PRIVACIDAD Y GOBERNANZA DE DATOS EN IA URBANA

Josuan Eguiluz Castañeira
Asesor jurídico, Adevinta

Carlos Fernández Hernández
Miembro del consejo asesor, Global LegalTech

1. Introducción

Desde que en 2018 la Unión Europea (UE) comenzó el diseño de su marco normativo sobre la inteligencia artificial (IA), puso especial énfasis en que esta tecnología debe ser «fiable» *(trustworthy)*. Se considera una IA fiable aquella que respeta el marco normativo aplicable y que es ética y robusta, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA, incluso si las intenciones son buenas, pueden provocar daños accidentales (Grupo de expertos de alto nivel sobre inteligencia artificial, 2019).

En consecuencia, el enfoque europeo en esta materia, incentiva el desarrollo y la adopción de una IA ética y fiable en toda la economía de la UE, a partir del principio de que dicha tecnología debe estar al servicio de las personas y ser una fuerza positiva para la sociedad (Libro Blanco sobre la inteligencia artificial, 2020, § 6).

Dado que la disponibilidad de datos es fundamental para entrenar a los sistemas algorítmicos, y que muchos de esos datos son de carácter personal, un componente de la IA ética es que debe incluir mecanismos de gestión de la privacidad y de los datos (Comisión Europea, Revisión de 2021 del plan coordinado sobre la IA). Esta exigencia ha sido plenamente acogida por el Reglamento europeo en materia de inteligencia artificial (RIA) (junio de 2024), que fija como uno de sus objetivos promover la adopción de una IA centrada en el ser humano y fiable (art. 1), respetando, a la vez, el marco normativo vigente en materia de protección de datos, constituido –principal pero no exclusivamente–, por el Reglamento general de protección de datos de 2016 (RGPD).

Como han señalado algunos autores (Almonacid Lamelas, 2024), el RIA representa un desafío no menor para los gobiernos locales, en tanto que deberán adaptar sus procesos, políticas y estrategias para cumplir con las nuevas exigencias. Sin embargo, también supone una oportunidad para mejorar su funcionamiento, así como la calidad y confiabilidad de los servicios basados en IA ofrecidos a los ciudadanos (*ibid*.). Esto explica la proliferación de sistemas de «inteligencia artificial urbana» (*urban AI),* un concepto que hace referencia a «la recopilación, interpretación y análisis de datos urbanos con el fin de apoyar la toma de decisiones relacionadas con las políticas, así como el desarrollo de soluciones que se utilizan, o podrían utilizarse, en un contexto urbano» (Galcerán-Vercher, 2023).

Con todo, el tratamiento de datos personales en el ámbito público-urbanístico puede plantear problemas específicos, desde la legitimidad de dicho tratamiento para una finalidad para la que originalmente no fue consentida, hasta la necesidad de realizar evaluaciones de impacto en los derechos fundamentales de las personas. Estos, inequívocamente, deberán ser tenidos en cuenta por los organismos públicos.

Los sistemas de IA deben garantizar la protección de los datos a lo largo de todo el ciclo de vida de dichos sistemas. Esto incluye la información inicialmente facilitada por el usuario, así como la que se genera sobre él en el contexto de su interacción con el sistema.

A la luz del nuevo marco legislativo, el objeto de este artículo es (i) presentar el marco jurídico y ético que regula el tratamiento de datos personales en el ámbito urbanístico por medio de sistemas de IA, en especial a nivel europeo (RIA); (ii) identificar los principales mecanismos para implementar el principio de privacidad, y (iii) analizar los desafíos que plantea este tipo de tratamiento de datos y ofrecer un conjunto de recomendaciones y buenas prácticas para minimizarlos o eliminarlos.

2. IA ética y privacidad

Una IA fiable debe ser ética, y para serlo debe, entre otros requisitos, respetar la privacidad de las personas. El RIA establece como objetivo específico «promover la adopción de una IA centrada en el ser humano y fiable». Con este fin, las normas comunes que establece para los sistemas de IA de alto riesgo deben ser coherentes con la Carta de los Derechos Fundamentales de la Unión Europea (2000), y tener en cuenta tanto la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2022), como las Directrices éticas para una IA fiable del Grupo independiente de expertos de alto nivel sobre inteligencia artificial (2019). Según estas directrices, en un contexto de rápido cambio tecnológico,

«La fiabilidad es un requisito previo para que las personas y sociedades desarrollen, desplieguen y utilicen sistemas de IA. Si estos sistemas –y las personas que se encuentran detrás de ellos– no demuestran ser merecedores de confianza, pueden producirse consecuencias no deseadas que obstaculicen su adopción, impidiendo el logro de los enormes beneficios económicos y sociales que pueden acarrear los sistemas de IA.» (Introducción, punto 13)

La fiabilidad de la IA se apoya en tres componentes, que deben satisfacerse a lo largo de todo el ciclo de vida del sistema de IA:

1. Debe ser lícita, de modo que se garantice el respeto de todas las leyes y normativa aplicables;
2. Ha de ser ética, es decir, debe asegurar el cumplimiento de los principios y valores éticos, y, finalmente,
3. Debe ser robusta, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA, incluso si las intenciones son buenas, pueden provocar daños accidentales.

Por tanto, se debe establecer la ética como pilar fundamental para garantizar y expandir una IA fiable. Esto implica que es preciso garantizar que se cumplan unas normas éticas básicas, así como las medidas que establece el RIA para la protección de los derechos fundamentales.

En este sentido, la protección de datos es un derecho fundamental que se ve especialmente afectado por los sistemas de IA, y que guarda una estrecha relación con el principio de prevención del daño. Dicho principio de prevención comienza por una adecuada gestión de esos datos, que abarque la calidad y la integridad de aquellos que sean utilizados, su pertinencia en contraste con el ámbito en el que se desplegarán los sistemas de IA, sus protocolos de acceso y la capacidad para procesar datos sin vulnerar la privacidad.

[El] RIA recoge el principio general de que el mismo respeta en su integridad el marco regulador de la Unión en materia de protección de datos establecido por el RGPD.

Entre esas medidas se incluye el hecho de que los sistemas de IA dispongan de un mecanismo de gestión de la privacidad y de los datos que incluya tanto el respeto de la privacidad, como la calidad y la integridad de dichos datos y el acceso a estos.

Además, los sistemas de IA deben garantizar la protección de los datos a lo largo de todo el ciclo de vida de dichos sistemas. Esto incluye la información inicialmente facilitada por el usuario, así como la que se genera sobre él en el contexto de su interacción con el sistema (por ejemplo, los productos que genere el sistema de IA para determinados usuarios o la respuesta de estos a ciertas recomendaciones). Los registros digitales del comportamiento humano pueden posibilitar que los sistemas de IA no solo infieran las preferencias de las personas, sino también su orientación sexual, edad, género u opiniones políticas y religiosas. Para permitir que los individuos confíen en el proceso de recopilación de datos, es preciso garantizar que la información recabada sobre ellos no se utilizará para discriminarlos de forma injusta o ilegal.

Del cumplimiento de estos requisitos tienen que encargarse los operadores, en particular, los desarrolladores de los sistemas de IA y los responsables del despliegue (que deben asegurarse de que los sistemas que utilizan y los productos y servicios que ofrecen cumplen los requisitos establecidos). Por otro lado, las personas que se vean afectadas por el funcionamiento de un sistema de IA tendrán derecho a estar informadas de dicha afectación y, en su caso, a presentar una reclamación por infracción del RIA (arts. 85 y 86).

2.1. La privacidad en el Reglamento europeo de IA

El art. 2.7 del RIA recoge el principio general de que el mismo respeta en su integridad el marco regulador de la Unión en materia de protección de datos establecido por el RGPD.

En primer lugar, las normas armonizadas que se establecen en el RIA deben aplicarse en todos los sectores y deben entenderse sin perjuicio del derecho vigente de la Unión. Es importante destacar, pues, que el RIA no pretende afectar a la aplicación del derecho de la Unión que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de supervisión independientes que vigilan el cumplimiento de dichos instrumentos. Del mismo modo, tampoco afecta a las obligaciones previas de los proveedores y los encargados del despliegue de sistemas de IA en su papel de responsables del tratamiento de datos personales. En particular, el RIA no debe afectar a las prácticas actualmente prohibidas por el derecho de la Unión, incluidos los derechos en materia de protección de datos.

Para las ciudades, garantizar que sus sistemas de IA cumplen con regulaciones como el RGPD o el RIA a lo largo de todo el ciclo de vida de la IA, resulta fundamental para salvaguardar los derechos de los ciudadanos y mantener la confianza pública.

En paralelo, el hecho de que un sistema de IA sea clasificado como de alto riesgo no debe interpretarse como indicador de que su uso sea lícito con arreglo a otros actos del derecho de la Unión o del derecho nacional, por ejemplo, en materia de protección de los datos personales. Todo uso de ese tipo de sistemas de IA debe seguir realizándose exclusivamente en consonancia con los requisitos oportunos derivados de la Carta, del derecho derivado de la Unión y del derecho nacional.

Además, el RIA no constituye un fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de dichos datos, salvo que se disponga específicamente otra cosa. Por ello, los interesados siguen disfrutando, tras la entrada en vigor del RIA, de todos los derechos y las garantías que les confiere el derecho de la Unión, incluidos los relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles. Las normas armonizadas que establece el RIA, pues, deben permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el derecho de la Unión en materia de protección de datos personales y otros derechos fundamentales.

Finalmente, a fin de facilitar el cumplimiento del derecho de la Unión en materia de protección de datos, en determinadas condiciones, el RIA proporciona la base jurídica para que, en un espacio controlado de pruebas, los proveedores (también los potenciales) utilicen datos personales recabados para otros fines para desarrollar determinados sistemas de IA en favor del interés público.

3. Mecanismos políticos para implementar el principio de privacidad en el ámbito urbanístico

La protección de la privacidad y los datos en la implementación de IA urbana requiere la adopción de mecanismos políticos específicos. Estos mecanismos permiten a las ciudades cumplir con las normativas vigentes y asegurar que la IA se despliegue de manera ética y responsable, respetando los derechos de los ciudadanos. A continuación, se identifican y explican los principales mecanismos políticos para implementar este principio ético.

a) Garantizar la conformidad legal

El cumplimiento de la regulación es un requisito ético esencial en la protección de la privacidad y los datos en la implementación de sistemas de IA en entornos urbanos por parte de las autoridades públicas. Para las ciudades, garantizar que sus sistemas de IA cumplen con regulaciones como el RGPD o el RIA a lo largo de todo el ciclo de vida de la IA, resulta fundamental para salvaguardar los derechos de los ciudadanos y mantener la confianza pública. Esto incluye la adhesión a requerimientos clave como la calidad e integridad de los datos utilizados, su pertinencia en contraste con el ámbito en el que se desplegarán los sistemas de IA, sus protocolos de acceso y la capacidad para procesar datos sin vulnerar la privacidad (Grupo de expertos de alto nivel sobre IA, 2018).

Precisamente, estos requerimientos se materializan en obligaciones concretas en el propio RIA, específicamente diseñadas para casos de alto riesgo, tales como los sistemas de IA de identificación biométrica remota –p. ej., el programa ABIS (Pascual, 2024)– o aquellos utilizados para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública –p. ej., el caso Syri (Digital Future Society, 2022)–.

b) Sistemas de gestión de riesgo y gobernanza de datos

El RIA incluye obligaciones específicas (arts. 9 y 10) estrechamente vinculadas al principio de privacidad y protección de datos. Por un lado, el artículo 9 se centra en la creación de un sistema de gestión de riesgos que sea capaz de identificar, documentar y mitigar aquellos que vayan asociados al uso de IA en las ciudades. Estos sistemas de gestión de riesgos deberán establecer procesos iterativos continuos, planificados y ejecutados a lo largo de todo el ciclo de vida de las tecnologías de IA, que, por supuesto, requerirán revisiones y actualizaciones sistemáticas periódicas. De hecho, no se trata solo de evaluar los posibles riesgos antes de la introducción en el mercado o puesta en servicio de estos sistemas de IA, sino también de establecer y/o supervisar el funcionamiento de un sistema de vigilancia poscomercialización para gestionar riesgos emergentes –arts. 17.1 h), 26.5 y 72 RIA–.

Por otro lado, la gobernanza de datos regulada en el artículo 10 exige que los conjuntos de datos de entrenamiento, validación y prueba utilizados en sistemas de IA de alto riesgo se sometan a prácticas de gobernanza y gestión de datos adecuadas para su finalidad prevista. Las prácticas a implementar por las ciudades para asegurar una gobernanza de datos efectiva y legal se centrarán en cuestiones como los procesos de recogida y origen de los datos, la finalidad del tratamiento, la evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios, el examen de posibles sesgos que puedan afectar a la salud, la seguridad o los derechos fundamentales de las personas, etc.

c) Evaluaciones de impacto

El artículo 35 del RGPD impone a los responsables del tratamiento (p. ej., ayuntamientos) la obligación de realizar una evaluación de impacto relativa a la protección de datos (EIPD). Esta evaluación se realizará cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto o fines (en particular si utiliza nuevas tecnologías), entrañe un alto riesgo para los derechos y las libertades de las personas físicas (AEPD, 2018; Grupo de Trabajo del art. 29, 2017; Friedewald *et al.*, 2022). Este enfoque preventivo es vital en los entornos urbanos para anticipar posibles vulnerabilidades en la protección de datos y tomar las medidas necesarias para corregirlas a tiempo.

Asimismo, para los sistemas de IA de alto riesgo, el artículo 27 RIA introduce la obligación de realizar una evaluación de impacto relativa a los derechos fundamentales (en sus siglas en inglés, FRAI) (Gobierno de Holanda, 2022; Instituto Danés de Derechos Humanos, 2020), que complemente la EIPD. Esta evaluación tiene como objetivo determinar los riesgos específicos para los derechos de las personas que probablemente se vean afectadas y definir las medidas que deben adoptarse en caso de que se materialicen dichos riesgos (Cdo. 96 RIA). Cabe destacar que las evaluaciones de impacto (Manzoni, M. *et al*., 2022) deben centrarse no solo en el retorno de la inversión, sino también en la sostenibilidad y el impacto ético de la tecnología, abordando aspectos financieros, humanos y medioambientales (OECD, 2024).

d) Realización de auditorías

Sentado lo anterior, será necesario poder demostrar ante las autoridades, las partes interesadas y los ciudadanos que se cumple con la legislación y todos sus requisitos de implementación específicos. En este sentido, se realizarán auditorías internas y externas, y se obtendrán certificaciones que verifiquen que los sistemas operan dentro de los marcos legales establecidos. Para ello, las ciudades europeas, por ejemplo, deberán realizar evaluaciones de conformidad (art. 43 RIA) con el fin de garantizar y demostrar que han cumplido con los requisitos asociados a sistemas de alto riesgo, alineándose con las normas armonizadas publicadas en el *Diario Oficial de la Unión Europea* (art. 41 RIA). También deberán seguir las especificaciones comunes establecidas por la Comisión Europea, asegurando así una implementación estandarizada y segura de los sistemas de IA (p. ej., certificaciones ISO).

Las auditorías de IA se consideran un mecanismo de gobernanza fundamental para asegurar que la implementación y operación de los sistemas de IA cumplen con las normativas legales y los estándares éticos y técnicos establecidos (Fernández, C. y Eguíluz, J. A., 2024). Con carácter general, estas auditorías deberán ser realizadas por entidades independientes y competentes. El proceso de auditoría incluye metodologías que incorporan evaluaciones de impacto ético (UNESCO, 2024; CEN-CENELEC, 2017), asegurando que los sistemas de IA se comportan de manera responsable y que sus efectos en la sociedad y los individuos son debidamente monitoreados y mitigados. No obstante, es recomendable plantear las auditorías de IA desde un punto de vista multidisciplinar –legal, técnico y ético– (Mökander, J., 2023). En esta dirección, surgen propuestas como la de «algo-scores» para clasificar y evaluar de manera accesible el nivel de conformidad de los sistemas algorítmicos en materias como el cumplimiento ético, la gobernanza de la IA, la equidad del modelo y su vigilancia posterior, siguiendo un enfoque similar al de las etiquetas de eficiencia energética (Galdon Clavell, 2024).

e) Repositorios de algoritmos y registros de sistemas de IA

En último lugar, conviene recordar la importancia de los repositorios de algoritmos públicos y los registros de sistemas de IA (art. 49 RIA), que promueven la transparencia en la toma de decisiones automatizadas en el sector público y desempeñan un papel crucial en la protección de la privacidad y los datos personales. Al hacer accesibles los detalles sobre cómo se diseñan, implementan y operan estos sistemas, los repositorios y registros permiten a los ciudadanos y a las organizaciones entender cómo y con qué finalidades se utilizan sus datos personales en estos procesos. Dichos repositorios incluyen también información sobre las fuentes de datos utilizadas y los mecanismos de supervisión, lo cual es esencial para evaluar el impacto de los sistemas en la privacidad de los individuos y garantizar que las medidas de protección de datos sean efectivas (Gutiérrez & Muñoz-Cadena, 2024).

4. Desafíos y recomendaciones

La gestión inadecuada de los datos es una de las principales limitaciones para la implementación de IA en el sector público. Igualmente, lo es también la falta de acceso a volúmenes suficientes de datos de alta calidad. Este problema se ve exacerbado por el intercambio insatisfactorio de datos entre organizaciones debido a la falta de estándares unificados y una gobernanza de datos subdesarrollada. Además, la desconfianza en los sistemas de IA agrava estos desafíos. Las leyes dispersas y la falta de conocimiento sobre los impactos de la IA también generan barreras significativas (Manzoni *et al*., 2023). Asimismo, el aumento de ciberataques ha llevado a que la Directiva NIS 2 (2022) refuerce la seguridad y la responsabilidad legal para los administradores. En 2023, la administración pública fue uno de los sectores más afectados, con el 19% de los incidentes reportados, destacando entre ellos el crecimiento de ataques como el *ransomware* y DDoS (ENISA, 2023).

Es esencial promover mecanismos de innovación, como los sandboxes regulatorios, que permiten a las ciudades experimentar con IA en un entorno controlado mientras se garantiza el cumplimiento regulatorio.

El complejo panorama regulatorio también representa un desafío significativo. La interacción entre las normativas urbanísticas a nivel europeo, nacional y local crea un entramado de reglas que complica la implementación efectiva de IA en las ciudades. La legislación urbanística y las regulaciones específicas de cada municipio deberán alinearse con normativas europeas como el Reglamento sobre la Europa Interoperable (Interoperable Europe Act) (2022), que busca mejorar la interoperabilidad de los servicios públicos digitales (Tangi *et al*., 2023).

Otra limitación importante es la falta de experiencia y conocimiento técnico dentro de las administraciones locales, lo que dificulta la correcta implementación de la IA. La escasez de profesionales en esta materia a nivel global, junto con la creciente competencia por el talento, representan una barrera significativa para las ciudades que intentan desarrollar y desplegar estos sistemas de manera efectiva (OECD, 2024).

Por otra parte, la recolección masiva de datos personales, necesaria para entrenar estos sistemas, puede infringir el derecho de los ciudadanos a controlar sus datos, ya que estos pueden ser sensibles o ser gestionados de manera inapropiada. Mientras que las aplicaciones de IA, como las utilizadas en el control policial, pueden intensificar la vigilancia masiva y comprometer aún más la privacidad de los individuos (Véliz, 2020; Agarwal, 2018; Dwivedi *et al*., 2019).

Para superar estas barreras, es esencial promover mecanismos de innovación, como los *sandboxes* regulatorios (Madiega, 2022), que permiten a las ciudades experimentar con IA en un entorno controlado mientras se garantiza el cumplimiento regulatorio (Tangi *et al*., 2023). Asimismo, la coordinación entre las autoridades nacionales (en el caso español, la

Agencia Española de Supervisión de la Inteligencia Artificial - AESIA) y europeas (Oficina Europea de IA) es crucial para garantizar que los sistemas de IA cumplan con las normativas vigentes y se implementen de manera segura y responsable.

La interoperabilidad y la colaboración son igualmente claves. Iniciativas como el sistema SALER - Sistema de Alertas Rápidas, utilizado en la Comunidad Valenciana para prevenir la corrupción en la administración, demuestran cómo la IA puede utilizarse de manera efectiva para mejorar los procesos de gobernanza (Digital Future Society, 2023). Igualmente, resulta esencial que la financiación pública esté condicionada a la disponibilidad de ciertos resultados por parte de las distintas administraciones (p. ej., generar conjuntos de datos públicos) (Comisión Europea, 2022). En este sentido, la Comisión Europea ha publicado, mediante el Reglamento de ejecución (UE) núm. 2023/138, una lista de conjuntos de datos específicos de alto valor que deberán estar disponibles para su reutilización gratuita, destacando el potencial de los datos públicos en beneficio de la sociedad, el medio ambiente y la economía (Comisión Europea, 2022). Además, el acceso a datos multilingües para entrenar modelos locales de IA que reflejen las características específicas de cada región (OECD, 2024) y la recopilación de casos de uso de IA en el sector público a nivel europeo (Comisión Europea, 2021) mejorarán la efectividad y equidad de los sistemas de IA, a la vez que proporcionarán una valiosa fuente de información sobre cómo se están implementando estas tecnologías en diversos contextos.

5. Conclusiones

El marco general de protección de datos en la UE está ya asentado en unos principios conocidos y sólidamente interpretados por los organismos administrativos y jurisdiccionales de la Unión. Sin embargo, la IA plantea unos problemas específicos, de naturaleza tecnológica y jurídica, que se encuentran en un momento incipiente de conocimiento y tratamiento.

Por ello, serán necesarios todavía numerosos estudios, experiencias y precisiones para dotarles de un marco jurídico que garantice la proclamada finalidad de que la IA debe estar centrada en el ser humano, ser una herramienta para las personas y tener por objetivo último aumentar su bienestar.

La implementación de mecanismos políticos específicos es esencial para garantizar que las ciudades utilicen sistemas de IA de manera ética y respetuosa con los derechos de la ciudadanía. El cumplimiento de regulaciones como el RGPD y el RIA resulta indispensable para salvaguardar la privacidad y los datos personales en entornos urbanos. Del mismo modo, es fundamental que las ciudades establezcan sistemas de gestión de riesgos que aborden de manera iterativa las contingencias asociadas a todo el ciclo de vida de la IA, incluyendo revisiones periódicas y auditorías externas que aseguren el cumplimiento normativo.

Por otra parte, la gobernanza de datos debe estar en el centro de las estrategias urbanas de IA. Las ciudades deben implementar prácticas de gobernanza y gestión de datos sólidas, centradas en la calidad, la pertinencia y la protección de los conjuntos de datos utilizados en los sistemas de IA. Esto incluye la realización de evaluaciones de impacto tanto para la protección de datos personales como para los derechos fundamentales, asegurando que las tecnologías implementadas no vulneren la privacidad ni la seguridad de la ciudadanía.

En definitiva, lograr una IA centrada en el ser humano exigirá un esfuerzo conjunto entre los responsables de desarrollar políticas públicas, las instituciones académicas y los sectores privados, que deben colaborar para asegurar que los sistemas de IA que sean implementados por las ciudades se alineen con los valores y principios éticos fundamentales.

Como se ha señalado, el futuro de las ciudades inteligentes se caracterizará por la síntesis de múltiples tecnologías orientadas a satisfacer el intrincado mosaico de necesidades humanas. Esta convergencia requerirá de una precisa optimización de las tecnologías aplicadas que asegure que la digitalización de los espacios urbanos se alinee con prácticas sostenibles y equitativas, así como de la atención a las dimensiones éticas que estas innovaciones conllevan. Por ello, es imperativo que la integración de la IA en el corazón de las ciudades inteligentes se rija por principios que defiendan la privacidad, la seguridad y la inclusión. En este sentido, y como apuntan Zhenjun *et al*. (2023): «Garantizar que los beneficios del desarrollo de las ciudades inteligentes se compartan equitativamente será esencial para evitar fracturas sociales y fomentar un entorno en el que la tecnología sirva de puente hacia una vida urbana más ilustrada y armoniosa».

Referencias bibliográficas

Agencia Española de Protección de Datos (AEPD). «Gestión del riesgo y evaluación de impacto en tratamientos de datos personales». Madrid, 2018 [Fecha de consulta: 02.09.2024]

Agencia Española de Protección de Datos. «Guía sobre Protección de Datos y Administración Local». Actualizada en 2023 [Fecha de consulta: 02.09.2024]

AI Ethics Impact Group. «From Principles to Practice: An interdisciplinary framework to operationalise AI ethics». 1 de abril de 2020 [Fecha de consulta: 02.09.2024]

Alan Turing Institute. «Urban analytics» [Fecha de consulta: 02.09.2024]

Alan Turing Institute. «Why the public sector needs to know about AI ethics (and how we're helping)». 2 de noviembre de 2023 [Fecha de consulta: 02.09.2024]

Almonacid Lamelas, V. «Reglamento (europeo) de Inteligencia Artificial: impactos y obligaciones que genera en los Ayuntamientos». El Consultor de los Ayuntamientos, LA LEY, 15 de julio de 2024 [Fecha de consulta: 02.09.2024]

Burbano, L. (1). «Privacy protection in smart cities: How are they taking care of citizens' most precious information?» *Tomorrow.city*, 23 de enero de 2024 [Fecha de consulta: 02.09.2024]

Burbano, L. (2). «AI urbanism: risks and benefits of a seemingly unstoppable movement». *Tomorrow.city*, 22 de febrero de 2024 [Fecha de consulta: 02.09.2024]

Canda, J. «AI in Urban Planning and Smart City Development». *Medium*, 7 de abril de 2024 [Fecha de consulta: 02.09.2024]

CEN-CENELEC. «Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework». CWA 17145-2, junio 2017 [Fecha de consulta: 02.09.2024]

Centro Latinoamericano de Administración para el Desarrollo (CLAD). «Carta Iberoamericana de Inteligencia Artificial en la Administración Pública». 20 de noviembre de 2023 [Fecha de consulta: 02.09.2024]

Comisión Europea (1). «Selected AI cases in the public sector (JRC129301)». Joint Research Centre (JRC), 2021 [Fecha de consulta: 02.09.2024]

Comisión Europea (2). «Revisión de 2021 del plan coordinado sobre la inteligencia artificial», Anexos de la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial, COM(2021) 205 final, 2021 [Fecha de consulta: 02.09.2024]

Comisión Europea (3). «Opportunities and challenges of artificial intelligence technologies for the cultural and creative sectors». Oficina de Publicaciones de la UE, Luxemburgo, 2022 [Fecha de consulta: 02.09.2024]

Comisión Europea (4). «Second Report on the application of the General Data Protection Regulation», COM(2024) 357 final, Bruselas, 25 de julio de 2024 [Fecha de consulta: 02.09.2024]

Digital Future Society (1). «Algorithmic discrimination in Spain: limits and potential of the legal framework», agosto de 2022 [Fecha de consulta: 02.09.2024]

Digital Future Society (2). «El acceso digital en las ciudades, entendido como algo más que un derecho fundamental», junio de 2023 [Fecha de consulta: 02.09.2024]

Digital Future Society (3). «El uso de algoritmos en el sector público en España: cuatro estudios de caso sobre ADMS», febrero de 2023 [Fecha de consulta: 02.09.2024]

European Data Protection Board (EDPB). «Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework», 16 de julio de 2024 [Fecha de consulta: 02.09.2024]

European Union Agency for Cybersecurity (ENISA). «Threat Landscape 2023», octubre de 2023 [Fecha de consulta: 02.09.2024]

Fernández, C. y Eguiluz, J. A. «Diez puntos críticos del Reglamento europeo de Inteligencia Artificial». *Diario LA LEY*, núm. 85, Sección Ciberderecho, 28 de junio de 2024 [Fecha de consulta: 02.09.2024].

Friedewald, M. *et al.* «Data Protection Impact Assessments in Practice: Experiences from Case Studies». *Computer Security, ESORICS 2021 International Workshops*, febrero de 2022, p. 424-443 [Fecha de consulta: 02.09.2024]

Galceran-Vercher, M. «Trustworthy Cities: Ethical Urban Artificial Intelligence». The GovLab, Course «AI Ethics, Global perspectives», diciembre de 2023 [Fecha de consulta: 02.09.2024]

Galceran-Vercher, M., y Vidal, A. «Mapeo de la inteligencia artificial urbana: primer informe del Atlas de la Inteligencia Artificial Urbana del GOUAI». Global Observatory of Urban AI (GOUAI), 2024 [Fecha de consulta: 02.09.2024]

Galdon, G. «AI Auditing. Proposal for Algo-scores». EDPB, 27 de junio de 2024 [Fecha de consulta: 02.09.2024]

Ghisleni, C. «Artificial Intelligence and Urban Planning: Technology as a Tool for City Design». *ArchDaily*, 8 de febrero de 2024 [Último acceso: 02.09.2024]

Gobierno de Holanda. «Impact Assessment Fundamental Rights and Algorithms», 31 de marzo de 2022 [Fecha de consulta: 02.09.2024].

Grupo de expertos de alto nivel sobre inteligencia artificial. «Directrices éticas para una IA fiable», abril de 2019 [Fecha de consulta: 02.09.2024]

Grupo de Trabajo del Art. 29. «Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679», Bruselas, 2017 [Fecha de consulta: 02.09.2024]

Gutiérrez, J. D. y Muñoz-Cadena, S. «Algorithmic transparency in the public sector: A state-of-the-art report of algorithmic transparency instruments». *Global Partnership on Artificial Intelligence*, mayo de 2024 [Fecha de consulta: 02.09.2024]

Hadec, J., Di Leo, M. y Kotsev, A. «AI generated synthetic data in policy applications». *Science for Policy Brief*, European Commission, Joint Research Center, 2024 [Fecha de consulta: 02.09.2024]

Imdat As, P.; Basu, P. y Talwar, P. *Artificial Intelligence in Urban Planning and Design. Technologies, Implementation, and Impacts*. Amsterdam: Elsevier, 2022.

Instituto Danés de Derechos Humanos. «Guidance on Human Rights Impact Assessment of Digital Activities». Copenhague, 2020 [Fecha de consulta: 02.09.2024]

Madiega, T. y Van De Pol, A. L. «Artificial intelligence act and regulatory sandboxes». European Parliamentary Research Service (EPRS), PE 733.544, junio de 2022 [Fecha de consulta: 02.09.2024]

Manzoni, M. *et al.* AI Watch. *Road to the adoption of Artificial Intelligence by the public sector*. Oficina de Publicaciones de la UE. Luxemburgo, 2022. JRC129100 [Fecha de consulta: 02.09.2024]

Mökander, J. «Auditing of AI: Legal, Ethical and Technical Approaches». *Digital Society*, vol. 2, artículo núm. 49, 2023 [Fecha de consulta: 02.09.2024]

Organización de Naciones Unidas (ONU). «Recommendation on the Ethics of Artificial Intelligence», 23 de noviembre de 2021 [Fecha de consulta: 02.09.2024]

Organización para la Cooperación y el Desarrollo Económico (OCDE) (1). «Advancing Accountability in AI: governing and managing risks throughout the lifecycle for trustworthy AI», *OECD Artificial Intelligence Papers,* núm. 349, 23 de febrero de 2023 [Fecha de consulta: 02.09.2024]

Organización para la Cooperación y el Desarrollo Económico (OCDE) (2). «Governing with artificial intelligence: Are governments ready?», *OECD Digital Economy Papers*, núm. 20, junio de 2024 [Fecha de consulta: 02.09.2024]

Pascual, M. G. «La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial». *El País*, 28 de mayo de 2024 [Fecha de consulta: 02.09.2024]

Pellegrin, J., Colnot, L. y Delponte, L. «Artificial Intelligence and Urban Development». Research for REGI Committee, European Parliament, Policy Department for Structural and Cohesion Policies, Bruselas, 2021 [Fecha de consulta: 02.09.2024]

Tangi, L. *et al.* «Artificial Intelligence for Interoperability in the European Public Sector: an exploratory study», Oficina de Publicaciones de la UE, Luxemburgo, 2023 [Fecha de consulta: 02.09.2024]

Tangi, L. *et al.* «AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector», Oficina de Publicaciones de la UE, Luxemburgo, 2022 [Fecha de consulta: 02.09.2024]

Timan, T., Van Veenstra, A. F. y Bodea, G. «Artificial Intelligence and public services». Policy Department for Economic, Scientific and Quality of Life Policies, PE 662.936, julio de 2021 [Fecha de consulta: 02.09.2024]

Véliz, C. *Privacidad es poder: Datos, vigilancia y libertad en la era digital*. Madrid: Debate, 2021.

Verhulst, S. G. «Are we entering a Data Winter? On the urgent need to preserve data access for the public interest». Frontiers Policy Labs, 2024 [Fecha de consulta: 02.09.2024]

Yan, Z. *et al.* «Intelligent urbanism with artificial intelligence in shaping tomorrow's smart cities: current developments, trends, and future directions». *Journal of Cloud Computing*, 18 de diciembre de 2023 [Fecha de consulta: 02.09.2024]