CAPÍTULO 3

Fundamentos de los principios éticos para la digitalización y el uso de la inteligencia artificial en los Gobiernos locales

Dolors Canals Ametller
Profesora titular de Derecho Administrativo.
Universitat de Girona

Agustí Cerrillo i Martínez
Catedrático de Derecho Administrativo.
Universitat Oberta de Catalunya

1. La transformación digital de los Gobiernos locales

En la sociedad contemporánea, las Administraciones públicas ejercen potestades y competencias y prestan servicios en entornos virtuales a través del uso y la aplicación de innovaciones tecnológicas digitales de nueva generación como la computación en la nube, los datos masivos y la inteligencia artificial (IA)*. Así, las instancias administrativas se presentan ante

* Abreviaturas utilizadas: IA: inteligencia artificial; IoT: Internet de las Cosas, por sus siglas en inglés.

la ciudadanía como plataformas digitales de tramitación y de provisión de servicios públicos. Para ello es indispensable la creación de un nuevo modelo de Administración pública, la denominada "Administración digital", es decir, una Administración que utilice la tecnología de manera intensiva e innovadora para recopilar y analizar de manera colaborativa los datos que genera con el fin prestar servicios digitales inclusivos, eficientes, resilientes, sostenibles y centrados en las personas.

Como es bien conocido, la digitalización de los servicios públicos y de la actuación administrativa supone una actividad y prestación en línea y a distancia en oposición a las tradicionales por medios presenciales, materiales y humanos. Además, también implica la automatización de la toma de decisiones o de la prestación de determinados servicios. De este modo, la Administración digital es mucho más que la Administración electrónica; las tecnologías de la información y la comunicación son utilizadas por las Administraciones con el objetivo tanto de mejorar la eficiencia interna como de facilitar sus relaciones con otras entidades públicas y con la ciudadanía (Cerrillo i Martínez, 2022).

La Administración digital se basa en el análisis de datos —la llamada "Administración de Datos" en palabras de Martínez Gutiérrez (2023)— y en el uso de las tecnologías disruptivas, gracias al cual se avanza en la automatización de la Administración pública, con lo que, más allá de ser un instrumento para mejorar y fortalecer la relación entre las instancias administrativas y la ciudadanía, también permite aportar valor a la sociedad (Cerrillo i Martínez, 2020a). Ello abre nuevas oportunidades para los Gobiernos locales; por ejemplo, ofreciendo servicios más personalizados y proactivos (Velasco Rico, 2020), o de manera predictiva (Rivero Ortega, 2023) o prospectiva (Sánchez Sánchez, 2022).

La digitalización de las Administraciones públicas en el sentido señalado pivota sobre tres elementos: la interconectividad gracias a las redes y los sistemas de información y comunicación que la permiten; la interoperabilidad indispensable para la efectividad de interconectividad administrativa y ciudadana (Expósito Gázquez, 2022), y, finalmente, la seguridad digital, ciberseguridad o seguridad del entorno cibernético (Canals Ametller, 2023). A un mismo tiempo, la actuación administrativa, incluso la de contenido jurídico, y la gestión de los servicios se encuentran cada vez más subordinadas al uso de tecnologías disruptivas como la IA y el internet de las cosas (IoT), y su interconexión a través de redes de telecomunicaciones de quinta generación (5G) (Cerrillo y Moro, 2021). Este marco exige altas medidas de seguridad en todos los sistemas interconectados e interoperativos para proteger

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

los datos de la ciudadanía, la accesibilidad al servicio público y la propia infraestructura administrativa operativa.

En el ámbito local, la digitalización y la automatización, en los términos indicados, engarzan con el concepto de "ciudades inteligentes" (Cerrillo i Martínez, 2020b) o el de "ciudades cognitivas" (Cotino Hueso, 2022), y, más recientemente, con lo que se ha denominado "urbes virtuales o redes digitales de Administraciones locales" (Canals Ametller, 2023). Porque las infraestructuras tecnológicas y los recursos digitales permiten también la interconexión de distintas entidades locales a través de redes, actuando a modo de "urbes virtuales o redes de ciudades digitales", constituidas por redes colaborativas de gestión pública de servicios de titularidad de distintos Gobiernos locales en un plano horizontal, o incluso vertical, desde diferentes partes de la geografía nacional. Tales redes se gestan y confluyen para la prestación digital de servicios municipales, como una incipiente modalidad del fenómeno de economía colaborativa aplicada a la gestión local a partir de la interconexión e interoperabilidad de sus sistemas y sus datos, un modelo de gestión administrativa inteligente y compartida (Canals Ametller, 2022a).

De manera resumida, la ciudad inteligente se caracteriza por el uso intensivo e innovador de la tecnología, la recopilación y el análisis de manera colaborativa de los datos, los servicios inclusivos, eficientes, resilientes y sostenibles, y la centralidad de las personas en el diseño de la ciudad inteligente y en la prestación de los servicios digitales (Cerrillo i Martínez, 2020b). La arquitectura tecnológica municipal se articula en redes de conectividad —con acceso de banda ancha, y, cada vez más, con banda 5G—, en las que se combinan e interconectan distintos sensores, servicios, aplicaciones, plataformas digitales y centros de almacenamiento de datos con los dispositivos inteligentes móviles de las personas o que están situados en el territorio. A través de estos dispositivos, el sector público municipal y los proveedores de servicios públicos recolectan, intercambian y reutilizan datos e información para la prestación y gestión digitalizada de aquellos, desde protocolos o esquemas de interoperabilidad. El uso masivo de los datos permite conocer los intereses y necesidades de la ciudadanía y con ello mejorar los servicios públicos y, en general, de los entornos urbanos (Valero Torrijos, 2015). De este modo, la ciudad inteligente se identifica con aquella que presta, total o parcialmente, algunos o todos sus servicios administrativos y servicios públicos (transportes, suministros de luz, agua y gas, gestión de residuos o ayudas sociales) (Mellado Ruiz, 2023). En última instancia, los servicios centrados en las personas permiten garantizar sus derechos y una mayor personalización y proactividad (Cerrillo i Martínez, 2022).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

2. Los riesgos que genera la transformación digital de los Gobiernos locales

El sociólogo alemán Ulrich Beck señaló en el año 1986 las coordenadas de la sociedad occidental ante las transformaciones iniciadas en aquellos años por la globalización y la revolución tecnológica, acuñando la conocida expresión *sociedad del riesgo* (Beck, 1998). En la actualidad, la expresión podría adjetivarse como *sociedad del riesgo digital* por las crecientes amenazas que emergen del entorno digital o ciberespacio, un lugar propenso a la conflictividad y la inseguridad cuya gestión es un reto difícil para el Estado y también para los Gobiernos locales (Canals Ametller, 2021); una inseguridad que, por otra parte, va en aumento con la automatización de la actividad administrativa a través del uso y la aplicación de tecnologías de IA.

Los riesgos que genera la digitalización acechan a cualquiera y en cualquier esfera de relación social, económica y/o jurídica, con independencia del lugar en el que nos encontremos en la realidad física. Basta con estar conectado a la red a través de cualquier aparato, sistema o servicio tecnológico para adentrarnos en un entorno inseguro. En consecuencia, garantizar esta nueva seguridad es una responsabilidad pública, del personal al servicio de las Administraciones públicas, y también privada, de los operadores económicos y las empresas, y asimismo individual para evitar daños propios y a terceros.

En este contexto, la transformación digital de las entidades locales no está exenta de riesgos. La mayoría derivan del uso intensivo e innovador de la tecnología. Otros pueden traer causa de la ausencia de una regulación adecuada, pudiéndose generar inseguridad jurídica o una vulneración de los derechos de la ciudadanía o de los principios de funcionamiento de las Administraciones públicas. Asimismo, algunos riesgos pueden estar originados por una falta de liderazgo o de capacidades en los Gobiernos locales.

A continuación, se hace una breve referencia a todos ellos.

2.1. Los riesgos relacionados con el uso de la tecnología

El uso intensivo de la tecnología genera distintos riesgos relacionados con el acceso a la misma. Al respecto, debe tenerse en cuenta la *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* del

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

Parlamento Europeo, el Consejo y la Comisión, de 15 de diciembre de 2022, que reconoce que toda persona ha de "tener acceso en línea a los servicios públicos esenciales de la Unión Europea", y añade: "No debe pedirse a nadie que facilite datos con más frecuencia de la necesaria al acceder a los servicios públicos digitales y utilizarlos"(apartado 7).

También puede generar riesgos vinculados a la accesibilidad a los contenidos o a los servicios digitales por parte de cualquier persona independientemente de sus circunstancias personales, en particular personas con discapacidad o personas mayores.

Junto a estos riesgos, la incorporación de la inteligencia artificial en las Administraciones públicas puede entrañar nuevos riesgos entre los que destacan, en particular, los relacionados con los errores de los algoritmos; los sesgos y las discriminaciones; la opacidad de los algoritmos y la falta de explicabilidad de las decisiones adoptadas automáticamente; o, también, los relacionados con la ausencia de supervisión humana de los procesos de automatización.

2.2. Los riesgos relacionados con la seguridad

Cada vez con mayor frecuencia se identifican riesgos relacionados con la seguridad de las redes, de las transacciones electrónicas o de los sistemas de información que se pueden materializar en el acceso ilícito a dichos sistemas de información, por accidentes de seguridad o por errores en la conservación de la información.

En la medida en que la transformación digital de las Administraciones públicas, en todos sus niveles, está edificando una extensa estructura en redes de interconexión e interoperabilidad, un fallo de seguridad de una red puede impactar de inmediato en otra, encadenándose y expandiéndose los eventuales daños.

La gestión de los riesgos y amenazas provenientes del mundo digital exige políticas y acciones tendentes a su minimización o mitigación. Debe ser así también en el ámbito de los Gobiernos locales, grandes, pequeños o medianos, de manera aislada o asistidos por entidades supramunicipales o, incluso, a través de novedosas fórmulas de agrupación (Canals Ametller, 2022b).

En esta dirección, la mencionada *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* del Parlamento Euro-

peo, el Consejo y la Comisión de 2022 expresa lo siguiente: "Toda persona debería tener acceso a tecnologías, productos y servicios digitales diseñados para estar protegidos, ser seguros y proteger la privacidad, lo que se traduce en altos niveles de confidencialidad, integridad, disponibilidad y autenticidad de la información tratada". También el *Programa Estratégico de la Década Digital para 2030* aprobado por la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, concreta una serie de objetivos generales para su consecución en esta década, para lo cual la Comisión y los Estados miembros deberán tener en cuenta los principios y derechos digitales establecidos en dicha declaración europea. Entre estos objetivos destaca, a los efectos de la seguridad digital, el de "mejorar la resiliencia frente a los ataques informáticos y contribuir a la sensibilización sobre los riesgos y al aumento del conocimiento sobre los procesos de ciberseguridad, e incrementar los esfuerzos de las organizaciones públicas y privadas para alcanzar, como mínimo, niveles básicos de ciberseguridad" (art. 3, letra k.).

La seguridad digital está estrechamente unida a los recursos de IA y la seguridad misma que ofrecen estos específicos productos industriales. Los recursos y sistemas de IA son susceptibles de sufrir ataques procedentes del entorno digital en el que actúan y que conforman —manipulando los datos algorítmicos o provocando decisiones no deseadas, por ejemplo—, por lo que se exige un desarrollo de la IA que sea seguro y confiable. Como producto industrial tecnológico, la IA genera riesgos de seguridad jurídica por los eventuales sesgos en los datos con que se nutren los algoritmos, susceptibles de generar discriminación (Soriano Arnanz, 2021), y por la opacidad del funcionamiento interno de los sistemas automatizados. Por ello, el afianzamiento de la confianza de las Administraciones públicas y de los usuarios privados en la IA y su aplicación requiere de instrumentos preventivos que protejan los derechos fundamentales (Presno Linera, 2023) y garanticen la ciberseguridad, como un marco legal armonizado en la Unión Europea que incluya los valores comunes y los principios jurídicos básicos del desarrollo y la utilización de este producto industrial avanzado —a modo del Reglamento General de Protección de Datos en lo que se refiere a los límites de la actuación administrativa automatizada según se desprende del art. 22—, la normalización técnica, la evaluación de la conformidad *ex ante* (datos, diseño y proceso) y su correspondiente certificación (Álvarez y Tahirí, 2023; Canals Ametller, 2023), además de un régimen claro de responsabilidad civil por daños, de manera particular para las aplicaciones de IA consideradas de *alto riesgo*, y, finalmente, la transparencia enfocada a la inteligencia artificial como garantía jurídica (Valero Torrijos, 2019).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

2.3. Los riesgos derivados de la brecha digital

La digitalización de los Gobiernos locales puede ampliar la brecha digital tanto entre personas como entre instituciones.

Desde la perspectiva de las personas, la transformación digital puede llevar a la exclusión de determinadas personas y colectivos del uso de los medios electrónicos en sus relaciones con la Administración pública, por su imposibilidad o dificultad de utilizar los medios electrónicos por motivos económicos, tecnológicos, educacionales o, incluso, de género.

Desde la perspectiva institucional, la brecha digital también puede surgir en aquellas entidades locales que no cuenten con determinadas características o que no dispongan de determinados recursos necesarios para abordar con plenas garantías su transformación digital.

2.4. Los riesgos de dependencia tecnológica

La digitalización implica la dependencia de las entidades administrativas y sus procesos de decisión y prestación de servicios del uso de redes y sistemas de información y comunicación en entornos virtuales. La dependencia de las tecnologías digitales es clave porque sobrevuela la transición de los Gobiernos locales hacia una plena digitalización y automatización de sus responsabilidades de cualquier tipo, políticas, jurídicas, de prestación de servicios, formales e informales. No obstante, también puede condicionar la consecución de las finalidades públicas, en la medida en que aquello que no se pueda digitalizar no se podrá hacer.

Asimismo, la transformación digital puede generar en los Gobiernos locales dependencia de sus proveedores de tecnología, en concreto cuando no dispongan de las competencias técnicas o de los recursos tecnológicos necesarios para abordar el proceso de digitalización y automatización.

2.5. Riesgos derivados de la regulación de la Administración digital

Con frecuencia las normas relativas a la Administración digital no regulan de manera suficientemente adecuada, detallada o actualizada el uso de los medios electrónicos o las garantías que se deben tomar cuando estos medios se utilizan en las relaciones entre las Administraciones públicas y la

ciudadanía. Esta situación puede generar inseguridad jurídica, así como una vulneración de los derechos de las personas.

Ante la digitalización existe un deber público de mitigar los riesgos digitales, las vulnerabilidades de ciberseguridad y privacidad que puedan poner en riesgo la protección de datos, en particular de los datos personales y otros datos sensibles, así como la veracidad de la información digital o generada por recursos automatizados o inteligentes.

Las limitaciones jurídicas son, en este caso, razón de peso para que el establecimiento de principios éticos y reglas de conducta del personal al servicio de las instancias administrativas sea el complemento indispensable de las reglas y los principios jurídicos, para atajar los riesgos que emergen de las tecnologías de nueva generación y su aplicación en la esfera pública.

2.6. Riesgos derivados de la falta de confianza de la ciudadanía

Una de las dimensiones fundamentales del proceso de digitalización es que la ciudadanía debe situarse en el centro del diseño y la prestación de servicios digitales, los cuales deberían ser de alta calidad.

La normalización del uso de los medios electrónicos por los Gobiernos locales y su transformación digital (en procedimientos, funciones y servicios) puede generar una falta de confianza en la ciudadanía preocupada principalmente por la protección de sus datos personales.

Esta falta de confianza también puede surgir por la mayor distancia con la que se prestan los servicios públicos o la menor proximidad al personal al servicio de las Administraciones públicas, lo que puede traducirse en una deshumanización de las relaciones con la ciudadanía o una menor empatía (Nogueira López, 2023). Esa desconfianza puede obstaculizar la efectividad de la Administración digital.

2.7. Riesgos derivados de la ausencia de capacitación digital

La consabida falta de capacidades tecnológicas de algunos segmentos sociales y, también, del personal al servicio de las entidades locales, especialmente de las pequeñas y medianas, puede sin duda generar riesgos. La transición hacia la digitalización administrativa exige una formación específica que ha de ser adaptada de manera constante al avance de las tecnologías emergentes y disruptivas, así como la formación en materia de protección

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

de datos personales como información digital sensible que manejan todas las entidades locales. No son pocas las dificultades estructurales para las organizaciones públicas que conlleva la adaptación a la digitalización y sus riesgos adyacentes. A este respecto la *Agenda España Digital 2025* señala que es "imprescindible el desarrollo de las capacidades de ciberseguridad de ciudadanía, empresas y Administraciones públicas, así como la generación de confianza a través de la cultura de la ciberseguridad que llegue a todas las capas de la sociedad".

Por ello, el deber de mitigación de los riesgos debería generar mayor confianza en la Administración digital mediante el desarrollo de capacidades suficientes para las personas al servicio de los Gobiernos locales y asimismo entre la ciudadanía.

3. Los principios éticos para la digitalización y el uso de la inteligencia artificial en los Gobiernos locales

Como se ha indicado con anterioridad, la transición hacia una plena transformación digital de los Gobiernos locales no está exenta de riesgos. Muchos de ellos pueden surgir por el propio uso de la tecnología. Otros por las limitaciones derivadas de la normativa vigente o por las carencias de la organización local. Asimismo, algunos riesgos surgen también del comportamiento de las personas electas, del personal directivo o del personal al servicio de las corporaciones locales dentro de entornos virtuales, en el diseño y la implementación de la Administración digital o en el uso y la aplicación de los sistemas de inteligencia artificial en los procesos de toma de decisiones administrativas.

Para dar respuesta a los riesgos derivados del comportamiento de las personas que participan en la transformación digital de los Gobiernos locales o en el diseño y la prestación de los servicios digitales, es imprescindible impulsar una cultura de la gestión pública de los riesgos de la digitalización. Esta cultura implica tomar conciencia de las contingencias a las que estamos expuestos a medida que avanza el proceso de transformación digital de todas las Administraciones, incluidos los Gobiernos locales. Esa concienciación debería conllevar una disminución de los riesgos digitales e incrementar la confianza de la ciudadanía y de las empresas, principalmente de las pequeñas y medianas, en la transición digital, y con ello en la Administración digitalizada.

En el marco de esta nueva cultura, es necesario fortalecer el compromiso ético de las personas electas, del personal directivo y del personal al servicio de las entidades locales. En esta dirección, los principios éticos que

contiene el Código Integral son también una garantía ante los riesgos de la digitalización en el ámbito local.

En todos los casos (riesgos tecnológicos, riesgos jurídicos o riesgos organizativos), el compromiso y la conducta de los cargos y del personal al servicio de los Gobiernos locales pueden ser fundamentales. En efecto, con independencia de que se adopten medidas tecnológicas, se aprueben normas o se impulsen estrategias para liderar la transformación digital, o se forme al personal al servicio de las Administraciones públicas para garantizar su capacitación digital, es necesario que todas las personas que participan en el proceso de transformación digital desarrollen su actividad de acuerdo con determinados principios que inspiren su actividad y orienten su conducta.

En el Código Integral, los distintos principios éticos se han articulado alrededor de cuatro dimensiones de la digitalización.

En primer lugar, la digitalización democrática. Los principios que se recogen en esta dimensión persiguen garantizar que el proceso de digitalización sea el resultado de un proceso democrático liderado por el pleno de cada corporación, y que cuente con la participación ciudadana de acuerdo con los principios de gobierno abierto.

En segundo lugar, la digitalización fiable. Los principios que se recogen en esta dimensión tienen por finalidad asegurar que la digitalización se realice de manera que se garantice el buen funcionamiento de los Gobiernos locales y se eviten errores, sesgos o incumplimientos de los principios de protección de datos personales.

En tercer lugar, la digitalización inclusiva. Los principios que se recogen en esta dimensión persiguen garantizar la equidad en la transformación digital de los Gobiernos locales y evitar cualquier tipo de vulnerabilidad digital de las personas.

Por último, en cuarto lugar, la digitalización colaborativa. Los principios que se recogen en esta dimensión buscan garantizar que la colaboración que con frecuencia se da entre las Administraciones públicas y las empresas y los centros de investigación sea íntegra, y se desarrolle bajo el impulso de cada Gobierno local.

4. Bibliografía

Álvarez García, V. y Tahirí Moreno, J. (2023). La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque. *Revista General de Derecho Administrativo*, 63.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3

Beck, U. (1998). *La sociedad del riesgo*. Barcelona: Paidós Ibérica.

Canals Ametller, D. (dir.). (2021). *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales*. Madrid: El Consultor de Los Ayuntamientos-Wolters Kluwer.

— (2022a). La seguridad digital en pequeñas y medianas entidades locales: hacia una gestión municipal colaborativa. En J. Fondevila Antolín (dir.). *La transformación digital en las medianas y pequeñas entidades locales. Retos en clave de eficiencia y sostenibilidad*. Madrid: Wolters Kluwer-El Consultor de los Ayuntamientos.

— (2022b). El fenómeno colaborativo en la gestión pública local: hacia una gestión local colaborativa. En E. Carbonell Porras (dir.). *Gobiernos locales y economía colaborativa*. Madrid: Iustel.

— (2023). Regulación y gestión de la seguridad híbrida en la prestación digital de servicios públicos y esenciales. En D. Canals, M. Fuertes, A. G. Orofino y J. Valero (2023). *La digitalización en los servicios públicos: Garantías de acceso, gestión de datos, automatización de decisiones y seguridad*. Madrid-Barcelona: Marcial Pons.

Cerrillo i Martínez, A. (2020a). Automatización e inteligencia artificial. En I. Martín Delgado (dir.). *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación tecnológica*. Madrid: Iustel.

— (2020b). La ciudad inteligente al servicio de las personas. *Revista Práctica Urbanística*, 164.

— (2022). La personalización de servicios digitales. En A. Cerrillo i Martínez (dir.). *La Administración Digital*. Madrid: Dykinson.

Cerrillo i Martínez, A. y Moro Cordero, M.ª A. (2021). La innovación local y las tecnologías disruptivas. La gobernanza inteligente de las ciudades. En A. Cerrillo i Martínez (coord.). *La transformación digital de la Administración local*. Madrid: Fundación Democracia y Gobierno Local.

Cotino Hueso, L. (2022). Ciberseguridad, privacidad y gobernanza para la explotación de datos por la ciudad inteligente. En L. Cotino Hueso y A. Todolí Signes (coords.). *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente* (pp. 81-124). Valencia: Tirant lo Blanch.

Expósito Gázquez, A. (2022). El principio de interoperabilidad como base para las actuaciones y los servicios administrativos personalizados, proactivos y automatizados. *Revista Vasca de Administración Pública*, 122, 45-78.

Martínez Gutiérrez, R. (2023). Reforma para una Administración de datos. *Revista catalana de dret públic*, 67, 67-81.

Mellado Ruiz, L. (2023). Retos regulatorios del derecho local ante la realidad de las *smart cities*. En M. Mora Ruiz (dir.). *De las Smart Cities a las Ciu-*

dades integradoras. Propuestas socio-jurídicas para una administración local del s. XXI (pp. 23-51). Madrid: Dykinson.

Nogueira López, A. (2023). Una Administración para el 99 %. Reforma administrativa para la igualdad real. *Revista catalana de dret públic*, 67, 18-35.

Presno Linera, M. Á. (2023). *Derechos fundamentales e inteligencia artificial*. Madrid: Marcial Pons.

Rivero Ortega, R. (2023). Algoritmos, inteligencia artificial y policía predictiva del estado vigilante. *Revista General de Derecho Administrativo*, 62.

Sánchez Sánchez, Z. (2022). *Regulación con prospectiva de futuro y de consenso: gobernanza anticipatoria y prospectiva administrativa*. Cizur Menor: Aranzadi.

Soriano Arnanz, A. (2021). Decisiones automatizadas y discriminación: aproximación y propuestas generales. *Revista General de Derecho Administrativo*, 56.

Valero Torrijos, J. (2015). Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de los datos de carácter personal. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 1025-1047.

— (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista catalana de dret públic*, 58, 82-96.

Velasco Rico, C. I. (2020). Personalización, proactividad e inteligencia artificial. ¿Un nuevo paradigma para la prestación electrónica de servicios públicos? *Revista de Internet, Derecho y Política*, 30.

Otras fuentes consultadas

Comisión Europea. (2020). *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza* [COM(2020) 65 final].

Diputación Foral de Gipuzkoa. (2023). *Código ético para la utilización de los datos y la inteligencia artificial*.

Gobierno de España. (2021). *Carta de Derechos Digitales*.

Grupo de expertos de alto nivel sobre inteligencia artificial. (2019). *Directrices éticas para una IA fiable*.

Jobin, A., Ienca, M. y Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1 (9), 389-399.

UNESCO. (2021). *Recommandation sur l'éthique de l'intelligence artificielle* (23 de noviembre de 2021).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 43
ISBN: 978-84-125912-9-3