Universitat Autònoma de Barcelona

MÁSTER UNIVERSITARIO EN INTEGRACIÓN EUROPEA

Curso 2024-2025

TRABAJO DE FIN DE MÁSTER

Transparencia y rendición de cuentas en el Reglamento de Inteligencia Artificial: algunos aspectos a reflexionar

AUTOR/A: ELISABETH VIVES ESCOBAR

TUTOR/A: Dra. SUSANA BELTRAN GARCÍA

Campus de la UAB, 20 de junio de 2025

Abstract:

La Inteligencia Artificial es hoy en día un elemento esencial en nuestras vidas que está en pleno descubrimiento por el usuario particular, este como sujeto de derechos, es vulnerable de su violación. Por ello y por el desafío que implica la protección de derechos, La Unión Europea materializa en el Reglamento de la Inteligencia Artificial, unos estándares de limitación de manera pionera. La Unión Europea aunque a la zaga de países más punteros como China y Estados Unidos, lucha por aprender de qué manera podemos prevenir posibles conductas delictivas y cómo podemos proteger los derechos de nuestros ciudadanos, los europeos, tarea sumamente relevante. El estudio de la categorización progresiva de los posibles daños y las posibles sanciones, abre ante nosotros una rendición de cuentas posible aunque compleja.
La clave se haya entonces en la entrega del peso burocrático a los proveedor de sistemas de inteligencia artificial y sus representantes legales principalmente como responsables de informar sobre el tipo de sistema, su alcance y proceso de integración a la novedosa Oficina de la Inteligencia Artificial. La posibilidad de rendir cuentas a toda aquella entidad, institución o compañía que busque vulnerar derechos de nuestros ciudadanos con un mal uso de la Inteligencia Artificial, queda opacada sin embargo con retos como la efectividad de las sanciones en y sobre Terceros Estados no miembros de la Unión Europea. Es de relevante preocupación ahora el tratamiento responsable de los datos y su protección. Documentos como el tercer borrador del código de buenas prácticas de la Oficina de la IA y concretamente la transparencia, nos hace verla como factor de protección ante conductas delictivas. La transparencia junto con la cooperación internacional serán claves para prevenir los riesgos de una Inteligencia Artificial sumamente novedosa pero también descuidada con los derechos fundamentales.

Abstract:

Artificial Intelligence is nowadays an essential element in our lives that is in full discovery by the individual user, who, as a subject of rights, is vulnerable to its violation. For this reason, and because of the challenge of protecting rights, the European Union is pioneering global standards of definition in the Artificial Intelligence Regulation. The European Union, although lagging behind leading countries such as China and the United States, is struggling to learn how we can prevent possible criminal conduct and how we can protect the rights of our citizens, Europeans, a highly relevant task. The study of the progressive categorisation of possible harms and possible sanctions opens up a possible, albeit complex, accountability. The key then lies in handing over the bureaucratic burden to the providers of artificial intelligence systems and their legal representatives primarily responsible for reporting on the type of system, its scope and integration process to the new Office of Artificial Intelligence. The accountability of any entity, institution or company that seeks to violate the rights of our citizens through the misuse of Artificial Intelligence is, however, overshadowed by challenges such as the effectiveness of sanctions in and on non-EU third states. Of relevant concern now is responsible data processing and data protection. Documents such as the third draft of the Code of Best Practices of the Office of the IA, and specifically transparency, make us see it as a factor of protection against criminal conduct. Transparency together with international cooperation will be key to prevent the risks of an Artificial Intelligence that is highly innovative but also careless with fundamental rights.

Palabras clave:

Inteligencia Artificial, Derechos Fundamentales, RIA, UE, Transparencia, Rendición de Cuentas, Cooperación Internacional, Oficina de la IA, Protección de Datos y Sanciones.

Keywords:

Artificial Intelligence, Fundamental Rights, Act of AI, EU, Transparency, Accountability, International Cooperation, AI Office, Data Protection and Sanctions.

Abreviaciones

IA: Inteligencia Artificial

TUE: Tratado de la Unión Europea

TFUE: Tratado de Funcionamiento de la Unión Europea

Reglamento de la IA/ Act of AI/RIA: Reglamento 2024/1689 sobre la inteligencia artificial

Convenio de Europa/IA: Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho

GDPR: General Data Protection Regulation (Regulación General de Protección de Datos)

Ley de California: Ley de privacidad de consumidor de California

DDHH: Derechos humanos

DDFF: Derechos fundamentales

UE: Unión Europea

EM: Estado Miembro/ Estados Miembros

El éxito en la creación de la IA podría ser el mayor acontecimiento de la historia de nuestra civilización. Pero también podría ser el último, a menos que aprendamos a evitar los riesgos.

Stephen Hawking

Físico teórico y cosmólogo inglés

Indice

Introducción

A lo largo de este trabajo la aproximación teórica tendrá un símil con cuan difícil es regular competencias como la IA y a la vez la protección de los derechos fundamentales ante el uso de esta. El eje sobre las complejas cuestiones que se me han planteado al repasar la bibliografía, han sido en primer lugar; ¿Cómo de viable es entregar la responsabilidad de información sobre el sistema de IA a un solo agente como es el proveedor de este? Y en segundo lugar, ¿Cuán efectivas pueden llegar a ser las posibles sanciones que se presentan para las conductas delictivas derivadas de las prácticas prohibidas dentro del RIA?

El planteamiento de estas cuestiones, viene a raíz prácticamente completa de una perspectiva desde el RIA y la integración europea de la normativa sobre la IA, siendo este material pionero en establecer criterios estandarizados para limitar los sistemas de IA, un aspecto todavía muy cambiante y dinámico.

He querido por tanto pivotar este trabajo alrededor de dos aspectos claves, que además representan la exigencia de un análisis más profundo para la comprensión de la IA y de su alcance en cuestión. Este trabajo pretende analizar las diversas cuestiones y plantear la transparencia como hilo conector. En primer lugar siendo esta una tarea a cumplir por ser parte de la información a compartir por los agentes. Y en segundo lugar, ya que por su ausencia, podemos hablar de posibles sanciones.

Por ello he estructurado el trabajo en tres capítulos, el primero abriendo el marco a perspectivas internacionales ya que como observaremos la problemática también radica en el concepto de Inteligencia Artificial y por ello también de transparencia. Las regulaciones son distintas a nivel europeo, que asiático o americano. En segundo lugar, trataré aspectos más concretos sobre transparencia y la creación de la Oficina de la IA, de la Comisión Europea. Finalmente un tercer capítulo con cuestiones más profundas sobre la rendición de cuentas y con la que trato de dar respuesta a las cuestiones planteadas anteriormente.

1. Las distintas aproximaciones a la IA

Desde la llegada de internet a hogares, escuelas, trabajos, ámbitos de ocio, sanidad, administración, etc., la facilidad de interconexión ha aumentado de tal manera que como ciudadanos europeos no somos capaces de concebir el día a día de nuestras tareas sin el uso de estas facilidades. La llegada de los sistemas de IA, sin embargo, no ha sido tan pautada, implicando la integración de esta en los diferentes ámbitos personales, laborales y sociales de manera más directa y rápida, a veces incluso descuidada. Sin embargo, esto, no debería implicar una falta de diligencia en la manera de regular los sistemas de IA, que muchas veces termina por reflejarse en una falta de conocimiento sobre el alcance de los sistemas novedosos para su regulación. No es sorpresa encontrar una primera idea de categorización, que ha resultado clave para la materialización de la regulación (dados por los capítulos III y V del reglamento de 2024/1689, en adelante RIA).

De la misma manera no resulta extraño hablar de un descuido de responsabilidad en el control de la veracidad de la información cotejada por la IA y en ocasiones mostrada hacia el usuario como información venida de cuentas veraces y fiables. El problema de la desinformación, surgido mucho antes del uso generalizado de la IA, cobra fuerza cuando el usuario medio, valida y legitima la IA como fuente siempre fiable y veraz de información.

Es por tanto lógico pensar que el uso de sistemas de IA debe venir acompañado de un control en su aplicación si tenemos en cuenta (según él art.1 RIA), que se habla del respeto al mercado interior, siendo este el núcleo sobre el cual pivota la Unión Europea.

La problemática que afronta cualquiera de las categorías de sistemas de IA a la que nos refiramos y sobre la cual he querido basar el trabajo, es la transparencia para el reconocimiento de contenido generado o proporcionado por un sistema de IA, el alcance de las actividades desarrolladas por ese sistema y las prácticas prohibidas o prohibiciones introducidas en el propio RIA.

La problemática se presenta cuando un conjunto de tecnologías debe tomar decisiones y responsabilizarse de tareas humanas. La privacidad en los datos, los sesgos según el origen del sistema de IA y la posibilidad de existir un control gubernamental que pueda llevar a la manipulación, puede comportar un condicionamiento en la predicción de comportamiento humano.

El problema del desarrollo de sistemas de IA con código abierto;

> "las tecnologías de IA cuyo código fuente está disponible libremente para que cualquiera pueda utilizarlo, modificarlo y distribuirlo."[1]

es precisamente aquello que lo caracteriza, la accesibilidad a los sistemas por parte de cualquier persona. Esto implica una falta de filtro sobre la finalidad con la que se quiere usar los sistemas de IA y algo que también es preocupante. La amenaza a la salud pública, la delincuencia o el terrorismo son entre otros posibles fines de uso de sistemas de IA de código abiertos que pueden terminar usándose mediante usuarios cuales fines malintencionados desconocemos.

El problema es que como ocurre con otros aspectos que impliquen un registro, como al que nos lleva el RIA por la entrega de la responsabilidad al usuario y ciudadano de la UE, la ocultación de las verdaderas intenciones de su uso puede implicar una "falsa" regulación.

En el caso de los sistemas de IA más allá del registro por parte de la Oficina de la IA, deberá existir una comprobación por parte de los funcionarios que registran esos sistemas para poder verificar el origen y uso que de verdad se le quiere dar a un tipo u otro de sistemas de IA.

En la actualidad, tanto EE. UU. como China son líderes en el desarrollo de sistemas de IA. Es por ello por lo que la UE opta por una "regulación ética materializada en un marco global único para el uso responsable de la tecnología" afectando a aquellos sistemas nativos de la UE como creados fuera de la misma pero que su uso sea generalizado en el territorio de la UE.

1.1. Perspectiva europea

Es relevante analizar qué tipo de perspectiva tenía la Europa del Consejo de Europa y en el contexto en el que el RIA, que luego veremos, se dio.

Pues pese a que la propuesta inicial del RIA llegó antes, la redacción y entrada en vigor del tratado fue pionera por parte del Consejo de Europa. Hablamos del Convenio Marco de este sobre la IA, los Derechos Humanos, Democracia y Estado de Derecho de mayo de 2024, (frente a la entrada en vigor de junio de 2024).

En el documento podemos observar cómo prima el objetivo por mantener la democracia, los principios fundamentales, tanto la gestión como la mitigación de los riesgos que la IA pueda ocasionar para los anteriores y para el propio Estado de Derecho sin dejar de introducir la IA y dar la bienvenida a los avances tecnológicos. Es El art. 5 del Convenio el que habla sobre la integridad de los procesos democráticos y el respeto del Estado de Derecho, el Capítulo III el que habla de

---

[1] Mucci, T. para IBM. (2024). *Open source AI tools*. IBM Think. Recuperado de https://www.ibm.com/es-es/think/insights/open-source-ai-tools#:~:text=La%20inteligencia%20artificial%20(IA)%20de,pueda%20utilizarlo%2C%20modificarlo%20y%20distribuirlo.

esos principios, en parte novedosos, pero sobre todo de suma importancia en este análisis. Y el art. 8 en este tercer capítulo el que menciona;

"Cada parte adoptará o mantendrá medidas para garantizar que existan requisitos adecuados de transparencia y supervisión adaptados a los contextos y riesgos específicos con respecto a las actividades de dentro del ciclo de vida de los sistemas de inteligencia artificial, incluso con respecto a la identificación de contenidos generados por sistemas de inteligencia artificial."[2]

Concretamente menciona en el art. 8 la importancia de adoptar y poder mantener las medidas garantistas de transparencia, siendo progresivas al riesgo que el sistema de IA presente en un momento determinado. También menciona el propio Convenio IA en otros artículos la evaluación del contenido creado por el sistema de IA y la creación de un foro o convención a la IA[3].
Por otra parte, existe además el derecho a un procedimiento legal que provea de un recurso especial para aquellas personas víctimas y que quiero relacionar con la búsqueda de resarcimiento de daños que tendrá tónica general de este trabajo. Hablamos en este caso del "acceso a recursos legales efectivos y accesibles"[4] esto busca de alguna manera poder facilitar el acceso a la rendición de cuentas, los posibles daños a las víctimas y las sanciones o penas que deban existir para los desarrolladores, proveedores y usuarios, que definiremos más adelante con ayuda del RIA.
Es relevante señalar el papel de Reino Unido, quien a pesar del brexit, si forma parte del Consejo de Europa y que con empresas como Deep Mind con sede en Londres destaca en el marco europeo, por haber sido adquirida 4 años después de su creación por Google o KaoData, empresa desarrolladora y operadora de data centers[5], infraestructura esencial que luego definiré y comentaré, es primordial para que Europa pase a tener un peso relevante en el ámbito del desarrollo de sistemas IA de cara a futuro.
Perspectiva de la UE

La UE fue consciente que los sistemas de IA son uno de los temas más relevantes, pero a la vez más controvertidos de actualidad[6] y es cierto que la tendencia de evolución de la geopolítica mundial revela una tendencia de entrega de tareas a diferentes países en los años pasados.

[2] Consejo de Europa. (2024). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)*. Disponible en https://rm.coe.int/1680afae3c
[3] Art. 23 - Consejo de Europa, *CETS 225*, 2024.
[4] Art. 14 y 15 - Consejo de Europa, *CETS 225*, 2024.
[5] Walker, J. (2024). *AI ambitions: Kao Data breaks ground on fourth UK data center*. *Data Center Knowledge*. Recuperado de https://www.datacenterknowledge.com/data-center-construction/ai-ambitions-kao-data-breaks-ground-on-fourth-uk-data-center
[6] *What's Inside the EU AI Act—and What It Means for Your Privacy*. Investopedia, 13 de junio de 2025. Disponible en https://www.investopedia.com/eu-ai-act-11737033

La idea es que, desde la pandemia y las crisis económicas, la soberanía económica de los EM se ha ido debilitando.[7] La falta de recursos crea la necesidad de importación y nos hace dependientes de otros Estados. [8]

La tónica generalizada a la hora de repartir tareas entre los Estados Unidos, pasa por considerar a los Estados Unidos como el cerebro creador e innovador mundial, China es hoy en día la encargada de la producción y la UE ha adoptado un papel regulador y un perfil de especialización muy elevado en diversos ámbitos, y por tanto competencias.[9]

La UE como organización internacional suis generis, pasa ahora a convertirse en pionera en la creación de una regulación con un marco de estándares legales globales para los sistemas de IA nunca conocidos, que senta precedente con el nivel de especialización y conocimiento con el Reglamento 2024/1689.

a. Reglamento (UE) 2024/1689

A principios de junio de 2024, entra en vigor el conocido como RIA o Act of IA. Este, fruto de la gran tarea de regulación que realiza la UE, supone un grado más de especialización no sólo para las instituciones europeas, sino también para todos los EM que ahora deberán conocer sobre una competencia más. Esta, además de ser una extensión más del uso de la tecnología como pasó con internet en su momento, es ahora necesaria para tener en cuenta que puede ser una posible fuente de vulneración de los derechos fundamentales garantizados por la Carta de Derechos Fundamentales de la UE. [10]

Una gran tarea de control nace a partir de este reglamento, pero también del documento del borrador del grupo de trabajo sobre transparencia que veremos más adelante y que emana del RIA bajo el amparo del desarrollo del trabajo de la Oficina de la IA, la comisión europea. En su conjunto, busca la promoción de una IA centrada en el ser humano y fiable. Aparecen una serie de controles en base a la transparencia por el conocimiento de los sistemas de IA y sus detalles, sobre los que hablaré en adelante.

---

[7] Frances G. Burwell y Kenneth Propp, *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?*, Atlantic Council, junio de 2020. Disponible en https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf

[8] *Thinking European first and its implications*. Bruegel, [2025]. Disponible en https://www.bruegel.org/analysis/thinking-european-first-and-its-implications

[9] Thomas Porwol, "Google kämpft gegen EU-KI-Regulierung: Berliner Gipfel beginnt", *Bild*, 16 de octubre de 2024. Disponible en https://m.bild.de/leben-wissen/digital/google-kaempft-gegen-eu-ki-regulierung-berliner-gipfel-beginnt-670f9777c383db1a97cd21e8

[10] Considerandos 15 al 44 - Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Diario Oficial de la Unión Europea, L 332, de 18 de diciembre de 2015, 1-10. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32015L2376

Antes de empezar a hablar del control y las categorías de los sistemas de IA, debemos saber qué tipo de agentes participan en el sistema de IA y hacia quien va dirigido el RIA. Así pues, el extenso art. 3 RIA habla del proveedor, distribuidor, importador, responsable del despliegue (usuario) y representante autorizado como agentes principales y a quienes en sí va dirigido el Act of IA.

El proveedor

"una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;"[11]

El distribuidor

"una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión;"[12]

El importador

"una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país;"[13]

El usuario, llamado en el RIA "responsable del despliegue"

"una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional;"[14]

El representante autorizado

"una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor;"[15]

Cabe destacar que el usuario convencional particular y no profesional, está exento de implicaciones de control y obligaciones técnicas. Se entiende implícitamente [16]que la posible mayor incidencia en el tipo de derechos del que tratamos y que el RIA quiere proteger como hemos visto anteriormente [17]no suelen ser del alcance a vulnerar al usuario particular promedio. Sin embargo, una de las posibles críticas es la falta de explicación concreta a la exención de particulares a las obligaciones descritas y que ahora veremos.

---

[11] Art. 3.3 Reglamento (UE) 2024/1689.
[12] Art. 3.7 Reglamento (UE) 2024/1689.
[13] Art. 3.6 Reglamento (UE) 2024/1689.
[14] Art. 3.4 Reglamento (UE) 2024/1689.
[15] Art. 3.5 Reglamento (UE) 2024/1689.
[16] De la definición del Art. 3.4 Reglamento (UE) 2024/1689.
[17] Considerandos 15 al 44 - Reglamento (UE) 2024/1689.

Respecto del control que antes mencionábamos y que es de suma importancia, existe primero una categorización de la IA en el propio reglamento según el alcance de publicación, acceso de información, derechos, etc.
En primer lugar, en el Cap. III del Reglamento encontramos aquellos sistemas de IA denominados de alto riesgo. En segundo lugar y a lo largo del Cap. V del Reglamento nos encontramos con los modelos de la IA de uso general.
Por otra parte, debemos saber a qué nos referimos con Sistema de IA:

"un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;"[18]

El nivel de formación y especialidad que se fomenta con el RIA, implica por ejemplo dar a conocer la existencia de promts, como las consultas generadas desde el usuario particular a la IA. La palabra promts utilizada en los años 70 [19]para definir un objeto o valor para significar dar o distribuir, es hoy en día usada como tecnicismo en el uso de la IA. [20]

Por ejemplo, también conocer la existencia y los costes de los data centres que implicaran un aumento de inversiones en España para el año 2026 y que nos hacen colocarnos en una posición muy favorable frente al resto de países europeos.[21]

Contexto empresarial en la UE

El desarrollo de los sistemas de IA en la UE viene marcado poco a poco por dos países punteros. Hablamos de Alemania y Francia, que aumentan poco a poco las inversiones en desarrollo de sistemas IA. Primero con Aleph Alpha, una empresa de desarrollo de sistemas de IA para empresas basados en el ser humano[22] y luego la francesa Mistral, empresa de desarrollo de sistemas de IA para compañías más abundantes y accesibles[23] como plataformas desarrolladas en suelo de la Unión, las cuales cuentan con inversiones públicas cada vez mayores.
El reto europeo es la independencia frente a las otras 2 potencias mundiales, China y Estados Unidos, de desarrollo de sistemas de IA y los componentes físicos, que muchas veces son limitados a pequeños desarrolladores europeos. Estos, terminan por someterse a organizaciones mayores que condicionan las cantidades y calidades de esos componentes físicos para el desarrollo de sistemas de IA. Por ejemplo, Mistral con Hugging Face y Aleph Alpha con Microsoft, ambas con sede en Estados Unidos.

---

[18] Art. 3.1 Reglamento (UE) 2024/1689.
[19] SEOZoom. (2025). *AI prompts: meaning, techniques, building examples*. SEOZoom. Retrieved June 19, 2025, from https://www.seozoom.com/prompts/
[20] Harper, D. (2024). *Etymology of prompt*. Online Etymology Dictionary. Retrieved June 19, 2025, from **https://www.etymonline.com/word/prompt**
[21] AEC Consultoras. (2025, enero 10). Data Centers: la nueva tendencia en la IA. AEC Consultoras. https://aecconsultoras.com/noticias-sectoriales/data-centers-la-nueva-tendencia-en-la/

[22] Aleph Alpha. (2019). *About us*. https://aleph-alpha.com/about-us/
[23] Mistral AI. (2023). *About*. https://mistral.ai/about

La aproximación alemana de los sistemas de IA como Aleph Alpha busca acelerar las administraciones públicas y facilitar el trabajo de los funcionarios. Sin embargo, es la independencia en la materia prima, en parte ahora dada por la empresa HPE (Hewlett Packard Enterprise), quien catapulta a la empresa en la búsqueda común de proveer un sistema de IA basada en la respuesta al cliente y la experiencia frente a la misma como consumidor. Asimilando la Administración europea a la Empresa americana y el público al consumidor.

La lucha se mantiene y en el caso de conseguir "sublevarse" frente a proveedores fuertes en otros países, implicaría liderar como proveedor mundial de sistemas de IA, evitando la dependencia como pasa con el gas en la UE.

La clave en lo que la UE busca para el desarrollo próspero de sistemas de IA "es la potencia de GPU, o la potencia de cálculo", que se mide en la cantidad de operaciones informáticas capaces de hacerse en un tiempo determinado. Con sistemas de IA la diferencia de cómo se han realizado operaciones informáticas es el hardware o sistema físico de ordenadores que pueden soportar el equipamiento tecnológico para que ese volumen de potencia de cálculo sea viable (y desde que se conoce como funciona la IA) también sostenible.

Por su parte empresas como Hugging Face en Francia son también una competencia fuerte en este tipo de sector de puesta a disposición de sistemas de IA para desarrolladores y la percepción de los inversores es siempre hacia un sistema de IA que pueda abarcar un alto nivel de desarrollo actualmente, pero también un uso responsable en el futuro. Tanto el número de usuarios como la cantidad de beneficios son resultados positivos, que atraen a futuros inversores en sistemas de IA. La financiación que es clave para el desarrollo a futuro de los sistemas de IA. La postura de Hugging Face sin embargo no es la de limitar y control por ahora los sistemas de IA de código abierto más bien de la creación de cara a un futuro de una herramienta para hacer más transparente si cabe el uso de este tipo de sistemas de IA garantizando el buen uso responsable de los sistemas.

El instituto de tecnología de Massachusetts tiene en cuenta dos tipos de corrientes de pensamiento sobre el uso de sistemas de IA; el primer el que considera el uso de la IA para todo[24] y el segundo, más escéptico sobre el uso de la tecnología en los procesos ahora guiados por seres humanos[25]. Respecto a esto y relacionado con el código abierto, Hugging Face si cree que es ahora importante considerar los límites del uso de la IA, por no robotizar casi todo los procesos desarrollados por humanos para en un futuro caer en la cuenta de que no ha sido lo más efectivo, ha sido peligroso y del todo no acertado.

En el medio de este conjunto de compañías en aumento de la investigación y el desarrollo en la IA, llega el Reglamento 2024/1686, RIA o Act of IA. En este caso en la UE, la distribución de data centers se ha dado principalmente en Alemania[26], Países bajos, Francia[27] y España. En un

---

[24] Howard, A. (2024). *In AI we trust — too much?* MIT Sloan Management Review. https://sloanreview.mit.edu/article/in-ai-we-trust-too-much/

[25] Primack, D. (2023). *In an AI arms race set off by ChatGPT, ethics may be the first casualty*. Axios. https://www.axios.com/2023/01/31/chatgpt-ai-arms-race-ethics-competition

[26] Eland Cables. (2021, mayo 28). *The growing number of data centres around the world*. https://www.elandcables.com/company/news-and-events/the-growing-number-of-data-centres-around-the-world

[27] Mordor Intelligence. (2025). *Europe colocation market industry report*. Recuperado el 17 de junio de 2025, **de https://www.mordorintelligence.com/es/industry-reports/europe-colocation-market-industry**

futuro el aumento de la inversión vendrá de los data centers ecológicos (con energía renovable)[28] y con menores costes como Polonia o Rumania[29].
Me gustaría recalcar el peso de relevancia que la UE en su influencia indirecta a nivel global, ya que muchas empresas tecnológicas internacionales podrían adaptar sus productos a estas normas. Como de igual manera podría servir para inspirar a otros países que no sean EM y provocar una creación o adopción de regulación.
Ejemplo como esto ocurrió con la regulación para la Protección de datos, **GDPR** en materia de privacidad de 2018, que inspiró países como Brasil LGPD, las conocidas leyes de California CCPA, las regulaciones en japón, Corea del Sur e India entre más países. Es quizás una vez más la representación que necesitamos para ver que países donde crean y arriesgan, la UE es protectora y garantista de derechos con regulaciones que luego sientan un modelo a inspirar por otros países.
En común con el mencionado GDPR[30], sigue el mismo tipo de alcance que ahora el RIA y es que las obligaciones impuestas para las compañías lo son para cualquier compañía con o sin sede en la UE, pero que afecta, al alcance del uso y disfrute de los ciudadanos europeos y a los derechos que se puedan vulnerar de no seguirse respetuosamente las obligaciones establecidas para las empresas sujetos al RIA, como vimos anteriormente.
Así pues, aunque la empresa tenga sede en Estados Unidos (como OpenAI) o en China (como Baidu), pero venga a la UE, deberá cumplir con la normativa de la UE. Pese a que la IA como regulación de tecnologías digitales forma parte de las competencias compartidas entre la UE[31] y los EM, no será necesario un Tratado Bilateral entre el EM del cual es nacional del ciudadano de la UE al cual se le han vulnerado sus derechos con el Estado en el que la compañía desarrolladora, proveedora, distribuidora, importadora y que ha ejercido sus funciones dentro de la UE para que se haga efectiva la pena o sanción[32].

---

[28] Gooding, M. (2024). *CBRE: Data center demand in Europe outstrips supply*. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/cbre-data-center-demand-in-europe-outstrips-supply/

[29] Research and Markets. (2024). *Central & Eastern Europe data center construction market Outlook 2024–2029: Digitalization to drive a surge in investments by colocation, cloud, internet, and telecommunication providers* [comunicado de prensa]. GlobeNewswire. https://www.globenewswire.com/news-release/2024/07/16/2913516/0/en/Central-Eastern-Europe-Data-Center-Construction-Market-Outlook-2024-2029-Digitalization-to-Drive-a-Surge-in-Investments-by-Colocation-Cloud-Internet-and-Telecommunication-Providers.html

[30] Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*. Diario Oficial de la Unión Europea, L 119, 1-88. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

[31] Al no encontrarse dentro del art. 4 TFUE - Unión Europea. (2016). *Tratado de Funcionamiento de la Unión Europea* (TFUE). Diario Oficial de la Unión Europea, C 202, 1-388. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:2016:202:TOC

[32] Del art. 99 RIA - Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828*

La problemática y que nos lleva a este último punto en la efectiva sanción a una compañía de un Tercer Estado fuera de la UE es la prohibición de "entrada" o comercialización del sistema de IA concreto de esa compañía como medida de previsión, pero el garantizar la efectividad de las sanciones es más difícil. Esto pasa en el momento en el que ese Tercer Estado no reconoce por ejemplo la efectivad de la jurisdicción europea, que sólo podrá tener autoridad legal dentro de la propia UE. Esto implica que por ejemplo en el caso de las sanciones si ninguno de los agentes cuenta con activos dentro del territorio de la UE, se complicará aplicar una sanción. Por ello este reglamento ha ido un paso más allá que el GDPR y es que establece la obligación de tener un representante legal dentro de la UE, funcionando como "enlace" entre la UE y la compañía fuera de la UE que ha vulnerado derechos de ciudadanos de la UE en la UE. Pese a existir este mecanismo de control, carecemos de toda garantía, pues no existe la obligación de que ese representante legal deba tener activos en territorio de la UE.

La aplicación práctica de las sanciones a Terceros Estados es de alguna manera dada en dos veces; primero con la existencia de una regulación desde y dentro de la UE y otra que implica la cooperación internacional y que no puede dotar al EM de poder para realizar una regulación en forma de acuerdo bilateral para reforzar las medidas por el tipo de naturaleza de la competencia que la materia tiene; es por ello la competencia compartida en este caso un arma de doble filo.

El problema es hacer cumplir las sanciones fuera de la UE. La cooperación necesaria para la efectividad en la sanción dependerá solo y exclusivamente de la UE ya que así lo ha determinado el reparto de las competencias compartidas entre la UE y los EM. La parte de la presión por parte del EM para que la UE cumpla con su parte, si puede venir por parte del Estado concreto que pida medidas más estrictas o mayores mecanismos de control, como el del representante legal dentro de la UE.

El efectivo cumplimiento de sanciones es hoy en día un desafío legal y práctico.

Por último, cabe recalcar el papel del administrador de la UE y de los funcionarios nacionales sobre los que las funciones de control de permisos, licencias o cualquier tipo de documento que habilite o de permiso recae desde hace unos años. Y es que existe una tendencia en la emisión de declaraciones de autorresponsabilidad por parte de las personas usuarias y no de un control exhaustivo por parte de la administración a priori (y que era más habitual antaño en el procedimiento administrativo).

No debe sorprendernos que la manera en la que se materializa la perspectiva de la UE bajando de la Ley a los códigos de buenas prácticas pueda implicar una cesión de esa responsabilidad en el usuario (tanto como proveedor, como responsable del despliegue del sistema de IA).

1.2. Perspectiva de China

El continente asiático con China como país a la cabeza del desarrollo tecnológico, sin embargo, normaliza y desarrolla sistemas de IA a mayor velocidad. Cuenta con la IA en el desarrollo de "la seguridad nacional, el ejército, la vigilancia del Estado, el trabajo policial, gestión de las ciudades, tráfico…",[33] este tipo de sistemas de IA se vende entre otros a Europa, que en comparación a China

---

(Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, L 2024/1689. https://op.europa.eu/es/publication-detail/-/publication/dc8116a1-3fe6-11ef-865a-01aa75ed71a1/language-es

[33] Human Rights Watch. (2019). *China's algorithms of repression: Reverse-engineering a Xinjiang police surveillance app*. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

y Estados Unidos entre otros no cuenta con tanta popularidad de interés ni inversión por parte de los fondos públicos.

El desarrollo de sistemas de IA en el continente asiático sin embargo no tiene como consumidor último el cliente o ciudadano, sino el cuerpo de ingenieros informáticos y desarrolladores. El código abierto de los sistemas de IA, ayudan a la evolución continua de los sistemas. Esto a su vez puede ayudar a generar un mayor espacio de creación y mejora de los sistemas IA ya existentes.

En China fue el Centro de Información de la Red de Internet de China[34] (CNNIC de ahora en adelante) el que impulsó la creación de medidas provisionales sobre la IA en 2023[35], que se ha materializado ahora en las medidas IA (AI mesures)[36], ahora promovidas por la Administración del Ciberespacio de China. En el conjunto de documentación vemos como el país asiático ya realizaba la definición de un sistema de IA, la IA generativa y los límites en el desarrollo tecnológico y de gobernanza de los modelo de IA.

Pese a ser una documentación corta (en comparación con el RIA), contempla en el art. 4.2.v)[37], la necesidad de crear contenido de la manera más transparente posible, adoptando medidas para garantizar esto, aunque no se indica que medidas como si lo hace la documentación de la Oficina de la IA con los códigos de buenas prácticas de marzo de 2025 y de los que hablaremos más adelante.

Al hablar de China como país impulsor de IA, hablamos no sólo de la cantidad de ámbitos para lo que esta es usada de manera generalizada o en la cantidad de desarrolladores y creadores de modelos de IA. Hablamos también de la iniciativa política desde 2017[38] por el consejo estatal de la república popular de China y en los pasos agigantados que el país asiático tomó en 2023 con la creación de las medidas provisionales para la Gestión de Servicios de IA Generativa.

Es curioso ver la creación de circulares alentando a las empresas a desarrollar por ejemplo investigación sobre creación de películas creadas con realidad virtual.[39]

---

[34] China Internet Network Information Center (CNNIC). (2017). *Introducción al CNNIC*. Recuperado de https://www.cnnic.com.cn/IC/Events/201706/t20170608_69324.htm

[35] China Cyberspace Administration. (2023). *Medidas provisionales para la gestión de servicios de inteligencia artificial generativa*. Recuperado de https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[36] Comité Técnico Nacional de Normalización de Seguridad de la Información (TC260). (2024). *Requisitos básicos de seguridad para los servicios de inteligencia artificial generativa (TC260-003)*. Recuperado de https://www.tc260.org.cn/

[37] China Cyberspace Administration. (2023). *Medidas provisionales para la gestión de servicios de inteligencia artificial generativa*. Recuperado de https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[38] State Council of the People's Republic of China. (2017). *Next Generation Artificial Intelligence Development Plan* (Document No. 35). Recuperado de https://english.www.gov.cn/policies/latest_releases/201707/201707/20170713/202207/t20220713_1071106.html

[39] China Film Administration. (2025). *China issues circular to boost well-regulated development of VR films*. Recuperado de https://english.www.gov.cn/news/202503/22/content_WS67de12a0c6d0868f4e8f10f2.html

Otro claro ejemplo es el ámbito de la regulación sobre reconocimiento facial[40], cuya ley entró en vigor el 1 de junio de 2025, e implica el uso limitado del reconocimiento facial para garantizar los derechos e intereses de los ciudadanos chinos, así como la información del método de archivo y tratamiento de los datos extraídos del uso del reconocimiento facial.
Por otra parte, también el uso del reconocimiento facial está limitado en espacios públicos y para el acceso a complejos residenciales o centros comerciales.[41]
Otras leyes que se aprobaron en el año 2021[42] y 2022[43] también fueron la de seguridad de datos, de protección de información personal y de ciberseguridad.
La cosa sin embargo cambia a partir de 2023, cuando China impulsa la ley llamada de medidas provisionales[44], pues hasta el momento, la intención de ampliar el alcance de la regulación por los países punteros en IA no era pensado que viniera de la mano de China, sino más bien del viejo continente y de su naturaleza reguladora. En Julio de 2023, sin embargo, se aprobó la ley y siendo aplicable desde septiembre de ese mismo año habla del objetivo común de crear una IA generativa más sana y protectora de los derechos. Que deba informar al usuario chino sobre el etiquetado, uso, tratamiento y entrenamiento de los modelos o sistemas de IA. Por otra parte, también menciona y es relevante mencionar que la regulación solo va dirigida a aquellos proveedores y responsables del despliegue[45].
Quedan exentas de cumplir la ley todas aquellas empresas, administraciones u organizaciones que usen un sistema de IA de manera interna y que no sea expuesto al público de manera general.
Dejando en mi opinión un amplio abanico de desarrollo y poca burocracia en el ámbito interno, lo que refuerza el discurso público de protección al usuario, pero no lo hace de manera interna, siendo más flexible. Existe un origen común de las mencionadas medidas provisionales y los artículos de

---

[40] Cyberspace Administration of China & Ministry of Public Security. (2025). *Measures for the Security Management of Facial Recognition Technology*. Recuperado de https://www.hunton.com/privacy-and-information-security-law/china-releases-new-rules-regarding-the-use-of-facial-recognition-technology

[41] Center for Security and Emerging Technologies. (2025). *China's facial recognition security measures*. Recuperado de https://cset.georgetown.edu/publication/china-facial-recognition-security-measures/

[42] Standing Committee of the National People's Congress. (2021). *Data Security Law of the People's Republic of China* (Ley No. 35). Recuperado de https://www.npc.gov.cn/zgrdw/npc/dbdhhy/12_1/2021-06/10/content_2068709.htm

[43] Cyberspace Administration of China. (2022). *Amendments to the Cybersecurity Law of the People's Republic of China*. Recuperado de https://www.cac.gov.cn/2022-07/01/c_1690898327029107.htm

[44] China Cyberspace Administration. (2023). *Medidas provisionales para la gestión de servicios de inteligencia artificial generativa*. Recuperado de https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[45] Entendidos como responsables del despliegue según la normativa europea, Ley IA 2024, pero no por la interpretación o definición de la Ley China de 2023.

interés sobre el reconocimiento facial y la protección de datos.[46] Se tratan de las leyes creadas antes del 2023 y que mencionaba anteriormente.

1.3. Perspectiva de EE. UU

Las violaciones de las regulaciones en Protección de Datos y la Ley de Privacidad de California[47], conocida por la controversia con la compañía Meta[48] y su venta de datos a una firma consultora británica, fue acusada de influir en la decisión política de las elecciones de 2016 y más tarde en la salida de Reino Unido de la Unión Europea.

Por controversias como la de la compañía Meta salió a la luz el gran vacío legal que existía sobre la protección de datos en internet y mediante el uso de sistemas de IA, lo que concienció a Estados Unidos para llevar adelante el proyecto de la ley de privacidad de california.

Con la creación de pautas sobre el uso de los sistemas de IA; Estados Unidos pretende controlar amenazas como el mercado de datos en ámbitos como el sanitario y el financiero (donde los datos personales pueden suponer un factor de riesgo sobre la seguridad en el uso de los sistemas). Actualmente el punto de vista estratégico está puesto a nivel federal en las directrices o guías de uso vinculantes sobre los sistemas de IA, pero sobre todo en el uso de la información que los sistemas de IA realizan con la subida de esa información a la nube y cómo se asegura una vez cargada en ella.

Propuestas como las de Clio[49] que analiza las posibles lagunas de uso abusivo de IA desde la perspectiva de uso de la plataforma Claude.ai., toma como referencia, los temas sobre los que se usa el sistema de IA y en diversas fases analiza también, de qué manera el usuario pregunta y en qué idioma lo hace.

Finalmente, el equipo de seguridad del propio sistema es el que analiza los datos extraídos en busca de violaciones en la política de uso del sistema, evitando solicitudes dañinas y procurando un uso responsable para el usuario (no con fines malintencionados) y el tratamiento de los datos. La violación de esos parámetros implicaría una prohibición del uso del sistema Claude.ai, es decir una manera de controlar y hacer seguimiento a todo mal uso del sistema de IA.[50]

Es curioso saber que para Clio por ejemplo es importante que, en la respuesta al usuario, la cantidad de datos privados que el propio usuario da al realizar la consulta no sea elevada.

Sin embargo, debe señalarse que herramientas como la descrita es generada igualmente por IA y que sirve para la facilitación de tareas que a priori podría hacer el ser humano pero que tardaría

---

[46] China Law Translate. (2023, 15 de agosto). *Comparison chart of current vs. draft rules for generative AI*. Recuperado el 18 de junio de 2025, de https://www.chinalawtranslate.com/comparison-chart-of-current-vs-draft-rules-for-generative-ai/

[47] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018). Recuperado de https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.100.&lawCode=CIV

[48] Pierson, B. (2024, octubre 15). *Meta must face US state lawsuits over teen social media addiction*. Reuters. Recuperado de https://www.reuters.com/legal/meta-must-face-us-state-lawsuits-over-teen-social-media-addiction-2024-10-15/

[49] Anthropic. (2024). *Clio: Privacy-preserving insights into real-world AI use*. arXiv. https://arxiv.org/abs/2412.13678

[50] Anthropic. (2025). *Anthropic's Transparency Hub*. Recuperado de https://www.anthropic.com/transparency

más tiempo. El sistema de IA puede ayudar a optimizar el tiempo dedicado a la tarea y es por ello por lo que también necesitan de control en sus tareas, que en la actualidad se verifica exhaustivamente manualmente. Por otra parte, y para garantizar un seguimiento lo menos invasivo posible se usa por parte del sistema la menore cantidad de información personal o privada posible, asumiendo de esa manera únicamente el error realizado en el procedimiento y no con la información del usuario.
La existencia además de auditorías periódicas para el tratamiento de esos datos privados y la reducción sobre fallos que sistemas de seguridad de uso "normal", es decir de uso habitual en internet y no sólo con IA ayuda a proporcionar un tratamiento de datos seguro. Por último y más importante la compañía busca la confianza en el usuario, siendo completamente transparente con el uso de datos que hace, los errores cometidos en la extracción de información y el seguimiento que se le hace a los datos, pero también lo es con la corrección de su uso y la expulsión de cuentas del sistema que usan patrones repetidos que no respetan los estándares de seguridad y diligencias de uso proporcionado por la compañía.

La pluralidad de perspectivas que el desarrollo de sistemas de IA nos aporta a lo largo de los diversos países punteros en su desarrollo, tienen el objetivo común de garantizar un uso seguro, ético, protegido y garantista no sólo de un proceso de información más detallado y que busque saber identificar un sistema en la producción de su contenido. Pero si en uno basado en el ser humano.
Poniendo de relieve la ética en el buen uso con regulación como el Act of AI o los guidelines americanos, se vincula a las administraciones para perseguir toda aquella institución o entidad que haga un mal uso de las herramientas.

El pasado marzo de 2025, acogimos en Barcelona un año más el Mobile World Congress con más 100.000 visitantes de 205 países[51]. Además de compartir las novedades en herramientas novedosas con IA y sin esta, como las que nos mencionaba la Dra. Susana Navas en su lectura el internet de los Cuerpos [52], las jornadas compartían también las preocupantes cifras [53] de aumento en ciberataques, [54] el punto de mira más importante la filtración de datos personales. Es por ello por lo que la creciente preocupación de las empresas es también sacar al mercado dispositivos más seguros que puedan hacer una gestión inteligente y responsable de los datos. [55]

---

[51] Serra, C. (2025, 6 de marzo). *El Mobile atrae a 109.000 visitantes y recupera niveles de asistencia récord*. Ara.cat. https://en.ara.cat/misc/the-mobile-attracts-109-000-visitors-and-recovers-record-attendance-levels_1_5306664.html
[52] Navas Navarro, S. (2022). El internet de los cuerpos: Una aproximación jurídica. *Revista de Derecho y Genoma Humano*, 56, 93–123. https://doi.org/10.14679/1323

[53] Red Seguridad. (2024). *Los ciberataques globales ya superan los 1.630 casos por semana*. https://www.redseguridad.com/actualidad/los-ciberataques-globales-ya-superan-los-1630-casos-por-semana_20240731.html

[54] El Debate. (2025). *Aumentan los ciberataques en España: malware y fraude, las mayores amenazas*. https://www.eldebate.com/espana/20250321/aumentan-ciberataques-espana-malware-fraude-mayores-amenazas_280728.html

[55] European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

No es sorprendente ver como la cantidad de concienciación[56] de la mano de programas de aprendizaje del uso de las nuevas tecnologías es cada vez mayor. Sin embargo, debemos recalcar acordándonos de a quién va dirigido regulación como el RIA, y no es precisamente al usuario particular en riesgo de caer en "trampas" de filtraciones de datos, sino más bien a las compañías o agentes en nombre de entidades que busquen la filtración de los datos de sus usuarios.

Quizás una idea que garantizaría mayor accesibilidad a aquellos grupos de edad (S. Tews, comunicación personal, 20 de febrero de 2025) con mayores factores de riesgo[57] y desprotección ante el desconocimiento tecnológico, sería la de habilitar entidades ya existentes, como la Oficina de la IA en el caso de la UE para atender y gestionar denuncias por parte de la población de ciber ataques, estafas o filtración de datos.

La geopolítica que mencionaba al inicio habla ahora de la necesidad de crear una armonización de leyes para que la prevención sea eficaz. La perspectiva pura y dura desde la UE[58] es que el estándar sentado por el RIA sea de aplicación general a todo Estado. Sin embargo, la creación de nueva normativa por diversos países es a mi parecer un acierto por enriquecer a la potestad legislativa con diversos mecanismos garantistas de derechos para el usuario.

2. La transparencia en el Reglamento de Inteligencia Artificial (Act of IA)

El mercado interior sobre el que se sustenta la UE, mencionado en los arts. 3.3 TUE, 3 y 4 TFUE, conforman el objetivo con el que el reglamento que entró en vigor el pasado junio de 2024 se creó. En su art. 1y qué cito textualmente del preámbulo del texto fundacional del TUE, menciona;

" El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.," [59]

El gran entramado de transparencia presentado en el Reglamento 2024/1689, nace de la necesidad de controlar una serie de inteligencias que desde su nacimiento a su publicación y en su uso, pueden conllevar una vulneración de los Derechos de los ciudadanos europeos. Debe quedar claro

---

[56] ENISA. (2023). *Cybersecurity awareness: Raising awareness and educating users to improve cyber resilience*. https://www.enisa.europa.eu/publications/cybersecurity-awareness-raising-awareness-and-educating-users-to-improve-cyber-resilience

[57] Tews, S. (2025, febrero 20). Securing our Digital Future: Balancing Innovation, Economic Growth, and Cybersecurity in a Connected World. Seminario presentado como parte del programa de seminarios externos en el Máster de Integración Europea, Universidad Autónoma de Barcelona.

[58] European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[59] Art. 1 Reglamento (UE) 2024/1689.

que la aplicación del RIA sigue una naturaleza progresiva. Es decir, a cuanto mayor el riesgo, mayor la cantidad de obligaciones que las compañías deben llevar a cabo.

Una perspectiva común que comparten desarrolladores, proveedores, productores y creativos de la IA es la del uso para la educación, el impulso educativo, la promoción personal siempre con el objetivo de agrandar y magnificar al productor propio, al ser humano en sí.
La garantía de mantenimiento de la esencia humana en todo aquello que la IA, hace, crea, retoca o ayuda no puede dejar atrás la característica única que el humano puede darle. Una regulación eficiente de la IA debería darse en un marco de colaboración mundial aplicable a nivel práctico que permitiera realizar inspecciones, **sancionar infracciones y expulsar del mercado** a los infractores.

2.1. La transparencia como herramienta de prevención criminológica

Irremediablemente y porque conozco por mis estudios de Criminología sobre cómo afecta la rendición de cuenta a la prevención del delito, relaciono las posibles conductas delictivas con dos teorías criminológicas.
En este caso sin embargo y observando cuan faltas de efectividad están las sanciones propuestas por el RIA, me lleva a plantearme como esto puede influenciar en la falta de ejemplo ante conductas delictivas y conllevar a un aumento en estas.
La primera con la clásica teoría de la oportunidad[60]; donde un delincuente motivado como un hacker, ante un objetivo adecuado como usuario en grupos sociales vulnerables (como los mencionados por S. Tews comunicación personal, 20 de febrero de 2025)[61], termina por delinquir cuando existe falta de control o vigilancia, por ejemplo, ausencia de políticas de seguridad que sean efectivas (como el problema de la efectividad en las sanciones impuestas por el RIA a Terceros Estados no EM de la UE).
La otra, es la teoría de la asociación diferencial[62] que señala que todo comportamiento es aprendido, incluso el delictivo y que por ello si existiera una mayor regulación sobre espacios ahora alegales dentro de internet. El delincuente terminaría por aprender que el castigo existe en primer lugar y que una educación que replique las facilidades de las tecnologías es posible en segundo lugar.

Respecto a los sistemas de riesgo general, se busca que existe la obligación de informar sobre la interacción del sistema, pero voluntarios de ética y de códigos de conducta.

---

[60] Cohen, L. E., & Felson, M. (1979). *Social change and crime rate trends: A routine activity approach*. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

[61] Tews, S. (2025, febrero 20). Securing our Digital Future: Balancing Innovation, Economic Growth, and Cybersecurity in a Connected World. Seminario presentado como parte del programa de seminarios externos en el Máster de Integración Europea, Universidad Autónoma de Barcelona.

[62] Sutherland, E. H. (1947). *Principles of criminology* (4th ed.). Philadelphia, PA: J. B. Lippincott Company. Disponible en: https://archive.org/details/principlesofcrim00suth

Respecto de los sistemas de alto riesgo, se busca la obligación de una evaluación de conformidad, necesidad de registrarse en la base de datos pública de la UE, presentación de documentación técnica, supervisión humana efectiva y obligatoria, vigilancia tras la comercialización.[63]

2.2. Posibles sanciones

Se plantea la retirada del mercado si se hubieran comercializado, aviso obligatorio a las autoridades nacionales y mitigación de daños.

Hablamos de 35 millones de euros o el 7% de su volumen de negocios mundial tota[64]l: Actuación contra aquellas prácticas prohibidas de uso[65] y comercialización.
Si estas prácticas del art. 5 RIA las lleva a cabo organismos o entidades de la Unión, hablamos de hasta 1,5 millones de euros o de hasta 500.000 euros [66]si unas prácticas parecidas pero no las del art. 5 RIA se cometieran.
Por último y teniendo en cuenta a los proveedores y por una cuestión tan relacionada con la transparencia como la de presentar la información requerida o infringiendo los artículos anteriores por un valor de hasta 15 millones de euros o el 3% de su volumen de negocio mundial total.[67]

2.3.El rol de la Oficina de la IA

Nacida del RIA como parte de la Comisión Europea, la Oficina de la IA[68], nace como una entidad para:

"contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del RIA (…), recopilar y compartir conocimientos técnicos y reglamentarios y mejores prácticas entre los Estados miembros, ofrecer asesoramiento sobre la aplicación del presente Reglamento, contribuir a la armonización de las prácticas administrativas en los Estados miembros, emitir recomendaciones y dictámenes por escrito en relación con cualquier asunto pertinente relacionado con la ejecución del presente Reglamento, apoyar a la Comisión en la promoción de la alfabetización en materia de IA, facilitar el desarrollo de criterios comunes, contribuir a la cooperación efectiva con las autoridades competentes de terceros países, asistir a las autoridades nacionales competentes, asistir a la Oficina de IA en el apoyo a las autoridades nacionales competentes para el establecimiento y el desarrollo de espacios controlados de pruebas para la IA, recibir dictámenes de los Estados miembros sobre alertas cualificadas relativas a modelos de IA de uso general y sobre las experiencias y prácticas nacionales en materia de supervisión y ejecución de los sistemas de IA, en particular los sistemas que integran los modelos de IA de uso general."[69]

---

[63] Arts. 9-14 y 60-62 Reglamento (UE) 2024/1689.
[64] Art. 99 Reglamento (UE) 2024/1689.
[65] Art. 5 Reglamento (UE) 2024/1689.
[66] Art. 100 Reglamento (UE) 2024/1689.
[67] Art. 101 Reglamento (UE) 2024/1689.
[68] Art. 64 Reglamento (UE) 2024/1689.
[69] Art. 66 Reglamento (UE) 2024/1689.

El reglamento de la IA y el efecto cinturón de seguridad: Quizás exista una pérdida de creatividad en el mercado de IA con la entrada del Reglamento, pero como paso con la implementación del cinturón de seguridad en los vehículos, esto aumentó la compra de vehículos cuando estos pasaron a ser obligatorios, quizás la demanda de sistemas de IA aumentará con el uso de las limitaciones y regulaciones impuestas por el Reglamento, por el hecho de tratarse de sistemas de IA más seguros y transparentes.
Con el establecimiento del calendario de aplicación desde la Oficina de la IA, la entrada de las primeras restricciones será clave para analizar el impacto de este tipo de regulación al menos en proveedores europeos, pero también en el resto de los competidores al tratarse de un efecto espejo sobre los que demandan IA y la proveen.
Aunque la Oficina de IA tiene mecanismos de inspección y sanción, aplicar sanciones a empresas fuera de la UE (como OpenAI o Baidu) sigue siendo un desafío legal.
Empresas extranjeras podrían relocalizar partes de su infraestructura fuera de la UE para evitar el control europeo.
Si la empresa tiene sede o activos en la UE, se le puede multar o restringir su actividad fácilmente.
Si la empresa solo opera desde fuera y no tiene activos en la UE, la UE puede imponer sanciones, pero hacerlas efectivas es complicado.

La Oficina de la IA que sigue su propio marco cronológico de implementación (ver Anexo 3), se encuentra actualmente terminando los códigos de buenos prácticas y esperando a los meses de agosto de 2025 en adelante para empezar con la aplicación de los capítulos III, V y VIII, basando gran parte del trabajo del 2026 en la aplicación del art. 6 RIA y 2027 a su implicación en el mercado. [70]

3. La rendición de cuentas en el Reglamento de Inteligencia Artificial

Basándonos en el último borrador de código de buenas prácticas presentado en el mes de marzo por la Oficina de la IA sobre la transparencia, debemos hablar de las obligaciones que los diversos participantes de la creación, soporte, fomento y uso de los sistemas de IA tienen en la UE.
Esta documentación va dirigida a los proveedores de sistemas de IA de propósito general (y con riesgo sistémico) y es sobre la que cual deriva una idea de formulario para que el usuario informe sobre las características de su sistema de IA (ver Anexo 1), hace referencia a la comprensión significativa del sistema de IA que se usará.
Esto implica que el código de buenas prácticas como mencionaba al inicio de este trabajo es una vez más una muestra de la entrega de responsabilidad al usuario.
Como pasa con las declaraciones auto responsables que mencionaba más arriba, es el particular el que debe rellenar el formulario que más abajo menciono y hacerlo constar de manera pública ante la Oficina de la IA.
Debemos tener en cuenta que, aunque pertenece a un marco de aplicación más amplio y duradero en el tiempo, el formulario es un documento por el momento voluntario a disposición de empresa, proveedores y usuarios de modelos de IA para con un proceso de compromiso de las obligaciones y principios nacidos con la Ley de la IA de junio de 2024.

---

[70] EU AI Act. (2024). *Implementation Timeline*. Recuperado de, https://artificialintelligenceact.eu/implementation-timeline/

3.1. ¿Qué se entrega y cómo se entrega?

Revisando dicha documentación, encontramos un formulario (ver Anexo 1) donde el usuario entre otras características debe indicar en primer lugar la información general sobre quién provee el modelo, que tipo de modelo y denominación tiene.

Por otra parte, deberá indicarse las propiedades del modelo es decir qué tipo de modalidades tiene tanto con ítems de entrada como de salida y que tamaño pueden tener esos ítems.

También debe constar el conjunto de métodos de distribución y de licencias, es decir qué tipo de acceso existirá, por ejemplo, por suscripción o con paquetes cerrados o si será completamente público. Deberá indicarse la licencia, su categoría y datos adicionales sobre los códigos de entrenamiento y de evaluación del modelo.

Sobre el uso mencionado en el formulario, será necesario indicar el propósito de la política aceptable sobre el uso del modelo y que tipo de soporte (software y hardware son necesarios).

Será necesario, además, indicar que tipo de proceso de formación ha tenido el diseño en su capacitación y porque se ha decidido utilizar un proceso sobre otro, indicando también los datos utilizados para el entrenamiento, las pruebas y la validación del sistema. En este caso es relevante que alcance y características deben tener los datos.

Es importante tener en cuenta además las medidas para detectar datos inadecuados (por ser personales o nocivos), así como el sesgo que puede tener la búsqueda.

Cómo adelanta la regulación en la Ley de la IA que mencionaba anteriormente, además, existe una cantidad de cálculo de referencia que deberá indicarse también en la especificación del consumo de energía.

Por último, los proveedores con modelos de propósito general con riesgo sistémico deberán además proporcionar que tipo de limitaciones han encontrado en el desarrollo de su modelo de IA y de qué manera se ha podido adaptar el modelo; con sus consiguientes pruebas y evaluaciones.

Los proveedores son los agentes principales encargados de presentar documentación relativa a la transparencia, el uso de esa documentación pasa por la evaluación, documentación y registro de los sistemas.

3.2. Críticas

Respecto de este tercer borrador en sí las exigencias con el copyright por ejemplo del contenido extraído para la creación de contenido a posterior, no quedan claras como en los borradores anteriores o en el borrador respecto a copyright.

Por lo que, si lo que queremos analizar, es de alguna manera cuan en serio se toma la Oficina de la IA la veracidad de la fuente del contenido que el usuario utiliza mediante el modelo de IA, muy probablemente lleguemos a la conclusión de que no es una prioridad para esta fase de definición e información del sistema de IA para el usuario.

Sin embargo, la crítica generalizada y en la que me gustaría también basarme es en el que sí bien el RIA, habla de la transparencia como principio, no lo hace de manera homogénea (ante todos los sistemas de IA de igual manera) ni con la misma intensidad (obligación de registrar, pero no de evaluar, por ejemplo).

Esto deja lagunas a los sistemas de IA que pasan desapercibidos, los de bajo riesgo, que no son ni mencionados en el RIA, pero si son implícitamente tratados.

Por otra parte, la falta de trato del RIA hacia el usuario particular que, en sus consultas, pueda terminar vulnerando posibles derechos fundamentales, en parte también debido a la baja formación sobre las consultas o promts de los sistemas.

La falta de formación en usuarios y claridad en los documentos burocráticos implica un sinsentido de formalidades que carece de lógica y finalidad objetivamente razonable.
Por último, pero no por ello menos relevante la incoherencia en la obligación estricta de por ejemplo tener un representante legal dentro de la UE, pero no la obligación de que tenga activos suficientes para que las sanciones se puedan hacer efectivas. Frente a por ejemplo lo laxos que pueden llegar a ser los códigos de conducta cuando las tareas de información por parte de determinados agentes son voluntarios.

Conclusiones

La Unión Europea tiene ante sí un reto importante: apostar más en innovación y desarrollos de sistemas IA. De nada sirve despuntar en regulación jurídica si ésta no está al servicio de una soberanía europea tecnológica real. A pesar de que despuntan países como Francia y Alemania con diversas empresas desarrolladoras de sistemas de IA (tanto de código abierto como de código cerrado), hace falta una apuesta más global en este sentido en el conjunto de la Unión.
Países como China, que lleva utilizando los sistemas de IA desde hace varios años en las tareas más diversas, pero también en su reciente creación de las "Medidas Provisionales para la Gestión de Servicios de IA Generativa" y también "Regulaciones para la Gestión de Recomendaciones Algorítmicas en Servicios de Internet" son un claro ejemplo de esta apuesta real por la innovación y el desarrollo en IA.
De forma parecida, Estados Unidos, que como sabemos carece de regulación federal al no ser competencia constitucional federal, pero que, con las leyes de California sobre protección de datos y transparencia, pareció estrenarse en el terreno en 2018. En este caso, el desarrollo viene de la mano de grandes empresas con sede en Estados Unidos, que además sirven como servidores a empresas de países de la UE.

En cuanto a aspectos positivos destacables, la Unión Europea es capaz de encontrar espacio físico donde instalar hardware, instrumento material soporte de sistema de IA software, que no es un tema menor. Espacio que ahora mismo es moneda de cambio en la geopolítica europea y que coloca a España en una buena posición de cara a futuro con competidores como Rumania o Polonia para establecer los ya conocidos como data centres.

Sobre la transparencia, a pesar de las incertidumbres sobre las consecuencias de una eventual opacidad en los sistemas de IA, es de esperar que cuando se adopte definitivamente el código de prácticas del RIA, éste sea útil a proveedores, responsables de despliegue y usuarios. Con todo, hablar de transparencia en el uso de la IA debería ir un paso más allá de la adopción de una regulación como el RIA que, aunque siendo novedoso al establecer categorías y sobre todo sanciones a los sistemas de IA, no nos permite conocer qué tipo de alcance van a tener las obligaciones exigibles a compañías de terceros estados no miembros de la UE, especialmente si no tienen sede en territorio de la UE, por falta de cooperación internacional en la efectividad de sanciones principalmente económicas.

En relación a la rendición de cuentas, el papel del compliance en el uso de formularios como los establecidos en el último informe de la nueva Oficina de la IA, de la Comisión Europea, puede darnos una idea de cuál será la comunicación necesaria que deba hacerse por parte del creador de sistemas de IA, pero el papel del usuario de a pie de estos sistemas queda todavía por determinar. En este sentido, se vuelve a insistir en la importancia de que se adopte un Código de prácticas que aporte claridad

Un punto de inflexión va a ser, sin duda, la educación que debería abordar en algún momento de la carrera curricular el conocimiento básico de los sistemas de IA y cómo puede ser exigible la transparencia y rendición de cuentas. Ésta debe garantizar a su vez el espíritu crítico y mediante la lectura logre formar en conocimiento al alumnado del futuro más cercano.

Una apuesta en la educación digital, y sobre la IA, reduciría el riesgo de que agentes o personas individuales de fines malintencionados, usen la IA para aprovecharse del desconocimiento de una herramienta que es todavía hoy desconocida. A su vez, la Unión ha de trabajar factores de protección para prevenir la conducta delictiva mediante políticas de seguridad tecnológica. Falta también una gran especialización académica en el ámbito de la IA, que la conozca y sepa de qué manera puede no ser del todo objetiva o como puede ser limitante a las políticas de seguridad.

En efecto, la IA promete ser una herramienta de provecho para el futuro evitando lagunas en las consultas y los promts. Los límites en su alcance han sido establecidos de manera efectiva por el RIA, siendo pionero y exitoso no solo en la UE, sino también como referente a nivel global. Sin embargo hay que hacerlo efectivo con medidas y, puntualmente, sanciones, exigibles a aquellos proveedores o responsables de despliegue que puedan vulnerar con la puesta en práctica de los sistemas de IA los derechos de las personas.

Es primordial, seguir trabajando para que los sistemas de IA sean transparentes y seguros sin perjudicar la innovación y la competitividad ¡Gran reto!

Es tarea de los europeos velar por una Unión Europea segura en todos sus aspectos y en esta novedosa competencia como es la Inteligencia Artificial para que no se queda atrás. Es inaceptable deber elegir entre progreso o protección.

Bibliografía

Administración del Ciberespacio de China. (2023). Medidas Provisionales para la Gestión de Servicios de IA Generativa. (Vigentes desde agosto de 2023).

Administración del Ciberespacio de China. (2022). Regulaciones para la Gestión de Recomendaciones Algorítmicas en Servicios de Internet. (Vigentes desde marzo de 2022).

AEC Consultoras. (2025, enero 10). Data Centers: la nueva tendencia en la IA. AEC Consultoras. https://aecconsultoras.com/noticias-sectoriales/data-centers-la-nueva-tendencia-en-la/
Aleph Alpha. (2019). About us. https://aleph-alpha.com/about-us/

Anthropic. (2024). Clio: Privacy-preserving insights into real-world AI use. arXiv. https://arxiv.org/abs/2412.13678

Arte.tv. (2023, noviembre 30). La carrera por la IA. Arte. https://www.arte.tv/es/videos/115067000-A/la-carrera-por-la-ia/

Asamblea Popular Nacional de China. (2021). Ley de Seguridad de Datos. (Vigente desde septiembre de 2021).

Asamblea Popular Nacional de China. (2021). Ley de Protección de Información Personal. (Vigente desde noviembre de 2021).

Asamblea Popular Nacional de China. (2017). Ley de Ciberseguridad. (Con borrador de enmiendas en 2022).

Ategi. (2025, marzo 20). La carrera global de la IA: EE.UU. crea, China copia y la UE regula. https://ategi.com/2025/03/20/la-carrera-global-de-la-ia-ee-uu-crea-china-copia-y-la-ue-regula/

Bruegel. (2024). Thinking European first and its implications. Bruegel. Recuperado de https://www.bruegel.org/analysis/thinking-european-first-and-its-implications

Burwell, F. G., & Propp, K. (2020, junio). The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf

California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018). Recuperado de https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.100.&lawCode=CIV

Center for Security and Emerging Technologies. (2025). China's facial recognition security measures. Recuperado de https://cset.georgetown.edu/publication/china-facial-recognition-security-measures/

Chairs & Vice-Chairs of the Working Groups. (2025). *Transparency (Third Draft): General-Purpose AI Code of Practice*. Archivo PDF. https://your-local-path/Transparency__Third_Draft_GeneralPurpose_AI_Code_of_Practice_ItcMzic7MB6QPLCwhT5zXs5HMI_113607.pdf originalmente recuperado de European Commission. (2025). *Third Draft of the General-Purpose AI Code of Practice published, written by independent experts*. *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts

China Cyberspace Administration. (2023). Medidas provisionales para la gestión de servicios de inteligencia artificial generativa. Recuperado de https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

China Film Administration. (2025). China issues circular to boost well-regulated development of VR films. Recuperado de https://english.www.gov.cn/news/202503/22/content_WS67de12a0c6d0868f4e8f10f2.html

China Internet Network Information Center (CNNIC). (2017). Introducción al CNNIC. Recuperado de https://www.cnnic.com.cn/IC/Events/201706/t20170608_69324.htm

CNNIC. (2020, mayo 13). Introducción al CNNIC [Archivo web]. https://web.archive.org/web/20200513134416/https://cnnic.net.cn/gywm/CNNICjs/jj/

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Comisión Nacional de Desarrollo y Reforma. (2022). Notificación sobre el Apoyo a la Construcción de Escenarios de Aplicación Demostrativa de IA de Nueva Generación. http://en.npc.gov.cn.cdurl.cn/

Comité Técnico Nacional de Normalización de Seguridad de la Información (TC260). (2024). Requisitos básicos de seguridad para los servicios de inteligencia artificial generativa (TC260-003). Recuperado de https://www.tc260.org.cn/

Consejo de Europa. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Disponible en https://rm.coe.int/1680afae3c

Curran, B. (2016). "The best or worst thing to happen to humanity" – Stephen Hawking launches Centre for the Future of Intelligence. University of Cambridge. https://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of

Cyberspace Administration of China. (2022). Amendments to the Cybersecurity Law of the People's Republic of China. Recuperado de https://www.cac.gov.cn/2022-07/01/c_1690898327029107.htm

Cyberspace Administration of China & Ministry of Public Security. (2025). Measures for the Security Management of Facial Recognition Technology. Recuperado de https://www.hunton.com/privacy-and-information-security-law/china-releases-new-rules-regarding-the-use-of-facial-recognition-technology

ENISA. (2023). Cybersecurity awareness: Raising awareness and educating users to improve cyber resilience. https://www.enisa.europa.eu/publications/cybersecurity-awareness-raising-awareness-and-educating-users-to-improve-cyber-resilience

Eland Cables. (2021). The growing number of data centres around the world. https://www.elandcables.com/company/news-and-events/the-growing-number-of-data-centres-around-the-world

EU AI Act. (2024). Implementation Timeline. Recuperado de, https://artificialintelligenceact.eu/implementation-timeline/

European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Gobierno Municipal de Shanghái. (2022). Regulaciones de Shanghai para Promover el Desarrollo de la Industria de IA.

Gobierno Municipal de Shenzhen. (2021). Normas Éticas para la IA en Shenzhen.

Gobierno de la República Popular China. (2017). Plan de Desarrollo de la Nueva Generación de Inteligencia Artificial. https://english.www.gov.cn/

Gooding, M. (2024). CBRE: Data center demand in Europe outstrips supply. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/cbre-data-center-demand-in-europe-outstrips-supply/

Harper, D. (2024). *Etymology of prompt*. Online Etymology Dictionary. Retrieved June 19, 2025, from **https://www.etymonline.com/word/prompt**

Hawking, S. (2014). Speech at the inauguration of the Centre for the Future of Intelligence, University of Cambridge. [Discurso]. University of Cambridge. https://www.bbc.com/news/technology-30290540

Howard, A. (2024). In AI we trust — too much? MIT Sloan Management Review. https://sloanreview.mit.edu/article/in-ai-we-trust-too-much/

Human Rights Watch. (2019). China's algorithms of repression: Reverse-engineering a Xinjiang police surveillance app. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Implementation Timeline. (2024) *EU Artificial Intelligence Act*. https://artificialintelligenceact.eu/implementation-timeline/

Investopedia. (2025). What's Inside the EU AI Act—and What It Means for Your Privacy. Investopedia. https://www.investopedia.com/eu-ai-act-11737033

Lang, J. M. (2025). AI as a thought partner in higher education. EDUCAUSE Review. https://er.educause.edu/articles/2025/4/ai-as-a-thought-partner-in-higher-education

Ministerio de Ciencia y Tecnología de China. (2023). Medidas de Revisión Ética en Ciencia y Tecnología (prueba). (Vigentes desde diciembre de 2023).

Mistral AI. (2023). About. https://mistral.ai/about

Moles (2024). Miedos a la inteligencia artificial. infoLibre. https://www.infolibre.es/opinion/plaza-publica/miedos-inteligencia-artificial_129_1546767.html

Mordor Intelligence. (2025). Europe colocation market industry report. Recuperado el 17 de junio de 2025, de https://www.mordorintelligence.com/es/industry-reports/europe-colocation-market-industry

Mucci. para IBM. (2024). Open source AI tools. IBM Think. Recuperado de https://www.ibm.com/es-es/think/insights/open-source-ai-tools#:~:text=La%20inteligencia%20artificial%20(IA)%20de,pueda%20utilizarlo%2C%20modificarlo%20y%20distribuirlo

OpenAI. (2025). ChatGPT (versión GPT-4) [Large language model]. https://chat.openai.com/

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, L 2024/1689. https://op.europa.eu/es/publication-detail/-/publication/dc8116a1-3fe6-11ef-865a-01aa75ed71a1/language-es

Porwol, T. (2024). Google kämpft gegen EU-KI-Regulierung: Berliner Gipfel beginnt. Bild. https://m.bild.de/leben-wissen/digital/google-kaempft-gegen-eu-ki-regulierung-berliner-gipfel-beginnt-670f9777c383db1a97cd21e8

Primack, D. (2023). In an AI arms race set off by ChatGPT, ethics may be the first casualty. Axios. https://www.axios.com/2023/01/31/chatgpt-ai-arms-race-ethics-competition

Research and Markets. (2024). Central & Eastern Europe data center construction market Outlook 2024–2029: Digitalization to drive a surge in investments by colocation, cloud, internet, and telecommunication providers [comunicado de prensa]. GlobeNewswire.

https://www.globenewswire.com/news-release/2024/07/16/2913516/0/en/Central-Eastern-Europe-Data-Center-Construction-Market-Outlook-2024-2029-Digitalization-to-Drive-a-Surge-in-Investments-by-Colocation-Cloud-Internet-and-Telecommunication-Providers.html

Rodríguez, J., & García-Herrero, A. (2023). ¿Innovar o morir? La UE ante el desafío industrial y tecnológico de EEUU y China: Hoja de ruta para la presidencia española de la UE [Policy Paper]. Real Instituto Elcano. https://www.realinstitutoelcano.org/policy-paper/innovar-o-morir-la-ue-ante-el-desafio-industrial-y-tecnologico-de-eeuu-y-china-hoja-de-ruta-para-la-presidencia-espanola-de-la-ue/

SEOZoom. (2025). *AI prompts: meaning, techniques, building examples*. SEOZoom. Retrieved June 19, 2025, from https://www.seozoom.com/prompts/

State Council of the People's Republic of China. (2017). Next Generation Artificial Intelligence Development Plan (Document No. 35). Recuperado de https://english.www.gov.cn/policies/latest_releases/201707/201707/20170713/202207/t20220713_1071106.html

Standing Committee of the National People's Congress. (2021). Data Security Law of the People's Republic of China (Ley No. 35). Recuperado de https://www.npc.gov.cn/zgrdw/npc/dbdhhy/12_1/2021-06/10/content_2068709.htm

Sutherland, E. H. (1947). Principles of criminology (4th ed.). Philadelphia, PA: J. B. Lippincott Company. Disponible en: https://archive.org/details/principlesofcrim00suth

Tews, S. (2025, febrero 20). Securing our Digital Future: Balancing Innovation, Economic Growth, and Cybersecurity in a Connected World. Seminario presentado como parte del programa de seminarios externos en el Máster de Integración Europea, Universidad Autónoma de Barcelona.

Unión Europea. (2016). Tratado de Funcionamiento de la Unión Europea (TFUE). Diario Oficial de la Unión Europea, C 202, 1-388. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:2016:202:TOC

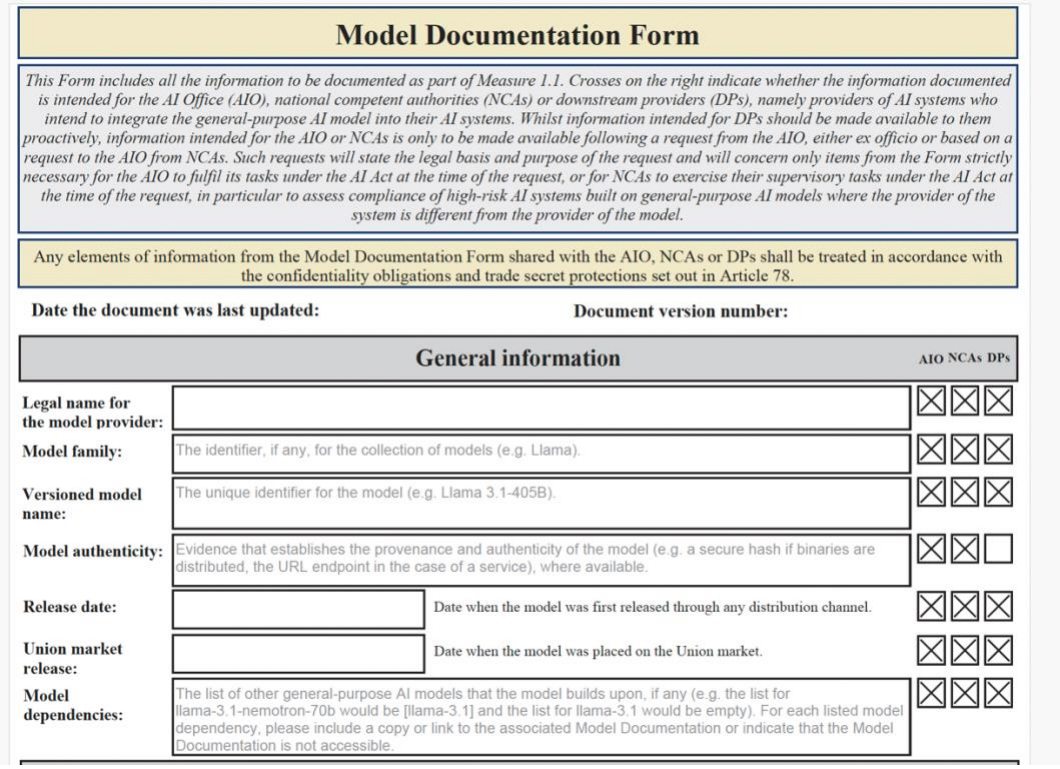
Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119, 1-88. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Walker, J. (2024). AI ambitions: Kao Data breaks ground on fourth UK data center. Data Center Knowledge. Recuperado de https://www.datacenterknowledge.com/data-center-construction/ai-ambitions-kao-data-breaks-ground-on-fourth-uk-data-center

Anexos

Anexo 1:

Chairs & Vice-Chairs of the Working Groups. (2025). *Transparency (Third Draft): General-Purpose AI Code of Practice*. Archivo PDF. https://your-local-path/Transparency__Third_Draft_GeneralPurpose_AI_Code_of_Practice_ItcMzic7MB6QPLCwhT5zXs5HMI_113607.pdf originalmente recuperado de European Commission. (2025). *Third Draft of the General-Purpose AI Code of Practice published, written by independent experts*. *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts



Model Documentation Form

This Form includes all the information to be documented as part of Measure 1.1. Crosses on the right indicate whether the information documented is intended for the AI Office (AIO), national competent authorities (NCAs) or downstream providers (DPs), namely providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Whilst information intended for DPs should be made available to them proactively, information intended for the AIO or NCAs is only to be made available following a request from the AIO, either ex officio or based on a request to the AIO from NCAs. Such requests will state the legal basis and purpose of the request and will concern only items from the Form strictly necessary for the AIO to fulfil its tasks under the AI Act at the time of the request, or for NCAs to exercise their supervisory tasks under the AI Act at the time of the request, in particular to assess compliance of high-risk AI systems built on general-purpose AI models where the provider of the system is different from the provider of the model.

Any elements of information from the Model Documentation Form shared with the AIO, NCAs or DPs shall be treated in accordance with the confidentiality obligations and trade secret protections set out in Article 78.

Date the document was last updated: **Document version number:**

General information		AIO	NCAs	DPs
Legal name for the model provider:		☒	☒	☒
Model family:	The identifier, if any, for the collection of models (e.g. Llama).	☒	☒	☒
Versioned model name:	The unique identifier for the model (e.g. Llama 3.1-405B).	☒	☒	☒
Model authenticity:	Evidence that establishes the provenance and authenticity of the model (e.g. a secure hash if binaries are distributed, the URL endpoint in the case of a service), where available.	☒	☒	☐
Release date:	Date when the model was first released through any distribution channel.	☒	☒	☒
Union market release:	Date when the model was placed on the Union market.	☒	☒	☒
Model dependencies:	The list of other general-purpose AI models that the model builds upon, if any (e.g. the list for llama-3.1-nemotron-70b would be [llama-3.1] and the list for llama-3.1 would be empty). For each listed model dependency, please include a copy or link to the associated Model Documentation or indicate that the Model Documentation is not accessible.	☒	☒	☒

Model properties

		AIO	NCAs	DPs
Model architecture:	A general description of the model architecture, e.g. a transformer architecture. [Recommended 20 words]	☒	☒	☒
	If the model is a general-purpose AI model with systemic risk, provide a detailed description of the model architecture, specifying where it departs from standard architectures where applicable. If the model is not a general-purpose AI model with systemic risk, write 'N/A'.	☒	☐	☐
Design specification of the model:	A general description of the key design choices of the model, including rationale and assumptions made, to provide basic understanding into how the model was designed. [Recommended 100 words]	☒	☒	☐
Input modalities: *For each selected modality, please include maximum input size or write 'N/A' if not defined.*	☐ Text; ☐ Images; ☐ Audio; ☐ Video; If any other please specify:	☒	☒	☒
	Maximum size: (Text) / Maximum size: (Images) / Maximum size: (Audio) / Maximum size: (Video) / Maximum size: (other)	☐	☐	☒
Output modalities: *For each selected modality, please include maximum output size or write 'N/A' if not defined.*	☐ Text; ☐ Images; ☐ Audio; ☐ Video; If any other please specify:	☒	☒	☒
	Maximum size: (Text) / Maximum size: (Images) / Maximum size: (Audio) / Maximum size: (Video) / Maximum size: (other)	☐	☐	☒
Total model size:	The total number of parameters of the model, recorded with at least two significant figures, e.g 7.3*10^10 parameters.	☒	☐	☐
Select the range that the total number of parameters belongs to.	☐ 1-500M; ☐ 500M-5B; ☐ 5B-15B; ☐ 15B-50B; ☐ 50B-100B; ☐ 100B-500B; ☐ 500B-1T; ☐ >1T	☐	☒	☒

Methods of distribution and licenses

		AIO	NCAs	DPs
Distribution channels:	A list of every distribution channel (e.g. enterprise or subscription-based access through existing software suites or enterprise-specific solutions; public or subscription-based access through an API; public or proprietary access through integrated development environments, device-specific applications or firmware, open-source repositories) where the model can be accessed by external parties to the knowledge of the model provider. For each listed distribution channel, please include a link to information about how the model can be accessed where available and the level of model access (e.g. weights-level access, black-box access) via the channel.	☒	☒	☒
License:	A link to model license(s) (otherwise attach a copy to this document) or indicate that none exists.	☒	☒	☐
	The type or category of license(s) under which the model could be made available to downstream providers.	☐	☐	☒
	A list of additional assets (e.g. training data, data processing code, model training code, model inference code, model evaluation code), if any, that are made available with a description of how each can be accessed and what licenses, if any, relate to their use.	☒	☒	☐

Use

		AIO	NCAs	DPs
Acceptable Use Policy:	Provide a link to the acceptable use policy applicable (or attach a copy to this document) or indicate that none exists.	☒	☒	☒
Intended uses:	A description of either (i) the uses that are intended by the provider (e.g. productivity enhancement, translation, creative content generation, data analysis, data visualisation, programming assistance, scheduling, customer support, variety of natural language tasks, etc..) or (ii) the uses that are restricted and/or prohibited by the provider (beyond those prohibited by EU or international law, including Article 5 AI Act), in both cases as specified in the information supplied by the provider in the instructions for use, terms and conditions, promotional or sales materials and statements, as well as in the technical documentation. If specifying (i) or (ii) is incompatible with the nature of the license under which the model is provided, then 'N/A' can be entered. [Recommended 200 words]	☒	☒	☒
Type and nature of AI systems in which the general-purpose AI model can be integrated:	A list or description of either (i) the type and nature of AI systems into which the general-purpose AI model can be integrated or (ii) the type and nature of AI systems into which the general-purpose AI model should not be integrated. Examples may include autonomous systems, conversational assistants, decision support systems, creative AI systems, predictive systems, cybersecurity, surveillance, or human-AI collaboration. [Recommended up to 300 words]	☒	☒	☒
Technical means for model integration:	A general description of the technical means (e.g. instructions for use, infrastructure, tools) required for the general-purpose AI model to be integrated into AI systems. [Recommended 100 words]	☐	☐	☒

		AIO	NCAs	DPs
Required hardware:	A description of any hardware, including the version, required to use the model where applicable. If not applicable (e.g. model offered via an API), 'N/A' should be entered. [Recommended 100 words]			☒
Required software:	A description of any software, including the version, required to use the model where applicable. If not applicable, 'N/A' should be entered. [Recommended 100 words]			☒

Training process

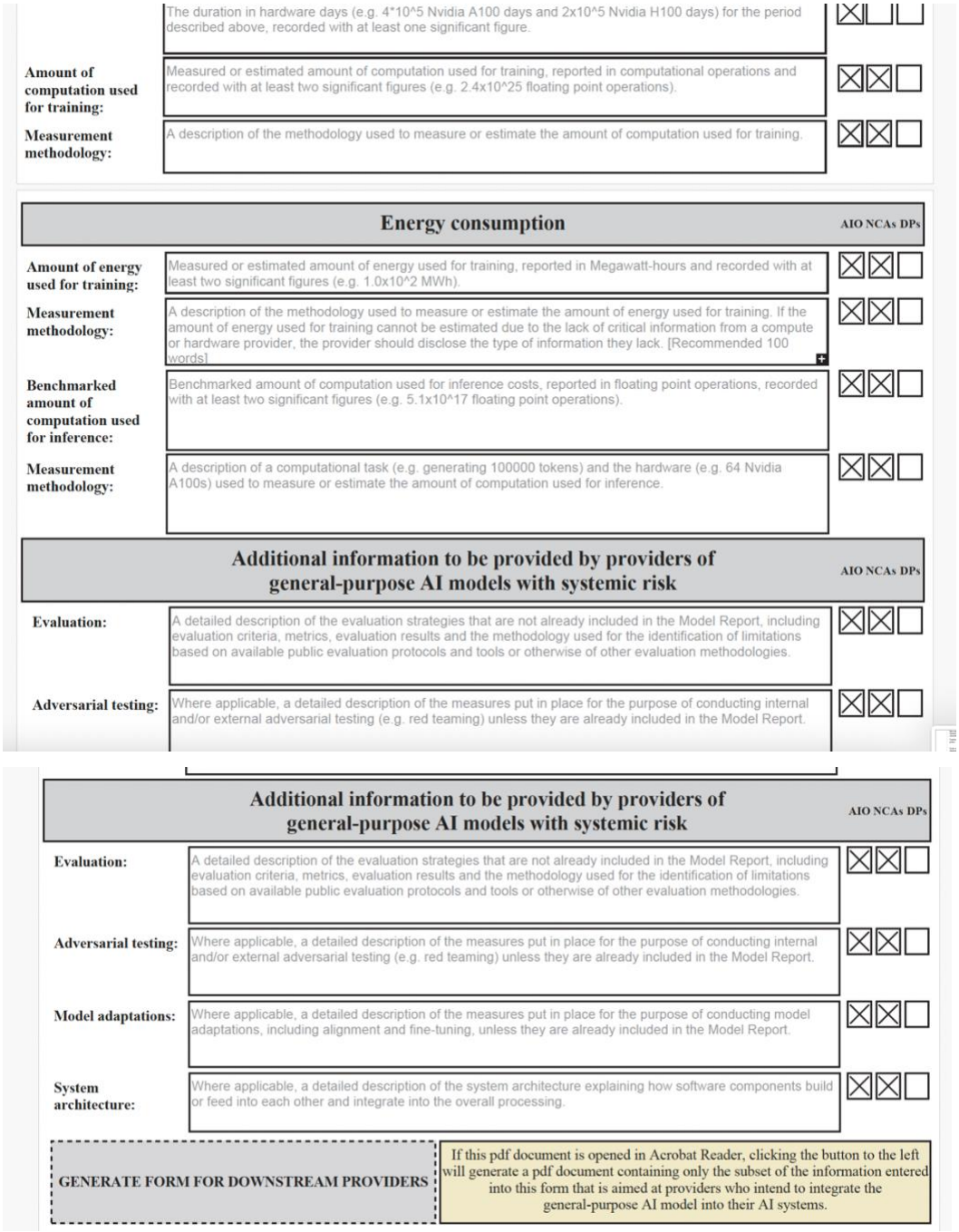
		AIO	NCAs	DPs
Design specification of the training process:	A general description of the main steps or stages involved in the training process, including training methodologies and techniques, the key design choices, assumptions made and what the model is designed to optimise for. For example, "the model is initialized with randomly selected weights and optimised using gradient-based optimization via the Adam optimizer in two steps. First, the model is trained to predict the next word on a large pretraining corpus using the cross-entropy loss, passing over the data for a single epoch. Second, the model is post-trained on a dataset of human preferences for 10 epochs to align the model with human values and make it more useful in responding to user prompts". [Recommended 200 words]	☒	☒	☐
Relevance of different parameters:	The relevance of different parameters, as applicable.	☒	☒	☐
Decision rationale:	A description of how and why key design choices were made in model training. [Recommended 200 words]	☒	☒	☐

Information on the data used for training, testing, and validation

		AIO	NCAs	DPs
Training data type/modality: *Select all that apply.*	☐ Text ☐ Images ☐ Audio ☐ Video If any other please specify:	☒	☒	☒
Training data provenance: *Select all that apply.*	☐ Web crawling ☐ Private data licensed by or on behalf of rights holders, or acquired from other third parties ☐ User data ☐ Publicly available datasets ☐ Data annotation or creation potentially through relationships with third parties ☐ Data collected through other means ☐ Synthetically generated data (when created directly by the provider or on behalf of the provider) If any other please specify:	☒	☒	☒
How data was obtained and selected:	A description of the methods used to obtain and select data, including methods and resources used to annotate data, and models and methods used to generate synthetic data where applicable. [Recommended 300 words]	☒	☒	☐
Number of data points:	The size (in number of data points) of the training, testing, and validation data respectively, together with the definition of the unit of data points (e.g. tokens or documents, images, hours of video or frames,...), recorded with at least two significant figures (e.g. 1.5x10^13 tokens).	☒	☒	☐
Scope and main characteristics:	A general description of the scope and main characteristics of the training data, such as domain (e.g. healthcare, science, law,...), geography (e.g. global, restricted to a certain region,...), language, modality coverage, where applicable. In the case that previously acquired data was used, a description of how the model provider acquired the rights to the data and which products and services were involved if the data corresponds to user data from products and services. [Recommended 200 words]	☒	☒	☐
Data curation methodologies:	General description of the data processing involved in transforming the acquired data into training data for the model, e.g. cleaning (e.g. filtering out irrelevant content such as ads), normalisation (e.g. tokenizing), augmentation (e.g. back-translation). [Recommended 300 words]	☒	☒	☒
Measures to detect unsuitability of data sources (harmful data):	A description of any methods implemented in data acquisition or processing, if any, to address illegal or harmful content in the training data, including, but not limited to, child sexual abuse material (CSAM) and non-consensual intimate imagery (NCII). [Recommended 300 words]	☒	☒	☐
Measures to detect unsuitability of data sources (personal data):	A description of any methods implemented in data acquisition or processing, if any, to address the prevalence of personal data in the training data, where relevant and applicable. [Recommended 200 words]	☒	☒	☐
Measures to detect identifiable biases:	A description of any methods implemented in data acquisition or processing, if any, to address the prevalence of identifiable biases in the training data. [Recommended 200 words]	☒	☒	☐

Computational resources

		AIO	NCAs	DPs
Training time:	A description of what period is being measured along with the duration in wall clock days (e.g. 9x10^1 days), recorded with at least one significant figure.	☒	☒	☐



		AIO NCAs DPs
	The duration in hardware days (e.g. 4*10^5 Nvidia A100 days and 2x10^5 Nvidia H100 days) for the period described above, recorded with at least one significant figure.	☒☐☐
Amount of computation used for training:	Measured or estimated amount of computation used for training, reported in computational operations and recorded with at least two significant figures (e.g. 2.4x10^25 floating point operations).	☒☒☐
Measurement methodology:	A description of the methodology used to measure or estimate the amount of computation used for training.	☒☒☐

Energy consumption		AIO NCAs DPs
Amount of energy used for training:	Measured or estimated amount of energy used for training, reported in Megawatt-hours and recorded with at least two significant figures (e.g. 1.0x10^2 MWh).	☒☒☐
Measurement methodology:	A description of the methodology used to measure or estimate the amount of energy used for training. If the amount of energy used for training cannot be estimated due to the lack of critical information from a compute or hardware provider, the provider should disclose the type of information they lack. [Recommended 100 words]	☒☒☐
Benchmarked amount of computation used for inference:	Benchmarked amount of computation used for inference costs, reported in floating point operations, recorded with at least two significant figures (e.g. 5.1x10^17 floating point operations).	☒☒☐
Measurement methodology:	A description of a computational task (e.g. generating 100000 tokens) and the hardware (e.g. 64 Nvidia A100s) used to measure or estimate the amount of computation used for inference.	☒☒☐

Additional information to be provided by providers of general-purpose AI models with systemic risk		AIO NCAs DPs
Evaluation:	A detailed description of the evaluation strategies that are not already included in the Model Report, including evaluation criteria, metrics, evaluation results and the methodology used for the identification of limitations based on available public evaluation protocols and tools or otherwise of other evaluation methodologies.	☒☒☐
Adversarial testing:	Where applicable, a detailed description of the measures put in place for the purpose of conducting internal and/or external adversarial testing (e.g. red teaming) unless they are already included in the Model Report.	☒☒☐

Additional information to be provided by providers of general-purpose AI models with systemic risk		AIO NCAs DPs
Evaluation:	A detailed description of the evaluation strategies that are not already included in the Model Report, including evaluation criteria, metrics, evaluation results and the methodology used for the identification of limitations based on available public evaluation protocols and tools or otherwise of other evaluation methodologies.	☒☒☐
Adversarial testing:	Where applicable, a detailed description of the measures put in place for the purpose of conducting internal and/or external adversarial testing (e.g. red teaming) unless they are already included in the Model Report.	☒☒☐
Model adaptations:	Where applicable, a detailed description of the measures put in place for the purpose of conducting model adaptations, including alignment and fine-tuning, unless they are already included in the Model Report.	☒☒☐
System architecture:	Where applicable, a detailed description of the system architecture explaining how software components build or feed into each other and integrate into the overall processing.	☒☒☐

GENERATE FORM FOR DOWNSTREAM PROVIDERS	If this pdf document is opened in Acrobat Reader, clicking the button to the left will generate a pdf document containing only the subset of the information entered into this form that is aimed at providers who intend to integrate the general-purpose AI model into their AI systems.

Anexo 2:

Implementation Timeline. (2024) *EU Artificial Intelligence Act*. https://artificialintelligenceact.eu/implementation-timeline/

This page lists all of the key dates you need to be aware of relating to the implementation of the EU AI Act.

Related resources

Tasks and Responbilities

For a summary of all tasks and responsibilities assigned to the AI Office or Member States by the EU AI Act, see our blog posts and infographics on the topic.

Historic Timeline

For a timeline of all key events in the AI Act's history so far, see our Historic Timeline of the AI Act.

EU AI Act Newsletter

If you want to be notified about significant updates to the Act and its implementation, subscribe to the EU AI Act Newsletter, a biweekly newsletter by the Future of Life Institute.

Timeline of key dates

Last updated: 1 August 2024

Items in blue relate to the Application of the Act.

Download timeline as image

2024

2024

Date		Related AI Act Content
12 July 2024	The AI Act is published in the Official Journal of the European Union. This serves as the formal notification of the new law.	Article 113
1 August 2024	**Application:** Date of entry into force of the AI Act. At this stage, none of the Act's requirements apply—they will begin to apply gradually over time.	Article 113
2 November 2024	**Member States:** Deadline for Member States to identify and publicly list the authorities / bodies responsible for fundamental rights protection, and to notify the Commission and other Member States.	Article 77(2)

2025

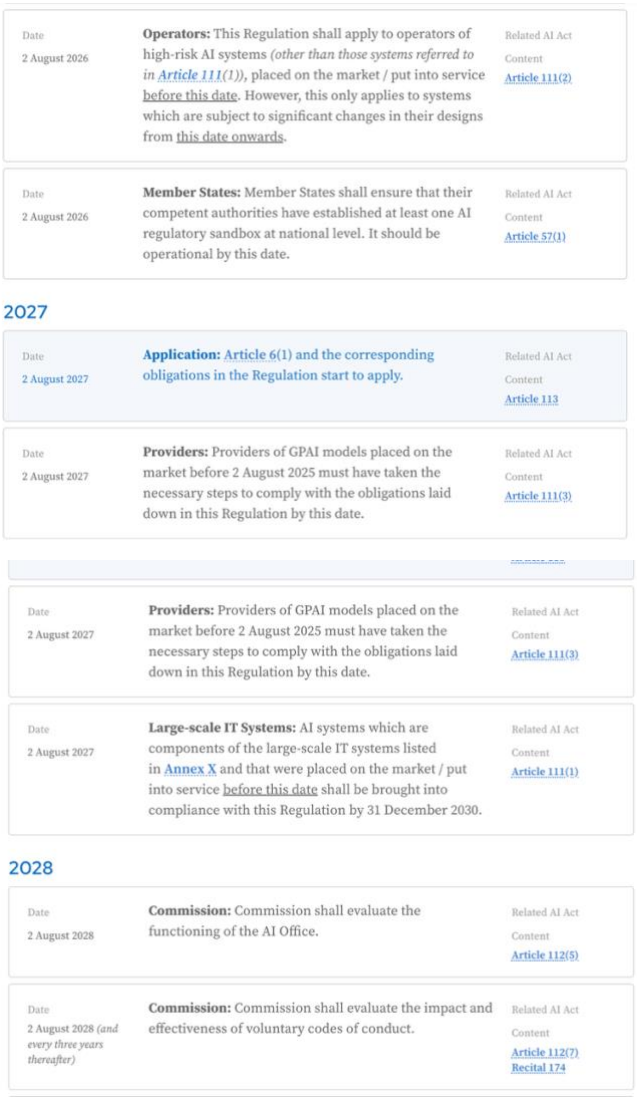
Date		Related AI Act Content
2 February 2025	**Application:** Prohibitions on certain AI systems and requirements on AI literacy start to apply (Chapter 1 and Chapter 2).	Article 113(a) Recital 179
2 May 2025	**Commission:** Codes of practice shall be ready by this date.	Article 56(9) Recital 179

YOU ARE HERE

Date		Related AI Act Content
2 August 2025	**Application:** The following rules start to apply: • Notified bodies (Chapter III, Section 4), • GPAI models (Chapter V), • Governance (Chapter VII), • Confidentiality (Article 78) • Penalties (Articles 99 and 100)	Article 113(b)
2 August 2025	**Providers:** Providers of GPAI models that have been placed on the market / put into service before this date need to be compliant with the AI Act by 2 August 2027.	Article 111(3)
2 August 2025 *(and every two years thereafter)*	**Member States:** Deadline for Member States to report to the Commission on the status of the financial and human resources of the national competent authorities.	Article 70(6)
2 August 2025	**Member States:** Deadline for Member States to designate national competent authorities *(notifying authorities and market surveillance authorities)*, communicate them to the Commission, and make their contact details publicly available.	Article 70(2)
2 August 2025 *(based on date of application of Articles on 'Penalties')*	**Member States:** Deadline for Member States to lay down rules for penalties and fines, notify them to the Commission, and ensure that they are properly implemented.	Recital 179
2 August 2025	**Commission:** *(If code of practice cannot be finalised, or if the AI Office deems it is not adequate)* Commission may provide common rules for the implementation of the obligations for providers of GPAI models via implementing acts.	Article 56(9)
2 August 2025 *(and every year thereafter)*	**Commission:** Deadline for annual Commission review and possible amendments on prohibitions.	Article 112(1)

2026

Date		Related AI Act Content
2 February 2026	**Commission:** Deadline for Commission to provide guidelines specifying the practical implementation of Article 6, including post-market monitoring plan.	Articles 6(5), 72(3)
2 August 2026	**Application:** The remainder of the AI Act starts to apply, except Article 6(1).	Article 113



Date		Related AI Act Content
2 August 2026	**Operators:** This Regulation shall apply to operators of high-risk AI systems *(other than those systems referred to in Article 111(1))*, placed on the market / put into service before this date. However, this only applies to systems which are subject to significant changes in their designs from this date onwards.	Article 111(2)
2 August 2026	**Member States:** Member States shall ensure that their competent authorities have established at least one AI regulatory sandbox at national level. It should be operational by this date.	Article 57(1)

2027

Date		Related AI Act Content
2 August 2027	**Application:** Article 6(1) and the corresponding obligations in the Regulation start to apply.	Article 113
2 August 2027	**Providers:** Providers of GPAI models placed on the market before 2 August 2025 must have taken the necessary steps to comply with the obligations laid down in this Regulation by this date.	Article 111(3)
2 August 2027	**Providers:** Providers of GPAI models placed on the market before 2 August 2025 must have taken the necessary steps to comply with the obligations laid down in this Regulation by this date.	Article 111(3)
2 August 2027	**Large-scale IT Systems:** AI systems which are components of the large-scale IT systems listed in Annex X and that were placed on the market / put into service before this date shall be brought into compliance with this Regulation by 31 December 2030.	Article 111(1)

2028

Date		Related AI Act Content
2 August 2028	**Commission:** Commission shall evaluate the functioning of the AI Office.	Article 112(5)
2 August 2028 *(and every three years thereafter)*	**Commission:** Commission shall evaluate the impact and effectiveness of voluntary codes of conduct.	Article 112(7) Recital 174

Total: 12.345 palabras