Los desafíos de la trazabilidad en la era de las black boxes

The Challenges of Traceability in the Era of Black Boxes

Mariana Soria Galvarro Gaillard

Católica Global School of Law • Lisboa, Portugal
https://orcid.org/0009-0009-2960-3052 • marianagaillard@gmail.com

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 Nº 18, abril 2026, pp. 179-193
ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).
DOI: https://doi.org/10.35319/lawreview.202618139
Recibido: 31 de octubre de 2025 • Aceptado: 16 de abril de 2026

Resumen

El presente artículo realiza una revisión crítica al AI Act, centrando el análisis en la estructura funcional que éste establece, a través de la cual, asigna roles y responsabilidades diferenciadas a los distintos actores de la cadena de valor de los sistemas de inteligencia artificial. Principalmente, examina la distribución de obligaciones a lo largo del ciclo de vida de dichos sistemas, con especial atención a los contextos de opacidad algorítmica en los sistemas de tipo Black Box, en los que los procesos decisionales internos resultan inaccesibles o complejos de reconstruir incluso para sus propios desarrolladores. Se plantea si el AI Act puede garantizar una atribución efectiva de responsabilidades frente al avance tecnológico y la proliferación de contenido sintético, dado que la trazabilidad técnica se torna progresivamente más dificultosa. La tesis central sostiene que una posible solución consiste en robustecer el entramado probatorio e incorporar la figura del Logger, lo que permitiría conservar evidencia del proceso decisional y prevenir que las obligaciones establecidas en el AI Act se reduzcan a una categoría formal e ineficaz. Sin embargo, concluye en que la implementación práctica enfrenta un desafío sustancial; pues,

el descomponer exhaustivamente la cadena de decisiones de un sistema de IA, cuando su diseño prioriza la eficiencia sobre la explicabilidad, sería, en muchos casos, incompatible con la propia lógica operativa de eficiencia.

Palabras clave: AI Act; Black Boxes; contenido sintético; opacidad algorítmica; responsabilidad; trazabilidad.

Abstract

This article offers a critical examination of the AI Act, centering its analysis on the functional framework it establishes and the way it allocates distinct roles and responsibilities to the several actors involved in the value chain of artificial intelligence systems. In particular, it examines the distribution of obligations throughout the lifecycle of such systems, with special attention to contexts of algorithmic opacity in Black Box systems, where internal decision-making processes are inaccessible or difficult to reconstruct, even for their own developers. The article questions whether the AI Act can ensure effective attribution of responsibilities in light of technological advancement and the proliferation of synthetic content, given that technical traceability becomes increasingly challenging. The central argument posits that a possible solution lies in strengthening the evidentiary framework and incorporating the figure of the Logger, which would allow for the preservation of decision-making records and prevent obligations from being reduced to a merely formal and ineffective categories. Nevertheless, it concludes that practical implementation poses a significant challenge; because the exhaustive decomposition of an AI system's decision-making chain, when its design prioritizes efficiency over explainability, would, in many cases, be incompatible with the very operational logic of efficiency.

Keywords: AI Act; Black Boxes; synthetic content; algorithmic opacity; responsability; traceability.

1. Confiar sin cuestionar

Si un modelo de aprendizaje automático ofrece un alto rendimiento, ¿por qué no limitarse a confiar en sus resultados sin cuestionar los motivos detrás de sus decisiones? El problema es que una sola métrica, como la exactitud de clasificación, es una descripción incompleta de la mayoría de las tareas del mundo real (Doshi-Velez & Kim, 2017).

El despliegue masivo de la inteligencia artificial (IA) plantea desafíos concretos para la atribución de responsabilidad en el Derecho contemporáneo. Sin duda, estamos viviendo algo que no se trata propiamente de una crisis ontológica del orden jurídico, pero sí de un desafío esencialmente práctico y probatorio; pues la IA difumina la autoría y erosiona la trazabilidad del contenido, dificultando la identificación del sujeto responsable de los sistemas de IA a partir de sus roles establecidos en el marco principal del presente artículo, que es el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de la Unión Europea, relativo a la inteligencia artificial (en adelante, el AI Act).

Antes de avanzar, conviene precisar que, a lo largo de este artículo, el término "responsabilidad" se emplea exclusivamente en el sentido de atribución de roles, funciones o cargos, y no como responsabilidad civil derivada de la reparación de daños ocasionados por el uso de sistemas de IA. Esta última, a la fecha, no se encuentra configurada como un régimen jurídico específico. En consecuencia, toda referencia que se haga a las responsabilidades de los distintos actores de los sistemas referidos, deberá entenderse exclusivamente como las obligaciones propias derivadas del cargo o rol específico que cada uno ocupa dentro de la cadena de valor, y no como una noción derivada del concepto de *liability* propio del Derecho de daños.

En ese entendido y regresando a la problemática de la referida trazabilidad; en definitiva, si bien la IA desempeña hoy un papel central en la automatización y optimización de la creación de contenidos en múltiples ámbitos, esta transformación digital exige, a su vez, la implementación de salvaguardas que permitan validar

la autenticidad de la información. Especialmente, en un contexto donde crece la producción y circulación de información sintética mediante modelos avanzados como las GANs[1], se requiere de instrumentos técnicos que transformen *outputs* opacos en cadenas de responsabilidad verificables.

En efecto, hoy en día, se están implementando métodos de validación de fidelidad estadística que garantizan que los datos sintéticos reflejen correctamente las relaciones y características de los datos reales. Paralelamente, se están diseñando marcos de auditoría que establecen salvaguardas socio-técnicas críticas, permitiendo evaluar tanto la integridad técnica como el impacto social de los conjuntos de datos sintéticos (Ghiurău & Popescu, 2025). Sin embargo, y pese a dichos esfuerzos, la velocidad y complejidad de los sistemas de IA dificultan significativamente la demostración técnica efectiva de estas salvaguardas o intentos de ellas. La actualización constante de modelos y datos, junto con la opacidad de muchas arquitecturas, limita la trazabilidad y la verificación ex post en tiempos compatibles con la supervisión regulatoria.

En línea con lo anterior y en el marco del AI Act, se plantea una problemática compleja: por un lado, se atribuye de forma abstracta una personalidad funcional a sistemas que, sin ser sujetos jurídicos, despliegan capacidades decisorias; por otro, los responsables de sistemas de IA asumen una responsabilidad condicionada por la opacidad algorítmica. En consecuencia, al momento de rendir cuentas, con frecuencia carecen del control o de la comprensión necesarios para explicar y demostrar cómo se generan las decisiones.

1 Las redes generativas adversativas (RGAs), también conocidas como GANs en inglés, son una red generativa adversarial. Es un modelo de Machine Learning diseñado para generar datos realistas mediante el aprendizaje de patrones a partir de conjuntos de datos de entrenamiento existentes. Opera dentro de una infraestructura de aprendizaje no supervisado mediante el uso de técnicas de aprendizaje profundo, donde dos redes neuronales trabajan en oposición: una genera datos, mientras que la otra evalúa si los datos son reales o generados (Varughese, 2026).

Si bien el principio antropocéntrico establecido en el AI Act afirma que los sistemas de IA deben servir al ser humano, respetar su dignidad, autonomía y derechos fundamentales, y permanecer bajo control humano efectivo a lo largo de todo su ciclo de vida (Parlamento Europeo y Consejo de la Unión Europea, 2024); este principio rector, requiere que la atribución de responsabilidades sea materialmente verificable, pues la mera asignación formal de deberes resulta insuficiente si no se acompaña de mecanismos probatorios y técnicos que permitan rastrear la procedencia de los *outputs* sintéticos y demostrar el control efectivo de los actores implicados.

¿De qué sirve hablar de personalidad humana si no puedo entender, trazar ni demostrar lo que se me exige?

Por ello, en este artículo, se propone una mirada crítica a la atribución de roles y responsabilidades establecidas por el AI Act; pues, más allá del diseño normativo, el problema aparece cuando esa arquitectura debe operar en contextos donde rastrear, controlar y, sobre todo, probar la influencia sobre resultados – en su mayoría sintéticos – se vuelve cada vez más difícil.

2. La "personalidad" funcional de la IA

En ciertos contextos, resulta legítimo hablar de una "personalidad electrónica" sin el fin, lógicamente, de atribuir conciencia o derechos a la IA, sino para reconocer que muchas decisiones nacen de una interacción compleja entre modelos, datos y operadores humanos, configurando así una hibridación funcional humano-máquina. Esto no supone, desde luego, reconocer personalidad jurídica a la IA ni exonerar a los seres humanos de responsabilidad; más bien pone de manifiesto una crisis en la atribución de obligaciones cuando las operaciones tecnológicas desbordan los parámetros de la práctica tradicional.

Dada la velocidad operativa de los sistemas de IA, la respuesta normativa y doctrinal debería orientarse a reforzar y reconfigurar

los instrumentos probatorios y técnicos que permitan esclarecer la contribución relativa de cada interviniente y evitar así una forma de "responsabilidad a ciegas".

Una de las razones principales para motivar el desarrollo e implementación de estos instrumentos probatorios técnicos, es que permitirían que los derechos de reclamación y explicación previstos en los artículos 85 y 86 del AI Act no queden en lo meramente formal, sino que se ejerzan de forma efectiva.

En particular, el artículo 86 reconoce el derecho a recibir explicaciones claras sobre cómo un sistema influyó en una decisión, lo que plantea una dificultad de fondo; lo cual nos conduce a la ardua tarea de cómo justificar resultados generados con información mayoritariamente sintética, generada automáticamente, no elaborada por humanos, y que no puede (dada su limitación técnica) ser reconstruida, revisada ni contrastada con un responsable humano identificable (aunque haya un deber de *human oversight*). A ello, se suma el uso de modelos opacos o *Black Boxes* cuyos resultados no permiten comprender de manera clara el razonamiento seguido.

En suma, el problema no es meramente técnico, sino profundamente procedimental, cíclico y de gran magnitud, pues no hay explicación sin responsable, no hay responsable sin capacidad real de comprensión y control del sistema; y, sin todo ello, el derecho a la explicación corre el riesgo de vaciarse de contenido y convertirse en una garantía difícil, cuando no imposible, de materializar.

3. Comprendiendo la opacidad algorítmica en sistemas de aprendizaje automático

Antes de adentrarse en la estructura de roles diseñada por el AI Act, resulta imprescindible precisar qué debe entenderse por opacidad algorítmica a lo largo del presente artículo.

Jenna Burrell, reconocida investigadora y profesora en la *School of Information* de la Universidad de California, Berkeley, la define como la incapacidad para conocer cómo y por qué un sistema algorítmico produce determinados resultados (*outputs*) a partir de sus datos de entrada (Burrell, 2016).

Burrell distingue tres formas de opacidad: (i) secreto corporativo, entendido como protección propietaria o confidencialidad empresarial; (ii) analfabetismo técnico, esto es, la ilegibilidad del código y la falta de competencias de programación en la mayoría de los públicos; y (iii) opacidad intrínseca del *machine learning*, que deriva de la desalineación entre los procedimientos matemáticos de los modelos y las formas humanas de interpretación semántica (Burrell, 2016).

En línea de lo anterior, en el ámbito del aprendizaje automático, los modelos entrenados con grandes volúmenes de datos generan correlaciones complejas que no siempre reflejan relaciones causales, dando lugar a sistemas de tipo *black box* cuya lógica interna permanece opaca e inaccesible (Burrell, 2016). Un modelo black box es un sistema que no revela sus mecanismos internos. En el ámbito de machine *learning*, el término *black box* se utiliza para describir un modelo que no se puede entender observando sus parámetros (por ejemplo, una red neuronal). Lo opuesto a un *black box* a veces se llama *white box*, también referidos como modelos interpretables (Molnar, 2019).

Naturalmente, esta opacidad algorítmica dificulta la trazabilidad, complica la auditoría y dispersa la responsabilidad entre múltiples actores; e incrementa riesgos sociales relevantes, como discriminación, exclusión y desinformación. Condicionando la confianza y el uso de la información generada.

4. Sujetos regulados y atribución de responsabilidad en el AI Act

Sentado el necesario preámbulo sobre la opacidad algorítmica y sus inherentes dificultades interpretativas; entremos de lleno en el Reglamento, el cual, conforme habíamos adelantado, despliega una cadena escalonada de responsabilidades entre los distintos actores de los sistemas de IA.

Dentro de la arquitectura establecida en el AI Act, el artículo 3, define las principales categorías de actores regulados en el ecosistema de la IA, incluyendo al proveedor, implantador (o usuario profesional), importador, distribuidor y representante autorizado; que, en conjunto, articulan un sistema integral de control a lo largo del ciclo de vida de los sistemas de IA. Sin embargo, el análisis conjunto revela una tensión estructural; mientras la normativa define con precisión las obligaciones formales de cada sujeto, la verificación material de su cumplimiento se diluye progresivamente, generando una trazabilidad fragmentada y, en última instancia, opaca.

El punto de partida lo constituye el Proveedor. Conforme al artículo 16, este actor asume la carga normativa más intensa, pues debe garantizar los requisitos técnicos y de seguridad, implementar sistemas de gestión de calidad, conservar documentación y registros, realizar evaluaciones de conformidad, emitir la declaración UE de conformidad y colocar el Marcado CE. Esta concentración de obligaciones lo sitúa como el nodo originario de la responsabilidad, desde el cual se proyecta la legitimidad del sistema hacia el resto de la cadena.

Mencionado anteriormente, el Marcado CE es, en primer término, una declaración jurídica de conformidad. Indica que el Proveedor afirma que el producto o sistema cumple los requisitos aplicables de la normativa de la UE. En suma, opera como un régimen de conformidad armonizado. Su función es doble, pues, por un lado, habilita la libre circulación del sistema dentro de la Unión; por otro, opera como punto de anclaje probatorio frente a las autoridades.

Sin embargo, su eficacia debe ser matizada. El Marcado CE se apoya en una presunción de conformidad que descansa en procedimientos de evaluación previos, pero cuya verificación sustantiva es limitada. En la práctica, el control se centra en la existencia de documentación y registros, sin garantizar el acceso a la lógica interna del sistema ni a los flujos de datos que determinan su comportamiento. De este modo, el marcado puede generar una apariencia de seguridad regulatoria que no siempre se corresponde con una trazabilidad efectiva.

A partir de este punto, la cadena de responsabilidades se despliega en actores cuya función es, en gran medida, de verificación y transmisión.

Consiguientemente, el Representante Autorizado, previsto en el artículo 22, actúa como extensión operativa del Proveedor cuando este se encuentra fuera de la Unión. Su papel consiste en servir de interlocutor con las autoridades y ejecutar las tareas delegadas. No obstante, su capacidad de control es estructuralmente limitada: depende de la documentación proporcionada por el propio Proveedor y carece de herramientas autónomas para verificar la conformidad técnica. En consecuencia, más que un garante sustantivo, se configura como un canal formal de comunicación, añadiendo un eslabón adicional a la cadena sin reforzar significativamente la capacidad de supervisión.

El siguiente escalón lo ocupan el Importador y el Distribuidor, cuyas obligaciones, establecidas en los artículos 23 y 24, refuerzan la dimensión documental del control. El Importador, responsable de introducir el sistema en el mercado de la UE, debe verificar la existencia de la evaluación de conformidad, la documentación técnica, la declaración UE de conformidad y el Marcado CE. Esta función es decisiva, pues su actuación habilita la entrada legal del sistema en el mercado. Sin embargo, su capacidad de evaluación es esencialmente formal; no dispone de medios para auditar de manera independiente la conformidad técnica ni la calidad de los procesos subyacentes.

El Distribuidor, por su parte, asume un rol posterior y correctivo. Debe asegurar que el sistema mantiene el Marcado CE y la documentación correspondiente, así como garantizar que las condiciones de almacenamiento y transporte no comprometan su conformidad. Ante indicios de incumplimiento, debe actuar retirando o corrigiendo el producto y colaborando con las autoridades. Aunque introduce una segunda instancia de control, su alcance es igualmente limitado: su intervención se basa en la documentación recibida y en verificaciones externas, sin acceso a auditorías profundas del sistema.

En conjunto, ambos actores evidencian un fenómeno de "traslado de complejidad"; cada nivel de la cadena verifica formalmente lo recibido del anterior, pero ninguno puede penetrar plenamente en la dimensión técnica del sistema. Así, la conformidad se reproduce como una cadena de confianza documental más que como un proceso de validación sustantiva, lo que incrementa la opacidad a medida que el sistema avanza hacia su puesta en el mercado.

Finalmente, el Implantador, regulado en el artículo 26, constituye el último eslabón y, paradójicamente, uno de los más críticos. Como usuario del sistema bajo su autoridad, asume obligaciones operativas relevantes, como: garantizar el uso conforme a las instrucciones del Proveedor, implementar supervisión humana, verificar la idoneidad de los datos bajo su control y monitorear el funcionamiento del sistema, informando sobre riesgos o incidentes. En este sentido, se configura como la última línea de defensa frente a fallos o impactos adversos.

Como se pudo ver, en conjunto, el modelo escalonado del AI Act mantiene una coherencia formal, roles definidos, obligaciones encadenadas y el Marcado CE como una suerte de prueba de conformidad; pero descansa en una lógica predominantemente documental. Esta dependencia debilita su eficacia, pues la trazabilidad se vuelve progresivamente opaca y el sistema se aproxima más a una presunción de cumplimiento que a un control material efectivo, dejando abiertas dudas sobre la atribución real de responsabilidad en entornos de alta complejidad tecnológica.

Como resulta evidente, la cadena de responsabilidades dentro de un sistema de IA, se degrada hasta quedar en una simple transmisión, acompañada de una verificación débil e ineficaz.

5. El rol no contemplado para la trazabilidad de sistemas de IA: el *Logger*

5.1 Un intento fallido: AI Liability Directive (AILD)

En este contexto de tensiones estructurales y limitaciones en la trazabilidad efectiva de responsabilidades, resulta especialmente revelador observar la evolución y eventual abandono de los instrumentos normativos complementarios diseñados para reforzar el sistema.

La retirada de la propuesta de AI Liability Directive (AILD) (Comisión Europea, 2022) evidencia la fragilidad del marco regulatorio de la IA actual. El diseño propuesto del AILD ofrecía, principalmente, una vía práctica para articular presunciones de responsabilidad derivadas del incumplimiento de deberes de diligencia y una posterior reparación de daños civiles.

Su propósito original era abordar deficiencias fundamentales en la legislación de responsabilidad vigente (ahora sí refiriéndonos a *liability*) al tratar los daños causados por sistemas de IA. No obstante, se reconoció que las normas locales de responsabilidad actuales, basadas principalmente en conceptos tradicionales de culpa, resultaban inadecuadas para la compleja realidad de la tecnología de IA moderna (Ashkara, 2025). En suma, no bastaba con afirmar que la responsabilidad seguía siendo humana.

5.2 Logger

A la luz de lo anterior, y ante la proliferación de contenido sintético, la dificultad para seguir el rastro de los *outputs* generados por

Black Boxes hace que la mera asignación de roles y la atribución formal de responsabilidad resulten verdaderamente insuficientes cuando los roles designados carecen de control efectivo sobre la generación, procedencia y circulación de dicho contenido, especialmente el sintético.

En el AI Act, los deberes de supervisión y verificación recaen en quienes desarrollan, integran o comercializan sistemas de IA, con el Marcado CE como referencia central. Sin embargo, la opacidad técnica y la fragmentación de la cadena limitan la eficacia de este esquema; los roles definidos carecen de registros verificables que respalden la responsabilidad en caso de infracción. Esto evidencia la necesidad de una figura similar a un *Logger*, encargada de custodiar de manera neutral la integridad, disponibilidad y verificabilidad de los registros de los sistemas de IA.

La idea de un Logger para los sistemas de IA encuentra inspiración en experiencias consolidadas en otros sectores altamente regulados, como el financiero o el de pagos electrónicos, donde existen entidades o mecanismos dedicados a la auditoría independiente, la conservación de logs y la verificación ex post de operaciones sensibles. Su papel consiste en materializar y preservar registros inmutables, incluyendo entradas, salidas, versiones, metadatos y condiciones operativas, responder a consultas mediante pruebas verificables (por ejemplo, hashes, firmas digitales o snapshots) y mantener la integridad de la cadena de custodia, garantizando así la trazabilidad y evidencia confiable a lo largo del ciclo de vida del sistema (Alda Rodríguez, Díaz López de la Llave, & Horrillo, 2026).

Estas pruebas retenidas en custodia por el Logger, permitirían a los auditores, actuando como verificadores, validar eficientemente los resultados. Como custodio neutral que materializa, sella y preserva registros técnicos verificables, el *Logger* permite reconstruir la génesis y evolución de los outputs sin sacrificar necesariamente la eficiencia operativa.

El *Logger* podría, entre otras potenciales funciones: mantener registros auditables e inmutables (*logs, hashes*) con conservación mínima legal. Esto reforzaría el esquema de roles agregando a

este actor como quien materializa y custodia registros que pueda proveer a los auditores (Alda Rodríguez, Díaz López de la Llave, & Horrillo, 2026). Recopilando documentación como resultado de los deberes de conservación, especialmente la relativa a los sistemas de IA de alto riesgo; preservando, por ejemplo, las *Model Cards y Data Sheets* como herramientas valiosas para el cumplimiento (Song, 2026).

Para su implementación, los sistemas de IA que opten por adoptar estándares elevados de diligencia podrían institucionalizar la figura del *Logger* como un rol técnico-jurídico clave dentro de la cadena de valor del AI Act, adaptado a sus marcos regulatorios nacionales y asignado a entidades públicas o privadas debidamente acreditadas. Esta función permitiría garantizar la trazabilidad y conservación verificable de los procesos decisionales de los sistemas de IA, condición indispensable para auditorías y ejercicio efectivo del derecho al reclamo y justificación de decisiones previsto en el Reglamento.

En efecto, aunque el AI Act se concibe como un marco esencialmente preventivo, su verdadera eficacia se dirime en el ámbito *ex post*, donde la posibilidad de atribuir responsabilidades y evaluar consecuencias, revela si la gobernanza algorítmica cumple, o no, su promesa regulatoria.

6. Conclusión

¿De qué sirve invocar la personalidad humana si no es posible comprender, rastrear ni demostrar aquello que se exige? La IA opera con una suerte de personalidad funcional; actúa, decide y ejecuta, mientras que el ser humano, en muchos casos, se limita a traducir sus efectos.

En definitiva, sin instrumentos que traduzcan la exigida centralidad humana en control verificable y trazabilidad causal, las responsabilidades asignadas por el AI Act se tornan meramente formales.

La retirada de la AILD es muestra clara de la fragilidad del marco regulatorio vigente, ya que los sistemas de IA generan decisiones y realidades sintéticas con una complejidad y velocidad que superan los límites de los tradicionales regímenes de culpa y responsabilidad. Así, mientras hoy podemos hablar de atribuciones y responsabilidades, con las complejidades que eso implique, en el futuro, si hablamos de *liability* plena, nos enfrentaremos a un problema estructural, pues no habrá medios probatorios suficientes para asegurar que los daños civiles sean reparados.

Cerrar esta brecha exige complementar la conformidad formal con evidencia técnica verificable e incorporar la figura del *Logger*. De esta manera (si es que acaso existe una salida perfecta frente al fenómeno que estamos viviendo) la conformidad puede transformarse en responsabilidad revisable, por tanto, exigible; y no una mera declaración. Aun cuando la descomposición exhaustiva de la cadena decisoria contradiga la lógica operativa de eficiencia para la cual los sistemas de IA fueron diseñados.

7. Referencias

Alda Rodríguez, Á., Díaz López de la Llave, G., & Horrillo, P. (2026). Construyendo un log verificable, parte 1: Ideas principales. BBVA. https://www.bbva.com/es/innovacion/construyendo-un-log-verificable-parte-1-ideas-principales/

Ashkara, Z. (2025). AI liability directive withdrawn: EU impact 2025. AI Act Blog. https://www.aiactblog.nl/en/posts/ai-liability-directive-withdrawal

Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. Big Data & Society, 3(1). https://doi.org/10.1177/2053951715622512

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning (arXiv:1702.08608). arXiv. https://doi.org/10.48550/arXiv.1702.08608

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI:

Approaches for Detecting Synthetic Content. Computers, 14(1), 1. https://doi.org/10.3390/computers14010001

Molnar, C. (2019). Interpretable machine learning: A guide for making Black Box models explainable. Leanpub. https://christophm.github.io/interpretable-ml-book/

Comisión Europea. (2022). Propuesta de Directiva del Parlamento Europeo y del Consejo sobre normas de responsabilidad civil extracontractual en materia de inteligencia artificial (COM (2022) 496 final)(AI Liability Directive). https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496

Parlamento Europeo y del Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (AI Act). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689

Song, P. (2026). Model cards and data sheets: documentation standards for ML. ML Journey. https://mljourney.com/model-cards-and-data-sheets-documentation-standards-for-ml/

Varughese, J. (2026). ¿Qué son las redes generativas adversariales (GAN)? IBM. https://www.ibm.com/mx-es/think/topics/generative-adversarial-networks