

ano 24 – n. 96 | abril/junho – 2024
Belo Horizonte | p. 1-282 | ISSN 1516-3210 | DOI: 10.21056/aec.v24i96
A&C – R. de Dir. Administrativo & Constitucional
www.revistaaec.com

A&C

**Revista de Direito
ADMINISTRATIVO
& CONSTITUCIONAL**

**A&C – ADMINISTRATIVE &
CONSTITUTIONAL LAW REVIEW**

FORUM

Todos os direitos reservados. É proibida a reprodução total ou parcial, de qualquer forma ou por qualquer meio eletrônico ou mecânico, inclusive através de processos xerográficos, de fotocópias ou de gravação, sem permissão por escrito do possuidor dos direitos de cópias (Lei nº 9.610, de 19.02.1998).

FÓRUM

Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430 – Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

Os conceitos e opiniões expressas nos trabalhos assinados são de responsabilidade exclusiva de seus autores.

A246 A&C : Revista de Direito Administrativo & Constitucional. – ano 3, n. 11, (jan./mar. 2003). – Belo Horizonte: Fórum, 2003-

Trimestral
ISSN impresso 1516-3210
ISSN digital 1984-4182

Ano 1, n. 1, 1999 até ano 2, n. 10, 2002 publicada pela Editora Juruá em Curitiba

1. Direito administrativo. 2. Direito constitucional.
I. Fórum.

CDD: 342
CDU: 342.9

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Aline Sobreira de Oliveira

Capa: Igor Jamur
Projeto gráfico: Walter Santos
Revisão: Maria Elizabete de Sousa
Diagramação: Derval Braga

Periódico classificado no Estrato A3 do Sistema Qualis da CAPES - Área: Direito.

Qualis – CAPES (Área de Direito)

Na avaliação realizada em 2022, a revista foi classificada no estrato A3 no Qualis da CAPES (Área de Direito).

Entidade promotora

A *A&C – Revista de Direito Administrativo & Constitucional*, é um periódico científico promovido pelo Instituto de Direito Romeu Felipe Bacellar com o apoio do Instituto Paranaense de Direito Administrativo (IPDA).

Foco, Escopo e Público-Alvo

Foi fundada em 1999, teve seus primeiros 10 números editorados pela Juruá Editora, e desde o número 11 até os dias atuais é editorada e publicada pela Editora Fórum, tanto em versão impressa quanto em versão digital, sediada na BID – Biblioteca Digital Fórum. Tem como principal objetivo a divulgação de pesquisas sobre temas atuais na área do Direito Administrativo e Constitucional, voltada ao público de pesquisadores da área jurídica, de graduação e pós-graduação, e aos profissionais do Direito.

Linha Editorial

A linha editorial da *A&C – Revista de Direito Administrativo & Constitucional*, estabelecida pelo seu Conselho Editorial composto por renomados juristas brasileiros e estrangeiros, está voltada às pesquisas desenvolvidas na área de Direito Constitucional e de Direito Administrativo, com foco na questão da efetividade dos seus institutos não só no Brasil como no Direito comparado, enfatizando o campo de interseção entre Administração Pública e Constituição e a análise crítica das inovações em matéria de Direito Público, notadamente na América Latina e países europeus de cultura latina.

Cobertura Temática

A cobertura temática da revista, de acordo com a classificação do CNPq, abrange as seguintes áreas:

- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Teoria do Direito (6.01.01.00-8) / Especialidade: Teoria do Estado (6.01.01.03-2).
- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Direito Público (6.01.02.00-4) / Especialidade: Direito Constitucional (6.01.02.05-5).
- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Direito Público (6.01.02.00-4) / Especialidade: Direito Administrativo (6.01.02.06-3).

Indexação em Bases de Dados e Fontes de Informação

Esta publicação está indexada em:

- Web of Science (ESCI)
- Ulrich's Periodicals Directory
- Latindex
- Directory of Research Journals Indexing
- Universal Impact Factor
- CrossRef
- Google Scholar
- RVBI (Rede Virtual de Bibliotecas – Congresso Nacional)
- Library of Congress (Biblioteca do Congresso dos EUA)
- MIAR - Information Matrix for the Analysis of Journals
- WorldCat
- BASE - Bielefeld Academic Search Engine
- REDIB - Red Iberoamericana de Innovación y Conocimiento Científico
- ERIHPLUS - European Reference Index for the Humanities and the Social Sciences
- EZB - Electronic Journals Library
- CiteFactor
- Diadorim

Processo de Avaliação pelos Pares (Double Blind Peer Review)

A publicação dos artigos submete-se ao procedimento *double blind peer review*. Após uma primeira avaliação realizada pelos Editores Acadêmicos responsáveis quanto à adequação do artigo à linha editorial e às normas de publicação da revista, os trabalhos são remetidos sem identificação de autoria a dois pareceristas *ad hoc* portadores de título de Doutor, todos eles exógenos à Instituição e ao Estado do Paraná. Os pareceristas são sempre Professores Doutores afiliados a renomadas instituições de ensino superior nacionais e estrangeiras.

El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización*

The EU Artificial Intelligence Act: risk regulation and standardization systems

Javier Miranzo Díaz**

Universidad de Castilla-La Mancha (Cuenca, España)
javier.miranzo@uclm.es
<https://orcid.org/0000-0002-3186-2848>

Recibido/Received: 08.04.2024 / 8 April 2024

Aprobado/Approved: 10.06.2024 / 10 June 2024

Resumen: La IA se ha consolidado en los últimos años como una herramienta central en la estrategia de actuación de las Administraciones públicas, y el Reglamento de IA aprobado por la UE pretende constituirse como una norma pionera a nivel mundial para la regulación de esta tecnología. En el presente artículo se analiza la naturaleza y principales características de esta normativa aprobada el 13 de marzo de 2024 por el Parlamento Europeo. El estudio parte de su conceptualización como parte de una tendencia normativa, existente tanto a nivel europeo como internacional, consistente en la regulación del riesgo y de situaciones de incerteza. Sobre esta premisa, se analiza la arquitectura

Como citar este artículo/*How to cite this article:* MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Derecho Administrativo & Constitucional*, Belo Horizonte, año 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/aec.v24i96.1932.

* Este trabajo ha sido desarrollado en el marco del proyecto de investigación PID2020-115774RB-I00 *Personalización de los Servicios Públicos, Sesgos e Inteligencia Artificial: hacia la Consolidación de los Derechos Digitales en las Administraciones Públicas*.

** Profesor Contratado Doctor de Derecho Administrativo de la Universidad de Castilla-La Mancha (Cuenca, España). Doctor en Derecho por la Universidad de Castilla-La Mancha. Máster en Contratación Pública. Máster en Derecho Medioambiental y Sostenibilidad. Licenciado en Derecho. Diplomado en Derecho británico (University of Kent). Investigador del Centro de Estudios Europeos “Luis Ortega Álvarez” y miembro del Observatorio de Contratación Pública de España. Director del Máster en Derecho Medioambiental de la UCLM.

que plantea la norma, y que gira en torno a un sistema de evaluación de conformidad que depende, a su vez, de tres elementos: (1) instrumentos de gestión de riesgo aplicables a los desarrolladores e implementadores de IA, (2) un procedimiento de elaboración de normas técnicas que determinarán el contenido específico de las obligaciones del reglamento, y (3) la creación de un sistema de gobernanza para la aplicación y verificación de dichas obligaciones.

Palabras clave: Inteligencia Artificial. Derecho Administrativo. Derecho de la Unión Europea. Regulación de riesgos. Normas técnicas.

Abstract: AI has been consolidated in recent years as a central line of action in the strategy of public administrations, and the AI Regulation approved by the EU intends to become a pioneering global standard for the regulation of this technology. This article analyses the nature and main characteristics of this regulation approved on 13 March 2024 by the European Parliament. The study conceptualises the EU Regulation as part of a normative trend, existing both at European and international level, consisting of the regulation of risks and situations of uncertainty. On this premise, the paper analyses the legal architecture of the norm, which revolves around a conformity assessment system that relies, in its turn, on three elements: (1) risk management instruments applicable to AI developers and implementers, (2) a procedure for the development of technical standards that will determine the specific content of the obligations of the regulation, and (3) the creation of a governance system for the implementation and verification of such obligations.

Keywords: Artificial Intelligence. Administrative law. European Union law. Risk regulation. Technical Standards.

Sumario: **1** Introducción – **2** La normativa de IA como instrumento de gradación del riesgo – **3** La categorización de los riesgos – **4** Los sistemas de gestión del riesgo – **5** El régimen sancionador del reglamento – **6** El sistema de estandarización como elemento determinante – **7** Reflexiones finales – Referencias

1 Introducción

La IA se ha consolidado en los últimos años como una herramienta central en la estrategia de actuación de las Administraciones públicas, como instrumento para ayudar a los responsables públicos de la toma de decisiones, para detectar los problemas sociales emergentes, o para identificar las preocupaciones de los ciudadanos con mucha prontitud, permitiendo respuestas oportunas y precisas.¹ Sin embargo, si bien los beneficios potenciales de la IA para la Administración Pública parecen ser casi ilimitados, desde diferentes sectores se lleva tiempo advirtiendo de ciertas contraindicaciones al usar sistemas de IA por parte del sector público.² A medida que los sistemas de IA se vuelven más sofisticados, generan ciertas

¹ MISURACA, G., AND VAN NOORDT, C. *Overview of the use and impact of AI in public services in the EU*, Luxemburgo: Publications Office of the European Union, 2020, p. 17.

² Por todos, véase CORBETT-DAVIES, S.; PIERSON, E.; FELLER, A.; GOEL, S. *et al.* Algorithmic Decision Making and the Cost of Fairness. *In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, Halifax, NS, Canada. Association for Computing Machinery*, p. 797–806. DOI: 10.1145/3097983.3098095. Disponible em: <https://doi.org/10.1145/3097983.3098095>.; PONCE SOLÉ, J. Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo*, n. 50, 2019; VALERO

opacidades en su funcionamiento, y deben considerarse las posibles consecuencias imprevistas que la IA puede tener en la actuación administrativa en la ciudadanía y en el sistema de garantías tradicional.³

No en vano, el Grupo de Expertos para la IA de la UE advertía ya en 2019, en su informe *Policy and investment recommendations for trustworthy AI* de que el desarrollo y el despliegue de esos sistemas deben producirse de manera transparente y responsable, a fin de garantizar que funcionen de manera compatible con los principios de la buena administración, el respeto de los derechos fundamentales, la democracia y el estado de derecho.⁴ El Consejo de Europa y la Comisión Europea han sido más vehementes, advirtiendo de que la IA puede afectar incluso a los valores sobre los que se fundamenta la UE, provocando la conculcación de derechos fundamentales en diferentes formas.⁵ Las ventajas y problemáticas que este tipo de decisiones, automatizadas o asistidas, deben ser, por tanto, evaluadas desde la perspectiva crítica del derecho administrativo para la configuración de un régimen jurídico que permita que estos sistemas actúen con las debidas garantías de seguridad jurídica.⁶

Por todo esto, la atención recibida en los últimos años por la implantación de IA en el sector público ha sido creciente, y cada vez son más los informes oficiales o estudios científicos que analizan los riesgos asociados a la implantación de esta tecnología y las posibles medidas para mitigarlos.⁷ Y en este sentido, las principales preocupaciones expresadas por la doctrina, tanto a nivel nacional como internacional, parten de una característica común, que diferencia esta tecnología de otras TICs, y

TORRIJOS, J. Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista catalana de dret públic*, n. 58, p. 82-96, 2019; COTINO HUESO, L. Ética en el diseño para el desarrollo de una inteligencia artificial, robótica. *Ibid.*, p. 29-48.

³ Véase, por todos, PONCE SOLÉ, J. *Acicates (nudges), buen gobierno y buena administración: Aportaciones de las ciencias conductuales, nudging y sector público y privado*. Marcial Pons, 2022b. 8413814103.

⁴ GRUPO DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL. *Policy and investment recommendations for trustworthy AI*, 2019., p. 18.

⁵ COMISIÓN EUROPEA. *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*. COM(2020) 65 final, p. 13. La Comisión advierte de que la implantación deficiente de la IA puede afectar a la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual, y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada, el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores.

⁶ Como ha expuesto en diferentes trabajos Martín Delgado. Véase, por todos MARTÍN DELGADO, I. Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi. *Istituzioni del federalismo*, 3, p. 643, 2019; MARTÍN DELGADO, I. La aplicación del principio de transparencia a la actividad administrativa algorítmica. *In: Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 131-194.

⁷ Este crecimiento lo expuso Zhang ya en 2019: ZHANG, D.; MISHRA, S.; BRYNJOLFSSON, E.; ETCHEMENDY, J. *et al.* The ai index 2021 annual report. *arXiv preprint arXiv:2103.06312*, 2021; XUNTA DE GALICIA. *Estrategia Galega de Inteligencia Artificial 2030: Cara a unha Galicia Intelixente*, 2021, p. 11.

que la hace especialmente incierta a ojos del jurista: la autonomía de los sistemas y su influencia en la toma de decisiones.⁸ Esta autonomía e influencia contrasta con la predictibilidad y automatización de otros sistemas informáticos “clásicos” utilizados por la Administración, que permitía clasificarlos como meras herramientas de apoyo, y obliga a reflexionar sobre la aplicabilidad de los principios básicos de un derecho público, históricamente consagrado a la seguridad jurídica.

En este contexto, en la última década se ha planteado cuál debe ser la estrategia legal a utilizar para diseñar un sistema de garantías sólido pero que, al mismo tiempo, no obstaculice el desarrollo e implantación de esta tecnología, que actúa como un pilar de desarrollo económico. En un primer momento, buena parte de las iniciativas se plantearon a través de iniciativas regulatorias privadas o de estándares en forma de *soft law* regulatorio. Muchos de los documentos aprobados antes de 2020 parecían confiar en los principios éticos para garantizar un uso de la IA garantista,⁹ priorizando mecanismos de *soft law* sobre otros estrictamente normativos.¹⁰ Sin embargo, una corriente cada vez más protagonista venía advirtiendo de la necesidad de aproximar los retos de la IA desde la base de un marco jurídico sólido, de carácter vinculante, que parta de los derechos humanos como referencia universalmente aplicable a todo intento de regulación de IA.¹¹ En este sentido, y aunque deben evitarse lo que el profesor VIDA FERNÁNDEZ ha denominado planteamientos adánicos, que desconozcan o desprecien el marco jurídico aplicable,¹² desde la UE se planteó la necesidad, hacia finales de la anterior década, de elaborar una norma que abordara de forma específica los retos que la IA estaba planteando en la sociedad actual.

⁸ VIDA FERNÁNDEZ, J.; QUADRA-SALCEDO Y FERNÁNDEZ DEL CASTILLO, T. D. L.; PIÑAR MAÑAS, J. L. Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. *In: Sociedad Digital y Derecho*. Madrid: Ministerio de Industria, Comercio y Turismo, 2018. p. 203-224.

⁹ Sobre este aspecto, puede verse COTINO HUESO, L. Ética en el diseño para el desarrollo de una inteligencia artificial, robótica. *Revista catalana de dret públic*, n. 58, p. 29-48, 2019a.

¹⁰ Sobre las interacciones y relaciones entre los documentos de *soft law* y la normativa, o de la ética y el Derecho Público en este ámbito, puede verse PONCE SOLÉ, J. *Acicates (nudges), buen gobierno y buena administración: Aportaciones de las ciencias conductuales, nudging y sector público y privado*. Marcial Pons, 2022b. 8413814103.

¹¹ MANTELERO, A. Analysis of international legally binding instruments, en BEN-ISRAEL, I. (et al.) *Towards Regulation of AI Systems: Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law*. Concil of Europe, 2020, pp. 61-97; en el mismo sentido lo advierte PONCE SOLÉ, J. Las relaciones entre inteligencia artificial, regulación y ética, con especial atención al sector público. *Revista General de Derecho Administrativo*, n. 61, p. 22, 2022a.

¹² VIDA FERNÁNDEZ, J. Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. *In: DE LA QUADRA SALCEDO, T. e PIÑAR MAÑAS, J. L. (Ed.). Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, 2018. p. 203-224; GAMERO CASADO, E. Compliance (o Cumplimiento Normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas. *Diario LaLey*, n. 50, 2021.

2 La normativa de IA como instrumento de gradación del riesgo

El problema de regular la IA con una norma jurídica vinculante y –podemos decir– tradicional, es que precisa de regular sistemas y usos muy heterogéneos, con un alto contenido técnico y cambiante. Además, estos sistemas algorítmicos no pueden garantizar, ni siquiera desde el punto de vista técnico (e incluso para sistemas aparentemente deterministas), una fiabilidad máxima, como han demostrado algunos estudios,¹³ y por tanto operan necesariamente en un escenario de incertidumbre. La predicción de los actos de los sistemas algorítmicos o de sus consecuencias sobre intereses individuales, así como la asignación de causalidad o responsabilidad¹⁴ en caso de daños o errores, es altamente compleja en este contexto.

Sin embargo, esta situación no es totalmente nueva para el Derecho Administrativo. Más bien al contrario, diferentes autores vienen advirtiendo sobre cómo desde inicios del siglo XX, la creciente intervención del poder público como organismo de control y de garantía le ha hecho adentrarse cada vez más en los terrenos de la “técnica”; y al mismo tiempo, sobre cómo la “técnica” o la ciencia, a pesar de sus avances, dista de ofrecer certezas.¹⁵ La necesidad del poder público de actuar en escenarios técnicos de incerteza dio lugar a lo que podríamos entender como una categoría específica del Derecho Administrativo, como es la de la regulación de los riesgos. Este formato de intervención pública a través de la regulación se ha materializado históricamente en sectores altamente tecnificados como el de medio ambiente, salud, seguridad alimentaria, o seguridad industrial, y desde hace algunos años viene utilizándose en el ámbito de la digitalización.¹⁶

En este contexto, existen diversas maneras de abordar legalmente los riesgos y el daño que pueden generar ciertas prácticas o actividades: desde prohibiciones

¹³ MÜLLER, M.; JOOSTEN, J. J. Model-checking in the Foundations of Algorithmic Law and the Case of Regulation 561. *arXiv preprint arXiv:2307.05658*, 2023.; WEN, L.; CAO, Y. A hybrid intelligent predicting model for exploring household CO2 emissions mitigation strategies derived from butterfly optimization algorithm. *Science of The Total Environment*, 727, p. 138572, 2020.

¹⁴ Sobre esta cuestión, puede verse MARTÍNEZ GUTIÉRREZ, R. Responsabilidad administrativa por el uso de la Inteligencia Artificial. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 227-253.

¹⁵ ESTEVE PARDO, J. *El desconcierto del Leviatán: política y derecho ante las incertidumbres de la ciencia*. Marcial Pons Madrid, Barcelona, Buenos Aires, 2009. 8497685857.

¹⁶ En particular, debemos destacar al profesor Esteve Pardo, de entre cuyas obras pueden consultarse: ESTEVE PARDO, J. *Técnica, riesgo y derecho: tratamiento del riesgo tecnológico en el derecho ambiental*. Ariel, 1999. 84-344-1625-5; ESTEVE PARDO, J. Ciencia y Derecho ante los riesgos para la salud: evaluación, decisión y gestión. *Documentación administrativa*, n. 265, p. 137-150, 2003b; ESTEVE PARDO, J. De la policía administrativa a la gestión de riesgos. *Revista española de derecho administrativo*, n. 119, p. 323-346, 2003a; ESTEVE PARDO, J. El Derecho del medio ambiente como Derecho de regulación y gestión de

preventivas, autorizaciones, licencias, medidas de fiscalización, etc. La regulación de riesgos generalmente conlleva una forma particular de definir y categorizar los problemas y daños, a lo que se asocia un conjunto determinado de herramientas regulatorias para abordarlos.¹⁷ Este tipo de construcción normativa crea una serie de marcos procedimentales y de gobernanza para la gestión de los riesgos que, sin embargo, no incluyen normalmente obligaciones específicas sobre el fondo, sino sobre el proceso o sobre las herramientas de control.¹⁸ Se exigen, así, sistemas de autoevaluación individuales y una supervisión previa y/o posterior de autoridades especializadas para garantizar unos estándares de calidad o seguridad; y a su vez, los requerimientos específicos de estos estándares se confían a un desarrollo posterior a través de normas técnicas.¹⁹

En el área de las nuevas tecnologías, esta tendencia se plasmó ya, particularmente, en el Reglamento General de Protección de Datos (RGPD), que actúa como base sobre la que se ha construido, al menos conceptualmente, el marco jurídico de la IA.²⁰ Este punto de partida –necesidad de minimizar los riesgos que

riesgos. In: *Estudios de derecho ambiental europeo*, 2005. p. 45-61; ESTEVE PARDO, J. Derecho y medio ambiente: problemas generales; El Derecho del medio ambiente como Derecho de decisión y gestión de riesgos. *Revista electrónica de Derecho de la Universidad de La Rioja – REDUR*, n. 4, 2006; ESTEVE PARDO, J. Convivir con el riesgo. La determinación del riesgo permitido. In: *Derecho, globalización, riesgo y medio ambiente*. Valencia: Tirant lo blanch, 2012, 2012. p. 273-302; ESTEVE PARDO, J. Las decisiones normativas sobre riesgos nucleares. Marco constitucional. In: *El futuro de la energía nuclear en España: perspectivas (no sólo) jurídicas*. Valencia: Tirant lo Blanch, 2013, 2013. p. 69-84; ESTEVE PARDO, J. La regulación de riesgos: gestionar la incertidumbre. *El Cronista del Estado Social y Democrático de Derecho*, n. 96, p. 32-45, 2021.

¹⁷ KAMINSKI, M. E. Regulating the Risks of AI. *Forthcoming, Boston University Law Review*, 103, 2023.

¹⁸ TAEIHAGH, A.; RAMESH, M.; HOWLETT, M. Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance*, 15, n. 4, p. 1009-1019, 2021.

¹⁹ Sobre las particularidades de este sistema y el papel de los órganos de certificación y estandarización volveremos más adelante. En todo caso, debemos referir que la adopción de este sistema de gestión del riesgo, o de normativa de “Nueva generación”, entraña algunos riesgos en sí misma, como señala ESTEVE PARDO, J. La administración garante. Una aproximación. *Revista de administración pública*, n. 197, p. 11-39, 2015; PONCE SOLÉ, J. *Acicates (nudges), buen gobierno y buena administración: Aportaciones de las ciencias conductuales, nudging y sector público y privado*. Marcial Pons, 2022b. 8413814103; o BARNÉS, J. La transparencia: cuando los sujetos privados desarrollan actividades regulatorias. In: GARCÍA MACHO, R. J. (Ed.). *Ordenación y transparencia económica en el Derecho público y privado*: Madrid [etc.]: Marcial Pons, 2014, 2014. p. 77-124.

²⁰ DE GREGORIO, G.; DUNN, P. The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, p. 473-500, 2022.; BUITEN, M. C. Towards Intelligent Regulation of Artificial Intelligence. *European Journal of Risk Regulation*, 10, n. 1, p. 41-59, 2019; FORTES, P. R. B.; BAQUERO, P. M.; AMARILES, D. R. Artificial Intelligence Risks and Algorithmic Regulation. *Ibid.* p. 1-16, 2022a; KOVAC, M. Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework. *Ibid.* 13, n. 1, p. 94-113; COTINO HUESO, L. Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial. In: BAUZÁ REILLY, M. e COTINO HUESO, L. (Ed.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*: Cizur Menor (Navarra) : Aranzadi, 2022, 2022. p. 69-105.

produce una actividad con riesgo inherente a la que no se puede o quiere renunciar– es el que subyace en las diferentes iniciativas normativas y/o reguladoras que han surgido en los últimos años a nivel internacional en torno a la IA.

Organismos como la OCDE apuestan claramente en sus documentos por esta política de gestión de riesgos, identificando factores de riesgo específicos que deben ser abordados por los reguladores y gestores.²¹ En otros países, como EEUU, también se están proponiendo iniciativas basadas en la gestión del riesgo.²² Pero quizá el más claro modelo de gestión de riesgos lo compone la normativa de referencia en torno a la IA a nivel europeo: el Reglamento Europeo de Inteligencia Artificial.²³ El proceso de elaboración del reglamento ha sido largo, y los textos originales han sufrido importantes cambios desde que en abril de 2021 la Comisión Europea publicara una propuesta legislativa para un enfoque europeo coordinado para abordar las implicaciones humanas y éticas de la IA. Finalmente, el proceso de enmiendas y propuestas,²⁴ entre los que habría que resaltar, por su relevancia, las del Consejo de la UE²⁵ y el Parlamento de la UE²⁶ en junio de 2023, finalizó con la aprobación del texto final por el Parlamento Europeo el 13 de marzo de 2024 (523 votos a favor, 46 en contra y 49 abstenciones).

La norma recibe el nombre de *Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial* (o Ley de Inteligencia Artificial), sigue un enfoque regulatorio horizontal y basado en el riesgo como el expuesto.²⁷

²¹ OCDE. “State of implementation of the OECD AI principles: insights from national AI policies”, *OECD Digital Economy Papers*, n. 31.1, 2021, p. 29. La OCDE identifica aquí los siguientes factores de riesgo:

1. El contexto en el que opera el sistema (por ejemplo, sector de aplicación, amplitud de despliegue).
2. Los datos y la entrada utilizados por el sistema (por ejemplo, la calidad, la privacidad de los datos).
3. El modelo de IA que sustenta el sistema (por ejemplo, modelos generativos o simbólicos); y
4. La tarea y la salida que produce el sistema (por ejemplo, el nivel de autonomía).

Así lo han expuesto también otros autores, como COTINO HUESO en COTINO HUESO, L. Riesgos e impactos del Big Data, la inteligencia artificial y la robótica. enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, n. 50, 2019b.

²² En este país, aunque no existe una legislación específica al respecto, en 2022, el senador Ron Wyden, el senador Corey Booker y la representante Yvette D. Clarke iniciaron el procedimiento para la aprobación de la Ley de Responsabilidad Algorítmica (KAMINSKI, M. E. Regulating the Risks of AI. *Forthcoming, Boston University Law Review*, 103, 2023).

²³ HUERGO LORA, A. El proyecto de Reglamento sobre la Inteligencia Artificial, *Almacén de Derecho*, Abril 2021: Disponible en: <https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial>.

²⁴ El procedimiento completo actualizado, incluyendo las alegaciones y comentarios de cada una de las instituciones que participan en el mismo, puede consultarse en el siguiente enlace: Disponible en: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/0106\(OLP\)](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/0106(OLP)).

²⁵ Disponible en: <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

²⁶ La propuesta de medicaciones por parte del Parlamento Europeo se realizó el 14 de junio de 2023, y puede consultarse en el siguiente enlace: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

²⁷ Entre los trabajos más relevantes publicados en torno a la normativa de IA como instrumento de gestión de riesgos puede destacarse: SCHUETT, J. Risk Management in the Artificial Intelligence Act. *European*

El propio legislador afirma en el considerando 5 que dependiendo de las “*circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos*”, la inteligencia artificial puede generar riesgos y perjudicar intereses públicos o privados y derechos fundamentales de las personas físicas protegidos por el Derecho de la Unión, y que dicho daño puede ser material o inmaterial, incluido el daño físico, psicológico, social o económico, asumiendo por tanto, un contexto de riesgo sobre el que se articula el resto del texto. De hecho, el legislador europeo plantea, como afirma Huergo Lora, algunas de las tradicionales fórmulas de intervención administrativa para la gestión del riesgo: la prohibición de actividades (siguiendo el principio de precaución), la autorización administrativa (mediante la evaluación de conformidad mediante organismos notificados), declaraciones responsables (declaraciones de conformidad con auditoría interna), la implantación de sistemas de gestión de riesgo o *compliance*, o la asignación y reconocimiento de responsabilidad civil o penal, “*todo ello acompañado de un aparato inspector, que actúa, normalmente, a instancia de los perjudicados, y que ayuda a éstos y a los tribunales a descubrir y acreditar las conductas infractoras*”.²⁸

Se trata, por tanto, de una decisión del legislador europeo, que apuesta por una normativa de gestión de riesgos, con las implicaciones jurídicas que esto plantea –incluyendo problemáticas identificadas por la doctrina, como la tendencia a obviar riesgos inobservables o las dificultades para derivar sanciones de obligaciones a menudo difusas.²⁹ En concreto, el Reglamento Europeo de IA apuesta por un modelo de normativa del riesgo que Kaminski ha denominado “centralizada”, que vincula la asignación de recursos escasos (autorizaciones, licencias, etc.) a la gradación del riesgo.³⁰ En esta metodología regulatoria, que se basa en el sistema preexistente de regulación de productos de la UE, el regulador: (1) identifica el riesgo que debe gestionarse; (2) selecciona un nivel de tolerancia al riesgo, evalúa los daños y la probabilidad de que ocurran; (3) asigna valores de riesgo a empresas, organizaciones

Journal of Risk Regulation, p. 1-19, 2023; FRASER, H.; BELLO Y VILLARINO, J.-M. Acceptable Risks in Europe’s Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. *Ibid.* p. 1-16; CHAMBERLAIN, J. The Risk-Based Approach of the European Union’s Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective. *Ibid.* 14, n. 1, p. 1-13; FORTES, P. R. B.; BAQUERO, P. M.; AMARILES, D. R. Artificial Intelligence Risks and Algorithmic Regulation. *Ibid.* 13, n. 3, p. 357-372, 2022b.

²⁸ HUERGO LORA, A. “El proyecto de Reglamento sobre la Inteligencia Artificial”, *Almacén de Derecho*, Abril 2021: Disponible en: <https://almacenederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial>.

²⁹ Sobre estas y otras consecuencias problemáticas de la elección de un sistema de regulación de riesgos, puede verse KAMINSKI, M. E. *Regulating the Risks of AI*. *Forthcoming*, *Boston University Law Review*, 103, 2023; HUERGO LORA, A. J. *Hacia la regulación europea de la inteligencia artificial*. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 743-761.

³⁰ KAMINSKI, M. E. *Regulating the Risks of AI*. *Forthcoming*, *Boston University Law Review*, 103, 2023.

o actividades, diseñando categorías específicas; y (4) vincula la exigencia de cumplimiento con certificados o estándares, así como posterior inspección, a la calificación dentro de una de estas categorías.³¹

3 La categorización de los riesgos

Para acometer estas tareas, el Reglamento no se habla de sectores y o usos de alto riesgo, como sí había hecho la Comisión en documentos anteriores,³² sino de sistemas de IA de alto riesgo –aunque en la práctica, muchos de los catalogados como sistemas de IA lo son por su vinculación o aplicación a sectores especialmente sensibles. Como exponíamos anteriormente, el grado de riesgo de un sistema de IA dependerá de determinados factores que deberían modular y condicionar la aplicación de una normativa u otra, con un carácter más o menos estricto.³³ La UE viene trabajando para depurar esta trascendental clasificación, y ha apuntado sobre todo a dos factores principales: las características de la aplicación y las condiciones en que va a utilizarse. Atendiendo a lo anterior, el legislador europeo elabora cuatro niveles de riesgo:

- Riesgo inadmisibile: se prohibirán los sistemas de inteligencia artificial que se consideren una clara amenaza para la seguridad, los medios de vida y los derechos humanos.³⁴

³¹ En concreto, el capítulo 2 de la norma contiene requisitos sobre gestión de riesgos (Art. 9); datos y gobernanza de datos (Art. 10); documentación técnica (Art. 11); mantenimiento de registros (Art. 12); transparencia y suministro de información a los usuarios (Art. 13); control humano (Art. 14); y precisión, robustez y ciberseguridad (Art. 15).

³² La referencia a los sectores de riesgo sí existía en otros documentos previos de la Comisión, en particular COMISIÓN EUROPEA. *Libro Blanco de la Comisión sobre inteligencia artificial*. COM(2020) 65 final, 2020, p. 21. En él se apuntaba a que la intervención reguladora, debe centrarse en aquellas áreas en las que, de manera general, se considere que hay más probabilidad de que surjan riesgos. En el nuevo marco regulador deben detallarse de manera específica y exhaustiva los sectores que englobe. Pueden ser, por ejemplo, la sanidad, el transporte, la energía y determinados ámbitos del sector público. Esta lista debe revisarse periódicamente y modificarse cuando proceda en función de los desarrollos pertinentes en la práctica. En segundo lugar, que la aplicación de IA en el sector en cuestión se use, además, de manera que puedan surgir riesgos significativos. Este segundo criterio refleja el reconocimiento de que no toda utilización de la IA en los sectores señalados implica necesariamente riesgos significativos. Por ejemplo, si bien la atención sanitaria puede ser un sector importante, un fallo en el sistema de asignación de citas de un hospital no supondrá en principio un riesgo. A nuestro juicio, es indudable que el sector de aplicación del sistema tendrá incidencias determinadas, que el Reglamento de IA, al prescindir de este criterio, deberá resolver de otra manera.

³³ Sobre los factores de riesgo, me remito a mi trabajo MIRANZO DÍAZ, J. *Inteligencia artificial y Derecho administrativo*. Madrid: Tecnos 2023.

³⁴ Esta prohibición había sido defendida con anterioridad por otros autores, especialmente para aquellos usos de IA que buscaban manipular al ser humano, por ejemplo, con objetivos electorales. MULLER, C., TALVITIE, C.; SCHÖPPL, N. "Our Minds, Monitored and Manipulated: How AI Impacts Public Discourse and Democracy", *VerfBlog*, 2022/3/28, disponible en: <https://verfassungsblog.de/roa-our-minds/>, DOI: 10.17176/20220329-011119-0.

- Alto riesgo: las tecnologías de IA utilizadas en infraestructura crítica, educación y formación profesional, componentes de seguridad de productos, empleo, servicios públicos y privados esenciales, aplicación de la ley, gestión migratoria y la administración de justicia y procesos democráticos serán consideradas de alto riesgo, entre otros.
- Riesgo limitado: se requerirán requisitos específicos de transparencia para sistemas como robots conversacionales, entre otros.
- Riesgo mínimo o nulo: se permitirá el uso libre de aplicaciones como videojuegos basados en IA o filtros de spam. La gran mayoría de los sistemas de IA entran en esta categoría.

3.1 Aplicaciones de riesgo inasumible

Como algunos autores han defendido, si bien no debemos caer en el recelo generalizado a la IA, tampoco podemos asumir que el uso de la IA es siempre y necesariamente positivo.³⁵ Y en consecuencia, la normativa debe plantear escenarios en los que no será posible utilizar la IA. El legislador europeo es consciente de que no todos los sistemas de IA conllevan beneficios para el ser humano y la sociedad, o que, en cualquier caso, aunque hubiera potenciales beneficios, entrañan un riesgo completamente inasumible. En este estudio de ponderación, el reglamento europeo selecciona un nivel de tolerancia al riesgo asumible, teniendo en cuenta los daños potenciales y la eventualidad de que se produzcan. Y consecuencia de ello, la propuesta de Reglamento sobre IA, en su artículo 5, enumera los casos en los que, bajo ningún concepto, está permitido el desarrollo e implantación de sistemas de IA:

- Los que “manipulen” a los ciudadanos con técnicas que trasciendan la consciencia (llevándolos a realizar conductas en su perjuicio);
- Los que provechen alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona de dicho grupo en su perjuicio.
- Los que tengan como fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, y tengan consecuencias perjudiciales o desfavorables

³⁵ NEMITZ, Paul; GRÄF, Eike: *Artificial Intelligence Must Be Used According to the Law, or Not at All*, *VerfBlog*, 2022/3/28, disponible en: <https://verfassungsblog.de/roa-artificial-intelligence-must-be-used-according-to-the-law/>, DOI: 10.17176/20220328-131134-0.

injustificadas, desproporcionadas, o fuera del contexto para el que fueron recabados los datos.

- Los que realicen evaluaciones de riesgos de personas físicas con el fin de evaluar o predecir la probabilidad de que cometa una infracción penal basándose únicamente en la elaboración del perfil.
- Los que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.
- Los que infieran las emociones de una persona física en los lugares de trabajo y en los centros educativos (salvo por motivos de salud y seguridad).
- Los que se basen en datos biométricos para deducir o inferir la raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.
- y los sistemas de vigilancia indiscriminada y general (“gran hermano”) a través de sistemas de identificación biométrica remota en tiempo real.³⁶

Este último punto, sin embargo, no supone una prohibición total, sino que la norma desglosa una serie de supuestos en los que podrá aplicarse la identificación biométrica en espacios públicos: cuando sea para identificar una víctima de delito, cuando se esté luchando contra una amenaza concreta, o cuando se pretenda la detención o identificación de una persona que ha cometido un delito. Además, en el caso de que se ampare en alguno de estos supuestos habilitantes, deberá realizarse un test de proporcionalidad en el que se tenga en cuenta la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema, así como consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas (5.2). Adicionalmente, se exige también la aplicación del principio de proporcionalidad en cuanto a su temporalidad y alcance geográfico, que debe tratar de minimizarse; y se garantiza que estos controles se llevarán a cabo de forma efectiva al imponer la autorización judicial previa para la implantación de este tipo de sistemas de IA (artículo 5.3), así como una notificación

³⁶ Salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

- i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;
- ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;
- iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo 62, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

posterior a los organismos de transparencia y de protección de datos (artículo 5.4), y un informe anual a la Comisión Europea (artículo 5.6).

3.2 Aplicaciones de alto riesgo

En un segundo lugar, encontraríamos los denominados sistemas de alto riesgo. Estos se corresponden con los que la Comisión había identificado previamente, en el *Libro Blanco de IA*, como aquellos que tienen incidencia sobre derechos individuales; con efectos jurídicos en los derechos de un particular o de una empresa; que presenten el riesgo de causar lesiones o daños materiales o inmateriales significativos; o que produzcan efectos que las personas físicas o jurídicas.³⁷ La Propuesta de Reglamento sobre IA sigue la línea interpretativa del Libro Blanco, con algunos matices y puntualizaciones relevantes. Así, de acuerdo con el artículo 6.1 un sistema de IA se considerará de alto riesgo cuando cumpla estos dos requisitos:

- el sistema de IA esté destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que contiene el anexo II del Reglamento, o sea en sí mismo uno de dichos productos;
- conforme a la legislación de armonización de la Unión que se indica en el anexo II debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio.

Los anteriores requisitos hacen que estén considerados como alto riesgo los sistemas aplicados a maquinaria, juguetes, equipos de protección, dispositivos médicos, etc.

Además, según el artículo 6.2 también se considerarán de alto riesgo los sistemas de IA que figuran en el anexo III –aunque en este último caso, el Parlamento Europeo ha realizado alegaciones proponiendo no siempre los sistemas de IA del Anexo III deban ser considerados de alto riesgo.³⁸ Dentro de este anexo la propuesta de reglamento incluye, entre otros, aquellos que se utilicen para (1) identificación biométrica y categorización de personas físicas, (2) gestión y funcionamiento de infraestructuras esenciales (funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad); (3) educación y formación profesional (acceso o la

³⁷ COMISIÓN EUROPEA. *Libro Blanco de la Comisión sobre inteligencia artificial*. COM(2020) 65 final, 2020, p. 21.

³⁸ A este respecto, la nueva redacción del artículo 6 propuesta por el Parlamento establece que únicamente serán considerados de alto riesgo los sistemas IA contenidos en el Anexo III “si suponen un riesgo significativo de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas.

asignación de personas físicas a los centros de educación y formación profesional o evaluación de estudiantes); (4) empleo, gestión de los trabajadores y acceso al autoempleo; (5) acceso y disfrute de servicios públicos y privados esenciales y sus beneficios; (6) asuntos relacionados con la aplicación de la ley (riesgo de que cometan infracciones penales o reincidan, o riesgo para las potenciales víctimas de delitos, pruebas en proceso penal, etc.); (7) gestión de la migración, el asilo y el control fronterizo; (8) administración de justicia y procesos democráticos.

Es en estos casos identificados como de alto riesgo donde el Reglamento deposita la mayoría de los esfuerzos regulatorios, con medidas de gestión de riesgos, de gobernanza de datos, de transparencia, certificación, etc. Por tanto, este Anexo III y su sistema clasificatorio asume una gran relevancia en el sistema de regulatorio de riesgos diseñado por la UE, y su gestión –supresión, modificación o aumento de categorías– se antoja un elemento fundamental del sistema.

A estos efectos, el artículo 7 del Reglamento prevé que el anexo III pueda ser modificado mediante actos delegados de la Unión (regulados en el art. 290 del TFUE), aunque eso sí, con algunos condicionantes. En primer lugar, no está permitido modificar o ampliar los sectores o ámbitos en los que un sistema de IA puede ser considerado de riesgo; es decir, cualquier modificación o adición de los sistemas de alto riesgo del Anexo III deberá estar referida a los ámbitos ya recogido en el propio anexo. Y en segundo lugar, que el riesgo identificado sea equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que conlleven los sistemas de IA de alto riesgo que ya se mencionan en el anexo III. Para esto último, además, el legislador da una serie de criterios que servirán de parámetros de medición: la finalidad del sistema de IA, la frecuencia o extensión de su uso, los datos utilizados, la autonomía del sistema, los potenciales daños a la salud o la seguridad, las personas potencialmente afectadas, su número y vulnerabilidad, la facilidad para corregir los potenciales daños, etc.

En este sentido, el mismo artículo 7, en su apartado tercero, diferencia los casos en los que lo que se pretenda se la supresión de sistemas de IA del Anexo III, en los que el acto delegado deberá justificar (1) que los sistemas de IA de alto riesgo en cuestión ya no plantean riesgos considerables, y (2) que la supresión

Cuando un sistema de IA esté incluido en el punto 2 del anexo III, se considerará de alto riesgo si plantea un riesgo significativo de daño al medio ambiente.

^{1a} Comisión, seis meses antes de la entrada en vigor del presente Reglamento, tras consultar a la Oficina de IA y a las partes interesadas pertinentes, proporcionará directrices que especifiquen claramente las circunstancias en las que el rendimiento de los sistemas de IA a que se refiere el anexo III plantearía un riesgo significativo de daño a la salud, la seguridad o los derechos fundamentales de las personas físicas o los casos en que no lo sería.”

no reduzca el nivel general de protección de la salud, la seguridad y los derechos fundamentales con arreglo al Derecho de la Unión.

Finalmente, conviene destacar en este punto cómo el texto final del Reglamento ha incluido una cláusula abierta salida, que permite que un sistema de IA de los incluidos en el anexo III pueda, de forma individual, no ser clasificado como de alto riesgo. Este nuevo apartado 3 del artículo 6 prevé que un sistema de IA no se considerará de alto riesgo si no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, en particular al no influir sustancialmente en el resultado de la toma de decisiones – aunque esta excepción no se aplica a los casos en los que el sistema lleve a cabo la elaboración de perfiles. Y para evaluar esta situación, añade que deben darse una o varias de las condiciones siguientes:

- a) que el sistema de IA tenga por objeto llevar a cabo una tarea de procedimiento limitada;
- b) que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada;
- c) que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o
- d) que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III.

Todos estos criterios entroncan, en definitiva, con uno de los factores de riesgo que habíamos identificado en anteriores trabajos como uno de los elementos centrales de la evaluación de riesgo de un sistema de IA: la relevancia del juicio emitido por el software de IA con respecto a la decisión administrativa final.³⁹ Y es que no debemos olvidar que, aunque una de las aplicaciones administrativas de la tecnología es la automatización de procesos y decisiones administrativas,⁴⁰ en un buen número de casos se utiliza IA como fundamento o fuente especializada para evaluar un aspecto concreto o específico que, sin embargo, únicamente tiene un peso relativo reducido en la decisión administrativa final. Es decir, hay una intermediación humana entre el algoritmo y la decisión administrativa. Los requerimientos jurídicos en materias de transparencia, responsabilidad e igualdad, y los posibles riesgos

³⁹ MIRANZO DÍAZ, J. *Inteligencia artificial y Derecho administrativo*. Madrid: Tecnos 2023.

⁴⁰ MARTÍN DELGADO, I. Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de administración pública*, n. 180, p. 353-386, 2009.

a considerar, deberán depender en buena medida de si existe un filtro humano efectivo o las decisiones son tomadas y ejecutadas de forma automatizada –y en el mismo sentido, en qué medida ese filtro humano tiene capacidad efectiva de revisar la decisión informática.⁴¹

Y en los casos en los que existe una revisión o validación humana, encontramos, a su vez, gradaciones. En algunos casos la decisión administrativa, o buena parte de ella, recae sobre un algoritmo: realizando, por ejemplo, una propuesta de resolución. En estos casos, se requerirá de una mayor exigencia de garantías jurídicas para su correcta implantación.

En otros casos, un software de IA puede ser utilizado como instrumento de asistencia técnica sobre un elemento concreto del procedimiento, por ejemplo para recopilar opiniones de la ciudadanía sobre una determinada cuestión,⁴² o para predecir las emisiones de CO2 de un determinado operador económico o proceso productivo.⁴³ En estos casos, la IA determina el resultado de dicha sub-valoración, pero en ninguno de los casos el resultado del juicio computacional implica una decisión administrativa final o acto administrativo resolutorio en un sentido u otro. Al contrario, la conclusión del programa tendrá que ser contrapuesta y combinada con otros múltiples factores o sub-valoraciones que, una vez ponderados en base a los criterios jurídicos y administrativos, darán lugar a una decisión final.

Además, en los casos en los que la actuación humana sea el motivo para entender la relegación del sistema de IA a una función meramente accesorio, tendrá que tenerse en cuenta en qué medida el sistema de IA podría afectar la autonomía humana a través de dos criterios: (1) si, como se ha mencionado, las conclusiones del sistema son realmente revisables por un humano; y (2) si aun siendo técnicamente posible su revisión, generan una dependencia excesiva en los individuos decisorios.

En definitiva, el papel que juega el algoritmo en el procedimiento administrativo para la conformación de la voluntad administrativa o para la emisión de actos administrativos adquiere una relevancia capital, y puede entrañar una modulación

⁴¹ PONCE SOLÉ, J. Capítulo V. Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 195-225.

⁴² CANALS AMETLLER, D. “El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)”, *Revista General de Derecho Administrativo*, n. 51, 2019.

⁴³ WEN, L.; CAO, Y. A hybrid intelligent predicting model for exploring household CO2 emissions mitigation strategies derived from butterfly optimization algorithm. *Science of The Total Environment*, 727, p. 138572, 2020.

relevante de los requisitos legales exigibles al algoritmo. El legislador europeo es consciente de ello, y por eso, a nuestro juicio de manera acertada, incluye esta cláusula de salida que permite excluir determinados sistemas de IA de la categoría de alto riesgo.

Se trate de un sistema de categorización que trata de ser altamente preciso, pero que ofrece también una alta complejidad interpretativa: la combinación de los criterios del propio artículo 6 con las particularidades de aplicación del anexo II y III, los diferentes mecanismos de modificación de los anexos, las excepciones a la aplicación de los anexos... El legislador europeo es consciente de ello, y por esta razón llama, en el artículo 6.5, a la Comisión a aprobar unas directrices que especifiquen y aclaren la aplicación práctica de las reglas del art 6, y a elaborar una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.

4 Los sistemas de gestión del riesgo

El Reglamento plantea así, en primer lugar, un sistema de riesgos en el que, con carácter general, es el propio legislador el que evalúa las situaciones problemáticas, las categoriza, y asigna unas determinadas obligaciones de cumplimiento.⁴⁴ Pero en este sistema de intervención administrativa hay que destacar una cláusula de cierre, contenida en el artículo 9, que prevé la implantación de sistemas de gestión del riesgo por parte de las organizaciones que utilicen IA. Se da forma de esta manera a una de las herramientas características de la regulación de riesgos, y es la imposición de mecanismos de autogestión o autorregulación que, sin embargo, no imponen medidas específicas. Estas obligaciones establecen aspectos relativos a la actividad o el procedimiento, pero no necesariamente sobre el fondo o contenido del sistema.

La versión final del reglamento define lo que entiende por “sistema de gestión de riesgos” –algo que no hacían las versiones anteriores–, como un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá revisiones y actualizaciones sistemáticas periódicas (artículo 9.2). De aquí se derivan obligaciones de contener los procesos, metodologías y demás instrucciones de forma ordenada y precisa, garantizar que este sistema

⁴⁴ Para un análisis más detallado de las obligaciones de cumplimiento, que no son objeto del presente estudio, véase HUPONT, I.; MICHELI, M.; DELIPETREV, B.; GÓMEZ, E. *et al.* Documenting High-Risk AI: A European Regulatory Perspective. *Computer*, 56, n. 5, p. 18-27, 2023.

de gestión de riesgo es efectivamente puesto en práctica, y de llevar a cabo una revisión del mismo de manera periódica.⁴⁵

En segundo lugar, el artículo 9 aporta algunas indicaciones qué etapas debe incluirse en la implementación de este sistema de gestión. En este sentido se dibuja un proceso con cuatro fases o etapas: (1) la identificación y el análisis de los riesgos conocidos y previsibles; 2) la estimación y la evaluación de los riesgos identificados, tanto cuando el sistema se utilice conforme a su finalidad prevista como cuando se le dé un uso indebido razonablemente previsible; 3) la evaluación a través el sistema de seguimiento posterior a la comercialización; y 4) la adopción de medidas oportunas de gestión de riesgos. La interacción entre las fases pretende actuar como un proceso cíclico. De esta manera, si en las fases iniciales o en la de monitoreo se identifica un riesgo no asumible en las condiciones existentes, se deben adoptar medidas de gestión o corrección (fase 4) y volver a realizar las evaluaciones iniciales y de monitoreo. Si resultara que no es posible reducir los riesgos residuales a un nivel aceptable, se debe detener el proceso de desarrollo e implementación.

Interpretando lo expuesto para las cuatro fases, debemos entender que el Reglamento crea un sistema en el que el proveedor de la IA tendrá que hacerse responsable únicamente de los riesgos que son potencialmente controlables o previsibles (y por tanto dentro de los usos previstos), lo cual trata de aportar cierta seguridad jurídica al sistema. Esto, de hecho, viene a ser clarificado en la versión definitiva del texto, que incluye una aclaración de que los riesgos a que se refiere este artículo son únicamente aquellos que pueden reducirse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema o aportando información técnica. Y con este mismo objetivo, los apartados 4 y 5 del artículo 9 incluyen algunas indicaciones sobre qué debe entenderse por “medidas oportunas de gestión de riesgos” –a adoptar en la fase 4–. En particular, aclara que las medidas deben lograr que los riesgos puedan considerarse razonablemente aceptables, y que, en todo caso, los resultados obtenidos y las medidas adoptadas se deberán comunicar al implementador –incluyendo los riesgos residuales, entendidos como los riesgos que persisten una vez aplicadas las medidas de eliminación o mitigación.

Finalmente, el artículo 9, en sus apartados 6 a 10 prevé que dentro de este sistema de gestión de riesgos debe contenerse un método de testeo o ensayo previo a la comercialización o implementación del sistema, con el fin de garantizar el

⁴⁵ Así lo ha entendido SCHUETT, J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, p. 1-19, 2023.

correcto funcionamiento e identificar, en su caso, las medidas de gestión de riesgos más apropiadas y específicas. Además, añade que estos ensayos se realizarán con parámetros definidos previamente y umbrales probabilísticos que sean adecuados para el propósito previsto.

Sin embargo, la normativa mantiene una cierta indefinición en cuanto a algunos términos fundamentales como “estimación de riesgo”, “evaluación de riesgo”, “riesgo conocido o riesgo previsible”, “riesgo asumible” (aceptable o tolerable), “parámetros y umbrales de probabilidades” o “ciclo de vida de un sistema IA”. Tampoco especifica algunos detalles de implementación de estos sistemas, como por ejemplo, si el test al que hacíamos referencia en el párrafo anterior debe realizarse por el propio desarrollador del sistema de IA o puede externalizarse –en la administración, a través de contratación pública u otros mecanismos.⁴⁶

En todo caso, la propia naturaleza del sistema de gestión de riesgos impide que una norma como el reglamento europeo llegue a un amplio grado de detalle. Esto que hace que se tenga que acudir a las técnicas de gestión de riesgo generales o preexistentes en otros ámbitos de actuación para definir o concretar estos extremos, y que, como el propio texto del reglamento reconoce, se confíe al sistema de estandarización, como estudiaremos a continuación, un desarrollo posterior.⁴⁷

5 El régimen sancionador del reglamento

Para garantizar el cumplimiento de todo lo expuesto, el reglamento plantea, en sus artículos 99 y siguientes, un sistema de sanciones que podríamos dividir en leves, graves y muy graves –unque el reglamento no utiliza esta nomenclatura. Entre las infracciones más graves, con multas de hasta 35 millones de euros o de hasta el 7% del volumen de negocio total anual (la que sea superior), se incluyen los usos prohibidos de Inteligencia Artificial (artículo 5).⁴⁸ Esta redacción final, endurece las sanciones impuestas con respecto al texto original, y por otro lado, elimina la cobertura de estas sanciones más duras a la infracciones relacionadas

⁴⁶ Sobre esta cuestión, puede verse GALLEGO CÓRCOLES, I. La contratación de soluciones de inteligencia artificial. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 503-567.

⁴⁷ La literatura ha ido identificando algunos requisitos que se pueden considerar implícitamente incluidos en el artículo 9 de acuerdo con las prácticas generalizadas en el sistema de estandarización gestión de riesgos en otros ámbitos. Así, puede entenderse que se exige identificar los potenciales usuarios y tipos de usos del sistema desde el principio, la utilización de técnicas reconocidas para la estimación de riesgos, como los diagramas de influencia o las redes Bayesianas, etc. SCHUETT, J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, p. 1-19, 2023.

⁴⁸ En el texto original, estas sanciones eran menores: hasta 30 millones de euros o de hasta el 6% del volumen de negocio total anual.

con la gobernanza de datos, cuyos incumplimientos quedan relegados a las sanciones graves.

En segundo lugar, encontramos las infracciones que podríamos denominar “graves”. Estas se prevén para los incumplimientos relacionados con los sistemas de alto riesgo, y en particular:

- Obligaciones de los proveedores de sistemas de IA de alto riesgo, contenidas en el artículo 16. Esto incluye, las obligaciones relacionadas con el sistema de gestión del riesgo y el sistema de gestión de la calidad (artículos 17 y 9).
- Obligaciones con respecto al representante autorizado que deben nombrar proveedores de terceros países (artículo 22).
- Obligaciones de las entidades que importen sistemas procedentes de fuera de la UE (artículo 23).
- Obligaciones de los distribuidores, entendidos como cualquier persona física o jurídica que participe de la cadena de suministro del sistema y que no esté incluido en los apartados anteriores (art. 24).
- Obligaciones de los responsables de despliegue, entendida como la persona o entidad que implemente el sistema (26).
- Los requisitos y obligaciones que el reglamento impone los organismos notificados –como encargados de la parte esencial del proceso de evaluación de conformidad– con arreglo al artículo 31, al artículo 33, apartados 1, 3 y 4, o al artículo 34.
- Obligaciones de transparencia de los proveedores y usuarios con arreglo al artículo 50.

Todas estas infracciones acarrearán una sanción de 15 millones de euros, o hasta el 3 % de su volumen de negocios mundial total, si esta cuantía fuese superior. Finalmente, entre las infracciones que podríamos denominar leves, de hasta 7,5 millones de euros o el 1% del volumen de negocio si esta fuera superior, encontraríamos la presentación de información inexacta, incompleta o engañosa.

Cabe mencionar también, en este punto, que las diferentes versiones del reglamento han ido concretando las obligaciones de cada uno de los sujetos intervinientes en el proceso de puesta en marcha del sistema de IA. Así, el texto final especifica cuáles de las obligaciones contenidas en la norma son de aplicación específica para cada uno de estos intervinientes en el desarrollo e implantación de IA: proveedores (artículos 20-22), importadores (artículo 23), distribuidores (artículo 24), responsables de despliegue (artículo 26), y obligaciones aplicables a todo el ciclo de vida, que son exigibles a cualquiera de los sujetos cuando se cumplan unas determinadas circunstancias (artículo 25). Esta clasificación y

asignación de responsabilidades, que, como se ha expuesto, no estaba en las primeras versiones del texto, viene a corregir la inseguridad jurídica que producía un sistema de obligaciones abstracto, que no asignaba obligaciones específicas a sujetos concretos y del que, en consecuencia, era difícil inferir sanciones. Esta nueva redacción garantiza el respeto del ineludible principio de legalidad en el sistema sancionador y contribuye a conseguir una suficiente seguridad jurídica, que se concibe como uno de los objetivos principales de la norma, tal y como se refleja en el considerando 12.

No obstante, desde el punto de vista del derecho administrativo sancionador, y en base a lo expuesto hasta ahora, este sistema de infracciones plantea una incertidumbre fundamental en relación con el principio de legalidad y la seguridad jurídica debido a la complejidad indefinición de las obligaciones a evaluar. Y es que, como se ha puesto de manifiesto en apartados anteriores, las obligaciones impuestas por el reglamento son a menudo difusas, genéricas o ambiguas, delegando un amplio margen de discrecionalidad en propio sujeto regulado. Al convertirlas en obligaciones sancionables, sin embargo, se traslada una parte importante de este margen de apreciación la autoridad sancionadora. Esto contrasta con los principios básicos derecho sancionador, que exige para la tipificación de infracciones administrativas la necesaria concreción de las conductas que se proscriben. No es posible, en este sentido, sancionar conductas indefinidas que no permitan al sujeto prever las consecuencias de su conducta.

Es cierto, en cualquier caso, que el largo proceso legislativo que ha experimentado el reglamento ha dado lugar, entre otras mejoras, a importantes intentos por definir y concretar las obligaciones impuestas a cada uno de los sujetos intervinientes en el proceso de desarrollo y despliegue de los sistemas de IA. Prueba de ello es, por ejemplo, la categorización de los sujetos intervinientes en este proceso (proveedores, distribuidores, importadores, responsable de despliegue, organismos notificados, etc.), y la asignación a cada uno de ellos de unas responsabilidades u obligaciones específicas, contenidas o aglutinadas en un único artículo para cada sujeto, y a las que se vinculan las posibles consecuencias punitivas. Así, el texto final especifica cuáles de las obligaciones contenidas en la norma son de aplicación específica para cada uno de estos intervinientes en el desarrollo e implantación de IA: proveedores (artículos 20-22), importadores (artículo 23), distribuidores (artículo 24), responsables de despliegue (artículo 26), y obligaciones aplicables a todo el ciclo de vida, que son exigibles a cualquiera de los sujetos cuando se cumplan unas determinadas circunstancias (artículo 25). Esta clasificación y asignación de responsabilidades, que, como se ha expuesto, no estaba en las

primeras versiones del texto, viene a corregir la inseguridad jurídica que producía un sistema de obligaciones abstracto, que no asignaba obligaciones específicas a sujetos concretos y del que, en consecuencia, era difícil inferir sanciones. Esta nueva redacción garantiza el respeto del ineludible principio de legalidad en el sistema sancionador y contribuye a conseguir una suficiente seguridad jurídica, que se concibe como uno de los objetivos principales de la norma, tal y como se refleja en el considerando 12.

Finalmente, se debe llamar la atención, en esta última versión del texto, a la variación en la intensidad de las sanciones. Por un lado, se intensifican las sanciones ante usos prohibidos de IA, mientras que se suavizan en los otros tipos de sanciones. Además, se modula su aplicación en el caso de las pequeñas y medianas empresas, algo que no estaba previsto en el texto original. Para este tipo de empresas, se invierte la regla general, de manera que se aplicará la cuantía económica fija o el porcentaje de volumen de negocios dependiendo de cuál represente una cifra final inferior (artículo 99.6).

6 El sistema de estandarización como elemento determinante

Lo expuesto hasta ahora muestra un marco general de obligaciones y reparto de responsabilidades, pero que mantiene importantes indefiniciones legales en cuanto a los límites y las exigencias con las que deben contar los sistemas de IA desarrollados o adquiridos por la Administración.⁴⁹ Por ello, desde hace ya tiempo, desde diferentes foros se ha venido insistiendo en la necesidad de acudir a un sistema de estandarización del control de las garantías de la IA para facilitar la labor a las Administraciones, estableciendo sistemas de clasificación o de habilitación con carácter previo, para certificar a aquellos proveedores que cumplan con estándares éticos y de calidad suficientes.⁵⁰ Así, por ejemplo, el Comité *ad hoc* de Inteligencia Artificial (CAHAI) ya venía advirtiendo de que, estos estándares y esquemas de

⁴⁹ HUERGO LORA, A. J. Hacia la regulación europea de la inteligencia artificial. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 743-761.

⁵⁰ Como se precisará unas líneas más abajo, existe un proceso de estandarización a nivel europeo que se encuentra apoyado y promovido, entre otros, por la Comisión Europea y el Comité de Regiones, y que busca crear unas cláusulas contractuales estandarizadas para la compra pública de IA. Véase <https://living-in.eu/groups/solutions/ai-procurement>. Otros autores ya han planteado la idoneidad de la creación de sistemas de certificación para otros servicios de software fundamentales en España y Europa para servicios de tecnología en la nube. Véase GIMENO FELIÚ, J. M.; GARCÍA ÁLVAREZ, G.; TEJEDOR BIELSA, J. La compra pública de tecnología en España: deficiencias y sugerencias de mejora. Thomson Reuters Aranzadi, 2022.

certificación que se utilizan ampliamente como indicadores de seguridad y calidad, podrían extenderse a los sistemas habilitados para IA y a los productores.⁵¹

Siguiendo esta línea, las agencias de estandarización internacionales llevan años impulsando diferentes iniciativas para la certificación de sistemas de IA en diferentes prestaciones. Por ejemplo, ISO se encuentra en proceso de elaboración de una serie de estándares relacionados con la seguridad y calidad de los sistemas de IA –la mayoría en proceso de desarrollo–, entre los que destacan el ISO/IEC JTC 1/SC 42, de Inteligencia Artificial,⁵² el ISO/IEC AWI TR 24368, relativo a la ética en la IA,⁵³ el ISO/IEC PDTR 24028, relativo a la confianza o robustez del software de IA,⁵⁴ o el ISO/IEC 23894, relativo a la gestión del riesgo de sistemas de IA.⁵⁵ Y de forma similar ocurre los estándares IEEE P7000™ que está desarrollando la *Institute of Electrical and Electronics Engineers (IEEE) Standards Association*, que abordan cuestiones específicas en la intersección de consideraciones tecnológicas y éticas.⁵⁶

Consciente de la incertidumbre que plantea una regulación de riesgos indeterminada como el Reglamento de IA, y de la necesidad de otorgar seguridad jurídica al sistema de sanciones, la UE ha incluido el desarrollo de este sistema de estandarización como una de sus prioridades dentro de la “Digital Agenda 2030” –especialmente en la Comunicación *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital* (COM/2021/118 final). En ella, la Comisión marca el objetivo de que “*asociaciones digitales internacionales de la UE [promuevan] la armonización o la convergencia con las normas y estándares de la UE sobre cuestiones como la protección de datos, la privacidad y los flujos de datos, el uso ético de la inteligencia artificial, la ciberseguridad y la confianza, la lucha contra la desinformación y los contenidos ilícitos en línea, la garantía de la gobernanza de internet y el apoyo al desarrollo de la financiación digital y la Administración electrónica*”. Y en la misma línea, el propio texto de la proposición de reglamento de IA, en su considerando 121, prevé que “*la normalización debe desempeñar un*

⁵¹ LESLIE, D.; BURR, C.; AITKEN, M.; COWLS, J. *et al.* Artificial intelligence, human rights, democracy, and the rule of law: a primer. Available at SSRN 3817999, 2021.

⁵² ISO/IEC JTC 1/SC 42 Artificial intelligence. Disponible en: <https://www.iso.org/committee/6794475.html>.

⁵³ ISO/IEC AWI TR 24368 INFORMATION TECHNOLOGY – ARTIFICIAL INTELLIGENCE – OVERVIEW OF ETHICAL AND SOCIETAL CONCERNS. Disponible en: <https://www.iso.org/search.html?q=artificial%20intelligence>.

⁵⁴ ISO/IEC PDTR 24028 INFORMATION TECHNOLOGY – ARTIFICIAL INTELLIGENCE (AI – OVERVIEW OF TRUSTWORTHINESS IN ARTIFICIAL INTELLIGENCE). Disponible en: <https://www.iso.org/search.html?q=artificial%20intelligence>.

⁵⁵ Disponible en: <https://www.iso.org/standard/77304.html>.

⁵⁶ Información disponible en: <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>.

papel fundamental para proporcionar soluciones técnicas a los proveedores, a fin de garantizar el cumplimiento del presente Reglamento, en consonancia con el estado actual de la técnica, para promover la innovación, así como la competitividad y el crecimiento en el mercado único”.

6.1 El sistema de conformidad

En el Reglamento de IA, el legislador europeo establece un sistema de presunción de cumplimiento con las obligaciones para los sistemas de alto riesgo a través de la figura de la “evaluación de conformidad”, que exige que el cumplimiento con las obligaciones impuestas por la norma se pueda acreditar de diferentes maneras (artículos 40 y siguientes). Esta evaluación de conformidad podrá realizarse de dos formas diferentes reguladas en el artículo 43. Un primer modelo, a través de la evaluación de conformidad *externa*, realizada por los denominados organismos notificados –que podríamos asimilar a las entidades colaboradoras del ordenamiento jurídico español en materia ambiental o sanitaria–,⁵⁷ siguiendo el Anexo VII del Reglamento. En este caso, además, conviene mencionar que los organismos notificados tendrán que ser designados por las Autoridades Notificantes de acuerdo con el procedimiento recogido en el artículo 31. Un segundo modelo sería un sistema de evaluación de conformidad fundamentado en un control interno, siguiendo el Anexo VI, lo que requeriría una declaración de conformidad por parte del propio proveedor (artículo 48).

La validación de los sistemas de IA de alto riesgo u otros que necesiten determinada ratificación dependerán, por tanto, de la evaluación de conformidad realizada en alguna de las formas descritas; y a su vez, esta evaluación de conformidad se realizará conforme a los estándares existentes elaborados por ISO, IEEE, o en particular, por las agencias europeas.⁵⁸ En concreto, el legislador prevé que las evaluaciones de conformidad se realizarán con respecto a normas armonizadas publicadas en el Diario Oficial de la Unión Europea (artículo 40) o especificaciones comunes adoptadas por la Comisión Europea mientras no existan las normas armonizadas anteriores (artículo 41). De esta forma, el texto

⁵⁷ PUERTA SEGUIDO, F. E.; ORTEGA ÁLVAREZ, L. I.; ALONSO GARCÍA, M. C. Las entidades colaboradoras en materia de protección ambiental. In: *Tratado de derecho ambiental*. Valencia: Tirant lo Blanch, 2013, 2013. p. 401-441.

⁵⁸ Este sistema se basa, por lo demás, en lo que prevé el RGPD para la protección de datos personales en su artículo 42, tal y como ha expuesto VIGURI CORDERO, J. A. Les normes ISO/IEC com a mecanismes de responsabilitat proactiva en el Reglament General de Protecció de Dades. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, n. 33, 2021.

delega una autoridad significativa a las organizaciones europeas de normalización (OEN), anteriormente mencionadas, para esta tarea, a través de una delegación genérica a los estándares que desarrollen (artículo 40). Esto, teniendo en cuenta el notable grado de indeterminación que muestra el texto del reglamento, atribuye una amplia autoridad para los órganos y agencias de estandarización a la hora de dotar de contenido detallado las obligaciones en torno al desarrollo e implantación de sistemas de IA, con claras implicaciones legales.

6.2 La aprobación de las normas técnicas

La elaboración y aprobación de normas técnicas implican seguir el procedimiento de aprobación de estándares establecido por la Directiva 98/34/CE, modificada por la Directiva 98/48/CE y el Reglamento (UE) No 1025/2012 del Parlamento Europeo y del Consejo, todo ello codificado posteriormente en la Directiva 2015/1535/UE, de 9 de septiembre por lo que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.⁵⁹

En este sentido, el artículo 40.2 insta a la Comisión a emitir, *sin demora indebida*, peticiones de normalización a las organizaciones europeas de normalización (OEN) que abarquen todos los requisitos establecidos en el Reglamento; y en su *Rolling Plan for ICT Standardisation 2021*, la Comisión afirmaba que se espera que se disponga de una normalización adecuada para apoyar el marco regulatorio de la IA en el momento en que el reglamento sea aplicable.⁶⁰ En particular, tres agencias – *European Committee for Standardisation (CEN)*, la *European Committee for Electrotechnical Standardisation (CENELEC)*, y la *European Telecommunications*

⁵⁹ GIMENO FELIÚ, J. M.; GARCÍA ÁLVAREZ, G.; TEJEDOR BIELSA, J. *La compra pública de tecnología en España: deficiencias y sugerencias de mejora*. Thomson Reuters Aranzadi, 2022. Explicitar esta obligación ha sido, de hecho, una de las propuestas de modificación deralizadas por el Parlamento Europeo para el artículo 40: “La Comisión emitirá solicitudes de normalización que abarquen todos los requisitos del presente Reglamento, de conformidad con el artículo 10 del Reglamento UE (nº) 1025/2012 a más tardar... [dos meses después de la fecha de entrada en vigor del presente Reglamento]” (traducción propia). Además, consciente de la trascendencia de estos estándares para el desarrollo del reglamento, el Parlamento propone incluir directrices explícitas para estos organismos “Los actores que participen en el proceso de normalización tendrán en cuenta los principios generales para una IA fiable establecidos en el artículo 4, letra a), intentarán promover la inversión y la innovación en IA, así como la competitividad y el crecimiento del mercado de la Unión, y contribuirán al fortalecimiento global y cooperación en materia de normalización y teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que sean coherentes con los valores, los derechos e intereses fundamentales de la Unión y garanticen una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes, de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) nº 1025/2012” (traducción propia).

⁶⁰ COMISIÓN EUROPEA. *Rolling Plan for ICT Standardisation 2021*.

Standards Institute (ETSI)– se encargan a nivel europeo de garantizar la armonización de determinados estándares técnicos.

Antes de realizar esta petición, en la que se establecerán directrices y requisitos, además de los plazos en que debe realizarse la norma, la Comisión está obligada por este mismo precepto a consultar al Comité Europeo de Inteligencia Artificial –compuesto por representantes de los Estados miembros y un grupo de expertos científicos para integrar a la comunidad científica, y regulado en el artículo 65 y siguientes– y a las partes interesadas pertinentes, incluido el foro consultivo –compuesto por miembros de las partes interesadas con conocimientos especializados reconocidos en el ámbito de la IA, que asesorará al Comité y a la Comisión en cuestiones técnicas, regulado en el artículo 67–.

Sin embargo, aunque entendemos que estas peticiones deberán realizarse a partir de la publicación del reglamento en el DOUE, las actuaciones previas de los procesos de estandarización relativos a la IA en la UE ya han comenzado. De hecho, el pasado mes de mayo ya se realizó una petición de estandarización (M/593 – C(2023)3215) sobre una solicitud de normalización al Comité Europeo de Normalización y al Comité Europeo de Normalización Electrotécnica en apoyo de la política de la Unión en materia de inteligencia artificial al amparo de la Propuesta de Reglamento disponible en ese momento (COM/2021/206). De forma similar, una acción conjunta CEN-CLC/JTC 21 aborda la normalización de la IA en Europa a través de un estudio y recopilación de los estándares disponibles a nivel internacional, tanto a través de un enfoque ascendente (similar a ISO/IEC JTC 1 SC 42), como de un enfoque descendente (concentrándose en un plan a largo plazo para la normalización europea), para diseñar una hoja de ruta de estandarización.⁶¹ ETSI, por su parte, también ha iniciado algunas acciones y está en proceso de elaborar algunos estándares en materia de *Experiential Networked Intelligence (ISG ENI)*, sobre mecanismos de IA para ayudar en la gestión y orquestación de la red, o *ISG F5G on Fixed 5G*, que busca definir la aplicación de la IA en la evolución hacia las nuevas redes de fibra e internet.

Una vez adoptados, los proyectos de normas están sujetos a un largo procedimiento de cumplimiento, primero por consultores HAS (consultores de normas armonizadas) contratados por la Comisión para realizar una revisión, y luego por funcionarios de la propia Comisión Europea, para posteriormente ser publicados en el DOUE. Este procedimiento responde a las exigencias establecidas por el

⁶¹ Información disponible en: <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/>.

TJUE al respecto y trae consecuencia de algunas modificaciones realizadas en los últimos años a este respecto, en las que la Comisión Europea ha ampliado sus competencias en los procesos de revisión de los proyectos de normas armonizadas para garantizar su conformidad con las solicitudes de normalización antes de su publicación en el Diario Oficial de la Unión Europea –que además, desde 2018, incluyeron una fecha de expiración para las solicitudes de normalización por parte de la Comisión y una lista de requisitos detallados que deben desarrollar las OEN.⁶²

Este procedimiento aporta importantes garantías jurídicas a la “incorporación” de los estándares al ordenamiento jurídico, pero ha provocado también retrasos significativos en algunos casos, así como situaciones en que se produce el rechazo del trabajo de las OENs por parte de la Comisión en otros, ejerciendo presión sobre el sistema y conduciendo a una disminución de la confianza entre las OEN, la Comisión y las partes interesadas de la industria. Quizá por ello, el sistema configurado permite que, en determinados casos, y con carácter supletorio, la Comisión de manera directa pueda aprobar directrices o especificaciones comunes que se utilizarán para la evaluación de conformidad de los sistemas de IA (artículo 41), otorgando un amplio poder de ejecución del Reglamento al poder ejecutivo europeo.

A este sistema habría que añadir la incorporación de los estándares armonizados a los sistemas jurídicos de los diferentes Estados de la Unión por los respectivos organismos nacionales de normalización, que editan normas técnicas estatales, en ocasiones de elaboración propia, aunque comúnmente a través de la transposición de normas técnicas de origen europeo e internacional.⁶³ Estas normas están sujetas a una obligación de publicación oficial que se circunscribe, al igual que ocurre a nivel europeo, exclusivamente a su título y a su código numérico, que se deben incluir en el Boletín Oficial del Estado.⁶⁴

6.3 Aspectos relevantes sobre el sistema de normalización de la UE

Aunque la UE, la doctrina y la comunidad internacional apuestan decididamente por una estrategia de normalización que fomenta expresamente incorporación de

⁶² ÁLVAREZ GARCÍA, V. *Las normas técnicas armonizadas (Una peculiar fuente del Derecho europeo)*. Madrid, España: Iustel, 2020.

⁶³ DARNACULLETA I GARDELLA, M. M. La producción de normas en un mundo global. In: ARROYO JIMÉNEZ, L.; MARTÍN DELGADO, I. *et al.* (Ed.). *Derecho público global: fundamentos, actores y procesos*. Madrid: Iustel, 2020. p. 245-273.

⁶⁴ ÁLVAREZ GARCÍA, V. La problemática de la publicidad oficial de las normas técnicas de origen privado que despliegan efectos jurídico-públicos. *Revista de Derecho Comunitario Europeo*, n. 72, p. 449-482, 2022.

estándares internacionales y la participación de la UE en su elaboración,⁶⁵ conviene tener presentes algunas de las controversias presentes en torno a los sistemas de certificación de origen privado como los mencionados, especialmente cuando actúan como instrumento de desarrollo o aplicación de la normativa o tienen incidencia directa o indirecta en los derechos del ciudadano.⁶⁶

Desde hace años, en la regulación de sectores complejos o altamente técnicos, y especialmente en la regulación de productos, la UE viene utilizando una técnica legislativa consistente en regular a través de actos legislativos únicamente los requisitos esenciales de los intereses generales de un producto –en nuestro caso, la IA–, remitiendo en la definición detallada de las exigencias técnicas a estas organizaciones de estandarización, compuestas por expertos y representantes del sector empresarial.⁶⁷ Esta referencia a los sistemas de certificación como elemento determinante de desarrollo normativo con efectos jurídicos ha generado un importante debate jurídico,⁶⁸ en tanto en cuanto los estándares marcan *de facto* las obligaciones técnicas específicas para operar un determinado producto, e incluso pueden esconder verdaderas decisiones estratégicas;⁶⁹ pero son de elaboración privada y, por tanto, aunque producen indudables efectos jurídicos, no están sujetos a las reglas de elaboración y publicidad de las normas tradicionales.⁷⁰

⁶⁵ Véase la Comunicación de la Comisión Europea *A strategic vision for European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020*, COM(2011) 311 final; o más recientemente la *An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market*. COM(2022) 31 final.

⁶⁶ SCHEPEL, H. *The constitution of private governance: Product standards in the regulation of integrating markets*. Hart Publishing, 2005. 1841134872; CANALS I AMETLLER, D. La jurisprudencia ante el ejercicio privado de la función pública de control técnico por razones de seguridad. *Revista del poder judicial*, n. 56, p. 459-482, 1999; ESTEVE PARDO, J. La administración garante. Una aproximación. *Revista de administración pública*, n. 197, p. 11-39, 2015; DARNACULLETA I GARDELLA, M. M. La producción de normas en un mundo global. In: ARROYO JIMÉNEZ, L.; MARTÍN DELGADO, I., et al. (Ed.). *Derecho público global: fundamentos, actores y procesos*. Madrid: Lustel, 2020. p. 245-273.

⁶⁷ La estrategia de estandarización como elemento del mercado común europeo data de mucho antes, en particular con la Comunicación *Completing the Internal Market. White Paper from the Commission to the European Council* (Milan, 28-29 June 1985) COM(85) 310 final; O la Resolución del Consejo de 7 de mayo de 1985 “*New Approach to Technical Harmonization and Standards*”, OJ 1985 C 136/1; o Resolución del Consejo de 21 de diciembre de 1989 “*Global Approach to Conformity Assessment*”, OJ 1990 C 10/1. Puede verse también TARRÉS VIVES, M. *Normas técnicas y ordenamiento jurídico*. Valencia: Tirant lo Blanch, 2003. 84-8442-861-3.

⁶⁸ SCHEPEL, H. *The constitution of private governance: Product standards in the regulation of integrating markets*. Hart Publishing, 2005. 1841134872; ELIANTONIO, M.; CAUFFMAN, C. The legitimacy of standardisation as a regulatory technique in the EU – A cross-disciplinary and multi-level analysis: An introduction. In: *The Legitimacy of Standardisation as a Regulatory Technique*. Edward Elgar Publishing, 2020. p. 1-18.

⁶⁹ WAGNER, W. E. Science Charade in Toxic Risk Regulation, *The. Colum. L. Rev.*, 95, p. 1613, 1995.

⁷⁰ ÁLVAREZ GARCÍA, V. La problemática de la publicidad oficial de las normas técnicas de origen privado que despliegan efectos jurídico-públicos. *Revista de Derecho Comunitario Europeo*, n. 72, p. 449-482, 2022; SAINZ MORENO, F. Ejercicio privado de funciones públicas. *Revista de Administración pública*, n. 100-102,

En este contexto, es de destacar que el TJUE ha tenido ocasión de analizar en diferentes pronunciamientos la medida en que los estándares elaborados de forma privada deben cumplir con los principios del derecho europeo –y cómo debe controlarse este extremo–. Así, en el asunto *James Elliott*, el Tribunal de Justicia estableció por primera vez jurisprudencia sobre la interpretación de una norma técnica adoptada con arreglo a una directiva europea, en este caso la Directiva sobre productos de construcción, asumiendo la capacidad del TJUE para controlar el contenido de las normas técnicas elaboradas por los organismos europeos de normalización en desarrollo de las exigencias esenciales establecidas por los instrumentos legislativos.⁷¹ En ella es de destacar la opinión del Abogado General Campos Sánchez-Bordona, que entendía que los estándares referidos en las directivas y/o reglamentos “*deben considerarse como actos de las instituciones, órganos y organismos de la Unión*” y constituyen un “*caso de delegación legislativa ‘controlada’ en favor de un organismo privado de normalización*” ya que estos estándares articulan la aplicación de la legislación de la Unión y dan forma concreta a nivel técnico al acto legislativo pertinente (apartados 36 y 55 de la sentencia citada).

De esta forma, las normas armonizadas formarían parte de la legislación europea, y podrían ser entendidas como actos de desarrollo *de facto* de la legislación de la UE, aunque eso sí, adoptados al margen del proceso ordinario establecido en el artículo 291 del TFUE y en el Reglamento (CE) n.º 182/2011 para los actos de ejecución de la Comisión, que recoge las normas y principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.⁷²

Esta posición del AG fue en lo esencial incorporada por el TJUE a su sentencia, aceptando la función de los estándares de medidas de ejecución de derecho europeo –aunque rechazando su categorización como actos delegados de las instituciones, órganos y organismos de la Unión, añadiendo cierta confusión al razonamiento⁷³– y

1983; MALARET GARCÍA, E. Una aproximación jurídica al sistema español de normalización de productos industriales. *Revista de administración pública*, n. 116, p. 287-339, 1988; LESLIE, D.; BURR, C.; AITKEN, M.; COWLS, J. *et al.* Artificial intelligence, human rights, democracy, and the rule of law: a primer. *Available at SSRN 3817999*, 2021.

⁷¹ Asunto C-613/14, *James Elliott Construction Limited v. Irish Asphalt Limited*. EU:C:2016:821; VOLPATO, A. Controlling the Invisible: Accountability Issues in the Exercise of Implementing Powers by EU Agencies and in Harmonised Standardisation. *Review of European Administrative Law*, 12, n. 1, p. 75-96, 2019.

⁷² SENDEN, L. The Constitutional Fit of European Standardization Put to the Test. *Legal Issues of Economic Integration*, 44, n. 4, 2017.

⁷³ La negativa del TJUE a considerar que las normas técnicas tengan consideración de actos de las instituciones, órganos y organismos de la Unión” y constituyan un “caso de delegación legislativa ‘controlada’ en favor de un organismo privado de normalización”, supone sin duda un elemento central del debate, pues afectan, como han señalado algunos autores, al alcance de la legitimación activa para interponer recurso en base al

asumiendo la capacidad del TJUE para ejercer control sobre ellos, ya que “*aunque la elaboración de una norma armonizada de ese tipo se confía a un organismo de Derecho privado, dicha norma constituye no obstante una medida de ejecución necesaria y estrictamente encauzada de las exigencias definidas por la Directiva 89/106, realizada a iniciativa y bajo la dirección y el control de la Comisión, y sus efectos jurídicos se condicionan a la previa publicación por ésta de sus referencias en el Diario Oficial de la Unión Europea*”.⁷⁴

Actualmente, el Reglamento 1025/2012, la Directiva 2015/1535/UE, de 9 de septiembre, y las disposiciones del Reglamento de la UE sobre IA imponen, como se ha comentado, un procedimiento que ofrece ciertas garantías de transparencia y seguridad jurídica al sistema de creación y aprobación de normas técnicas, incluyendo su publicación en el DOUE. Conviene recalcar que estas garantías incluyen, entre otras cuestiones, una clara diferenciación entre los organismos europeos de normalización, por un lado, y los organismos internacionales de normalización por otro, de forma que sólo los europeos –el ETSI y el CEN/CENELEC– tienen facultades, de acuerdo con el artículo 40 y siguientes, de crear normas armonizadas europeas con carácter vinculante.

Esta distinción implica, *a priori*, que las normas armonizadas son desarrolladas únicamente por las agencias europeas conforme al procedimiento descrito en apartados anteriores, y que los estándares internacionales como ISO podrán adquirir fuerza vinculante de acuerdo al Reglamento de IA únicamente de forma indirecta, mediante su incorporación a través de las OEN y del procedimiento ordinario del Reglamento 1025/2012 que exige la publicación en el DOUE. Sin embargo, no debemos obviar que los acuerdos de Viena y Frankfurt entre estas y las organizaciones internacionales de normalización (como ISO) buscan alinear las normas internacionales y europeas y reconocer el papel principal de ISO/IEC en la formulación de estándares, lo que en la práctica supone que las instituciones europeas buscarán que los estándares europeos se correspondan en lo máximo posible con las normas internacionales.⁷⁵ De hecho, la versión final del texto

artículo 263 TFUE (VOLPATO, A. Controlling the Invisible: Accountability Issues in the Exercise of Implementing Powers by EU Agencies and in Harmonised Standardisation. *Review of European Administrative Law*, 12, n. 1, p. 75-96, 2019).

⁷⁴ El TJUE acepta también una excepción a dicha norma general, y es que sí que pueden imponerse y desplegar efectos sobre las empresas cuando estas «tienen acceso a la versión oficial y auténtica» de las mismas». Asunto C-613/14, *James Elliott Construction Limited v Irish Asphalt Limited* EU:C:2016:821. Apartado 43.

⁷⁵ Así lo ha evidenciado para los mercados financieros y contables, o la seguridad alimentaria, DARNACULLETA I GARDELLA, M. M. La producción de normas en un mundo global. In: ARROYO JIMÉNEZ, L.; MARTÍN DELGADO, I., et al. (Ed.). *Derecho público global: fundamentos, actores y procesos*. Madrid: lustel, 2020.

incluye una alusión expresa en el artículo 40.3 a esta necesidad de coordinación con los sistemas de estandarización europeos, exhortando a los organismos de estandarización a tener en cuenta “las normas internacionales existentes en el ámbito de la IA que sean coherentes con los valores, los derechos e intereses fundamentales de la Unión”.⁷⁶

7 Reflexiones finales

El Reglamento de IA aprobado por la UE es, sin duda, una norma ambiciosa que se sitúa de forma pionera a nivel mundial. La Unión, fiel a su tradición, pretende posicionar al ciudadano en el centro del marco legal y regular un amplio sistema de garantías que ofrezca seguridad jurídica a los usuarios sin desincentivar la inversión. En todo caso, las complejidades de esta nueva tecnología han hecho que el proceso de elaboración haya sido complejo y largo –incluso para los estándares de la UE– dando lugar a un texto con un alto grado de complejidad.

El legislador opta por un sistema de normativa de riesgo que sigue la estela de anteriores normas, y en es particular, del Reglamento Europeo de Protección de Datos. Con este espíritu, realiza la categorización de tipos de IA, a los que asocia niveles de cumplimiento diferenciado, con obligaciones individualizadas por categorías de sujetos, y que a su vez se vinculan con un sistema de sanciones. Sin embargo, el carácter marcadamente técnico, novedoso y cambiante de las tecnologías aplicables hace que el texto no llegue a un alto grado de concreción en obligaciones impuestas a los sistemas. En su lugar, el legislador europeo delega gran parte de la concreción de estas obligaciones en un sistema de evaluación de conformidad que descansa, a su vez, sobre el necesario desarrollo de normas técnicas, que serán, en última instancia, las que determinen si un sistema de IA se considera conforme a las estipulaciones del reglamento o no.

Se trata de una técnica regulatoria que ha generado ciertos celos en las últimas décadas, debido a que aleja el poder de decisión de los órganos representativos, situándolo en esferas privadas apartadas de la fiscalización y escrutinio público, y con unas exigencias de transparencia limitadas. No obstante, se debe reconocer, por un lado, que en la última década se han corregido algunas de las principales carencias de esta técnica regulatoria, dotándolas de procesos más transparentes y con un

p. 245-273. DARNACULLETA I GARDELLA, M. M. Los instrumentos normativos de regulación bancaria en el sistema de fuentes del derecho. *In*: Regulación bancaria: transformaciones y estado de derecho: Cizur Menor (Navarra): Aranzadi, 2014, p. 131-183.

⁷⁶ Texto disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

mayor control por parte de las instituciones de la UE –tanto de la Comisión como del TJUE–, y por el otro, que esta forma de regulación a través de normas técnicas ha demostrado ser una práctica eficiente en otras áreas de intervención administrativa de la UE. Además, en gran medida puede afirmarse que es la única forma viable de aproximar una realidad tan cambiante, asegurando una actualización técnica a través un sistema de verificación que atribuyen una importante responsabilidad a los propios agentes desarrolladores e implementadores de IA y a los organismos intermedios de verificación –agentes notificados y autoridades de notificación– al tiempo que genera un robusto marco de garantías y de gobernanza.

La reflexión final, por tanto, debe llevarnos a realizar una valoración positiva del Reglamento, pero también debemos ser conscientes de que su aplicación efectiva requerirá de un esfuerzo colectivo significativo, tanto por parte de los Estados, para implantar el sistema de gobernanza y de evaluación de conformidad con las debidas garantías, como por parte de los usuarios la sociedad civil y el resto de autoridades de control, que deben permanecer vigilantes a posibles vulneraciones del sistema o deficiencias de su construcción –algo que, dada la complejidad de lo expuesto, va a requerir especial celo y cuidado. Finalmente, debemos ser conscientes de que el Derecho Público europeo tendría, además, la función adicional de interpretar cuáles de las garantías que nos encontramos en el reglamento precisan de desarrollo o adaptación para la implantación en la Administración Pública, donde las particularidades de la actuación pública pueden exigir garantías adicionales.

Referencias

ÁLVAREZ GARCÍA, V. La problemática de la publicidad oficial de las normas técnicas de origen privado que despliegan efectos jurídico-públicos. *Revista de Derecho Comunitario Europeo*, n. 72, p. 449-482, 2022.

ÁLVAREZ GARCÍA, V. *Las normas técnicas armonizadas (Una peculiar fuente del Derecho europeo)*. Madrid, España: Lustel, 2020.

BARNÉS, J. La transparencia: cuando los sujetos privados desarrollan actividades regulatorias. In: GARCÍA MACHO, R. J. (Ed.). *Ordenación y transparencia económica en el Derecho público y privado*. Madrid: Marcial Pons, 2014, 2014. p. 77-124.

BUITEN, M. C. Towards Intelligent Regulation of Artificial Intelligence. *European Journal of Risk Regulation*, v. 10, n. 1, p. 41-59, 2019.

CANALS AMETLLER, D. “El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)”, *Revista General de Derecho Administrativo*, n 51, 2019.

CANALS I AMETLLER, D. La jurisprudencia ante el ejercicio privado de la función pública de control técnico por razones de seguridad. *Revista del poder judicial*, n. 56, p. 459-482, 1999.

CHAMBERLAIN, J. The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective. *European Journal of Risk Regulation*, 14 (1), p. 1-13.

COMISIÓN EUROPEA. *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*. COM(2020).

CORBETT-DAVIES, S.; PIERSON, E.; FELLER, A.; GOEL, S. *et al.* Algorithmic Decision Making and the Cost of Fairness. In: *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017, Halifax, NS, Canada. Association for Computing Machinery, p. 797-806. DOI: 10.1145/3097983.3098095. Disponible em: <https://doi.org/10.1145/3097983.3098095>.

COTINO HUESO, L. Ética en el diseño para el desarrollo de una inteligencia artificial, robótica. *Revista catalana de dret públic*, n. 58, p. 29-48, 2019a.

COTINO HUESO, L. Riesgos e impactos del Big Data, la inteligencia artificial y la robótica. enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, n. 50, 2019b.

COTINO HUESO, L. Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial. In: BAUZÁ REILLY, M. e COTINO HUESO, L. (Ed.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*. Cizur Menor (Navarra): Aranzadi, 2022, 2022. p. 69-105.

DARNACULLETA I GARDELLA, M. M. La producción de normas en un mundo global. In: ARROYO JIMÉNEZ, L.; MARTÍN DELGADO, I., *et al.* (Ed.). *Derecho público global: fundamentos, actores y procesos*. Madrid: Iustel, 2020. p. 245-273.

DARNACULLETA I GARDELLA, M. M. Los instrumentos normativos de regulación bancaria en el sistema de fuentes del derecho. In: *Regulación bancaria: transformaciones y estado de derecho*. Cizur Menor (Navarra): Aranzadi, 2014, p. 131-183.

DE GREGORIO, G.; DUNN, P. The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, p. 473-500, 2022.

ELIANTONIO, M.; CAUFFMAN, C. The legitimacy of standardisation as a regulatory technique in the EU—A cross-disciplinary and multi-level analysis: An introduction. In: *The Legitimacy of Standardisation as a Regulatory Technique*. Edward Elgar Publishing, 2020. p. 1-18.

ESTEVE PARDO, J. Ciencia y Derecho ante los riesgos para la salud: evaluación, decisión y gestión. *Documentación administrativa*, n. 265, p. 137-150, 2003b.

ESTEVE PARDO, J. Convivir con el riesgo. La determinación del riesgo permitido. In: *Derecho, globalización, riesgo y medio ambiente*. Valencia: Tirant lo Blanch, 2012, p. 273-302.

ESTEVE PARDO, J. De la policía administrativa a la gestión de riesgos. *Revista española de derecho administrativo*, n. 119, p. 323-346, 2003a.

ESTEVE PARDO, J. Derecho y medio ambiente: problemas generales. El Derecho del medio ambiente como Derecho de decisión y gestión de riesgos. *Revista electrónica de Derecho de la Universidad de La Rioja – REDUR*, n. 4, 2006.

ESTEVE PARDO, J. El Derecho del medio ambiente como Derecho de regulación y gestión de riesgos. *In: Estudios de derecho ambiental europeo*, 2005. p. 45-61.

ESTEVE PARDO, J. *El desconcierto del Leviatán: política y derecho ante las incertidumbres de la ciencia*. Madrid, Barcelona, Buenos Aires: Marcial Pons, 2009.

ESTEVE PARDO, J. La administración garante. Una aproximación. *Revista de administración pública*, n. 197, p. 11-39, 2015.

ESTEVE PARDO, J. La regulación de riesgos: gestionar la incertidumbre. *El Cronista del Estado Social y Democrático de Derecho*, n. 96, p. 32-45, 2021.

ESTEVE PARDO, J. Las decisiones normativas sobre riesgos nucleares. Marco constitucional. *In: El futuro de la energía nuclear en España: perspectivas (no sólo) jurídicas*. Valencia: Tirant lo Blanch, 2013, 2013. p. 69-84.

ESTEVE PARDO, J. *Técnica, riesgo y derecho: tratamiento del riesgo tecnológico en el derecho ambiental*. Ariel, 1999. 84-344-1625-5.

FORTES, P. R. B.; BAQUERO, P. M.; AMARILES, D. R. Artificial Intelligence Risks and Algorithmic Regulation. *European Journal of Risk Regulation*, vol. 13, n. 3, p. 1-16, 2022.

FRASER, H.; BELLO Y VILLARINO, J.-M. Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. *European Journal of Risk Regulation*, 14 (1), p. 1-16, 2023.

GALLEGO CÓRCOLES, I. La contratación de soluciones de inteligencia artificial. *In: Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 503-567.

GAMERO CASADO, E. Compliance (o Cumplimiento Normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas. *Diario La Ley*, n. 50, 2021.

GIMENO FELIÚ, J. M.; GARCÍA ÁLVAREZ, G.; TEJEDOR BIELSA, J. *La compra pública de tecnología en España: deficiencias y sugerencias de mejora*. Madrid: Thomson Reuters Aranzadi, 2022.

GRUPO DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL. *Policy and investment recommendations for trustworthy AI*, 2019.

HUERGO LORA, A. El proyecto de Reglamento sobre la Inteligencia Artificial, *Almacén de Derecho*, Abril 2021: Disponible en: <https://almacenederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial>.

HUERGO LORA, A. J. Hacia la regulación europea de la inteligencia artificial. *In: Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 743-761.

HUPONT, I.; MICHELI, M.; DELIPETREV, B.; GÓMEZ, E. *et al.* Documenting High-Risk AI: A European Regulatory Perspective. *Computer*, 56, n. 5, p. 18-27, 2023.

ISO/IEC AWI TR 24368 INFORMATION TECHNOLOGY – ARTIFICIAL INTELLIGENCE – OVERVIEW OF ETHICAL AND SOCIETAL CONCERNS. Disponible en: <https://www.iso.org/search.html?q=artificial%20intelligence>.

ISO/IEC JTC 1/SC 42 Artificial intelligence. Disponible en: <https://www.iso.org/committee/6794475.html>.

ISO/IEC PDTR 24028 INFORMATION TECHNOLOGY – ARTIFICIAL INTELLIGENCE (AI – OVERVIEW OF TRUSTWORTHINESS IN ARTIFICIAL INTELLIGENCE. Disponible en: <https://www.iso.org/search.html?q=artificial%20intelligence>.

KAMINSKI, M. E. Regulating the Risks of AI. *Forthcoming, Boston University Law Review*, 103, 2023.

KOVAC, M. Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework. *European Journal of Risk Regulation*, 13 (1), p. 94-113, 2022.

LESLIE, D.; BURR, C.; AITKEN, M.; COWLS, J. *et al.* Artificial intelligence, human rights, democracy, and the rule of law: a primer. *Available at SSRN 3817999*, 2021.

MALARET GARCÍA, E. Una aproximación jurídica al sistema español de normalización de productos industriales. *Revista de administración pública*, n. 116, p. 287-339, 1988.

MANTELERO, A. Analysis of international legally binding instruments, en BEN-ISRAEL, I. (*et al.*) *Towards Regulation of AI Systems: Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law*. Council of Europe, 2020, pp. 61-97.

MARTÍN DELGADO, I. Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi. *Istituzioni del federalismo*, v. 3, p. 643, 2019.

MARTÍN DELGADO, I. La aplicación del principio de transparencia a la actividad administrativa algorítmica. *In: Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 131-194.

MARTÍN DELGADO, I. Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de administración pública*, n. 180, p. 353-386, 2009.

MARTÍNEZ GUTIÉRREZ, R. Responsabilidad administrativa por el uso de la Inteligencia Artificial. *In: Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 227-253.

MIRANZO DÍAZ, J. *Inteligencia artificial y Derecho administrativo*. Madrid: Tecnos, 2023.

MISURACA, G.; AND VAN NOORDT, C. *Overview of the use and impact of AI in public services in the EU*. Luxemburgo: Publications Office of the European Union, 2020.

MULLER, C., TALVITIE, C.; SCHÖPPL, N. "Our Minds, Monitored and Manipulated: How AI Impacts Public Discourse and Democracy", *VerfBlog*, 2022/3/28, <https://verfassungsblog.de/roa-our-minds/>, DOI: 10.17176/20220329-011119-0.

MÜLLER, M.; JOOSTEN, J. J. Model-checking in the Foundations of Algorithmic Law and the Case of Regulation 561. *arXiv preprint arXiv:2307.05658*, 2023.

NEMITZ, PAUL; GRÄF, EIKE: *Artificial Intelligence Must Be Used According to the Law, or Not at All*, *VerfBlog*, 2022/3/28, <https://verfassungsblog.de/roa-artificial-intelligence-must-be-used-according-to-the-law/>, DOI: 10.17176/20220328-131134-0.

PONCE SOLÉ, J. *Acicates (nudges), buen gobierno y buena administración: Aportaciones de las ciencias conductuales, nudging y sector público y privado*. Madrid: Marcial Pons, 2022b.

PONCE SOLÉ, J. Capítulo V. Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana. In: *Inteligencia artificial y sector público: retos, límites y medios*. Valencia: Tirant lo Blanch, 2023. p. 195-225.

PONCE SOLÉ, J. Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo*, n. 50, 2019.

PUERTA SEGUIDO, F. E.; ORTEGA ÁLVAREZ, L. I.; ALONSO GARCÍA, M. C. Las entidades colaboradoras en materia de protección ambiental. In: *Tratado de derecho ambiental*. Valencia: Tirant lo Blanch, 2013, p. 401-441.

SAINZ MORENO, F. Ejercicio privado de funciones públicas. *Revista de Administración pública*, n. 100-102, 1983.

SCHEPEL, H. *The constitution of private governance: Product standards in the regulation of integrating markets*. Hart Publishing, 2005.

SCHUETT, J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, p. 1-19, 2023.

SENDEN, L. The Constitutional Fit of European Standardization Put to the Test. *Legal Issues of Economic Integration*, 44, n. 4, 2017.

TAEIHAGH, A.; RAMESH, M.; HOWLETT, M. Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance*, 15, n. 4, p. 1009-1019, 2021.

VALERO TORRIJOS, J. Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista catalana de dret públic*, n. 58, p. 82-96, 2019.

VIDA FERNÁNDEZ, J. Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. In: DE LA QUADRA SALCEDO, T. e PIÑAR MAÑAS, J. L. (Ed.). *Sociedad digital y Derecho*. Ministerio de Industria, Comercio y Turismo, 2018. p. 203-224.

VIDA FERNÁNDEZ, J.; QUADRA-SALCEDO Y FERNÁNDEZ DEL CASTILLO, T. D. L.; PIÑAR MAÑAS, J. L. Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. In: *Sociedad Digital y Derecho*. Madrid: Ministerio de Industria, Comercio y Turismo, 2018. p. 203-224.

VIGURI CORDERO, J. A. Les normes ISO/IEC com a mecanismes de responsabilitat proactiva en el Reglament General de Protecció de Dades. *IDP. Revista de Internet, derecho y política*. (*Revista d'Internet, Dret i política*), n. 33, 2021.

VOLPATO, A. Controlling the Invisible: Accountability Issues in the Exercise of Implementing Powers by EU Agencies and in Harmonised Standardisation. *Review of European Administrative Law*, 12, n. 1, p. 75-96, 2019.

WAGNER, W. E. Science Charade in Toxic Risk Regulation, The. *Colum. L. Rev.*, v. 95, p. 1613, 1995.

WEN, L.; CAO, Y. A hybrid intelligent predicting model for exploring household CO2 emissions mitigation strategies derived from butterfly optimization algorithm. *Science of The Total Environment*, 727, p. 138572, 2020.

XUNTA DE GALICIA. *Estratexia Galega de Intelixencia Artificial 2030: Cara a unha Galicia Intelixente*, 2021.

ZHANG, D.; MISHRA, S.; BRYNJOLFSSON, E.; ETCHEMENDY, J. *et al.* The AI index 2021 annual report. arXiv preprint arXiv:2103.06312, 2021.

WEN, L.; CAO, Y. A hybrid intelligent predicting model for exploring household CO2 emissions mitigation strategies derived from butterfly optimization algorithm. *Science of The Total Environment*, 727, p. 138572, 2020.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/aec.v24i96.1932.
