



Centro de
Estudios Europeos
Luis Ortega Álvarez

*Centro de excelencia
Jean Monnet*

 **UCLM**
Universidad
Castilla-La Mancha



Cofinanciado por
la Unión Europea

La regulación de la Inteligencia Artificial: perspectiva europea y comparada

Miguel Beltrán de Felipe. 0000-0002-0417-9533

5/2025

Serie EU Law

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union.

La regulación de la Inteligencia Artificial: perspectiva europea comparada.

Autor:

Miguel Beltrán Felipe, Universidad de Castilla- La Mancha

Cita sugerida: Beltrán Felipe, M. (2025). “La regulación de la Inteligencia Artificial: perspectiva europea y comparada”, 5/25 Preprints Series in EU Law, Centre for European Studies “Luis Ortega Álvarez”- Jean Monnet Centre of Excellence, 2025.

Cita alternativa: Martín Delgado, Muñoz de Morales, Alonso García (Dirs), *Inteligencia Artificial y Contratación Pública: propuestas para una buena regulación*, Iustel, Madrid, 2025.

RESUMEN: El trabajo pasa revista a las regulaciones nacionales e internacionales de la inteligencia artificial, intentando extraer algunas características comunes. Se pone especial atención en el Reglamento Europeo de Inteligencia Artificial del año 2024. Se intenta una síntesis explicativa de las técnicas de intervención en la inteligencia artificial.

ABSTRACT: The paper analyses the main national and international regulations on artificial intelligence, and tries to establish some common features. The 2024 European Union Regulation on Artificial Intelligence is one of the main norms the paper refers to. The paper deals also with the regulation and intervention techniques which are normally used in the artificial intelligence laws.

PALABRAS CLAVE: Inteligencia Artificial, Regulación, Sanciones Administrativas, Derecho internacional, Derecho comparado

KEY WORDS: Artificial Intelligence, Regulation, Administrative Fines, International Law, Comparative Law

SUMARIO:

1. Previo: la(s) noción(es) de inteligencia artificial

Siguiendo a Huergo (2023: 112 y ss.), que se pregunta “*De qué se habla cuándo se habla de IA*”, para escribir sobre la regulación jurídica de la inteligencia artificial (en adelante IA) el paso previo es partir de una definición de IA. Y eso no es tan fácil como podría parecer, no sólo porque no está claro lo que sea IA desde el punto de vista general, o desde el punto de vista tecnológico, sino sobre todo porque, desde el punto de vista normativo varias de las regulaciones a las que aquí se va a aludir pueden partir de concepciones distintas y además pueden – y suelen - tener finalidades distintas. Smuha (2021: 7) escribe que “*no existe sólo una cosa llamada IA, sino varias distintas técnicas y aplicaciones a las que se aplica esa noción-paraguas de IA*”¹. Y por ello Huergo (2023: 113) distingue entre automatización (o robotización) e IA, y explica las diferencias entre una y otra². En cualquier caso, actualmente por IA se suele entender IA “generativa”, es decir, programas y algoritmos que identifican y codifican enormes cantidades de datos con el fin de simular los procesos de aprendizaje y toma de decisiones del cerebro humano y que se pueden exteriorizar en productos (textos o imágenes) que tienen gran similitud con los que generan los humanos. O sea: replicar tanto el pensamiento humano como algunas de sus manifestaciones (escritas, gráficas, artísticas, etc.).

Para la UE, “sistema de IA” es “*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*”

¹ Por ejemplo, no es lo mismo la IA generativa que la no generativa (o menos avanzada), y dentro de aquella tampoco es lo mismo la IA que podríamos llamar “textual” o “aprendizaje profundo” (porque genera textos escritos) que la IA “gráfica” (porque genera imágenes), al margen de otras técnicas de uso policial, o de política criminal, por ejemplo.

² Según Huergo, las diferencias esenciales, en la IA aplicada a los poderes públicos, se refieren a si la tecnología se limita a acelerar procesos decisionales reglados (por ejemplo, tributarios, como sucede en la actualidad), o si se aplica en contextos con margen de apreciación, o si lo que se pretende es “responder a una pregunta, hacer una predicción o tomar una decisión”.

que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales” (art. 3 del RIA)³.

En el presente trabajo se asume que la IA es IA generativa, entendiéndose por tal aquellos sistemas informáticos que imitan, o intentan hacerlo, el pensamiento y el obrar humanos, reproduciendo procesos cognitivos o creativos como la percepción, la creatividad, la comprensión, el lenguaje o el aprendizaje (Presno y Meuwese 2024: 140)⁴. Y también cabe destacar que una de sus manifestaciones más llamativas son las conocidas como *deep-fake*, o sea las “*ultrasuplantaciones*” (Estella 2025a: 2) mediante las que la tecnología pretende hacer pasar por ciertas o verdaderas imágenes o contenidos audiovisuales artificialmente creados.

2. Síntesis de algunos modelos regulatorios

A) Normas que tienen por objeto la IA

A continuación, se va a hacer una síntesis explicativa de las principales normas que han regulado la IA. Primero se hablará de algunos países, y después se mencionarán brevemente otras regulaciones que podríamos considerar transversales y cuyo objeto no es específicamente la IA, pero la incluyen en su ámbito de aplicación. Naturalmente, tanto uno como otro enfoque no tienen pretensión de exhaustividad⁵.

Entre las normas relativas a la IA destaca el RIA de la UE, de junio de 2024⁶. Se trata de una regulación con un amplio ámbito de aplicación que tiende no tanto a fomentar o a apoyar el uso de la IA sino a restringir o incluso a prohibir determinados usos considerados indebidos. El RIA se fundamenta en consideraciones éticas: la regulación no es neutral o indiferente hacia la

³ Es más o menos la definición que daba la OCDE de noviembre de 2023, en el documento “Updates to the OECD’s definition of an AI system explained”: <https://oecd.ai/en/wonk/ai-system-definition-update>: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”. Como explica Huergo (2025: 2 y ss.), no debe confundirse “sistema de IA” con “modelo de IA”, si bien las definiciones que da el RIA son difícilmente inteligibles: según el art. 3.1 un sistema de IA es “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”. Un modelo de IA de uso general es, según el art. 3.63, “un modelo de IA, también uno entrenado con un gran volumen de datos utilizando supervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de desarrollar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado”. Estella (2025a: 27-28 y 2025b: 4 a 8) explica que el modelo puede ser un componente del sistema, y pone el siguiente ejemplo: mientras que ChatGPT es un sistema de IA, GPT 3.5 es el modelo de uso general que alimenta al chatbot, o sea al ChatGPT.

⁴ Similarmente, Pérez Ugena (2024: 132) se fija en que la IA pretende replicar actividades vinculadas al pensamiento humano como el razonamiento y la resolución de problemas.

⁵ Para una panorámica comparada pueden verse Estella (2025a: 51 y ss), Castellanos (2023: 267 a 273), Pérez Ugena (2024), Hacker, Engel, Hammer y Mittelstadt (2025: 8 y ss.), y específicamente para Europa, con atención a la Convención del Consejo de Europa, Presno y Meuwese (2024) y Hernández Ramos (2025).

⁶ 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° 300/2008, (UE) n° 167/2013, (UE) n° 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. En vigor desde febrero de 2025 (y algunos artículos desde agosto de 2026 y de agosto de 2027). Al respecto puede verse, de entre la vastísima bibliografía, Gago Fernández (2025) y las obras colectivas de Cotino y Simón (2024) y de Huergo y Díaz (2025).

tecnología, sino que le impone condicionamientos basados en valores y en derechos fundamentales. Para ello, lo que se hace es atribuir distinto nivel de riesgo a los usos de la IA (riesgo inaceptable, elevado, limitado y mínimo), y establecer distintas consecuencias en cuanto a su régimen jurídico.

Por su riesgo excesivo, el art. 5 del RIA prohíbe, y en su caso somete a ciertas excepciones o a autorización judicial, ocho usos (entre otros, sistemas biométricos, toma de imágenes faciales, y usos que se refieran a “reconocimiento de emociones” en según qué lugares, al “crédito social”, y a la manipulación del comportamiento humano). Para los otros tipos de riesgo, sobre todo los usos de riesgo alto⁷, las obligaciones de transparencia, auditoría y control van aumentando conforme aumenta el riesgo: accesibilidad a su documentación técnica o transparencia, evaluación de impacto sobre los derechos fundamentales, control sobre los registros de actividad, presentación de quejas, información a la Comisión, ciberseguridad, etc. Es por tanto una regulación que parte de la sospecha o de la desconfianza, y que por tanto hace del riesgo su elemento central, y que representa una continuidad respecto a la idea protectora de la ciudadanía, ya plasmada en el Reglamento Europeo de Protección de Datos de 2016. Como luego se dirá, el RIA contiene una parte sancionadora, aplicable a aquellos proveedores, importadores, distribuidores o “responsables del despliegue” que incumplan las obligaciones que se establecen. Tratándose de una norma de aplicación directa los Estados no necesitarían transponerla o concretarla, pero parece que no será así, en parte por razones de cosmética política y en parte porque el RIA requiere expresamente a los Estados miembros que se doten de órganos o procedimientos ad hoc⁸.

La regulación europea, o por lo menos su inspiración “ética”, está siendo replicada en Brasil⁹, Corea del Sur¹⁰, Canadá¹¹ y la Santa Sede¹².

⁷ Se consideran de riesgo alto los sistemas de IA con peligro significativo de causar daño a la salud, la seguridad o los derechos fundamentales (anexos I y III: biometría, educación, infraestructuras críticas, migración, procesos político-electorales, etc.).

⁸ En España ya existe una iniciativa legislativa que se superpone al marco sancionador del RIA: proposición de Ley Orgánica, GP Sumar, presentada en octubre de 2023 y retirada en marzo de 2024, de regulación de las simulaciones de imágenes y voces de personas generadas por medio de IA, que modificaría la Ley 13/2022 General de Comunicación Audiovisual para considerar como infracciones muy graves, entre otras “La difusión de imágenes o vídeos generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial sin la previa autorización o consentimiento expreso de la persona o personas objeto, salvo que incluyan de forma clara y sobresaliente una advertencia de su condición de imagen generada artificialmente por inteligencia artificial. La advertencia deberá figurar sobreimpresa y claramente legible en la imagen, recayendo en caso contrario la responsabilidad sobre la persona que accione dicha generación”. La iniciativa se volvió a tramitar en abril de 2024 para añadir modificaciones del CP, de la LOREG, de la LEC, de la Ley de Defensa de la Competencia y de varias leyes más. Recientemente, en marzo de 2025, el Consejo de Ministros ha enviado al Congreso el Proyecto de ley orgánica para la protección de los menores en los entornos digitales (BOCG, Congreso de los Diputados, serie A, núm. 52-1, de 11/04/2025).

⁹ Proyecto de Ley 2338/2023

¹⁰ “On 26 December 2024, the South Korean National Assembly approved and adopted the AI Basic Act. The AI Basic Law, also known as the South Korean AI Act (SKAIA), will take effect as of January 2026. This law unifies AI regulation in South Korea, consolidating 19 separate AI-related regulatory proposals”: tomado de <https://artificialintelligenceact.com/south-korean-ai-basic-law/>

¹¹ Artificial Intelligence and Data Act (AIDA), en fase de tramitación parlamentaria

¹² Decreto della Pontificia Commissione per lo Stato della Città del Vaticano recante “Linee Guida in materia di intelligenza artificiale” de 16/12/2024: <https://www.vaticanstate.va/it/novita/1355-i-principi-delle-linee-guida-in-materia-di-intelligenza-artificiale.html>. La finalidad de estos criterios son “valorizzare e promuovere un utilizzo etico e trasparente dell’intelligenza artificiale, in una dimensione antropocentrica e affidabile, nel rispetto della dignità umana e del bene comune” (art. 1), conforme a principios fundamentales de “rispetto della dignità umana, del bene comune e sia ispirato ai principi di responsabilità etica, trasparenza e proporzionalità dell’azione amministrativa” (art. 3). Se trata en general no de normas completas y autoaplicables sino de orientaciones y de principios, que deberán ser completadas mediante leyes y reglamentos (art. 15), pero sí hay partes de aplicación directa como las

En paralelo a la larga tramitación del RIA se promulgó en los EEUU, bajo la presidencia de Biden en octubre de 2023, el decreto (*Executive Order*) nº 14110 sobre *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Su finalidad era esencialmente potenciar y favorecer la AI (con el respaldo de las grandes compañías tecnológicas norteamericanas) mediante medidas de innovación, de concurrencia y de competitividad, al tiempo que también se quería proteger los derechos de los consumidores y de los ciudadanos en general (por ejemplo mediante sistemas de marcas de agua) así como de los titulares de derechos de autor y de patentes. La norma estuvo en vigor un año y unos meses, y fue derogada por el Presidente Trump en el tercer día de su mandato, en enero de 2025, argumentando que establecía barreras y restricciones injustificadas e inconstitucionales¹³. En paralelo a estas normas federales, algunos Estados han adoptado regulaciones propias cuya eficacia no está clara, pues se suelen aplicar únicamente a las respectivas Administraciones y a las empresas radicadas en el Estado¹⁴.

Por otro lado, está el Reino Unido, que a decir de Estella (2025a: 62) ha adoptado un “abordaje pragmático” – parece que el autor opone el pragmatismo a los enfoques principales o éticos. De momento lo que parece haber es un “libro blanco” (un “*playbook*”) de febrero de 2025 que actualiza el de 2023 y que establece orientaciones políticas para el uso de la IA por el sector público¹⁵, y al igual que la normativa anterior a la que se refería Estella, contiene sólo principios, en lugar de un texto legal acabado¹⁶.

Los cinco principios que el libro blanco de 2023 dirigía a las autoridades reguladoras (seguridad y robustez; transparencia y explicabilidad; equidad; responsabilidad y gobernanza; y capacidad de impugnación y reparación de daños y perjuicios) son ahora 10 “*principles for AI use in government and public sector organisations*”:

Principle 1: You know what AI is and what its limitations are

Principle 2: You use AI lawfully, ethically and responsibly

Principle 3: You know how to use AI securely

Principle 4: You have meaningful human control at the right stage

prohibiciones del uso de IA del art. 4 (similares a los usos prohibidos del RIA). Puede verse al respecto Balsamo (2025).

¹³ Decreto 14179 *Removing Barriers to American Leadership in Artificial Intelligence*, de 23 de enero de 2025.

¹⁴ Según los datos que aporta Estella (2025: 56), California es uno de los Estados de los EEUU que más han legislado, hasta el punto de que hay quien habla de “furia regulatoria”, aludiendo a un paquete legislativo que se refiere a la IA en general, a los menores, a los consumidores, a los periodos electorales, etc. Se trata de una normativa importante porque se aplica a las grandes empresas tecnológicas de Silicón Valley. También han promulgado leyes Estados como Oregón (ley de 2019 sobre toma de decisiones basadas en la IA), Tennessee (ley de 2024 denominada Ensuring Likeness, Voice and Image Security Act of 2024 - ELVIS), Colorado (ley de mayo de 2024 Colorado Artificial Intelligence Act), Washington (Ley de responsabilidad de la IA de 2020): al respecto puede verse Castellanos (2023: 274).

¹⁵ <https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government/artificial-intelligence-playbook-for-the-uk-government-html>

¹⁶ El prefacio del *playbook* de 2025 dice claramente que no pretende crear reglas jurídicas sino que su objetivo es actualizar el “libro blanco” de 2023, que por su parte tampoco era una norma autoaplicable sino que establecía una especie de paraguas principal del cual penderían otras regulaciones: “In 2021, the National AI Strategy set out the *government’s proposals for implementing a proportionate, future-proof and pro-innovation framework for regulating AI*. In 2025, the AI Opportunities Action Plan highlighted how the government can leverage AI to boost productivity and improve services. This updated version of the framework has been expanded to cover new developments, and we’ve retitled it to encompass all current forms of AI. As well as a general overview, it includes primers on various AI fields for the curious, and links to learning resources for those who want to dive deeper. The AI Playbook now covers the important and emerging discipline of conducting research with the users of AI systems. It addresses emerging cyber threats to those systems, and the ways that attackers are using AI to create new threats” – el subrayado es mío.

- Principle 5: You understand how to manage the AI life cycle
- Principle 6: You use the right tool for the job
- Principle 7: You are open and collaborative
- Principle 8: You work with commercial colleagues from the start
- Principle 9: You have the skills and expertise needed to implement and use AI
- Principle 10: You use these principles alongside your organisation's policies and have the right assurance in place

Finalmente está la normativa china, sobre la que puede verse Pérez Ugena (2024: 146 a 148) y Alvarez y Palayer (2024: 189 y ss.). Teniendo en cuenta la cautela con la que es preciso tratar la información disponible en relación con países no democráticos, parece que se trataría esencialmente de un reglamento sobre algoritmos de 2022 y de otro sobre IA generativa de 2023. Estas normas se caracterizan por tres cosas: por un lado, un intenso control gubernativo sobre los proveedores de IA y sobre los contenidos (al menos sobre los considerados ilegales o indeseables). Por otro lado, estas normas reflejan una apuesta de las autoridades porque el país se convierta en el líder mundial de la tecnología más avanzada en IA. Y finalmente está lo que Alvarez y Palayer denominan la “fusión militar-civil”, destacando que algún documento oficial alude expresamente a un horizonte de “guerra inteligente” para la que China se estaría preparando.

Así pues, cabría muy sintéticamente hablar de tres modelos: el modelo europeo de protección de los derechos de los ciudadanos (bastante a la defensiva respecto de la IA), el modelo autoritario chino y el modelo liberal o de mercado de los EEUU.

B) Normas transversales (o con incidencia indirecta sobre la IA)

Además de normas específicamente alusivas a la IA, como las que se acaban de mencionar, son de destacar otras normas de ámbito más general. Por ejemplo, las que tienen por objeto los denominados mercados digitales, o los servicios digitales, o la ciberseguridad, o la seguridad a secas (que incluyen técnicas de reconocimiento facial). También influyen sobre la IA las normas sobre propiedad intelectual (patentes y marcas de los programas informáticos), sobre protección de datos (puesto que la IA funciona empleando ingentes cantidades de datos)¹⁷, sobre protección de los consumidores¹⁸, y sobre intimidad o privacidad¹⁹. Asimismo, deben tenerse en cuenta normas de regulación de la competencia, que en los últimos años han afectado a las grandes compañías norteamericanas (con la imposición de sanciones, sobre todo por parte de la Comisión Europea).

Hasta la entrada en vigor del RAI (agosto de 2024) estas normas eran las únicas que disciplinaban la materia en los países europeos. A partir de entonces habría que examinar cuál es su relación aplicativa con el RAI.

¹⁷ Directiva 2016/680 del Parlamento Europeo y del Consejo (27 de abril de 2016) relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

¹⁸ Directiva 2011/83/UE del Parlamento Europeo y del Consejo (25 de octubre de 2011) sobre los derechos de los consumidores, y normas posteriores sectoriales.

¹⁹ En enero de 2025 la compañía china propietaria de la aplicación Tik-Tok llegó a estar temporalmente prohibida en los EEUU porque las autoridades consideraban que los derechos de los usuarios no estaban suficientemente protegidos.

3. Técnicas regulatorias

Las regulaciones de la IA suelen contener un amplio catálogo de técnicas o modalidades de intervención. Voy a limitarme ahora al RIA. Además del habitual listado de definiciones presente en el art. 3 (como las antes citadas de “modelo” y de “sistema”, o de los sujetos que participan en los procesos de IA – “proveedor”, “responsable del despliegue”, “distribuidor”, “operador”), entre estas técnicas encontramos

- establecimiento de “obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo” (art. 16 del RIA), así como otras muchas obligaciones y deberes para proveedores (por ejemplo creación e implantación de un sistema de vigilancia postcomercialización – art. 72 del RIA), para importadores (art. 23 del RIA), para distribuidores (art. 24 del RIA), deberes de darse de alta en registros públicos (arts. 6.5 y 49 del RIA); y una obligación de cooperación con las autoridades (art. 21 del RIA), así como obligaciones de conservación de documentación (art. 18 del RIA) y de suministro de información (art. 8.2 del RIA), en particular comunicaciones o notificaciones previas o posteriores (art. 5.4 del RIA), en particular de incidentes graves (art. 73 del RIA),
- prohibiciones (singularmente las actividades o prácticas prohibidas del art. 5 del RIA),
- autorizaciones (el propio art. 5.3 del RIA permite autorizar algunas de las prácticas prohibidas)²⁰,
- códigos de buenas prácticas (art. 56 del RIA) y códigos de conducta para la aplicación voluntaria de requisitos específicos (arts. 95 y ss. del RIA);
- reglas procedimentales (art. 52 del RIA);
- evaluación del riesgo por los fabricantes y proveedores (arts. 6.4 del RIA), y del impacto sobre los derechos fundamentales (art. 27 del RIA);
- medidas de apoyo a la innovación, mediante espacios controlados de pruebas (arts. 57 y ss. del RIA);
- elaboración de “instrucciones de uso” por parte de los responsables de los sistemas de IA (art. 13 del RIA);
- medidas de “supervisión humana” (art. 14 del RIA);
- y finalmente un régimen sancionador (arts. 99 y ss.) cuya potestad se distribuye entre los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión.

De todas ellas posiblemente las más relevantes sean estas dos últimas. Estella (2025b: 14) subraya que la supervisión humana es una de las claves del RIA, habida cuenta de que, según los apartados 1 y 2 del art. 14 del RIA “los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas” y de que “El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo”. Es decir, el hombre es quien está al cargo de la máquina, y quien verifica que sus riesgos son asumibles. El propio art. 14, junto a las “obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo” de los arts. 16 y ss., establece mecanismos de control y de asignación de responsabilidades de los actores que participan en los procesos de IA.

²⁰ Art. 5.3 del RIA: “Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5”.

Las herramientas sancionadoras de los arts. 99 a 101 del RIA son bastante peculiares, en la medida en que combinan obligaciones a los Estados (propias de las directivas) con previsiones normativas muy concretas que no admiten margen de transposición. Y es muy llamativo que el RIA prevea sanciones a los órganos e instituciones de la UE: se hace difícil de imaginar que el Supervisor Europeo de Protección de Datos sancione a la Comisión o al Consejo.

El RIA contiene, además, habilitaciones a la Comisión: elaboración de directrices (art. 6.5 del RIA) y adopción de actos de ejecución (art. 41 del RIA); creación de órganos (la oficina de IA dentro de la Comisión y el Consejo Europeo de Inteligencia Artificial – art. 65 del RIA); creación de una base de datos de la UE para los sistemas de IA de alto riesgo (arts. 71 y ss. del RIA); y, en general, un denominado “sistema de gestión del riesgo” (art. 9 del RIA) que incluye diversos tipos de técnicas de intervención (pruebas, suministro de información, supervisión).

Junto a los largos listados de deberes y obligaciones, y de habilitaciones para el ejercicio de las potestades, los arts. 85 y 86 del RIA prevén derechos de recurso y a pedir explicaciones. El RIA establece asimismo deberes a los Estados miembros: el art. 5.6 les obliga a presentar a la Comisión informes anuales, y el art. 28.1 les obliga a “nombrar o constituir al menos una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión”, lo cual se desarrolla en los arts. 70 y ss. del RIA; quedan asimismo obligados a crear procedimientos ad hoc aplicables a escala nacional a los sistemas de IA que presenten un riesgo (art. 79 del RIA).

Como puede verse, el RIA contiene prácticamente todas las técnicas administrativas de intervención conocidas, que crean en general una situación muy similar a lo que en España se venía conociendo como relaciones de sujeción especial.

4. Generalidades comparadas acerca del escenario regulatorio

Previamente a extraer cualquier conclusión o idea general sobre los modelos regulatorios cabría plantearse la pregunta de hasta qué punto los países (o las OOI) están en condiciones de regular la AI, entendida como producto comercial creado por multinacionales tecnológicas o superpotencias privadas. Estas tienen capacidades y presupuestos mayores a los de muchísimos Estados, Estados que les compran y utilizan programas informáticos por ellos creados. Así que, tal vez, antes de reflexionar sobre la regulación de los legisladores y de las autoridades nacionales, habría que preguntarse si unos y otras disponen verdaderamente de un poder regulatorio real y efectivo, y si es realista la pretensión de defenderse del riesgo de ser condicionados o capturados por las superpotencias tecnológicas.

Siguiendo a Hacker, Engel, Hammer y Mittelstadt (2025: 7) lo primero que hay que constatar es la fragmentación y la complejidad del escenario regulatorio comparado. No sólo por los rapidísimos avances tecnológicos, que dejan obsoletas las reglas jurídicas que se refieran a la AI. También por la antes citada amplitud de lo que se entienda por IA (lo cual hace que las regulaciones puedan no ser en realidad comparables), y por los distintos enfoques, prioridades, finalidades o principios a los que respondan las distintas normas. Ello vendría si no a invalidar por lo menos sí a limitar enormemente la utilidad de estos estudios comparados.

En relación con esto último, cabe destacar que las regulaciones pueden contener, o no, una toma de postura ideológica o “ética” de las autoridades respecto de la IA²¹. En realidad todas tienen “ideología”, tal vez también aquellas como la del Presidente Trump de enero de 2025 que dicen no tenerla y que derogan la anterior normativa, retraen la intervención pública y dejan más espacio al mercado o desregulan parcialmente la actividad y los usos de la IA. “Ética” equivaldría, según Innerarity (2025: 89) a una especie de llamamiento a una IA responsable y humanista, a través de los denominados “códigos éticos”, y ello, a su juicio, es del todo insuficiente. Un paso más avanzado, y más jurídico, relacionado con la ética, consistiría en reclamar de la tecnología de IA que cumpliera ciertas exigencias de “transparencia, responsabilidad, privacidad y no discriminación” (Hacker, Engel, Hammer y Mittelstadt 2025: 11). Este tipo de consideraciones éticas han sido llevadas por la UE al RIA, en el que se considera la IA un riesgo potencial nada menos que para la democracia, según se verá más adelante.

Al igual que en muchos otros sectores, algunas de las principales tendencias regulatorias de la IA compiten entre sí (*regulatory competition*) bien con la finalidad de favorecer la tecnología de IA, bien con la finalidad de someterla a exigencias “democráticas” o “éticas”. Y, lógicamente, esa competencia puede generar externalidades negativas – sobre todo dependiendo de si el país regulador produce y exporta tecnología de IA. Es decir, la regulación de la IA en EEUU o en China (países con un potente sector industrial-tecnológico, con empresas que manejan enormes cantidades de datos y que venden y difunden sus productos en todo el mundo) difícilmente va a poder situarse en un plano similar a la regulación de la IA en países como España o Portugal. Por ello, la comparación entre los modelos regulatorios puede ser hasta cierto punto engañosa. Porque el enfoque de países exportadores de tecnología como China o los EEUU no es el mismo que el de países importadores (todos los demás)²². Quizás tampoco sea posible comparar o valorar conjuntamente las regulaciones de países autocráticos como Rusia o China y las regulaciones de países democráticos. Y al revés, una regulación de la IA como la europea, que descansa en las exigencias “éticas” de la tecnología, y que establece trabas a su empleo, puede terminar siendo una ventaja competitiva – probablemente necesite para ello incentivos económicos–, o no, dependiendo de que a los suministradores de tecnología les interese y les sea rentable acogerse a esas regulaciones o, por el contrario, les interese intentar sortearlas.

Como es fácilmente comprensible, algunas de estas normas se han elaborado y aprobado a golpe de innovación tecnológica: el lanzamiento del programa chino DeepSeek, en enero de 2025 (sistema de lenguaje abierto parecido al chat GPT pero más barato, más sencillo y en código abierto) está moviendo a países como los EEUU a actualizar su legislación en sentido si no proteccionista, sí por lo menos para que las empresas de los EEUU no pierdan la carrera tecnológica respecto de China. Es decir, no sólo hay una competencia regulatoria entre los Estados, sino también una competencia tecnológica público-privada, y ambas están interrelacionadas.

Otro aspecto relevante es qué puede o debe regular una normativa sobre IA. ¿Puede o debe regular la tecnología en sí misma? ¿O más bien puede o debe regular las aplicaciones o los usos, y no la

²¹ El ejemplo de ello es el documento Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, *Directrices éticas para una IA fiable*, Oficina de Publicaciones, 2019, <https://data.europa.eu/doi/10.2759/14078>, que sirvió de base, junto a otros, al vigente RIA de la UE.

²² Si duda hay excepciones a esta división: Francia tiene una empresa (Mistral AI) que aspira a competir con las grandes tecnológicas norteamericanas y chinas (“Arthur Mensch, CEO de Mistral AI: “La regulación no es el mayor reto que afronta la IA en Europa””: *EL PAÍS* 12 de marzo de 2025 <https://elpais.com/tecnologia/2025-03-12/arthur-mensch-ceo-de-mistral-ai-la-regulacion-no-es-el-mayor-reto-que-afronta-la-ia-en-europa.html>).

tecnología? Las leyes tienen muy complicado establecer reglas sobre cómo sean o deban ser los procesos de innovación tecnológica. El derecho y la ciencia, o la tecnología, operan en planos distintos. Al igual que las leyes de bioética no suelen regular lo que se hace en los laboratorios, sino que se ocupan del uso que el Derecho admite para esos experimentos o innovaciones, las leyes de IA no le dicen a las corporaciones tecnológicas cómo ha de ser el proceso de creación de las aplicaciones que luego se comercializarán.

No menos evidente es que la IA (o sea, las herramientas de IA generadas por empresas tecnológicas ubicadas en un determinado país) “no conocen límites geográficos y su impacto se produce a nivel mundial” (Pérez Ugena 2024: 133), lo cual determina por un lado la escasa eficacia de las regulaciones nacionales y por otro la conveniencia –al menos como hipótesis– de buscar estándares internacionales comunes. Que las regulaciones nacionales de una tecnología de ámbito mundial plantean muchos problemas de aplicabilidad, de eficacia, de verificación, etc. es del todo sabido y no merece mayor comentario. Ni tampoco creo que merezca demasiado comentario la idea, que a veces está presente en el discurso de algunos reguladores o de algunos grupos sociales, de que con las normas nacionales se debería perseguir la “soberanía tecnológica”²³. Lo que verdaderamente parece importante, en cambio, a efectos de la aplicación de las normas europeas como el RIA, es la localización física de los centros de almacenamiento de datos y de supercomputación. A decir de un tecnólogo importante, “*es crítico tener los datos en suelo europeo, gestionados por nosotros. Y contar con modelos fundacionales propios, que representen los valores de la Unión, construidos con datos que tengan las acreditaciones correctas, que representen todos los idiomas de una forma fehaciente, etc.*”²⁴

Sí cabe decir algo sobre la regulación del Derecho internacional, actualmente casi inexistente. Ha habido intentos de buscar convergencias regulatorias, hasta el momento de efecto limitado. Smuha (2021:19-20) habla de acuerdos de cooperación bilaterales entre la UE y Japón, o entre Francia y el Canadá, así como de directrices de la OCDE (a remolque de la regulación de la UE), de la UNESCO (Instrumento global sobre la ética de la IA, adoptado por la Conferencia General en noviembre de 2021), del Consejo de Europa (Convenio Marco sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho, de mayo de 2024). Este último es hasta el momento el único tratado internacional sobre la IA –pero sus efectos vinculantes y su eficacia son aún escasos, y su interés práctico se limita a aquellos de los 46 estados-parte que no sean miembros de la UE, porque estos últimos ya aplican el RIA²⁵. Finalmente, ISO/IEC publicó en 2023 el documento nº 42001 sobre IA²⁶. No es un tratado internacional, ni como tal vincula a los Estados, pero puede ser mucho más eficaz.

Desde el punto de vista jurídico, las regulaciones de la IA se encuentran con muchos problemas. Uno de ellos es que, como toda norma, aspira a regular la materia con una cierta estabilidad,

²³ Recuperar, a estas alturas, la idea de “soberanía” es del todo llamativo, pero más lo es aún que se pretenda aplicar la “soberanía” a la tecnología, queriéndose al parecer decir que los países no deberían depender de otros tecnológicamente hablando, o no depender de las grandes empresas tecnológicas.

²⁴ “Cristian Canton, del BSC: “Es crítico tener los datos en suelo europeo, gestionados por nosotros”, EL PAÍS, 18 de junio de 2025 (<https://elpais.com/tecnologia/2025-06-18/cristian-canton-del-bsc-es-critico-tener-los-datos-en-suelo-europeo-gestionados-por-nosotros.html>).

²⁵ Sobre el Convenio marco del Consejo de Europa pueden verse Hernández Ramos (2025) y Presno y Meuwese (2024: 136), insistiendo en las diferencias estructurales con el RIA.

²⁶ ISO/IEC 42001 “is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems”: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en>.

permanencia o previsibilidad. Pero esa materia es enormemente cambiante desde el punto de vista tecnológico, por lo que las normas pueden quedar rápidamente obsoletas e inservibles, creando además rigideces y externalidades negativas. En este aspecto queda patentemente claro que el Derecho va muy por detrás de la tecnología.

Las peculiaridades y dificultades del objeto de la regulación (o sea, de la IA) no pueden dejar de influir sobre las herramientas o las técnicas jurídicas que se han mencionado en el apartado 3. Me refiero por ejemplo a que se emplean con bastante frecuencia instrumentos de “derecho blando” tales como códigos de conducta o directrices (“*guidelines*”). Efectivamente, se ha propuesto emplear la autorregulación por parte de los operadores de IA, que se someterían a códigos de conducta bajo una cierta supervisión de las autoridades. Como en otras ocasiones referidas a sectores nuevos, o a los que los derechos nacionales y el Derecho internacional llegan con dificultad, se intenta combinar la regulación legal y la autorregulación empresarial. La denominada “autorregulación regulada” plantea el problema de si la prevención, gestión y detección los riesgos puede o debe dejarse en manos de quienes los crean (las empresas que fabrican y comercializan los programas de IA generativa), asunto en el que no es posible entrar ahora²⁷. En cuanto a la elaboración de criterios, en estos momentos (junio de 2025) el RIA está siendo objeto de unas directrices interpretativas que carecen de valor vinculante y que tienen como finalidad ayudar tanto a la UE como a los Estados miembros a aplicar el RIA²⁸.

Prácticamente todas las regulaciones de la IA se enfrentan a una disyuntiva de muy difícil solución en lo relativo a los objetivos que persiguen. Porque pretenden “promover la innovación y la competitividad de la IA de una manera compatible con la garantía de los derechos fundamentales y del Estado social y democrático de derecho” (Presno y Meuwese 2024: 156). O en palabras de Smuha (2021: 14), la regulación tendría al mismo tiempo un papel favorecedor (*enabling role*) y un papel protector o defensivo (*protecting role*). En el fomento y desarrollo de la IA se estaría jugando gran parte del futuro de los países, o sea de su competitividad tecnológica e industrial, pero al mismo tiempo esa apuesta por el uso de la IA podría erosionar algunos derechos importantes –y, según la UE, también nada menos que la democracia misma–.

En relación con esto último, el propio RIA, en el casi ininteligible párrafo 110 del preámbulo, dice expresamente que los sistemas de IA “pueden dar lugar a sesgos dañinos y discriminación que entrañan riesgos para las personas, las comunidades o las sociedades, a la facilitación de la desinformación o el menoscabo de la intimidad” y por tanto “suponen una amenaza para los valores democráticos y los derechos humanos”. Al respecto habría dos maneras de razonar. Una sería la más moderada, o en términos de Huergo, “no catastrofista”, conforme a la cual lo que

²⁷ Baste recordar que Estella (2025b: 11), citando a Wachter, se muestra en desacuerdo con lo que considera una “huida del derecho público hacia el derecho privado” – porque “el sistema de evaluación de la conformidad de los sistemas de IA de alto riesgo establecido por el reglamento es, esencialmente, un control interno, y privado. Incluso en los casos de sistemas de IA en el ámbito de la biometría, el proveedor puede optar, y optará casi de forma natural, por el control interno”.

²⁸ Conforme al texto actualmente disponible (en idioma inglés), “*these Guidelines aim to increase legal clarity and to provide insights into the Commission’s interpretation of the prohibitions in Article 5 AI Act with a view to ensuring their consistent, effective and uniform application. They should serve as practical guidance to assist competent authorities under the AI Act in their enforcement activities, as well as providers and deployers of AI systems in ensuring compliance with their obligations under the AI Act. They strive to interpret the prohibitions in a proportionate manner that achieves the objectives of the AI Act to protect fundamental rights and safety, while promoting innovation and providing legal certainty. These Guidelines are non-binding*”: “La Comisión publica las Directrices sobre prácticas prohibidas de inteligencia artificial (IA), tal como se definen en la Ley de IA” (<https://digital-strategy.ec.europa.eu/es/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>).

sucedo es que el derecho público (no sólo el derecho constitucional) debe adaptarse al nuevo escenario tecnológico. En palabras de Bustos (2025: 22), y en línea con el punto de vista de Sunstein en su Republic.com,

“En el análisis tradicional del derecho constitucional se partía de que el Estado era el presupuesto ontológico de la Constitución y con ello del constitucionalismo, del derecho constitucional y de la ciencia del derecho constitucional. Sin embargo, con la IA se produce un desplazamiento del objeto de la Constitución por lo que las herramientas de una ciencia encuentran dificultades graves para ser útiles en su análisis. Construir un constitucionalismo dirigido al ejercicio de poder por parte de herramientas no necesariamente estatales como son las derivadas de la IA es un reto de enorme magnitud”²⁹.

El otro enfoque sería el catastrofista, bastante ideologizado, que ve en la IA una amenaza clara para los sistemas democráticos (y que caería, a decir de Innerarity, en la “histeria digital”). A la hora de elaborar sus normas sobre IA casi todos los países, y a la hora de escribir sobre la IA gran parte de los autores, han considerado que representa, o puede hacerlo, peligros para la democracia³⁰. Schaake (2024) habla en el título de su libro del “golpe de estado” de la tecnología, y tiene por objeto “salvar la democracia frente a Silicon Valley”. No creo sin embargo que esté del todo claro cómo o por qué esos peligros de la IA sean, o deban ser, necesariamente distintos a los de otros mecanismos de expresión de ideas o de contenidos. Por ejemplo, la posibilidad de falsear la realidad lleva ya tiempo presente en las sociedades tecnologizadas. Tal vez la AI no cambie mucho la transparencia de los procesos de toma de decisiones (públicas y privadas), que hasta ahora no eran en general ni públicos ni transparentes, incluyendo naturalmente la motivación de las decisiones administrativas. Me refiero a que puede resultar igual de potencialmente lesivo para la igualdad o la no discriminación un proceso selectivo laboral resuelto con IA que sin él³¹. Todo indica que la IA puede estar en condiciones de dar prácticamente a cualquiera – no sólo a las grandes empresas tecnológicas proveedoras de IA – la posibilidad de incidir *indebidamente* sobre los procesos democráticos³². Lo que parece estar detrás de esta consideración antidemocrática de la IA sería más bien la constatación de que los hombres están dejando de controlar la toma de ciertas decisiones (políticas, económicas, laborales, etc.) que estarían siendo tomadas por máquinas, y eso vendría a quebrar los cimientos de la cultura occidental. Y también otra constatación: la incapacidad de los Estados de regular y

²⁹ Bustos propone adoptar tres líneas de transformación y adaptación del constitucionalismo al mundo de la IA: responsabilidad (o rendición de cuentas), ponderación y procedimientos de decisión. En línea similar, García Roca (2025: 473-474) escribe que “La democracia no está amenazada por la IA: no se va a producir un sorpasso. Tampoco va a desaparecer el pensamiento humano ni la política ni la filosofía: la capacidad de razonamiento y la búsqueda de la sabiduría”.

³⁰ A decir de Huergo (2025: VI), “there are catastrophist, interventionist or neoliberal approaches that are the result of the authors’ previous positions”, es decir, que los autores a los que se refiere Huergo vendrían a replicar el mismo sesgo – o más grave – que le reprochan a la IA.

³¹ Al menos como hipótesis, si el empleador utiliza sistemas de IA para saber qué decisión le interesa (o sea, a qué persona contratar, durante cuánto tiempo y a cambio de qué retribución), y en caso de impugnación o de tener que justificar o motivar su decisión, posiblemente pueda motivarla de manera tradicional, enmascarando así un posible resultado discriminatorio o lesivo de derechos. Sigo aquí a Huergo (2023: 122), quien sostiene que “Todos estos riesgos no deben hacernos olvidar que las decisiones tomadas por operadores humanos sin interferencia de la IA también están llenas de sesgos y muchas veces sus razones verdaderas no son las que aparecen en la motivación. Se podría motivar jurídicamente una decisión y también la contraria, y las razones de que la decisión sea una u otra son ocultas. Los sistemas de IA pueden cometer errores o estar mal diseñados, pero, por oscuros que sean, son mucho más transparentes que el comportamiento humano”.

³² Utilizar la tecnología (la IA u otra igualmente avanzada) como medio demoscópico, como instrumento de propaganda electoral y como cauce de difusión de programas e ideas no parece ser ilegítimo y todos los partidos políticos se sirven de ella. Me refiero aquí, como “peligro”, a usos que van más allá de esto: por ejemplo, replicar, falseándolos o jaqueándolos, los resultados electorales, suplantación de la imagen o de la voz de los candidatos, etc.

controlar estos nuevos mecanismos tecnológicos. La denominada “*tecnodemocracia*” vendría a hurtar a los hombres el relato de sí mismos que han venido construyendo en los últimos 21 siglos, por lo menos desde la Ilustración.

Sin embargo, la IA y su relación con la democracia no opera sólo en el mismo sentido “ético” al que se acaba de aludir y que es el que últimamente parece ser preponderante. Porque la tecnología de IA da herramientas a los gobiernos –en teoría sólo a los autocráticos– para controlar y reprimir a la población. Feldstein (2021) analiza en detalle Tailandia, Etiopía y Filipinas, y alude también a China, Irán, Rusia y Arabia Saudí para poner de manifiesto cómo en esos países la IA no es un instrumento en manos del “mercado” o de las grandes corporaciones tecnológicas en contra del sistema político, sino que, por el contrario, es utilizado por las autoridades para falsear la democracia, limitar derechos, controlar a la población y perseguir a disidentes. Resulta llamativo que la misma idea (o ideas similares como la democracia y las libertades) sirvan de fundamento a planteamientos tan distintos. Me refiero a algo del todo evidente: que en muchos países la amenaza para las libertades no es en absoluto la tecnología sino las autoridades mismas.

5. Bibliografía

Álvarez Verdugo, Milagros – Palayer, Jules (2024): “La inteligencia artificial en perspectiva comparada”, *Cuadernos de Estrategia* n° 224, pp. 183-214

Balsamo, Fabio (2025): “Le Linee Guida in materia di intelligenza artificiale per lo Stato della Città del Vaticano (16 dicembre 2024)”, en <https://www.rivistadirittoereligioni.com/newscitta-del-vaticano-le-linee-guida-in-materia-di-intelligenza-artificiale-per-lo-stato-della-citta-del-vaticano-del-16-dicembre-2024-fabio-balsamo/>

Bustos Gisbert, Rafael (2025): “Constitucionalismo e Inteligencia Artificial: Marco conceptual”, en VV.AA. R. Bustos Gisbert y F. J. García Roca (coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, IVAP, pp. 13-41

Castellanos Claramunt, Jorge (2023): “Sobre los desafíos constitucionales ante el avance de la inteligencia artificial. Una perspectiva nacional y comparada” *UNED. Revista de Derecho Político* n° 118, pp. 261-287

Criado, J. Ignacio (2024): “Inteligencia Artificial en el Sector Público Latinoamericano. Estudio Comparado a partir de la Carta Iberoamericana de Inteligencia Artificial en la Administración Pública”, *Revista del CLAD Reforma y Democracia* n° 88, pp. 116-143

Estella de Noriega, Antonio (2025a): *Derecho, confianza y regulación de las deepfakes para proteger la democracia*, inédito

Estella de Noriega, Antonio (2025b): “La regulación de los sistemas de IA de alto riesgo en el Reglamento sobre IA: en particular, la supervisión humana”, *Revista Española de Derecho Administrativo* n° 238

Feldstein, Steven (2021): *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, Oxford University Press

Gago Fernández, Alberto (2025): “El Reglamento Europeo sobre Inteligencia Artificial”, en VV.AA. (R. Bustos Gisbert y F. J. García Roca coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial* IVAP, pp. 73-91

García Roca, Javier (2025): “El fortalecimiento de la democracia y del Estado de derecho a través de la inteligencia artificial: conclusiones del seminario”, en VV.AA. (R. Bustos Gisbert y F. J. García Roca coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial* IVAP, pp. 443-474

Hacker, Philipp - Engel, Andreas - Hammer, Sarah - Mittelstadt, Brent (2025): “Introduction to the Foundations and Regulation of Generative AI”, de próxima publicación en *The Oxford Handbook of the Foundation and Regulation of Generative AI* (Oxford University Press, 2025), disponible en SSRN: <https://ssrn.com/abstract=>

Hernández Ramos, Mario (2025): “La Convención Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, democracia y Estado de Derecho. El primer tratado internacional en la materia”, en VV.AA. (R. Bustos Gisbert y F. J. García Roca coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial* IVAP, pp. 93-123

Huergo Lora, Alejandro (2023): “Inteligencia artificial: una aproximación jurídica no catastrofista”, *Revista Española de Control Externo*, vol. XXV, nº 74-75 pp. 110-129

Huergo Lora, Alejandro (2025): “Subject Matter, Scope and Definitions of the AIA (articles 1 to 3)”, en VV.AA. Huergo Lora, Alejandro –Díaz González, Gustavo Manuel, coords. (2025): *The EU Regulation On Artificial Intelligence: A Commentary*, Wolters Kluwer – Cedam, pp. 1-29

Innerarity, Daniel (2025): *Una teoría crítica de la Inteligencia Artificial*, Galaxia Gutenberg, Madrid

Pérez Ugena, María (2024): “Análisis comparado de los distintos enfoques regulatorios de la inteligencia artificial en la Unión Europea, EE.UU., China e Iberoamérica” *Anuario Iberoamericano de Justicia Constitucional* nº 28(1), pp. 129-156.

Presno Linera, Miguel A. – Meuwese, Anne (2024): “La regulación de la inteligencia artificial en Europa”, *Teoría y Realidad Constitucional* nº 54, pp. 131-161

Quijano Sánchez, Lara (2025): “La IA ante las exigencias del Estado de Derecho y la democracia”, en R. Bustos Gisbert y F. J. García Roca (coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, IVAP, pp. 43-71

Schaake, Marietje (2024): *The Tech Coup: How to Save Democracy From Silicon Valley*, Princeton University Press

Smuha, Nathalie A. (2021): “From a ‘Race to Ai’ To a ‘Race to Ai Regulation’: Regulatory Competition for Artificial Intelligence”, *Law, Innovation & Technology*, vol. 13, issue 1

VV.AA. Cotino Hueso, Lorenzo - Simón Castellano, Pere, coords. (2024): *Tratado sobre el reglamento de inteligencia artificial de la Unión Europea*, Aranzadi

VV.AA. R. Bustos Gisbert y F. J. García Roca (coords.), *Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial*, IVAP

VV.AA. Huergo Lora, Alejandro –Díaz González, Gustavo Manuel, coords. (2025): *The Eu Regulation On Artificial Intelligence: A Commentary*, Wolters Kluwer – Cedam

