Working Papers
2025, 1(6):71-90, © DIGITAPIA
Universitat Oberta de Catalunya
https://blogs.uoc.edu/digitapia/
DIGITAPIA

Evaluaciones de impacto y herramientas para su cumplimiento normativo en la implantación de algoritmos y tecnologías de IA

Impact assessments and its compliance tools for the implementation of algorithms and AI solutions

Eduardo Gamero Casado[1]
Catedrático de Derecho Administrativo, Universidad Pablo de Olavide
gamero@upo.es

Antonio David Berning Prieto[2]
Profesor Contratado Doctor de Derecho Administrativo, Universidad Pablo de Olavide
aberning@upo.es

Resumen

La normativa reguladora de la IA, con un enfoque basado en riesgos, establece una serie de obligaciones de evaluación de impacto y deberes de supervisión y control, que incluyen actuaciones tanto materiales (técnicas) como documentales (información de soporte). En este momento es de la mayor importancia determinar el alcance de esos deberes, y concretar la manera de satisfacer las exigencias regulatorias. En este trabajo se procede, en primer lugar, a identificar los diferentes ámbitos en los que realizar evaluaciones de impacto y tareas de supervisión y control. En segundo lugar, se exponen las herramientas y técnicas que se están desarrollando para articular esas tareas. Y en tercer lugar, se ofrece una propuesta normativa que pretende garantizar la toma en consideración de las mejores prácticas en la materia al implantar tecnologías de IA en

[1] Consejero Académico de la firma Montero Aramburu & Gómez-Villares Atencia. Académico correspondiente de la Real Academia de Legislación y Jurisprudencia de España y de la Real Academia San Dionisio de Ciencias, Artes y Letras de Jerez. Autor de nueve monografías y director o coordinador de otras quince, publicadas en reputadas editoriales jurídicas; autor de más de un centenar de artículos de revista y capítulos de libro, en los más variados campos del Derecho administrativo. Premio Blas Infante de investigación en Administración Pública. Ha sido Secretario General de la Universidad de Huelva y Defensor Universitario en esa universidad y en la UPO. Premio de investigación de la Real Academia Sevillana de Legislación y Jurisprudencia. Investigador principal de varios proyectos del Plan Nacional de IDi y del Plan Andaluz de I+D+i. Actualmente, co-IP del proyecto de Generación de Conocimiento "La potestad reglamentaria. Concepto y régimen jurídico de los reglamentos" (POTERES: poteres.es), del Programa Estatal de Investigación Científico y Técnica (PID2022-139090NB-I00).

[2] Doctor en Derecho Administrativo con mención internacional. Premio extraordinario de doctorado. Máster en Derecho de las Nuevas Tecnologías. Máster en Derechos Fundamentales. Experto en Contratos Públicos. Miembro del Research Network on EU Administrative Law (ReNEUAL). Miembro del Editorial Board de la revista European Review of Digital Administration & Law (ERDAL) y revisor por pares en diversas revistas científicas de la disciplina. Autor de la monografía Validez e invalidez de los actos administrativos en soporte electrónico (Aranzadi) y de diversos capítulos de libro y artículos en revistas científicas de prestigio en la disciplina. Investigador responsable científico de diversos Contratos de Transferencia de Investigación con entidades públicas y privadas. Actualmente, miembro del equipo de investigación del proyecto de Generación de Conocimiento "La potestad reglamentaria. Concepto y régimen jurídico de los reglamentos" (POTERES: poteres.es), del Programa Estatal de Investigación Científico y Técnica (PID2022-139090NB-I00).

el sector público.

Palabras clave: Inteligencia Artificial, Evaluación de impacto, Auditoría, Supervisión, Algoritmos, Derechos fundamentales, Control.

Abstract

The regulatory framework for AI, with a risk-based approach, establishes a series of impact assessment obligations and supervisory and control duties, which include both material (technical) and documentary (supporting information) actions. It is now of the utmost importance to determine the scope of these duties, and to specify how the regulatory requirements can be met. This paper first identifies the different areas in which impact assessments and monitoring and control tasks can be carried out. Secondly, it sets out the tools and techniques that are being developed to articulate these tasks. Thirdly, it offers a policy proposal that aims to ensure that best practices are taken into account when implementing AI technologies in the public sector.).

Keywords: Artificial Intelligence, Impact Assessment, Auditing, Supervision, Algorithms, Fundamental Rights, Control.

1. Introducción

Progresivamente van surgiendo iniciativas que configuran un marco regulatorio específico de la IA. Unas son más prolijas y minuciosas, y otras más esquemáticas, pero todas gozan de un cierto mínimo común denominador, replicando una serie de problemas y preocupaciones que se ven correspondidos con soluciones muy análogas. Podemos mencionar, en ese sentido, algunos hitos relevantes, como la Recomendación sobre ética de la IA de la UNESCO de 2021, la Carta Iberoamericana de la IA en la Administración Pública elaborada por el CLAD de 2023, la Ley peruana 31.814, de 5 de julio de 2023, que promueve el uso de la inteligencia artificial (muy embrionaria, pero sujeta a desarrollo reglamentario), el Convenio Marco del Consejo de Europa sobre inteligencia artificial y derechos humanos, democracia y Estado de Derecho (2024) y, por último, el Reglamento (EU) 2024/1689, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial (RIA).

Aunque son grandes las diferencias que separan estos instrumentos, también son muchas sus similitudes. Coinciden en ciertas preocupaciones, como la protección de los derechos fundamentales, el antropocentrismo, la supervisión humana, o la transparencia y explicabilidad de los algoritmos. Asimismo, un enfoque basado en los riesgos es una aproximación cada vez más frecuente al problema, clasificando los sistemas (y modelos) de IA en función del riesgo potencial que pueden suponer y conduciendo a la imposición de evaluaciones de impacto (*impact assessment*) sobre diferentes bienes o valores: los derechos de la ciudadanía, la salud, la seguridad… Todo ello va conformando una suerte de *ius commune* en materia de IA. En los pliegos de la contratación de IA se debe estipular expresamente el escrupuloso respeto de estas previsiones.

Se trata aquí, por tanto, de apoyar la implantación de soluciones de IA por el sector público, ofreciendo una serie de pautas y herramientas con las que lograr no solo una buena solución tecnológica, sino, además, una solución acorde con el régimen jurídico de la IA en general y de la actuación de los poderes públicos en particular, focalizando el interés en las herramientas y soluciones articuladas para la evaluación de impacto, la supervisión y el control de las soluciones de IA.

Toda la intensa actividad reseñada en este trabajo, en el que nos vemos obligados a dar tan solo cuenta de su existencia, es reveladora no solo de la preocupación de todos los operadores por articular herramientas de evaluación de impacto, auditoría, supervisión y control de los sistemas: también es exponente de la centralidad de la cuestión. En efecto, una vez que la tecnología algorítmica y la IA van alcanzando cada vez más madurez, y que asimismo se consolidan los enfoques para embridar sus riesgos, aprobando normas que obligan a la evaluación de impacto, la auditoría, supervisión y control del sistema, resulta imprescindible desarrollar las técnicas y herramientas mediante las que llevar a cabo esas labores. Es evidente que tales herramientas y técnicas se encuentran aún en una fase embrionaria de desarrollo; pero también —como veremos— que ya existen relevantes instrumentos con los que llevar a cabo estas actuaciones.

Debido al enfoque de este trabajo, prescindimos de aportar un pormenorizado aparato bibliográfico sobre

cuestiones generales[3], centrándonos en las aportaciones que afectan directamente al objeto central del estudio, esto es, las herramientas y técnicas previstas para articular y facilitar el cumplimiento normativo de las obligaciones de evaluación de impacto, supervisión y control de las soluciones y sistemas de IA.

2. Alcance de las evaluaciones de impacto, auditorías y suspensión y control de soluciones de IA en el derecho positivo vigente

2.a. En aplicación del Derecho interno: el art. 41 LRJSP

El artículo 41.1 LRJSP regula la actividad administrativa automatizada (AAA), de forma que se define como "cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público", y el art.41.2 dispone que, al implantar una actuación administrativa automatizada, "deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente". Como hemos destacado en otro lugar[4], el precepto establece la necesidad de llevar a cabo la supervisión, el control de calidad y la auditoría del sistema de información y de su código fuente. Es una disposición vanguardista y muy anticipada a su tiempo. Cuando se formuló, los términos que utiliza (supervisión, control de calidad, auditoría) no estaban suficientemente decantados y aun hoy no lo están completamente. Son técnicas en implementación al mismo tiempo que se desarrolla la propia tecnología.

En la actualidad no es difícil entablar una conexión entre la supervisión a que alude el art.41 LRJSP y la supervisión humana establecida por el RIA. En cuanto al control de calidad, podría interpretarse actualmente que evoca la necesidad de someter las tecnologías de IA a revisiones y controles de funcionamiento antes de su despliegue. La auditoría podría referirse a la evaluación y control ex post del funcionamiento de la solución o del sistema, una vez desplegado y hasta el fin de su ciclo de vida.

2.b. En aplicación del Reglamento de Inteligencia Artificial de la UE

A continuación, exponemos las exigencias que el RIA impone sobre los sistemas y soluciones de IA, en la medida que suponen un parámetro de cumplimiento normativo a la hora de desplegar tanto las evaluaciones de impacto de dichas soluciones y sistemas, como la manera de implantar la supervisión y control de los mismos. Es una exposición necesariamente telegráfica y desprovista de aparato documental, dada la amplitud de las cuestiones a tratar, pues en relación con este trabajo revisten un interés puramente instrumental, toda vez que, de lo que se trata aquí es de ofrecer las herramientas que se están desarrollando para articular esas evaluaciones de impacto y las técnicas de supervisión y control de las soluciones y sistemas de IA.

2.b.1. Enfoque general

La regulación del RIA, como es sabido, pivota en torno a varias previsiones:

- Enfoque basado en riesgos, con una categorización de soluciones y sistemas de IA articulada en sistemas prohibidos y niveles de riesgos de los

[3]Sin ánimo de ser exhaustivos, y mencionando tan solo las obras más representativas publicadas en España en los últimos dos años —especialmente en lo relativo al sector público—, pueden citarse las siguientes contribuciones: El Derecho administrativo en la era de la inteligencia artificial. Actas del XVIII Congreso de la Asociación Española de Profesores y Profesoras de Derecho Administrativo (Valcárcel Fernández & Hernández González, dirs., 2024); Inteligencia artificial y sector público: Retos, límites y medios (Gamero Casado, dir., 2023); Inteligencia artificial y administraciones públicas: Una triple visión en clave comparada (Cerrillo i Martínez, Di Lascio, Martín Delgado & Velasco Rico, dirs., 2024); El Reglamento de inteligencia artificial de la Unión Europea de 2024, el derecho a una buena administración digital y su control judicial en España (Ponce Solé, 2024); Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea (Cotino Hueso & Simón Castellano, dirs., 2024); From bureaucracy to artificial intelligence. The tension between effectiveness and guarantees (Menéndez Sebastián, 2023); Desafíos éticos, tecnológicos y jurídicos del avance digital (Domínguez Álvarez & Terrón Santos, dirs., 2023); The EU Regulation on Artificial Intelligence: a commentary (Huergo Lora, ed., 2025); Comentarios al Reglamento Europeo de inteligencia artificial (Barrio Andrés, dir., 2024a); El reglamento europeo de inteligencia artificial (Barrio Andrés, dir., 2024b); Las Administraciones públicas ante la inteligencia artificial (Carlón Ruiz, 2024); Inteligencia artificial y Derecho administrativo (Miranzo Díaz, 2023); Derecho y tecnologías (Casas Baamonde, dir., 2024); Reglamento Europeo de IA. Monográfico de la Revista Privacidad y Derecho Digital (García Mexía, dir., 2024); Inteligencia artificial y justicia (Peralta Gutiérrez & Pedrosa del Pino, dirs., 2024); Una panorámica de los sistemas de inteligencia artificial desde la perspectiva del Derecho administrativo (Tahirí Moreno, 2024a); y, finalmente, la Guía básica de la IA (Aguilar et al., 2024).

[4]Véase Gamero Casado (2023, pp. 403 y ss), donde hemos analizado el precepto detalladamente. Aquí nos limitamos a reseñar los aspectos esenciales que guardan conexión con la temática de este trabajo.

admitidos, estableciendo requisitos de cumplimiento que varían en función de estos (artículo 5).

- Establecimiento de obligaciones a usuarios y proveedores (artículo 16).

- Sistemas de Gestión de la Calidad durante el ciclo de vida del sistema de IA (artículo 17).

- Evaluación de la conformidad con el RIA (artículo 43), declaración UE de conformidad del proveedor (artículo 47) y marcado CE (artículo 48).

- Creación de una base de datos europea de sistemas de alto riesgo (artículo 71): inscripción del proveedor, sin que se precise si se trata de una base de datos meramente registral o a efectos de comprobaciones ulteriores de conformidad con el RIA.

- Monitorización tras la comercialización del sistema de IA (artículos 72 y ss.): obligación del proveedor de establecerlo, con análisis de interacción con otros sistemas, durante toda su vida útil. La Comisión Europea elaborará un modelo.

El RIA, para sistemas de IA de alto riesgo, prevé el establecimiento de un sistema de gestión de riesgos (que es el principal objeto de interés en esta aportación), con las siguientes características:

- Se define 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 RIA), con la obligación de establecerlo, implantarlo, documentarlo y mantenerlo (artículo 9.1 RIA).

  - Las etapas que comprende (artículo 9.3 RIA) son:

- Determinación y el análisis de los riesgos conocidos y previsibles que el sistema de IA de alto riesgo pueda plantear para la salud, la seguridad o los derechos fundamentales.

- Estimación y evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible.

- Evaluación de otros riesgos que podrían surgir, a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización a que se refiere el artículo 72.

- Adopción de medidas adecuadas y específicas de gestión de riesgos diseñadas para hacer frente a los riesgos detectados en el primer punto (no se prevé para el resto).

  - Para el establecimiento de las medidas de control de riesgo, se exige (artículo 9.5 RIA):

- Eliminar o reducir los riesgos detectados y evaluados de conformidad con el apartado 2 en la medida en que sea técnicamente viable mediante un diseño y un desarrollo adecuado.

- mplantar, cuando proceda, unas medidas de mitigación y control apropiadas que hagan frente a los riesgos que no puedan eliminarse.

- Proporcionar la información requerida conforme al artículo 13 y, cuando proceda, impartir formación a los responsables del despliegue, teniendo en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que se espera de estos.

- Si afecta negativamente a las personas menores de dieciocho años o a otros colectivos vulnerables (artículo 9.9 RIA).

Adicionalmente, los sistemas de IA serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas, comprobando que funcionan de manera coherente con su finalidad prevista y cumplen los requisitos establecidos (podrán incluir pruebas en condiciones reales), con las particularidades que a continuación se examinarán en cada ámbito de actuación.

Por otra parte, la Comisión Europea creó, mediante Decisión C(2024) 390 final, la Oficina Europea de Inteligencia Artificial (EAIO) para garantizar el cumplimiento del RIA.

La supervisión administrativa implica un amplio reconocimiento de potestades administrativas en orden a controlar efectivamente el cumplimiento normativo, por lo que las funciones y competencias de dicha Oficina están orientadas a la coordinación y contribución al desarrollo de sistemas de IA en colaboración con las entidades nacionales de supervisión (elaboración de guías, cooperación, estudio del mercado de IA, etc.).

Conforme al artículo 75.1 RIA, para las tareas de vigilancia y control la Oficina tendrá todos los poderes (entiéndase potestades) de una autoridad de vigilancia del mercado en el sentido del Reglamento (UE) 2019/1020, a pesar de que la tarea supervisora recae principalmente en los estados miembros a través de sus respectivas oficinas de supervisión de IA; no obstante, la propia Comisión Europea afirma que, entre las competencias de la EAIO está "incluida la capacidad de llevar a cabo evaluaciones de modelos de IA de propósito general, solicitar información y medidas a los proveedores de modelos y aplicar sanciones"[5].

El artículo 3.1.d) de la Decisión recoge entre las funciones de la Oficina "investigar posibles infracciones de las normas sobre modelos y sistemas de IA de uso general, en particular mediante la recogida de reclamaciones y alertas, la asistencia en la preparación de las decisiones de la Comisión y la realización de evaluaciones de conformidad con el próximo Reglamento". Adicionalmente, debe tenerse en cuenta que es posible que en el futuro intervenga en los sistemas de IA el European Centre for Algorithmic Transparency, el cual vigila actualmente el funcionamiento de buscadores y servicios online (Very Large Online Platforms –VLOPs- y Very Large Online Search Engines –VLOSEs-) conforme a la Digital Services Act (DSA).

En cuanto al supervisor en Derecho interno, acaba de conocerse el Anteproyecto de Ley para el buen uso y la gobernanza de la IA, que aborda su determinación. Dado el carácter embrionario de la propuesta, omitimos su análisis detallado.

En cuanto a las previsiones del RIA para sistemas de IA de alto riesgo se prevén medidas específicas para la gobernanza de datos (artículo 10), a saber:

- Si utilizan técnicas que impliquen el entrenamiento de modelos de IA con datos, se deben desarrollar a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad siguientes.
- Los conjuntos de datos de entrenamiento, validación y prueba se deben someter a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista (artículo 10.2), centradas en:
- Las decisiones pertinentes relativas al diseño.
- Los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos.
- Las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación.
- Información relativa a lo que miden y representan los datos.
- Evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios.
- Examen atendiendo a posibles sesgos a que puedan dar lugar.
- Medidas adecuadas para detectar, prevenir y mitigar posibles sesgos.
- Detección de lagunas o deficiencias en los datos y su subsanación.

Igualmente, los conjuntos de datos de entrenamiento, validación y prueba deben ser pertinentes, suficientemente representativos y, en la mayor medida posible, carecer de errores, teniendo en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico.

Se permite que los proveedores de los sistemas traten, excepcionalmente, las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas, siempre y cuando se haga para garantizar la detección y corrección de los sesgos, cumpliendo los requisitos del artículo 10.5 RIA (esto es, que no pueda llevarse a cabo con datos sintéticos o anonimizados, que se pseudonimicen,

[5] Véase Comisión Europea (2025a).

no se transmitan ni transfieran a terceros, se eliminen una vez que se haya corregido el sesgo).

En este sentido, el artículo 14 RIA establece la supervisión humana como método esencial para la protección en el tratamiento de los datos. En los supuestos de IA de alto riesgo, se exige que el diseño se haga de forma que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso mediante interfaz humano-máquina, con la finalidad de prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales.

Así, las medidas de supervisión deben ser proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA, pudiendo tratarse de:

- Medidas que el proveedor defina e integre en el sistema previamente a su puesta en uso.
- Medidas que el proveedor defina antes de la introducción del sistema en el mercado para que las ponga en práctica el responsable del despliegue.
- Estas medidas garantizarán que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación en caso de sistemas de IA del anexo III.1.a (sistemas de identificación biométrica remota, salvo los empleados únicamente para confirmar que una persona física es quién dice ser).

Adicionalmente, conforme al artículo 14.5 RIA, el sistema se debe ofrecer al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan:

- Entender adecuadamente las capacidades y limitaciones del sistema y poder vigilar su funcionamiento (detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados).
- Ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por el sistema ("sesgo de automatización").
- Interpretar correctamente los resultados de salida del sistema.
- Decidir, en cualquier situación concreta, no utilizar el sistema o descartar, invalidar o revertir los resultados de salida que este genere.
- Intervenir en el funcionamiento del sistema o interrumpirlo pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

Asimismo, se establecen requisitos de solidez, precisión y seguridad en los sistemas de IA de alto riesgo (artículo 15 RIA), a cuyo fin:

- La Comisión Europea establecerá parámetros de referencia y metodologías de medición en colaboración con autoridades de metrología y evaluación comparativa.
- Las instrucciones de uso incluirán la precisión del sistema y cómo medirla (artículo 15.3 RIA).
- Para garantizar la solidez de los sistemas se establecerán copias de seguridad y planes de prevención.
- Reducción del riesgo de introducción de sesgos y retroalimentación durante el aprendizaje posterior.
- Deben evitarse situaciones de vulnerabilidad, con medidas de seguridad que impidan acceso a terceros.
- Deben preverse medidas para prevenir, detectar, combatir, resolver y controlar los ataques que traten de manipular:

  - Conjunto de datos de entrenamiento ("envenenamiento de datos").

  - Los componentes entrenados previamente utilizados en el entrenamiento ("envenenamiento de modelos").

  - La información de entrada diseñada para hacer que el modelo de IA cometa un error ("ejemplos adversarios" o "evasión de modelos").

  - Los ataques a la confidencialidad.

  - Los defectos en el modelo.

También se establecen medidas de control a los sujetos que intervienen en la puesta en marcha de un sistema de IA de alto riesgo, como, por ejemplo:

- Proveedores: pruebas de conformidad, sistemas documentados de gestión de calidad, conservación de documentación del sistema, custodia de registros, colaboración con autoridades, notificación de incumplimientos o riesgos y medidas de corrección, etc.

- Importadores, distribuidores: conservación de documentación técnica, control de evaluación de conformidad, marcado CE, colaboración con autoridades, etc.

- Usuarios: supervisión humana, monitorización de los sistemas, conservación de registros, etc.

Las autoridades notificantes de cada Estado Miembro deben evaluar, designar, notificar y monitorizar los organismos de evaluación de la conformidad, pudiendo delegar en un organismo nacional de acreditación. Además, el registro de un sistema de IA de alto riesgo se debe registrar en la base de datos de la UE por parte de los siguientes sujetos responsables:

- El proveedor, previamente a la puesta en marcha o en el mercado del sistema IA de alto riesgo.

- El usuario, cuando pertenezca al sector público, salvo cuando se vaya a emplear en materias relativas a orden público, control de fronteras, inmigración o asilo.

- Otras medidas de control en relación con los sistemas de alto riesgo que tienen relación con el tratamiento de datos son:

  - Monitorización tras la comercialización: a través de la comprobación de que se cumplen los requisitos normativos.

  - Comunicación de incidentes relevantes a las autoridades de supervisión.

  - Las autoridades de supervisión deben informar a la Comisión Europea acerca de la aplicación del RIA.

  - El Supervisor Europeo de Protección de Datos, quién supervisará los sistemas de IA que empleen los órganos e instituciones de la UE.

  - Las autoridades de supervisión de mercado, las cuales deben tener acceso a los datos de entrenamiento usados y si es necesario al código para verificar el cumplimiento del RIA, pudiendo comprobar si existen riesgos y en caso de incumplimiento de normativa exigir medidas correctivas llegando a prohibir el sistema si no se adoptan.

2.b.2. Evaluación de impacto sobre derechos fundamentales

La previsión más relevante del RIA en cuanto a su supervisión y control de los sistemas de IA por su posible incidencia en los derechos fundamentales pivota en torno a la evaluación de impacto relativa a los derechos fundamentales cuando el sistema sea de alto riesgo, regulada en el artículo 27 RIA[6]. Dicha evaluación tiene las siguientes características:

- Es necesaria efectuarla previamente a su puesta en marcha, siendo el encargado el responsable del despliegue.

- La evaluación debe consistir en:

  - Descripción de los procesos en que se utilizará.

  - Tiempo durante el que se utilizará y frecuencia de uso.

  - Categorías de personas físicas o grupos a los que puede afectar.

  - Riesgos, de conformidad con la documentación remitida por el proveedor.

  - Medidas de supervisión humana a aplicar, conforme a las instrucciones de uso.

  - Medidas que deben adoptarse en caso de materializarse los riesgos, conforme a la gobernanza interna.

  - Mecanismos de reclamación.

[6]Sobre esta cuestión, además de las obras citadas en la nota 3, vid. especial y recientemente Mantelero (2024).

- Puede complementar a la Evaluación de impacto relativa a la Protección de Datos.

- Se permite utilizar los realizados por el proveedor, salvo que se detecten cambios, caso en que deberá volver a realizarse y notificarse los resultados.

- Tras la realización de la evaluación se comunicará a la autoridad de vigilancia del mercado.

- Ante cualquier riesgo de vulneración de derechos fundamentales, se notificará a la autoridad de vigilancia del mercado, la cual dispondrá las pruebas necesarias para comprobarlo (artículo 77 RIA).

2.b.3. Evaluaciones de impacto sobre la salud y la seguridad; consideraciones acerca del impacto sobre el medio ambiente

El RIA alude repetidamente a los potenciales efectos de la IA sobre la salud y la seguridad: así, considerandos 8, 20, 47, 48, 52, 53, 55, 64, 65, 67, 110, 130, 140; y arts.7, 10, 13, 57.6, 58.9, 70.3, 112.10, Anexo IV.3. Sin embargo, es tan solo en este último donde se vincula la salud y la seguridad con la evaluación de impacto, estableciendo que la documentación técnica de los sistemas de IA debe incluir "los resultados no deseados previsibles y las fuentes de riesgo para la salud y la seguridad, los derechos fundamentales y la discriminación, en vista de la finalidad prevista del sistema de IA". En la misma línea, se establece una conexión entre ambas cuestiones en el considerando 48: "Cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, también en lo que respecta a la salud y la seguridad de las personas, también se debe tener en cuenta el derecho fundamental a un nivel elevado de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión". También el art.10.2 f), cuando regula la gobernanza de datos, establece que: "2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente: [...] f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas". El art.13.3 iii) RIA, relativo a las instrucciones de uso que se deben facilitar al responsable del sistema de IA, han de incluir "cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad". Y el art.70.3 RIA establece que los Estados miembros garantizarán que sus autoridades nacionales competentes dispondrán de personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo, entre otras cosas, de los riesgos para la salud y la seguridad potencialmente derivados de las tecnologías de IA. Todo ello hace pensar en la necesidad de articular evaluaciones de impacto, con un enfoque basado en riesgos, acerca de los potenciales efectos sobre la salud y la seguridad de las tecnologías de IA; pero el Reglamento no lo impone tan claramente como en relación con los derechos fundamentales, ni detalla cómo llevarlas a efecto.

En análogo sentido, los considerandos del RIA aluden repetidamente a la necesidad de preservar el medio ambiente en la implantación de los sistemas de IA, y suelen incluir esa alusión en el mismo entorno en el que se refiere a la salud y a la seguridad, con ocasión del enfoque basado en riesgos: así considerandos 8, 27, 48, 130, 155, 176; y art.1 RIA. Sin embargo, cuando el Reglamento regula las evaluaciones de impacto, la mención al medio ambiente desaparece y es aun más débil que cuando alude a la salud y la seguridad, si bien existe en esta materia la misma conexión establecida por el considerando 48, que expusimos en el párrafo anterior. Se diría, entonces, que la evaluación de impacto también debe incluir el ambiental, pero en el contexto de su carácter de derecho fundamental, pues es lo que expresa el considerando 48. Pero no se contiene referencia alguna al medio ambiente en la evaluación de impacto sobre los derechos fundamentales que regula el art.27 RIA, anteriormente expuesto. Tampoco parece promoverse una metodología determinada o específica para medir el impacto ambiental de los sistemas de IA en ningún otro precepto. Sin embargo, de alguna manera debería articularse la consideración del impacto ambiental a la hora de implantar un sistema o solución de IA.

2.c. Las especialidades a considerar cuando se implanta la IA en el sector público

Para concluir, debemos resaltar las particularidades que han de cumplir las soluciones de IA implantadas por el sector público. En efecto, como recuerda el *Joint Research Centre* de la Comisión Europea[7], cuando se aplican soluciones de IA al sector público hay

[7] Véase Manzoni et al (2022).

que tomar en consideración reglas y principios específicos aplicables a la actuación de los poderes públicos. En particular, han de respetarse los principios de actuación predicables de la actuación pública, así como, cuando se trata de sistemas de soporte a la toma de decisiones, las garantías y derechos de la ciudadanía ante la tramitación de los procedimientos administrativos: posibilidad de subsanación, de presentar alegaciones o sustanciar el trámite de audiencia, la motivación de decisiones que afecten a derechos e intereses legítimos, la recurribilidad de tales decisiones… Estas garantías no decaen cuando el medio de actuación es la IA o la actividad automatizada, y las soluciones que se implanten deben tenerlas muy presentes y asegurar su compliance o cumplimiento normativo.

3. Herramientas para la evaluación de impacto, la suspensión y el control de las soluciones de IA

3.a. La decisión misma de implantar o no una solución de IA, especialmente en atención a su impacto ambiental

La primera cuestión a dilucidar es si conviene o no implantar un sistema de IA para resolver un problema o gestionar un determinado ámbito de la actuación pública. La IA es una moda, pero no vale para todo, aunque valga para casi todo. Pero, aun siendo potencialmente apta para infinidad de ámbitos diferentes, no siempre puede ser oportuno apostar por ella. Y, de otro lado, ante un mundo casi infinito de posibilidades, parece necesario priorizar los ámbitos en los que implantar en primer lugar las soluciones, ampliando el espectro poco a poco.

Al margen de estos ámbitos en los que la implantación de la IA en el sector público resulta particularmente fructífera, antes de lanzarse a desarrollar estas soluciones conviene sopesar otros factores que pueden influir en la decisión. Por ejemplo: ¿Hay datos suficientes? ¿Son de calidad? Porque un determinado campo puede resultar particularmente adecuado para el desarrollo de soluciones de IA, pero si no hay datos suficientes para entrenar el sistema, o los disponibles no son de calidad, resultará imposible desarrollar una solución lo suficientemente afinada como para ser útil.

También resulta necesario tomar en consideración el coste ambiental de implantar soluciones de IA, como vienen resaltado algunos autores[8]. Así, Strubell, Ganesh y McCallum señalaron ya en 2019 que el entrenamiento de un modelo como GPT-3 de Open AI, o BERT de Google, equivale al consumo total en ciclo-vida de 5 automóviles, o lo que es lo mismo, a 300 vuelos entre Nueva York y San Francisco[9]. Otro estudio (en este caso, de la Amherst Massachussets University) concluyó que solo la fase de aprendizaje de los algoritmos produce más de 280 t. de CO2 por cada sistema, sin contar producción del hardware, enfriamiento de los centros de datos y demás fases del desarrollo. A lo cual debe añadirse que la cantidad de potencia informática necesaria para construir grandes sistemas de IA se duplica en promedio cada 3 meses y medio.

Antes de decidir la implantación de una solución de IA se debería afrontar un balance de costes/beneficios, en el que se pondere si el desarrollo e implantación de soluciones de IA produce más beneficios que perjuicios, aunque los factores de valoración tengan un componente altamente subjetivo en la medida que no son términos de comparación equiparables, pues ¿cómo medir qué grado de consumo de recursos es tolerable para lograr una mejora de un determinado servicio público? Aunque también se están intentando desarrollar metodologías de medida en este aspecto[10], de momento la actitud del órgano de contratación ha de guiarse por consideraciones un tanto de *brocha gorda*, pero que le deben llevar, cuando menos, a preguntarse si tiene verdaderamente sentido implantar un sistema de IA en el ámbito en cuestión.

Lo más cercano a nuestro objeto de interés es el Programa Nacional de Algoritmos Verdes, aprobado por el Gobierno de España. Constituye la Medida 20 de la Estrategia Nacional de Inteligencia Artificial 2020 (en cuadrada, a su vez, en el plan estratégico España Digital 2026), y se asienta en la siguiente premisa: “La inteligencia artificial debe ser desarrollada dentro de un contexto de responsabilidad y sostenibilidad, comprendiendo el impacto medioambiental que suponen y fomentando el desarrollo de una inteligencia artificial verde, desarrollada con criterios de sostenibilidad medioambiental y aplicada al desarrollo de acciones contra el cambio climático”. A este fin,

[8] Entre nosotros, Sanz Larruga (2024).

[9] Strubell, Ganesh y McCallum (2019).

[10] Por ejemplo, el Programa Nacional de Algoritmos Verdes, incluido en la Estrategia Nacional de Inteligencia Artificial 2020 del Gobierno de España, pretende desarrollar estándares para cuantificar el coste ambiental, así como técnicas para reducir tales costes.

[11] Véase sobre los algoritmos verdes en Gobierno de España. Ministerio para la Transformación Digital y la Función Pública. (s. f.).

promueve la adopción de buenas prácticas en el desarrollo de modelos inteligencia artificial sostenibles[11].

3.b. Las guías y herramientas generales elaboradas por los poderes públicos y mediante aportaciones doctrinales

Por lo que se refiere, en primer lugar, a guías o herramientas generales que apoyan la implantación de soluciones y sistemas de IA por parte de los poderes públicos, ya han aparecido relevantes algunas guías e indicadores, impulsadas tanto por los poderes públicos como por la doctrina académica, que permiten orientar los esfuerzos de implantación de la IA hacia los ámbitos en que puedan ofrecer mejores resultados. Por ejemplo, el documento de la Comisión Europea (2024) *Adopt AI. Final Study Report*[12]; la herramienta elaborada por el G7 en colaboración con la UNESCO y la OCDE, *G7 Toolkit for Artificial Intelligence in the Public Sector. Report prepared for the 2024 Italian G7 Presidency and the G7 Digital and Tech Working Group; el Public Sector AI Playbook*, Gobierno de Singapur[13]; o la herramienta para evaluación de impacto de los algoritmos desarrollada por el Gobierno de Canadá[14].

También se dispone ya de relevantes aportaciones doctrinales que pretenden servir de guía y soporte a la implantación de soluciones y sistemas de IA, articulando fórmulas diversas para desplegar la evaluación de impacto y el control y auditoría; cabe reseñar las ofrecidas por Criado y Guevara-Gómez[15], Mökander[16]; Novelli et al.[17]; Laux, Wachter y Mittelstadt[18]; Mota y Herrera[19]; y Ortega Giménez[20].

En segundo lugar, pueden destacarse las guías y herramientas que se han elaborado en relación con el impacto o la salvaguardia de los derechos de la ciudadanía. Destacan los siguientes:

- Agencia Catalana de Protección Datos: *Modelo para la evaluación de impacto sobre derechos fundamentales en diseño y desarrollo de la IA, 2025.*

- HUDERIA, del Council of Europe (2024): *Methodology for the risk and impact assessment of AI systems from the point of view of human rights, democracy and the rule of law*[21].

En este mismo ámbito resaltan las herramientas elaboradas por autores como Mantelero[22], o Wierzbowski et al en el seno del *European Law Institute*[23].

En este contexto son también muy relevantes las guías para la contratación de soluciones de IA por el sector público. Estas herramientas son muy relevantes porque el sector público, por lo general, carece de capacidades técnicas para desarrollos de IA y, por tal motivo, debe externalizar su provisión, de modo que articular adecuadamente el procedimiento de contratación es crucial para lograr unas prestaciones adecuadas, no solo en cuanto al nivel técnico, sino también en lo que se refiere a las exigencias jurídicas. La más interesante herramienta desarrollada hasta hoy son las cláusulas contractuales tipo, o *model clauses*, elaboradas por la Comisión Europea. Se han ido preparando diferentes versiones, en función del estado de la ciencia y del avance progresivo que ha experimentado el marco regulatorio. La última actualización es de febrero de 2025[24], tomando en consideración la aprobación del RIA; todavía se encuentran disponibles únicamente en inglés (las traducciones subsiguientes son nuestras). Son dos documentos:

- Model contractual clauses for the public procurement of High-Risk AI ('MCC-AI-High-Risk'),

[12] Véase Comisión Europea (2024).

[13] Elaborado con apoyo de la industria para facilitar la implantación de sistemas de IA en el sector público. Véase Gobierno de Singapur (2024).

[14] Véase Government of Canada (2024).

[15] Criado y Guevara-Gómez (2024).

[16] Mökander (2023).

[17] Novelli et al (2024).

[18] Laux, Wachter y Mittelstadt (2024).

[19] Mota Sánchez y Herrera Expósito (2024).

[20] Ortega Giménez (2024).

[21] v

[22] Mantelero (2022).

[23] Se trata de las Model Rules on Impact Assessment of Algorithmic Decision-Making System Used by Public Administration. Son una relevante guía, focalizada esencialmente en el impacto sobre derechos fundamentales (y esencialmente, en relación con el régimen de protección de datos), elaborada por reputados académicos en el marco del European Law Institute. Véase European Law Institute (2022).

[24] Véanse Comisión Europea (2025b) y Comisión Europea (2025c).

es decir, para la contratación de sistemas de IA de alto riesgo (Comisión Europea, 2025b).

- Model contractual clauses for the public procurement of Non-High-Risk AI ('MCC-AI-High-Light Version'), para sistemas de bajo o nulo riesgo (Comisión Europea, 2025c).

La incorporación de estas cláusulas a las licitaciones de la contratación pública pretende facilitar el cumplimiento normativo, de manera que las soluciones desarrolladas se ajusten al marco regulatorio, evitando fracasos en los resultados debido a la inadecuación del sistema. Están concebidas para poderes adjudicadores de la UE, y son una valiosa guía para lograr el pleno cumplimiento normativo de las obligaciones de evaluación de impacto, supervisión y control de los sistemas y soluciones de IA.

3.c. Los Anexos del RIA y sus desarrollos normativos previstos

Una relevante fuente de concreción de las determinaciones del RIA y de su modo de cumplimiento se encuentra en el propio Reglamento.

Comenzando por los Anexos, varios de ellos se dedican precisamente a concretar el alcance de las evaluaciones de impacto, de la supervisión y demás controles, así como de su reflejo documental. Destacan a estos efectos los siguientes Anexos:

- Anexo IV, Documentación técnica de los sistemas de alto riesgo a que se refiere el art.11.1.
- Anexo V, Declaración UE de conformidad.
- Anexo VI, Procedimiento de evaluación de la conformidad fundamentado en un control interno.
- Anexo XI, Documentación técnica para proveedores de modelos de IA de uso general.
- Anexo XII, Información sobre transparencia: documentación técnica de los proveedores de modelos de IA de uso general para los proveedores posteriores que integren el modelo en su sistema de IA.

Además de estas especificaciones, que se incorporan directamente al cuerpo del Reglamento, éste contempla también una serie de instrumentos de desarrollo que contribuyen al mismo propósito; en particular, los siguientes:

- Directrices de la Comisión (art.96): orientarán la aplicación práctica del RIA, concretando definiciones, cumplimiento de requisitos, etc. Ya se han producido dos relevantes ejemplos: Guidelines on prohibited AI practices C(2025) 884 final (Comisión Europea, 2025d), y Guidelines on the definition of an AI system C(2025) 924 final (Comisión Europea, 2025e).
- Normas armonizadas de la UE (art.40.1; Anexo I): es decir, normativa específica que establece requisitos aplicables en su concreto ámbito de reglamentación técnica.
- Normalización técnica (art.40.2): dada la relevancia de la estandarización en este ámbito, el Reglamento contempla la posibilidad de que la Comisión Europea dirija solicitudes a organismos de normalización (como el Centro Europeo de Normalización, CEN), a fin de que elaboren especificaciones técnicas relacionadas con la IA.
- Código buenas prácticas modelos IA de propósito general (art.56), que se encuentra actualmente en elaboración.
- Códigos de conducta (art.95): para aplicación voluntaria a sistemas no alto riesgo (art.95.1) y a todos los sistemas (art.95.2).

Todas estas fuentes normativas representan un claro cambio de paradigma respecto de lo que sucedió con ocasión del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), por cuanto que este último establecía toda una serie de obligaciones sin concretar su manera de cumplimiento, generando una gran ansiedad en los operadores jurídicos. Solo el transcurso del tiempo, y las actividades del supervisor, han ido decantando y concretando tales obligaciones. En cambio, en relación con el RIA parece claro que se van a ir dictando, con ocasión de su progresiva entrada en vigor, las disposiciones necesarias para incrementar la seguridad jurídica y determinar de manera precisa el

modo de cumplir sus exigencias.

3.d. La normalización y estandarización técnicas

En cuanto a la normalización técnica y la estandarización, debe partirse de la base de que en materia de administración electrónica en general ya se está extendiendo la constante referencia normativa a estándares no sólo nacionales, sino también internacionales.

En este sentido, la normativa que desarrolla los requisitos técnicos (Normas Técnicas de Interoperabilidad) pertenece a la reglamentación técnica nacional, disposiciones vinculantes por su naturaleza reglamentaria. Pero sucede que cada vez más se aprecia la concurrencia de ésta con otro tipo de requerimientos que pertenecen a la normalización o estandarización, de forma que[25]: se individualizan los sistemas, equipos y procesos, estableciendo fórmulas comunes; se verifica su calidad; se controla su seguridad; y permite la interoperabilidad.

Especialmente relevante es el ámbito de la seguridad, en el que se plantean cuestiones capitales relativas al empleo de normas estandarizadas para garantizar sistemas seguros, como son la aplicación de las normas UNE-ISO/IEC 27001:2023 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos"; ISO/IEC 27017: norma que despliega controles para la seguridad de la información en la nube; o la ISO/IEC 27005, norma que incluye metodologías para desarrollar el proceso de gestión de riesgos de seguridad de la información, entre otras.

De hecho, el ENS, en su DA 2ª (modificado recientemente por la DF 2ª del Real Decreto 1125/2024, de 5 de noviembre para sustituir la Secretaría de Estado de Digitalización e Inteligencia Artificial por el titular ministerial), relativa al desarrollo del mismo, dispone que: "La persona titular del Ministerio para la Transformación Digital y de la Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la persona titular de la Secretaría de Estado de Función Pública".

A tal fin, se hace referencia a continuación a que las "instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables" (se consideran Derecho de la Unión desde la STJUE de 27/10/2016, As. C-613/14 - James Elliott c. Irish Asphalt Ltd.).

Y, adicionalmente, se prevé que "el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad", por lo que se aprecia cómo la estandarización aparece expresamente en disposiciones normativas tradicionales.

A pesar de su carácter voluntario (Carrillo Donaire[26], Álvarez García[27]), se comienzan a publicar guías de adecuación al ENS con previsiones relacionadas con este tipo de normas. A título ejemplificativo, la "Guía de seguridad de las TIC" de julio de 2023, del Centro Criptológico Nacional, pone énfasis en el cumplimiento del ENS a través del cumplimiento de normas ISO.

Existe, por tanto, una creciente compatibilidad que se manifiesta en las sinergias que provoca la adecuación de los sistemas de administración digital desarrollados por las AAPP con cumplimiento de normas ISO/UNE. Manifestación de ello es el aumento de la imposición del cumplimiento de normas ISO/UNE como requisitos en las licitaciones públicas, de forma que las propias AAPP exigen su cumplimiento para los sistemas de administración digital a desarrollar e implantar, como se puede apreciar efectuando una simple consulta a las licitaciones de servicios relativos a administración electrónica publicadas en la Plataforma de Contratos del Sector Público.

En el Reglamento europeo de Inteligencia Artificial (RIA) se prevé (artículo 17), para los sistemas de alto riesgo, el establecimiento de un sistema de gestión de la calidad, para lo cual uno de los enfoques más habituales es la observancia de la serie ISO 9000 (como la ISO 9001, base de los sistemas de gestión de la calidad).

De hecho, el propio artículo 40 RIA establece que las normas armonizadas europeas [reguladas por el Reglamento (UE) 1025/2012], las cuales son un instrumento de reglamentación técnica "de nuevo enfoque" por tratarse de una técnica regulatoria de colabora-

[25] Gamero Casado y Fernández Ramos (2024, p. 846).
[26] Véase Carrillo Donaire (2000).
[27] Véase Álvarez García (2024).
[28] Véase Tahirí Moreno (2024b, pp. 457 ss).

ción público-privada[28] en virtud de la cual se encarga a Organismos europeos de Normalización su confección por ostentar mayor capacidad técnica para ello, pero que al tener control por parte de la Comisión, suponen "Derecho de la UE" y, por tanto, son fiscalizables ante el TJUE (*cfr.* la precitada STJUE de 27/10/2016, caso *James Elliot c. Irish Asphalt Ltd.)*.

En estos casos se reconoce una presunción de conformidad de los sistemas IA de alto riesgo si han sido desarrollados con observancia de las normas armonizadas europeas.

No es, por tanto, una problemática estrictamente nacional, sino que a nivel europeo también existen dudas en relación con este tipo de disposiciones, al coexistir, junto con los actos legislativos ordinarios, (i) normas técnicas en sentido estricto; (ii) normas técnicas armonizadas europeas; (iii) especificaciones comunes europeas; y (iv) reglamentaciones técnicas nacionales.

Como puede advertirse, la proliferación de este tipo de normas es inevitable, y su reconocimiento también (de hecho, la Abogada General en la ya citada STJUE de 27/10/2016, instó al Tribunal a que se pronunciarse respecto a su naturaleza jurídica y encaje en el ordenamiento jurídico de la UE, sin que se localice ningún pronunciamiento al respecto en la sentencia.

En conclusión, si bien resulta complejo categorizar jurídicamente todos los instrumentos de *soft law* existentes en la actualidad, dado su elevado volumen y casuística tan variada, debe proporcionarse seguridad jurídica en cuanto a los procedimientos necesarios para su aprobación (en especial los relativos a la transparencia y participación) y su posterior control judicial, especialmente cuando regulan aspectos jurídico-públicos y no meramente privados.

Determinadas normas ISO resultan especialmente relevantes en materia de IA[29] ya que, además de respetar las exigencias normativas y éticas básicas, su contenido ha sido consensuado por parte de los diversos actores presentes en la industria y, por ende, las soluciones de IA que se desarrollan en el mercado y que podrían ser empleadas por las administraciones públicas las habrán tenido en cuenta o, de ser una solución a medida cuyo desarrollo haya sido requerido por parte de la Administración a través de cualquiera de las fórmulas de contratación previstas en la LCSP, los licitadores estarán familiarizados con ellas.

En este sentido, en primer lugar, la norma "UNE-EN ISO/IEC 22989:2023: *Tecnología de la información. Inteligencia artificial. Conceptos y terminología de inteligencia artificial*", establece una serie de definiciones terminológicas que resultan de mucha utilidad práctica, en tanto en cuanto en cada ámbito sectorial un mismo término puede tener diferentes connotaciones y resulta imprescindible unificar el criterio interpretativo. En este sentido, aparecen definidos no sólo conceptos, sino también procesos como el "proceso de verificación de la calidad de los datos" o el de "muestreo de datos", ambos fundamentales para garantizar la calidad de los datos de los que se va a nutrir el sistema de IA y de los que dependerá su funcionamiento.

Por su parte, entre los conceptos que define destacan algunos de especial relevancia para la actividad administrativa basada en sistemas de IA, tales como "explicabilidad" (propiedad de un sistema de IA para expresar factores importantes que influyen en los resultados del sistema de IA de una manera que los humanos puedan entender), "confiabilidad" (propiedad de consistencia del comportamiento previsto y de los resultados), "robustez" (capacidad de un sistema para mantener su nivel de rendimiento bajo cualquier circunstancia) y "transparencia", en el que la propia norma ISO efectúa una importante distinción que debería tenerse presente, entre la transparencia relativa a una organización (propiedad de una organización según la cual las actividades y decisiones apropiadas se comunican a las partes interesadas pertinentes de una manera completa, accesible y comprensible) y la relativa a un sistema de IA (propiedad de un sistema que permite que la información apropiada sobre el sistema esté disponible para las partes interesadas relevantes).

La precitada norma UNE-EN ISO/IEC 22989:2023 no sólo recoge conceptos y definiciones, sino que regula el ciclo de vida de los sistemas de IA, desde una descripción funcional de los mismos (datos como combustible, aprendizaje, predicciones y decisiones) hasta el ecosistema en el que funcionan, partiendo de los campos de aplicación (visión artificial, reconocimiento de imágenes, minería de datos, etc.) hasta las aplicaciones prácticas a las que pueden servir (vehículos autónomos, detección de fraudes, etc.). Entre otros aspectos, también dedica parte de su contenido a regular el espectro de riesgos que puede provocar un sistema de IA, determinado por la gravedad del potencial impacto de un fallo o un comportamiento inesperado, estableciendo diferentes niveles de evaluación de tales riesgos, en función de la presencia o ausencia de supervisión externa, en caso de supervi-

[29] Véase especialmente Laux, Wachter y Mittelstadt (2024).

sión externa, su tipología (automatizada o humana), el nivel de transparencia de las decisiones y el grado de automatización del sistema. Igualmente, se establecen medidas de mitigación del riesgo que serían muy útiles en el ámbito de las administraciones públicas, que se concretan, entre otras, en:

- Desarrollo de un plan de supervisión.
- Desarrollo de un plan para monitorear y responder a cualquier cambio normativo sobrevenido.
- Adopción de enfoques flexibles de diseño, implantación y operatividad de los sistemas de IA.

La propia norma UNE-EN ISO/IEC 22989:2023 establece que lo deseable es que la gestión de riesgos esté basada en un enfoque integrado, estructurado y global a todos los niveles, aspecto que deberá tenerse en cuenta por las administraciones públicas con la puesta en marcha de este tipo de sistemas. En este sentido, se establece la necesidad de determinar los órganos con competencias en esta materia en cada Administración Pública, desde órganos superiores (de gobierno), que definirán los objetivos generales, hasta los órganos de dirección que serán los que tomen las decisiones concretas respondiendo a las exigencias de los objetivos generales previamente establecidos. A tal fin, la citada norma hace depender el éxito de la gestión de riesgos de la identificación, establecimiento y aplicación de procesos que definan correctamente los criterios de riesgo a valorar, y que concreta en incertidumbres, probabilidad, consecuencias, nivel de riesgo y capacidad de respuesta de la Administración. Sería conveniente que cada entidad, a la hora de poner en marcha un sistema de IA, tenga en cuenta las previsiones de la norma UNE-EN ISO/IEC 22989:2023 en cuanto a:

(i) Evaluación de riesgos: deben identificarse, cuantificarse o describirse cualitativamente y priorizarse en función de criterios y objetivos de riesgo pertinentes para la organización (vid. catálogo en Anexo B de la norma), como:

a) Identificación de activos y su valor (materiales e inmateriales –salud, seguridad–)

b) Identificación de fuentes de riesgo (datos, procesos, personal, entorno, hardware…)

c) Identificación de posibles acontecimientos y resultados (los riesgos potenciales se identifican a través de normas publicadas, especificaciones técnicas, ensayos, simulaciones…)

d) Identificación de los controles (los cuales deben documentarse en sistemas internos, procedimientos, informes de auditoría…)

e) Identificación de las consecuencias (tiempo de investigación y reparación, reputacionales, amenazas para la salud o seguridad de las personas, sanciones, eventuales litigios…)

(ii) Análisis de riesgos, que comprende:

a) Identificación de las consecuencias: impacto potencial en sesgo a personas, potencial impacto a los derechos fundamentales o seguridad de individuos, protección ante eventuales injusticias…

b) Evaluación de la probabilidad: de que se produzcan sucesos y resultados que causen riesgos (a través del estudio de amenazas, mitigación del riesgo o fracaso de los controles…)

(iii) Elaboración de un plan de tratamiento de riesgos, que a su vez puede prever una posible compartición de riesgos (mediante la contratación de seguros o inclusión de estos riesgos en las pólizas ya contratadas) o fórmulas específicamente previstas para paliar sus consecuencias.

Dado que en la gestión de riesgos uno de los aspectos más relevantes es la posible presencia de sesgos durante el empleo de sistemas de IA, otra de las normas de esta naturaleza a tener en cuenta debería ser la UNE-CEN/CLC ISO/IEC/TR 24027:2023, que establece una clara distinción entre los tipos de sesgos que se pueden presentar (definiciones que podrían incluirse igualmente en el RD 203/2021, como se apuntó anteriormente), de forma que se minimicen los efectos negativos que pueden provocar. Y es que debe tenerse en cuenta que la presencia de sesgos no siempre provocará decisiones injustas[30], ya que el impacto de un sesgo puede ser también positivo o neutral. Piénsese por ejemplo en supuestos en que la decisión administrativa es injusta, caso en que podría introducirse de forma controlada un sesgo para corregirla y llegar a un

[30]Es importante tener en cuenta, de un lado, que los datos sesgados no siempre dan lugar a predicciones y acciones injustas y, de otro, las predicciones y acciones injustas no siempre son causadas por un sesgo.

resultado justo y razonable. Sin embargo, cuando se trata de sesgos con efectos negativos en la imparcialidad que debe sustentar toda actuación administrativa, es importante proporcionar una respuesta rápida, ya que se pueden propagar rápidamente en el sistema (especialmente en los sistemas de IA más avanzados) y complicar su posterior reconocimiento y mitigación. Por tanto, en la norma ISO se prevén garantías para tratar convenientemente los sesgos no deseados a lo largo del ciclo de vida de un sistema de IA, como, por ejemplo:

a) La necesidad de una evaluación de riesgos, como ya se apuntó anteriormente.

b) Notificación a los usuarios de que están sujetos a una decisión automatizada, y reconocimiento del derecho a que la decisión administrativa sea revisada posteriormente, en vía de recurso, por un humano.

c) Garantizar un cierto nivel de auditabilidad o explicabilidad en la solución, con el fin de respaldar el análisis de una decisión (motivación).

d) Actividades para cuantificar o mitigar riesgos, como la recopilación de metadatos sobre las fuentes de datos para comprender la procedencia y la calidad de éstos.

e) Previsión de la participación significativa de un ser humano en el proceso de toma de decisiones.

Existen otras normas de trascendencia para toda organización que emplee sistemas de IA, tales como la norma ISO/IEC 42001:2023, relativa al sistema de gestión de la IA, la cual especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de IA dentro del contexto de una organización, entre cuyas previsiones más relevantes se encuentra la de identificar a los responsables de fase del sistema de IA (implementación, operación, gestión…); la norma UNE-CEN/CLC ISO/IEC/TR 24029-1:2023, relativa a la evaluación de la robustez de las redes neuronales en caso de emplearse esta tipología específica de IA; o la norma EN ISO/IEC 23053:2023, que establece un marco para sistemas de IA que utilizan aprendizaje automático (*machine learning*), que incluye tanto sistemas basados en redes neuronales como en aprendizaje profundo (*deep learning*).

Otro de los aspectos más interesantes que prevé la norma UNE-EN ISO/IEC 22989:2023 y debería implantarse en el seno de las administraciones públicas que empleen sistemas de IA en su actividad administrativa es la distinción entre las figuras del "auditor de sistemas de IA", que se encargaría de evaluar la conformidad de los sistemas de IA con estándares, políticas o requisitos jurídicos, y del "evaluador de sistemas de IA", quién evaluaría el desempeño de uno o varios sistemas de IA durante su vida útil. Estas figuras deberían ser objeto de una correcta definición normativa tal y como se apuntó anteriormente (*vid. supra*), ya que resulta indispensable tener claras las funciones de cada sujeto que, durante el ciclo de vida de un sistema de IA, se encargue de supervisar unos aspectos u otros relativos al mismo, toda vez que lo que un técnico interprete como "auditor" no siempre coincidirá con el criterio de un jurista o economista, siendo importante que los roles están bien definidos en este ámbito.

En cuanto al ciclo de vida de un sistema de IA, la norma UNE-EN ISO/IEC 22989:2023 establece que todas las fases, que enumera: inicio, diseño, desarrollo, verificación, validación, implementación, operación, monitoreo, validación continua, reevaluación y retirada (literalmente el término empleado por la norma es "jubilación") por obsolescencia, deben tener una adecuada gobernanza, tanto con carácter general como especialmente en ámbitos concretos como la privacidad y la seguridad (al trabajar con grandes cantidades de datos, en ocasiones sensibles), las potenciales amenazas o en materia de explicabilidad y transparencia, no sólo en cuanto a la procedencia de los datos empleados, sino también, respecto a los datos de salida o resultados.

4. Propuesta normativa

Los preceptos que se proponen a continuación deberían tener carácter básico.

Pueden insertarse en una norma básica específica sobre IA o en las diversas normas que regulan las respectivas materias:

> i. La propuesta relativa a disposiciones generales, puede introducirse en La Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público; o en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

ii. La propuesta relativa a la contratación de tecnologías de IA, en la Ley 9/2017, de 8 de noviembre, de contratos del sector público.

iii. La propuesta relativa a subvenciones e incentivos, en la Ley 38/2003, de 17 de noviembre, general de subvenciones.

4.a. Régimen general y evaluación previa

Artículo XX. Requisitos para la implantación de sistemas de inteligencia artificial

1. El despliegue y funcionamiento de los sistemas de inteligencia artificial, incluyendo aquellos que se utilicen en actuaciones administrativas automatizadas, se gestionará con un enfoque basado en los riesgos, y exigirá:

a) El análisis previo de los datos disponibles, valorando y promoviendo su suficiencia y calidad en orden a decidir la implantación del sistema.

b) Una evaluación del nivel de riesgo. En caso de que el nivel sea alto tal y como se defina en la normativa aplicable en materia de inteligencia artificial, se precisará una evaluación de impacto sobre los derechos fundamentales de las personas, así como la salud y la seguridad.

c) La evaluación de impacto respecto a la protección de datos personales.

d) La evaluación de su ajuste a los derechos y garantías de las personas interesadas establecidos en la legislación del procedimiento administrativo común.

e) La transparencia en el diseño y la implementación, así como la capacidad de interpretación de las decisiones.

f) La consideración de su sostenibilidad.

2. La implantación de la IA en el sector público se ajustará a las mejores prácticas disponibles, a cuyo efecto, además del Reglamento (EU) 2024/1689, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial y sus disposiciones de desarrollo, se tomará especialmente en consideración lo dispuesto en los tratados internacionales y las guías, códigos de conducta y directrices de mayor reputación, así como teniendo presente los estándares técnicos aprobados por las entidades nacionales e internacionales de normalización.

4.b. Contratación pública

Como se expone en el trabajo, el sector público carece, por lo general, de capacidad para desarrollar tecnologías de IA, debiendo acudir al mercado para la compra de soluciones o para su diseño y despliegue. Por esta razón, regular adecuadamente la contratación de sistemas y soluciones de IA permitirá cumplir las exigencias de evaluación de impacto, supervisión, auditoría y control del sistema.

Artículo XX. Contratación de tecnologías de inteligencia artificial

1. En la contratación pública de tecnologías de inteligencia artificial, los pliegos establecerán el deber del adjudicatario de desarrollar el sistema verificando que, tanto en su diseño, como a lo largo de todo su ciclo de vida, se satisfarán las exigencias establecidas en el Reglamento (EU) 2024/1689, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial, y en el resto del Ordenamiento jurídico.

2. Antes del desarrollo o contratación de un sistema de inteligencia artificial, y en particular, durante la fase de preparación del expediente de contratación, se justificará que la implantación del sistema de inteligencia artificial es la opción óptima para el problema requerido de solución, a cuyo efecto se ponderará adecuadamente el valor añadido que aporte el sistema frente a otras alternativas, la existencia de suficientes datos y su calidad, así como el coste ambiental de su implantación.

3. En los procedimientos de contratación se implantarán las mejores prácticas, tomando en consideración las propuestas de cláusulas contractuales tipo elaboradas

por la Comisión Europea para la contratación de soluciones de inteligencia artificial y otras herramientas de similar naturaleza.

4. De acuerdo con lo establecido en el apartado anterior, los poderes adjudicadores promoverán pliegos-tipo de prescripciones técnicas y de cláusulas administrativas generales en los que se detallen y concreten todos los aspectos implicados en la contratación pública de sistemas de inteligencia artificial.

5. Tanto los pliegos correspondientes a cada licitación, como, en su caso, los pliegos-tipo, concretarán:

a) Las técnicas y procedimientos aplicables a efectos de llevar a cabo las evaluaciones de riesgo e impacto, conforme a lo estipulado en el Reglamento europeo de Inteligencia Artificial, en sus disposiciones de desarrollo, en las normas estatales y autonómicas aplicables, y en las mejores prácticas nacionales e internacionales del sector.

b) Los códigos de conducta y buenas prácticas, así como los estándares y normas técnicas establecidos por los organismos de estandarización y las reglamentaciones técnicas que representen las mejores prácticas en la materia y deban seguirse para el desarrollo de los sistemas.

c) El modo de garantizar los derechos de las personas interesadas en los procedimientos administrativos, cuando el sistema se implante como soporte a la toma de decisiones soporte a la toma de decisiones que afecten a derechos e intereses legítimos de las personas interesadas en procedimientos administrativos.

6. En todas las fases de la contratación administrativa se velará por la participación efectiva, tanto en la entidad contratante como en el contratista, de equipos de profesionales multidisciplinares, capaces de comprender e interpretar las implicaciones técnicas y tecnológicas, organizativas, éticas, jurídicas y lingüísticas derivadas de la implantación del sistema de inteligencia artificial.

7. El responsable del contrato se asegurará, antes de la puesta en marcha y aceptación del sistema de inteligencia artificial, que se cumplen los requisitos impuestos a estos sistemas en el Reglamento Europeo de Inteligencia Artificial y en el resto del Ordenamiento jurídico; en especial:

a) Que se ha llevado a cabo con carácter previo a la implantación del sistema la evaluación de riesgos sobre la salud, la seguridad y los derechos de la ciudadanía, y, en su caso, evaluación de impacto, y se han tomado en consideración sus resultados.

b) Que en el desarrollo del sistema de inteligencia artificial se han seguido las guías o códigos de buenas prácticas, así como los estándares y normas técnicas establecidos por los organismos de estandarización y las reglamentaciones técnicas que representen las mejores prácticas en la materia.

c) Que se dispone de la información necesaria en materia de transparencia y, en su caso, explicabilidad, de los algoritmos y de los sistemas de inteligencia artificial, así como para motivar las decisiones adoptadas con soporte en los mismos.

d) Que se dispone de la información relativa a las medidas de supervisión, auditoría y control a que se debe someter el sistema.

4.c. Subvenciones e incentivos

La principal justificación de esta previsión normativa es extender al sector privado las mejores prácticas en materia de IA, de manera que las bases reguladoras y las convocatorias de subvenciones contemplen expresamente la sujeción por el beneficiario a determinaciones análogas a las anteriormente previstas para el propio sector público. De este modo se promueve que los fondos públicos se apliquen de la manera más respetuosa, garantizando no solo las evaluaciones de impacto en el marco de un enfoque basado en riesgos, sino también las mejores prácticas derivadas de guías, directrices, códigos de conducta y normas técnicas.

Artículo XX. Régimen de fomento de tecnologías de inteligencia artificial

Las bases reguladoras y las convocatorias de incentivos que fomenten el desarrollo

o implantación de sistemas de inteligencia artificial concretarán los requisitos que deben reunir a fin de que los proyectos y los gastos de las solicitudes resulten elegibles, y en particular:

a) Las técnicas y procedimientos aplicables a efectos de llevar a cabo las evaluaciones de riesgo e impacto, conforme a lo estipulado en el Reglamento europeo de Inteligencia Artificial, en sus disposiciones de desarrollo, en las normas estatales y autonómicas aplicables y en las mejores prácticas nacionales e internacionales del sector.

b) Las guías o códigos de buenas prácticas, así como los estándares y normas técnicas establecidos por los organismos de estandarización y las reglamentaciones técnicas que representen las mejores prácticas en la materia, que las personas beneficiarias deban aplicar para el desarrollo de los sistemas y para su implantación.

Referencias

Aguilar, I., y cols. (2024). *Guía básica de la IA*. Smart Digital.

Álvarez García, V. (2024). La tipología de documentos normativos que regulan especificaciones técnicas. *Revista General de Derecho Administrativo*, *64*, 1–24.

Barrio Andrés, M. (Ed.). (2024a). *Comentarios al reglamento europeo de inteligencia artificial*. La Ley. ((Dir.))

Barrio Andrés, M. (Ed.). (2024b). *El reglamento europeo de inteligencia artificial*. Tirant lo Blanch. ((Dir.))

Berning Prieto, A. D. (2022). Implicaciones de la inteligencia artificial y los algoritmos en el sector público y sus particularidades en la administración tributaria. En B. D. Olivares Olivares (Ed.), *La inteligencia artificial en la relación entre los obligados y la administración tributaria: retos ante la gestión tecnológica* (pp. 23–45). La Ley.

Carlón Ruiz, M. (2024). *Las administraciones públicas ante la inteligencia artificial*. Tirant lo Blanch.

Carrillo Donaire, J. A. (2000). *El derecho de la seguridad y la calidad industrial*. Marcial Pons.

Casas Baamonde, M. E. (Ed.). (2024). *Derecho y tecnologías*. Fundación Ramón Areces. ((Dir.))

Cerrillo i Martínez, A., Di Lascio, F., Martín Delgado, I., y Velasco Rico, C. I. (Eds.). (2024). *Inteligencia artificial y administraciones públicas: una triple visión en clave comparada*. Iustel. ((Dirs.))

Comisión Europea. (2025a). *Guidelines on prohibited ai practices c(2025) 884 final.* ((2025d))

Comisión Europea. (2025b). *Guidelines on the definition of an ai system c(2025) 924 final.* ((2025e))

Comisión Europea. (2025c). *Model contractual clauses for the public procurement of high-risk ai ('mcc-ai-high-risk').* https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses. ((2025b))

Comisión Europea. (2025d). *Model contractual clauses for the public procurement of non-high-risk ai ('mcc-ai-high-light').* https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses. ((2025c))

Comisión Europea. (2025e). *Oficina europea de ia.* https://digital-strategy.ec.europa.eu/es/policies/ai-office. ((2025a))

Cotino Hueso, L., y Simón Castellano, P. (Eds.). (2024). *Tratado sobre el reglamento de inteligencia artificial de la unión europea*. Aranzadi-La Ley. ((Dirs.))

Criado, J. I., y Guevara-Gómez, A. (2024). *Hacia un uso responsable de los algoritmos: métodos y herramientas para su auditoría y evaluación*. Digital Future Society.

Domínguez Álvarez, J. L., y Terrón Santos, D. (Eds.). (2023). *Desafíos éticos, tecnológicos y jurídicos del avance digital*. Iustel. ((Dirs.))

Europea, C. (2024). *Adopt ai. final study report.* https://ec.europa.eu/newsroom/dae/redirection/document/108555.

Europea, J. R. C. C. (2022). *Ai watch. road to the adoption of artificial intelligence by the public sector.*

G7-UNESCO-OECD. (2024). *G7 toolkit for artificial intelligence in the public sector.* https://www.oecd.org/en/publications/g7-toolkit-for-artificial-intelligence-in-the-public-sector_421c1244-en.html.

Gamero Casado, E. (Ed.). (2023). *Inteligencia artificial y sector público: Retos, límites y medios*. Tirant lo Blanch. Descargado de https://rio.upo.es/entities/publication/06dc1a44-5034-4b58-b38b-3385656c0790 ((Dir.))

Gamero Casado, E., y Fernández Ramos, S. (2024). *Manual básico de derecho administrativo*. Tecnos.

García Mexía, P. (Ed.). (2024). Reglamento europeo de ia. *Revista Privacidad y Derecho Digital*, *34*. ((Dir.))

Gobierno de España. Ministerio para la Transformación Digital y la Función Pública. (s.f.). *Algoritmos verdes.* https://algoritmosverdes.gob.es/es.

Gobierno de Singapur. (2024). *Public sector ai playbook.* https://ibl.ai/blog/singapore-public-sector-ai-playbook/.

Government of Canada. (2024). *Algorithmic impact assessment tool.* https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

Huervo Lora, A. (Ed.). (2025). *The eu regulation on artificial intelligence: a commentary*. Wolters Kluwer-CEDAM.

Institute, E. L. (2022). *Eli model rules on impact assessment of algorithmic decision-making systems used by public administration.* https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on__Impact_Assessment_of_Algorithmic_Decision-Making_Systems_Used_by_Public_Administration.pdf.

Laux, J., Wachter, S., y Mittelstadt, B. (2024). Three pathways for standardisation and ethical disclosure by

default under the european union artificial intelligence act. *Computer & Law Security Review*, *53*, 1–13. doi: 10.1016/j.clsr.2024.105957

Mantelero, A. (2022). *Beyond data. human rights, ethical and social impact assessment in artificial intelligence.* Asser Press–Springer.

Mantelero, A. (2024). The fundamental rights impact assessment (fria) in the ai act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, *54*.

Menéndez Sebastián, E. M. (2023). *From bureaucracy to artificial intelligence. the tension between effectiveness and guarantees.* Wolters Kluwer-CEDAM.

Miranzo Díaz, J. (2023). *Inteligencia artificial y derecho administrativo.* Instituto Clavero Arévalo-Tecnos.

Mökander, J. (2023). Auditing of ai: Legal, ethical and technical approaches. *Digital Society*, *2*(49), 1–32. doi: 10.1007/s44206-023-00074-y

Mota Sánchez, E. M., y Herrera Expósito, E. (2024). Auditoría algorítmica en la inteligencia artificial en el sector público. *Proyecciones. Revista Digital del Instituto de Investigaciones y Estudios Contables*, *17*, 1–8. doi: 10.24215/26185474e025

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., y Floridi, L. (2024). Generative ai in eu law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, 1–16. doi: 10.1016/j.clsr.2024.106066

of Europe, C. (2024). *Committee on artificial intelligence (cai): Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (huderia methodology).* https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f.

Ortega Giménez, A. (Ed.). (2024). *Implantación práctica de sistemas de inteligencia artificial en el sector público y derecho internacional privado.* Aranzadi La Ley. ((Dir.))

Peralta Gutiérrez, A., y Pedrosa del Pino, J. (Eds.). (2024). *Inteligencia artificial y justicia.* Consejo General del Poder Judicial. ((Dirs.))

Ponce Solé, J. (2024). *El reglamento de inteligencia artificial de la unión europea de 2024, el derecho a una buena administración digital y su control judicial en españa.* Marcial Pons.

Sanz Larruga, F. J. (2024). Inteligencia artificial y sostenibilidad ambiental en la unión europea: algunos apuntes provisionales. En P. Valcárcel Fernández y F. L. Hernández González (Eds.), *El derecho administrativo en la era de la inteligencia artificial. actas del xviii congreso de la asociación española de profesores de derecho administrativo.* INAP.

Strubell, E., Ganesh, A., y McCallum, A. (2019). *Energy and policy considerations for deep learning in nlp.* https://arxiv.org/abs/1906.02243.

Supervisor, E. D. P. (2024). *Generative ai and the eudpr.* https://edps.europa.eu.

Tahirí Moreno, J. A. (2024a). Artículo 40: Normas armonizadas y documentos de normalización. En M. Barrio Andrés (Ed.), *Comentarios al reglamento de inteligencia artificial.* La Ley. ((2024b))

Tahirí Moreno, J. A. (2024b). Una panorámica de los sistemas de inteligencia artificial desde la perspectiva del derecho administrativo. *Revista Aragonesa de Administración Pública*, *61*, 137–168. ((2024a))

Valcárcel Fernández, P., y Hernández González, F. L. (Eds.). (2024). *El derecho administrativo en la era de la inteligencia artificial. actas del xviii congreso de la asociación española de profesores y profesoras de derecho administrativo.* INAP.

Velasco Rico, C. I. (2024). Marco regulatorio de los sistemas algorítmicos y de inteligencia artificial: el papel de la administración. En P. Valcárcel Fernández y F. L. Hernández González (Eds.), *El derecho administrativo en la era de la inteligencia artificial. actas del xviii congreso de la asociación española de profesores de derecho administrativo.* INAP.

Wierzbowski, M., y cols. (2022). *Model rules on impact assessment of algorithmic decision-making system used by public administration.* https://www.europeanlawinstitute.eu/projects-publications/publications/eli-model-rules-on-impact-assessment-of-algorithmic-decision-making-systems-usey-by-public-adminstration/.