por diseño y construcción.

- Huella ecológica: por otra parte, consciente de la elevada huella de carbono e hídrica de las infraestructuras que generan servicios de IA masivos, se presta atención al medio ambiente y a la sostenibilidad. La huella ecológica de las tecnologías ligadas a la IA debe mantenerse lo más pequeña posible y, a su vez, la aplicación de la IA debe apoyar los avances sociales y medioambientales. Esto se ajusta al artículo 37 de la Carta de los Derechos Fundamentales de la UE y el Green Deal de la UE, que lucha por la descarbonización de nuestra sociedad.

Desafíos y preocupaciones identificados

Resaltamos tres desafíos relevantes para la regulación de la Inteligencia Artificial que propone el Reglamento de la AI Act:

1. Incertidumbres propias de un primer intento
   Cualquier intento de regulación en un campo donde el mercado ha estado autorregulado o limitadamente regulado como es el caso de la IA introduce reacciones negativas, destacando los desafíos de la nueva regulación o las incertidumbres que genera. AI Act es sin duda un intento pionero de establecer un primer marco regulador global para la IA, centrado en lograr un equilibrio entre el riesgo, la innovación y las consideraciones éticas. A su vez, se trata de una primera regulación que se desarrolla en paralelo a otras relevantes, como el *Cyber Resiliency Act* que tiene por objeto imponer obligaciones de ciberseguridad a todos los productos con elementos digitales (incluidos los sistemas basados en IA) cuyo uso previsto y previsible incluya la conexión directa o indirecta de datos a un dispositivo o red. El despliegue de la AI Act y sus implicaciones en la industria de la IA generará una narrativa clave mientras navegamos en un futuro cada vez más definido por la IA, tanto en su aspecto de impacto económico como sobre todo social.

2. Incertidumbres propias de un campo en constante evolución
   En el momento de la génesis de la AI Act, tecnologías como la IA generativa eran poco conocidas en la sociedad. Hoy día la explosión de servicios de IA generativa para imagen, texto o incluso multimodales ha colocado a esta tecnología como un elemento clave de regulación. Sin embargo, el desarrollo de la IA no se detiene, y no son pocos los expertos en el desarrollo de métodos y técnicas hacia la llamada "IA General" que especulan sobre el impacto que puede tener su aparición, como una suerte de "día cero" de la Inteligencia Artificial. La actual AI Act menciona la "IA de propósito general" como una IA multimodal que puede tener aplicaciones en campos para los que no fue definida, a priori, pero no entra (a pesar de las múltiples sugerencias recibidas) a tratar los desafíos que podría generar la aparición de una IA General real. Otro de los desarrollos prácticos con potencial de alterar los cimientos de nuestra concepción de la IA actual es el relacionado con la computación cuántica y su potencial disruptor. En este sentido, se echa en falta alguna consideración sobre los mecanismos de control necesarios para que dichos desarrollos no sobrepasen el marco regulatorio previsto.

3. Incertidumbres sobre el desarrollo de la IA en campos de aplicación excluidos, en particular el militar.
   Es relevante recordar que la AI Act excluye las aplicaciones en Defensa, donde la conversión de la IA en arma o como elemento central de armas ya muestra un grado de desarrollo difícil de controlar.

Efectos previstos de la AI Act en la industria tecnológica

Conscientes del inmenso potencial, así como de los graves riesgos que el uso inadecuado de la Inteligencia Artificial puede conllevar, la industria y el sector tecnológico han recibido positivamente la idea de que exista legislación específica para regularla, desde su concepción y desarrollo hasta su despliegue en productos, servicios y herramientas.

Se prevé que AI Act:

- Brinde mayor seguridad jurídica a las empresas.
- Defina clara y unívocamente qué se entiende por IA.
- Catalogue sus posibles tipos y usos, aclarando cuáles son permisibles, cuáles no y bajo qué circunstancias.
- Especifique qué condiciones han de cumplir los sistemas basados en o que contengan IA y que entrañen un riesgo para la seguridad o derechos fundamentales de los ciudadanos.
- Especifique diversos roles y responsabilidades de las organizaciones según su posición y papel en la cadena de valor de la IA.
- Defina cómo ha de evaluarse el cumplimiento de la normativa.
- Defina las consecuencias de posibles incumplimientos por proveedores y usuarios.

En ausencia de legislación, es probable que se diera un escenario en el que – por mala fe, negligencia u otras causas – se hiciera un mal uso de la IA o se originasen impactos potencialmente muy negativos sobre la sociedad, los estados y los negocios.

Con una AI Act armonizada, se potenciará la inversión en IA y su uso, y se minimizarán los posibles efectos negativos. Sin embargo, una redacción no equilibrada de la ley puede llevar a que en la Unión Europea se paralicen o minimicen las inversiones en IA, a que su uso no sea extendido, a que no se materialice todo el valor potencial, a que se excluya de los beneficios de la IA a ciertos segmentos de la población o de la industria (como PYME o start-ups), entre otros.

Oportunidades y desafíos para las empresas del sector

Las principales oportunidades se derivan de la seguridad, confianza y transparencia que la normativa aportaría:

- El potencial aumento de inversión y financiación para la IA en la UE, de fuentes internas y externas.
- El desarrollo de un ecosistema tecnológico e innovador más fuerte.
- La adopción extendida de la IA por parte de todos los sectores: mayor demanda de productos y servicios basados en la IA, mayor volumen de mercado, mayor creación de empleo.
- La claridad en los usos aceptables, las condiciones a cumplir y los papeles de cada *stakeholder* de la cadena de valor.
- Claridad en los procesos de certificación o cumplimiento, para los casos de riesgo en los que sea requerido.
- El desarrollo de soluciones europeas de cumplimiento que fijen un estándar de IA responsable a nivel internacional.
- La mejora generalizada de la calidad de los datos en las organizaciones que habilite el desarrollo de nuevos casos de uso.
- La certidumbre, para empresas que tratan datos sensibles, de que existe un proceso armonizado para el correcto desarrollo de sistemas de alto riesgo.
- A medida que la regulación permee en países ajenos a la Unión Europea, podrá originar oportunidades de negocio en proyectos internacionales a las

compañías europeas, que contarán con mayor experiencia, frameworks y mejores prácticas en el desarrollo de sistemas que cumplan con los requisitos.

Los principales desafíos se derivan del ámbito de aplicación y de los procesos de certificación o cumplimiento de la normativa:

- Una definición excesivamente amplia de la IA comprendería casos de *big data*, analítica de datos o estadística que no son IA, lo que podría hacer el cumplimiento inabordable por su extensión. Una definición excesivamente restrictiva, por el contrario, dejaría usos relevantes fuera de la aplicación, creando desigualdades entre sectores, aplicaciones o tipos de empresas.
- Si los procesos de cumplimiento son complicados, numerosos y solapados y no se basan en la autoevaluación responsable (i.e., requieren de terceros), el uso de la IA en la UE se estancará por el coste y demora asociados al proceso del cumplimiento. Esto afectará a todos los sectores y *stakeholders*, pero todavía más a las PYME, con un impacto negativo en la innovación y la competitividad.
- Si no se define adecuadamente la cadena de valor de la IA y/o no se asignan correctamente las responsabilidades de cada parte, la colaboración en IA desde la investigación hasta el negocio se verá dañada, causando igualmente un parón de actividad.

Recomendaciones específicas para abordar los impactos sectoriales

- Una definición correcta de qué es IA, del ámbito de la AI Act, consensuada con el sector tecnológico que invierte, la produce y ayuda a desplegar.
- Una definición correcta de la cadena de valor de la IA y las responsabilidades de cada parte, consensuada con el sector tecnológico.
- Procesos de evaluación y cumplimiento basados lo más posible en la autoevaluación responsable, que optimicen el cumplimiento en tiempo y costes. En particular, ha de evitarse que el proceso de cumplimiento en Europa se convierta en un negocio que encarezca innecesariamente toda actividad en IA haciendo que Europa pierda competitividad, así como la necesidad de re-certificar o re-evaluar sistemas o modelos cada vez que haya que reentrenarlos o recalibrarlos.
- La extensión del uso de Sandboxes que permitan experimentar el impacto en el cumplimiento de nuevos modelos, sistemas o aplicaciones. Sería deseable articular mecanismos de apoyo a las empresas en función de métricas como su tamaño o nivel de facturación, así como a agentes de desarrollo tecnológico e innovación en IA aplicada sobre retos económicos y sociales, que facilite la entrada y desarrollo de proyectos sobre los Sandbox regulatorios para garantizar el *level playing field,* la competencia y la innovación.
- IA ética y confiable: es necesario explicitar en forma de valor en el mercado las propuestas de valor basadas en IA que cumple cuatro principios básicos de toda IA ética y confiable: (1) IA que genera resultados justos, (2) transparente y explicable en cuanto a sus decisiones o prescripciones, (3) al servicio de las personas y (4) que garantice los máximos niveles de privacidad y seguridad desde el diseño.
- El sector tecnológico y digital tiene dinámicas complejas de trabajo en ecosistema cuando se aplica alguno de los innumerables modelos de licenciamiento de fuente abierta que facilitan el avance de un determinado

producto software en base a la colaboración de competidores potenciales. Una vez alterado el licenciamiento para generar un producto comercial con licenciamiento cerrado (si es que es posible) pueden permanecer obligaciones derivadas de las licencias abiertas previas. En relación con AI Act se ha generado incertidumbre en base a la IA desarrollada en ecosistemas de fuente abierta. AI Act establece que los desarrolladores de IA basada en fuente abierta no están sujetos a la regulación. Sin embargo, esta exención solo se aplica cuando los componentes no se comercializan o utilizan por un proveedor como parte de un sistema de IA de alto riesgo. Los desarrolladores no estarán obligados a cumplir los requisitos incluso si el tercero utiliza sus modelos de código abierto, pero si el tercero construye un nuevo producto por encima del componente de código abierto, estará obligado a certificarse. Será sin duda necesario ver en la práctica cómo estas excepciones y obligaciones se despliegan sin que afecten al valor que supone para la industria digital el impulso de ecosistemas de fuente abierta y su posterior traducción en productos de alto valor añadido basados en IA.

4. POSICIONAMIENTO DE AMETIC

Declaración de posición de AMETIC sobre la AI Act

Apoyamos los esfuerzos de la UE para implementar un enfoque efectivo basado en el riesgo para la regulación de la IA que proteja los derechos civiles y, al mismo tiempo, permita la innovación continua y la aplicación práctica de esta importante tecnología. Al igual que otras tecnologías, la mayoría de los riesgos asociados con la IA no se encuentran en los sistemas de IA en sí mismos, sino en la aplicación de la tecnología y en casos de uso específicos.

Sin duda, la IA se utilizará para abordar algunos de los mayores desafíos a los que se enfrenta la sociedad, desde la seguridad alimentaria, el cambio climático y la seguridad energética, hasta la seguridad de la cadena de suministro. Por lo tanto, los requisitos deben orientarse para garantizar las salvaguardas apropiadas sin limitar involuntariamente los usos que no suponen un riesgo y que, posiblemente, salven vidas.

En la AI Act, los responsables políticos deben equilibrar adecuadamente dos conjuntos de intereses: por un lado, los ciudadanos y la industria de la UE deberían poder disfrutar de los beneficios personales, económicos y sociales que la IA puede producir. Por otro lado, la UE debe contar con las políticas adecuadas para mitigar los riesgos y proteger a los ciudadanos de daños significativos que pudieran surgir. Para trílogos de la AI Act, recomendamos:

- Ajustar la definición de IA y adaptar la categorización de IA de alto riesgo y prohibida para garantizar que el alcance de ésta esté vinculado a los riesgos reales.
- Garantizar obligaciones proporcionadas, claras y técnicamente viables para la IA de alto riesgo.
- Adoptar esquemas internacionales para fomentar la interoperabilidad global, como las definiciones y estándares de conducta acordados por la OCDE.

El legislador debe adoptar un enfoque pragmático abordando solo cuestiones clave claramente identificadas para las cuales existe consenso. Hacer lo contrario supondría el riesgo de retrasar la adopción de la AI Act. Este enfoque pragmático también debería garantizar que las obligaciones y restricciones estén justificadas y respaldadas por pruebas claras. Solo una AI Act que proporcione respuestas claras, efectivas y proporcionadas a los riesgos reales servirá como un modelo atractivo y poderoso también para los reguladores y legisladores fuera de la UE.

Propuestas concretas

Desde AMETIC ofrecemos algunas sugerencias para la mejora de las realidades del ecosistema de IA en la actualidad y en el futuro.

1) **Las prohibiciones deberían limitarse rigurosamente a casos de uso específicos**

- **Inferir a las emociones** (Art. 5): El Parlamento ha propuesto prohibir cualquier inferencia de emociones en el lugar de trabajo. Esto es muy amplio y no está respaldado por ninguna evidencia o análisis de riesgo. En la práctica, esta propuesta corre el riesgo de prohibir muchos casos de uso que no suponen ningún riesgo y son altamente beneficiosos, como el uso de IA para la seguridad del tráfico, la predicción del estado cognitivo de operadores de maquinaría sensible o la prescripción en la asignación de turnos de trabajo basada en factores emocionales en líneas de producción. Ni la propuesta de la Comisión, ni el Enfoque General del Consejo incluyen esta disposición.

Propuesta: rechazar la propuesta del Parlamento de prohibir la inferencia de emociones en el lugar de trabajo y evitar la manipulación de las emociones con fines que atenten contra los derechos de privacidad, intimidad y laborales. En cualquier caso, muchos usos de la IA en el lugar de trabajo caerán en la categoría de alto riesgo, Anexo III.

2) <u>La IA de alto riesgo debería limitarse a casos de uso específicos que puedan causar daño significativo y no es puramente accesorio</u>

- **Definición de IA de "alto riesgo"** (Art. 6): muchas categorías de alto riesgo reflejadas en el Anexo III no están concretadas; algunos incluso incluyen sectores enteros. Cualquier IA definida como de alto riesgo debe cumplir con amplios requisitos reglamentarios. Deben evitarse cargas injustificadas para la IA que no supongan un riesgo a fin de no obstaculizar la innovación en la UE.

  Propuesta: apoyar la propuesta del Consejo que excluye de la definición de "alto riesgo" los sistemas de IA cuyo resultado es "puramente accesorio". Además, apoyar la propuesta del Parlamento que limita la clasificación de alto riesgo a la IA que impone un riesgo significativo de daño a la salud, la seguridad y los derechos fundamentales. El "daño significativo" debe especificarse de manera que se centre en los riesgos materiales adversos.

3) <u>Asignación de responsabilidades y AI de propósito general / generativa</u>

- **IA de Propósito General** (GPAI) (Art. 4b, c): el Consejo propone que GPAI, un término general para las herramientas de IA neutrales de uso común, como la conversión de voz a texto o el reconocimiento de objetos, debe estar sujeta a una selección de los requisitos para los sistemas de alto riesgo especificados por la Comisión Europea. Esto supone el riesgo de extralimitación regulatoria ya que la GPAI a menudo se implementa en casos de uso que no suponen un riesgo, por ejemplo, software de traducción de voz en un videojuego. Debido a su naturaleza, los sistemas GPAI no tienen un 'propósito previsto' y los proveedores de GPAI no necesariamente saben si el cliente implementa la IA en un caso de uso de alto riesgo o si se basa en ella para desarrollar un sistema de IA entrenando el sistema con nuevos datos para cumplir con un propósito determinado, agregando nuevas características y/o integrándolo en otro sistema de IA. Estos clientes son los más indicados para saber si puede surgir un riesgo potencial con su uso específico del sistema GPAI. En algunas circunstancias, la GPAI se desarrolla y se implementa dentro de la misma empresa. En estas situaciones, el desarrollador y el implementador son la misma entidad que tiene control total y certeza sobre si la GPAI se implementará en un caso de uso de alto riesgo o no.

  Propuesta: la GPAI no debe considerarse IA de alto riesgo. La legislación de la GPAI debe consistir en requisitos personalizados y técnicamente factibles basados en estándares existentes y principios interoperables como los de la OCDE. Apoyar la propuesta del Consejo de que los implementadores deben tener la oportunidad de aclarar en las instrucciones de uso que una GPAI no debe implementarse en áreas de alto riesgo, considerando situaciones en las que el desarrollador tiene el control total del despliegue. El desarrollador de GPAI debe tener la obligación de apoyar al implementador de GPAI para garantizar el cumplimiento cuando sea necesario (similar a los mecanismos del Reglamento General de Protección de Datos en el Art. 28).

- **Modelos Fundacionales (FM)**: el Parlamento propone la regulación de los FM, basándose en una definición que se superpone en parte con la propuesta GPAI del Consejo. Se supone que los requisitos específicos propuestos para los FM se aplican independientemente de si el FM se puede utilizar para un sistema de alto riesgo. Los

requisitos seleccionados también incluyen obligaciones específicas de derechos de autor para FM que se utilizan como IA generativa (por ejemplo, divulgar datos de entrenamiento protegidos por la ley de derechos de autor). Varios de estos requisitos para los FM imponen altas cargas de cumplimiento. Algunos no son técnicamente factibles (p. ej., entrenamiento solo con conjuntos de datos especialmente diseñados). Esto prohibiría de facto el desarrollo de FM que son modelos de lenguaje extenso (LLM), ya que los LLM se entrenan esencialmente en Internet. Dichas reglas socavarían los objetivos de la Ley de IA, ya que los LLM pueden aumentar significativamente la productividad y mejorar la competitividad de la UE.

Propuesta: los FM no deben considerarse, en general, de alto riesgo. En caso de que las instituciones de la UE en trílogo acuerden imponer obligaciones a los FM, estas deben ser proporcionadas, técnicamente factibles y alineadas con legislación europea y con estándares internacionales y principios de interoperabilidad como los acordados en la OCDE. Se deberían considerar los mecanismos existentes sobre extracción de texto y datos incluidos en la Directiva de derechos de autor de la UE y la jurisprudencia, como motores de búsqueda e índices. Esto evitaría sobrecargar las negociaciones específicas de la AI.

- **Responsabilidad en la cadena de valor**: la terminología de IA Act (por ejemplo, "proveedor" y "usuario") propuesta por la Comisión y el Consejo no distingue suficientemente entre roles en la cadena de valor de IA (es decir, desarrolladores de IA, implementadores, usuarios finales, y otros actores); y las obligaciones de la Act no consideran los diferentes roles de estas partes, ni brindan claridad sobre qué partes son responsables. Las empresas quieren entender claramente cómo y cuándo cumplir con los requisitos legales. Los implementadores suelen ser los más adecuados para saber si su caso de uso será de alto riesgo pero también tener problemas con los requisitos relacionados con el desarrollo. Por lo general, los desarrolladores no están bien ubicados para certificar los requisitos relacionados con el caso de uso.

  Propuesta: para garantizar la claridad legal, las obligaciones deben dirigirse principalmente al actor mejor ubicado para cumplir con los requisitos. Esto incluiría el reconocimiento por parte del desarrollador del uso de su IA en un sistema de alto riesgo, las obligaciones específicas de las que sería responsable el desarrollador y la obligación del desarrollador de ayudar con las solicitudes de una autoridad nacional. Este mecanismo no se aplicaría en situaciones en las que el desarrollador de GPAI haya aclarado en las instrucciones de uso que la GPAI no debe utilizarse en un caso de uso de alto riesgo (ver más arriba las sugerencias sobre GPAI). Este enfoque equilibrado inspirado en el Reglamento General de Protección de Datos garantizaría el cumplimiento por parte del implementador habilitado por el desarrollador. Además, se deben aclarar las terminologías, particularmente entre los desarrolladores de IA (es decir, aquellos que ponen a disposición IA modelos preentrenados y similares), implementadores (es decir, aquellos que implementan un sistema de IA o que implementan el caso de uso para usuarios finales) y usuarios finales (es decir, consumidores o aquellos que usan IA para uso personal). Deben aclararse las responsabilidades por las obligaciones, en particular con respecto a los sistemas de IA de alto riesgo. Tanto el Consejo como el Parlamento incluyen propuestas útiles en este contexto que deberían especificarse más detalladamente.

Relación con otra reglamentación

Debido a su carácter horizontal, la propuesta debe ser plenamente coherente con la legislación vigente de la Unión Europea y de los estados miembros aplicable a los sectores donde ya se utilizan o es probable que se utilicen en un futuro próximo sistemas de IA de alto riesgo. A nivel europeo, existe una serie de normas jurídicamente vinculantes, tanto a nivel nacional como internacional, que ya se vienen aplicando o son relevantes para el desarrollo, despliegue y uso de sistemas de IA. Las fuentes legales incluyen, pero no se limitan a: Derecho primario de la UE (los Tratados de la Unión Europea y su Carta de los Derechos Fundamentales), Derecho derivado de la UE (como el Reglamento general de protección de datos (la Directiva sobre responsabilidad por productos defectuosos, el Reglamento sobre la libre circulación de datos no personales, las Directivas contra la discriminación, el Derecho de los consumidores y las Directivas sobre seguridad y salud en el trabajo), los tratados de derechos humanos de las Naciones Unidas y los convenios del Consejo de Europa (como el Convenio Europeo de Derechos Humanos), y numerosas leyes de los Estados miembros de la UE.

Además de las normas aplicables horizontalmente, existen varias reglas específicas de dominio que se aplican a aplicaciones particulares de IA (como, por ejemplo, el Reglamento sobre dispositivos médicos en el sector sanitario).

La AI Act hace énfasis en el respeto y coherencia con el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre protección de datos en el ámbito penal, a los cuales complementa con un conjunto de normas armonizadas aplicables al diseño, el desarrollo y la utilización de determinados sistemas de IA de alto riesgo y con restricciones de determinados usos de los sistemas de identificación biométrica remota. Además, una de las dos bases jurídicas utilizadas por la Comisión Europea para justificar la propuesta de la AI Act es el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), que obliga a la UE a establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Esto significa que, al menos en cierta medida, las normas de la AI Act complementarán las protecciones otorgadas a los interesados en virtud del RGPD, que también se basa en el artículo 16 del TFUE. De hecho, en su Dictamen conjunto de 2021 sobre la Ley de la IA, el Supervisor Europeo de Protección de Datos (SEPD) y la Junta Europea de Protección de Datos (JEPD) han sugerido que el cumplimiento del RGPD sea una condición previa para permitir que un sistema de IA entre en el mercado europeo como producto con marcado CE en virtud de la Ley de la IA.

Otro de los debates normativos que han surgido en torno al AI Act es la cuestión relativa a la propiedad intelectual, especialmente cuando se trata de IA generativa. No obstante, la actual Ley de Propiedad Intelectual no parece dar respuesta a los retos regulatorios que trae el desarrollo de la IA. Dado a esto, inicialmente se planteó prohibir totalmente el uso de material protegido por derechos de autor para entrenar modelos generativos de IA, pero se abandonó la propuesta en favor de un requisito de transparencia. Así, en las últimas enmiendas para la propuesta, se ha decidido añadir la obligación de que los proveedores que utilicen herramientas de IA generativa, tales como ChatGPT, también tendrán que revelar cualquier material protegido por derechos de autor que hayan utilizado para desarrollar sus sistemas.

En cuanto a los sistemas de IA de alto riesgo, que son componentes de seguridad de productos específicos, (p. ej., máquinas, productos sanitarios, juguetes), AI Act se integrará en la legislación sectorial vigente en materia de seguridad para garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas para los proveedores de estos sistemas o productos. En particular, establece que se comprobarán como parte de los procedimientos de evaluación de la conformidad previstos en la legislación

pertinente del nuevo marco legislativo. Por lo tanto, a pesar de que la AI Act busca cubrir los riesgos de seguridad específicos de los sistemas de IA, la legislación busca garantizar la seguridad general del producto final, por lo que podría contener requisitos específicos relativos a la integración segura de un sistema de IA en el producto final.

Finalmente, la promoción de la innovación impulsada por la IA está estrechamente vinculada a la Ley de Gobernanza de Datos, la Directiva relativa a los datos abiertos y otras iniciativas emprendidas en el marco de la Estrategia de Datos de la UE, que establecerán mecanismos y servicios de confianza para reutilizar, compartir y poner en común datos esenciales para el desarrollo de modelos de IA de gran calidad basados en datos. De esta forma, los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas adecuadas de gobernanza y gestión de datos, siendo pertinentes, representativos, completos y libres de errores.

Recomendaciones específicas para abordar los impactos sectoriales

En línea con el punto anterior cabe destacar que todos los comentarios y propuestas que desde AMETIC reflejadas a continuación además de cumplir con la legislación vigente, respetan los derechos a la intimidad en el ámbito laboral que en España se encuentra regulada por diversas leyes, como el Reglamento General para la Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD) y el Estatuto de Trabajadores, unidos a los derechos y libertades recogidas en la Constitución Española.

- Definir correctamente qué es IA, del ámbito de la AI Act, previo consenso con el sector tecnológico que invierte, produce y ayuda a su despliegue.
- Definir correctamente la cadena de valor de la IA y las responsabilidades de cada parte, consensuándola con el sector tecnológico. Clarificar las responsabilidades en toda la cadena de valor de la IA. Cuando proceda, el Reglamento de IA debería aportar una mayor flexibilidad, garantizando la libertad de las partes para asignar responsabilidades a través de obligaciones contractuales.
- Garantizar la armonización del Reglamento con legislación ya vigente, para evitar la duplicación de procedimientos y simplificar el cumplimiento de la normativa en muchos sectores en los que Europa es hoy líder y debe seguir siendo competitiva.
- Designar un punto de contacto centralizado en cada Estado y articular un sólido mecanismo de coordinación para garantizar una aplicación y un cumplimiento coherente.
- Gestionar lo más posible los procesos de evaluación y cumplimiento basándolos en procesos de autoevaluación responsable, que optimicen el cumplimiento en tiempo y costes. En particular, ha de evitarse que el proceso de cumplimiento en Europa se convierta en un negocio que encarezca innecesariamente toda actividad en IA haciendo que Europa pierda competitividad, así como la necesidad de re-certificar o re-evaluar sistemas o modelos cada vez que haya que reentrenarlos o recalibrarlos.
- Utilizar los Sandboxes para testar el impacto potencial de la regulación en las empresas y ayudarles también a prepararse para su cumplimiento. Los Estados miembro deben comprometerse a la creación de Sandboxes de escala europea. Sería deseable articular mecanismos de apoyo a las empresas en función de métricas como su tamaño o nivel de facturación, así como a agentes de desarrollo tecnológico e innovación en IA aplicada sobre retos económicos y sociales, que

facilite la entrada y desarrollo de proyectos sobre los Sandbox regulatorios para garantizar el level playing field, la competencia y la innovación.

- IA ética y confiable: es necesario explicitar en forma de valor en el mercado las propuestas de valor basadas en IA que cumple cuatro principios básicos de toda IA ética y confiable: (1) IA que genera resultados justos, (2) transparente y explicable en cuanto a sus decisiones o prescripciones, (3) al servicio de las personas y (4) que garantice los máximos niveles de privacidad y seguridad desde el diseño.
- AI Act establece que los desarrolladores de IA basada en fuente abierta no están sujetos a la regulación. Sin embargo, esta exención solo se aplica cuando los componentes no se comercializan o utilizan por un proveedor como parte de un sistema de IA de alto riesgo. Los desarrolladores no estarán obligados a cumplir los requisitos incluso si el tercero utiliza sus modelos de código abierto, pero si el tercero construye un nuevo producto por encima del componente de código abierto, estará obligado a certificarse. Será sin duda necesario ver en la práctica cómo estas excepciones y obligaciones se despliegan sin que afecten al valor que supone para la industria digital el impulso de ecosistemas de fuente abierta y su posterior traducción en productos de alto valor añadido basados en IA.
- Implantar y desarrollar nuevos marcos de seguridad. Aplicar y desarrollar nuevos marcos de seguridad de la IA dirigidos por los gobiernos. Para esta acción se considera oportuno aprovechar los éxitos y las buenas ideas de otros. En este caso, existe una importante oportunidad de aprovechar el trabajo realizado hace sólo cuatro meses por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST).
- Requerir a los operadores de infraestructuras críticas que incorporen "frenos de seguridad" eficaces para que los sistemas de IA puedan controlar el funcionamiento de estas.
- Definir la clase de sistema de IA de alto riesgo que controlan las infraestructuras críticas y que garanticen las medidas de seguridad como parte de un enfoque integral de la gestión del sistema.
- Los sistemas de IA que controlan el funcionamiento de infraestructuras críticas designadas se desplegarían únicamente en centros de datos de IA autorizados que garanticen una segunda capa de protección para aplicar estos frenos de seguridad, garantizando así un control humano.
- Desarrollar un marco jurídico y normativo más amplio basado en la arquitectura tecnológica de la IA.
- Promover la transparencia y garantizar el acceso académico y público a la IA.
- Promover la colaboración público-privada para utilizar la IA como herramienta eficaz para abordar los inevitables retos sociales que conllevan las nuevas tecnologías. Definición de grupos de interés externos para la mejora de la implementación de AI Act.

Otros aspectos relevantes a considerar en la regulación

- Favorecer la formación y capacitación sobre IA y/o acceso a documentación que facilite el entendimiento y/o cumplimiento de la AI ACT.

5. CONSIDERACIONES ÉTICAS Y SOCIALES

La Inteligencia Artificial tiene muchos beneficios sociales y puede ayudar a resolver grandes retos de la humanidad que de otra manera podrían llevar muchísimos años o resultaría inviable económicamente o en tiempo.

Ejemplos de cómo puede ser una gran aportación a nuestras vidas son innumerables, potencia los estudios de investigadores, facilita el identificar y entender mejor la realidad; ayuda a determinar grupos vulnerables, mejoras que tienen impacto sobre ellos y a definir políticas que tengan un fuerte impacto social; permite establecer métodos de cultivo óptimos y rentables, anticipar plagas o potenciar el uso responsable del agua para el riego; detectar grupos de crimen organizado, agilizar la toma de decisiones que impacten a la ciudadanía o mejorar los cuidados hospitalarios y detención de enfermedades o creación de nuevos fármacos; proveer de sistemas de enseñanza personalizados para regiones con poco acceso a formación de calidad o la optimización de recursos de movilidad o energéticos. Estos son algunos de los ejemplos del gran impacto está teniendo y el salto cualitativo y cuantitativo que va a suponer para innumerables sectores.

En el otro lado de la moneda está los muchos retos éticos, legales y de robustez que implica su uso y que tienen que abordarse para garantizar que se respetan los principios éticos de justicia, explicabilidad, prevención de daños y respeto a la autonomía humana. Para lograr tener el control sobre el impacto de la IA en la sociedad se necesita crear arquitecturas y procedimientos que garanticen que su explicabilidad y que favorezcan la monitorización de su comportamiento de manera que se asegure que el comportamiento concuerde con el esperado.

Enfoques recomendados para abordar las consideraciones éticas y sociales

Es imprescindible trabajar para asegurar una IA técnicamente robusta, que cumpla las leyes y regulaciones y que obedezca con una serie de requerimientos como son: la supervisión humana; la transparencia y explicabilidad; la robustez técnica y la seguridad; la privacidad del dato; la monitorización constante; la definición de métricas de rendimiento, fiabilidad y seguridad.

La IA debe desarrollarse de manera que respete, sirva y proteja los derechos físicos y mentales de los seres humanos. También deben garantizar la libertad y autonomía de los individuos que en el contexto de la Inteligencia Artificial implica varios conceptos como son; la mitigación de la vigilancia injustificada; el engaño o la manipulación injusta. Además, el respeto a la democracia, la justicia y el estado de derecho de manera que la IA debe servir para mantener y fomentar los procesos democráticos, respetar los diferentes valores y opciones de la vida de las personas. Deben además garantizar los compromisos fundamentales sobre los que se basan los estados de derecho, las leyes y regulaciones. Otro punto fundamental que se debe asegurar es el derecho a la igualdad, solidaridad y no discriminación, por el que la IA debe garantizar el mismo respeto por el valor moral y la dignidad de todos los seres humanos. Los sistemas de IA no deben causar daño ni afectar negativamente a los seres humanos.

Los sistemas de IA deben ser diseñados para aumentar, complementar, potenciar las habilidades cognitivas. Los sistemas de IA deben proteger la integridad mental y física de los seres humanos por tanto los sistemas de IA como los entornos en los que operan deben ser seguros y protegidos. Por otro lado, el desarrollo y despliegue de los sistemas basados en IA debe ser justo, garantizando una distribución equitativa y asegurando que los individuos o grupos estén libres de prejuicios injustos. Los profesionales deben

respetar el principio de proporcionalidad entre los medios y los fines y equilibrar los intereses y objetivos en conflicto. Por último, los procesos deben ser transparentes, las decisiones deben poder ser explicadas a los afectados directa e indirectamente ya que sin esto una decisión no puede ser debidamente impugnada.