



PRIVACIDAD Y DERECHOS FUNDAMENTALES EN LA SMART CITY La utilización de la Inteligencia Artificial en los sistemas de videovigilancia

FRANCISCO J. ARANDA SERNA (FJARANDA@UCAM.EDU)¹,

¹ Universidad Católica San Antonio de Murcia, España

PALABRAS CLAVE

Smart City
Inteligencia Artificial
Videovigilancia
Privacidad
Derechos fundamentales
Seguridad ciudadana
Protección de datos

RESUMEN

Este artículo analiza las implicaciones sociales, éticas y jurídicas del uso de la Inteligencia Artificial en los sistemas de videovigilancia dentro del contexto de las ciudades inteligentes. Se plantean varios conceptos esenciales, desde la Smart City, hasta la transformación de la seguridad ciudadana por medio de la videovigilancia «inteligente». Se abordan las aplicaciones actuales tales el análisis predictivo del delito o el reconocimiento facial y los riesgos asociados que esto puede provocar, como son la falta de privacidad y transparencia. Mediante el estudio de algunos modelos internacionales de Smart City, se pondrá en evidencia la necesidad de un marco normativo que garantice la protección de los derechos fundamentales y la promoción de un modelo de Smart City que equilibre el desarrollo tecnológico con principios legales y democráticos.

Recibido: 01 / 02 / 2026

Aceptado: 03 / 05 / 2026

1. Introducción

Las tecnologías de la información y la comunicación (TICS) permiten nuevas formas de interacción que, en el ámbito urbano, generan dinámicas positivas y de retroalimentación para el patrimonio cultural, los ciudadanos y la Administración pública. En este marco surge el concepto de «Smart City», un término que implica una transformación social que se manifiesta en diversos contextos, desde una mayor conciencia y cuidado del patrimonio, a una mayor participación ciudadana y la utilización de nuevas aplicaciones de Inteligencia Artificial (IA) integradas en la propia ciudad.

La hiperconectividad sin precedentes, especialmente incisiva tras la COVID-19, se manifiesta con el uso de dispositivos fijos y móviles que amplían las capacidades comunicativas de los ciudadanos. También los fenómenos de las redes sociales, el *cloud computing* y el *big data* han configurado una sociedad interconectada, cambiando las formas de comunicación, consumo, trabajo, ocio y gestión del tiempo (Fuentes i Gasó, 2021).

Como novedad, la utilización de la IA puede suponer una oportunidad para la transformación de la ciudad, haciéndola más eficiente y accesible. Sin embargo, también preocupa en todas sus posibles aplicaciones la posible pérdida del factor «humano» y especialmente las complejidades éticas y legales que puede acarrear (Galarza Quinto et al., 2024).

En este contexto, las administraciones públicas, están incorporando progresivamente todas estas novedades tecnológicas, con el fin de articular un sistema de ciudad verdaderamente inteligente, que no se conciba únicamente como receptor pasivo de servicios, sino que también actúe como un actor activo y corresponsable de la ciudad (Cotino Hueso, 2018).

Dentro de las posibilidades que tienen estas aplicaciones, el Internet de las Cosas constituye una herramienta fundamental para la recolección masiva de datos urbanos. Semáforos, señales de tráfico, edificios, señales luminosas o aparcamientos, son algunos ejemplos de cómo las administraciones públicas pueden obtener información en tiempo real sobre algunas variables como es el movimiento de los ciudadanos, la intensidad de la luz, entre otros.

La utilización de IA va a permitir a los sistemas informáticos analizar e interpretar los datos obtenidos, aprender de ellos y adaptarse a las nuevas situaciones que puedan surgir. La aplicación más destacada es la de los algoritmos predictivos, los cuales son capaces de anticipar situaciones y facilitar la toma de decisiones en base a los datos obtenidos. Estos algoritmos permiten a la IA evolucionar con procesos de aprendizaje automático, mejorando de forma progresiva la capacidad de ir resolviendo problemas cada vez más complejos (Aguado i Cudolá, 2022).

La incorporación de estas nuevas tecnologías en IA presenta, no obstante, algunos riesgos para los ciudadanos y en lo que respecta al Derecho, varios desafíos por abordar. El empleo de estas tecnologías puede vulnerar algunos de los derechos fundamentales más sensibles, como son la intimidad o la privacidad. Especialmente en el caso de que la videovigilancia incorpore sistemas que están automatizados, va a ser necesario una regulación de un marco jurídico nuevo y una supervisión, siempre humana, que garantice la protección de estos derechos.

2. Metodología y objetivos

El presente artículo tiene como objetivo analizar las implicaciones sociales y jurídicas de la implementación de la IA en las actuaciones de las administraciones públicas, particularmente en el contexto de las ciudades inteligentes (Smart Cities). El análisis se va a centrar en cómo estas tecnologías afectan a los sistemas de videovigilancia y, en consecuencia, inciden en la protección de la privacidad y los derechos fundamentales de los ciudadanos.

Para ello, se va a abordar el concepto de Smart City, identificando los elementos que la caracterizan como una ciudad «inteligente». También se van a presentar las principales características que posee la IA y se pondrá en contexto el uso de la videovigilancia mediante una revisión de su evolución como herramienta tecnológica.

Más concretamente se examinará el marco jurídico que regula el uso de las tecnologías de videovigilancia, prestando especial atención a las nuevas posibilidades que introduce la IA, tales

como son el reconocimiento facial, la detección de movimiento, la identificación de comportamientos y las decisiones automatizadas.

Se incluirá también la revisión de modelos internacionales de Smart Cities en los que estos nuevos sistemas de videovigilancia ya han sido implementados, con el objetivo de evaluar su grado de compatibilidad con los principios democráticos, la transparencia de las administraciones públicas y el principio de proporcionalidad.

A través del análisis documental y una revisión de las publicaciones científicas más relevantes en el ámbito de la Smart City, la videovigilancia y la IA, se pretende poner de relieve los dilemas éticos y las dificultades jurídicas que plantea su regulación. Además, también se pondrá de manifiesto las oportunidades que plantea la aplicación de la IA en la Smart City.

Esta tecnología es una herramienta que, al mismo tiempo supone un gran potencial para transformar la sociedad y también supone un desafío complejo para la protección de los derechos fundamentales. En el contexto específico de la videovigilancia «inteligente», es esencial comprender los antecedentes técnicos, jurídicos y sociales que configuran su desarrollo, así como el marco normativo en el que se va a insertar.

Como último fin, esta aproximación crítica pretende fijar un contexto para el estudio normativo y promover también una utilización ética, transparente y responsable de estas nuevas tecnologías, que en todo caso debe respetar los derechos de privacidad de los ciudadanos y los principios democráticos en el espacio público de la ciudad.

3. La ciudad ante los desafíos jurídicos y tecnológicos

Si bien el concepto de Smart City ya no es del todo novedoso, este continúa siendo objeto de debate y de análisis, lo cierto es que tampoco hay un consenso consolidado acerca de su definición. Esta es una concepción que se aborda desde diferentes disciplinas: arquitectura, ingeniería, las ciencias políticas y empresariales, y también el Derecho.

Si se identifican los denominadores comunes se verá que el más repetido es el concepto que aborda la utilización de las «TICS» con el propósito de mejorar la calidad de vida de la población y establecer un desarrollo sostenible. Si bien, es necesario aclarar que la presencia del elemento tecnológico no es definitorio por sí mismo para la Smart City.

La implementación de estas tecnologías posee un impacto relevante en los derechos fundamentales, destacando entre ellos la privacidad y la protección de datos personales. Como ya se ha mencionado en la introducción, aún no se ha desarrollado un marco normativo que regule estos conflictos de manera integral dentro de la Smart City (Aguado i Cudolà et al., 2018).

La Smart City representa una oportunidad estratégica tanto en el ámbito político como en el empresarial, sin embargo, dichas expectativas pueden ser excesivas y comparables a otros fenómenos que con el tiempo pierden vigor. En cualquier caso, resulta incuestionable que el despliegue de tecnologías de videovigilancia redefine la seguridad en la ciudad, y abre nuevas posibilidades para la protección, promoción y análisis del patrimonio cultural, por ejemplo, a través de una monitorización más precisa de los espacios públicos (Fuentes i Gasó, 2021).

El estudio de la Smart City requiere entender como la incorporación de la IA redefine las relaciones de la ciudadanía con el espacio público. En el contexto que se va a estudiar, el de la videovigilancia, habrá que tener en cuenta como esta herramienta surge, no solo para garantizar la seguridad, sino también como un mecanismo que recopila masivamente los datos de los ciudadanos. Esta interconexión entre Smart City, IA y videovigilancia va a plantear una serie de desafíos éticos y jurídicos, en los cuáles al final deberá concurrir un equilibrio entre derechos e innovación tecnológica

3.1. ¿Qué es una «Smart City»?

La ciudad como entidad política siempre ha desempeñado un papel crucial a lo largo de la historia, distantes y paradigmáticos quedan los ejemplos de la polis griega y la urbe romana. Pero por

supuesto, la visión de la ciudad «moderna» comenzó con la aparición del Estado moderno y también contemporáneo.

Sin embargo, ha sido la evolución tecnológica la que ha sido determinante para la concepción de «Smart City», en este contexto la ciudad ha vuelto a recuperar protagonismo como un espacio estratégico para la toma de decisiones públicas y que están orientadas a proveer servicios esenciales a los ciudadanos (Aguado i Cudolá, 2022).

Este proceso se ha articulado en torno a dos fenómenos clave: el primero, la creciente concentración de población a escala mundial en las áreas urbanas, la cual es actualmente y de forma aproximada la mitad de la población mundial y según las proyecciones aumentará en el futuro. Y segundo, el desarrollo de las nuevas Tecnologías de la Información y la Comunicación (TICS) que han supuesto un marco de transformación digital en la Smart City, entendiendo por tal la aplicación de las TICS al entorno urbano (Font i Llove, 2021).

Según la Unión Europea, para que una ciudad sea considerada «inteligente» debe configurarse como un ecosistema en el cual la tecnología se pone al servicio del ciudadano, este además es un agente activo y esencial en la interacción con los actores políticos, sociales y económicos (Velasco Rico, 2019).

Se recogen varios conceptos que analizaremos a continuación (Villarejo Galende, 2015):

- *Smart Economy*. Referido a la incorporación de tecnologías que fomenten la creación de nuevos productos y modelos de negocio, el comercio electrónico y vías orientadas al emprendimiento, la empleabilidad y la conectividad internacional.
- *Smart People*. Implica una sociedad más inclusiva que promueva la creatividad y la innovación, especialmente en el ámbito educativo, la formación continua y el desarrollo de competencias digitales, fortaleciendo el capital humano.
- *Smart Mobility*. Engloba sistemas de transporte que prioricen soluciones sostenibles, seguras y eficientes, los más avanzados monitoreando en tiempo real. Se permite así optimizar los desplazamientos, reducir costes y minimizar las emisiones contaminantes.
- *Smart Environment*. Comprende la implementación de redes energéticas basadas en fuentes renovables, y sistemas de medición, control y vigilancia ambiental. También la gestión eficiente de los residuos y la reutilización de los recursos.
- *Smart Governance*. Consiste en la inclusión de procesos participativos de toma de decisiones que involucren tanto a actores públicos como privados y civiles, en diferentes niveles. De este modo se promueve que la ciudadanía lidere los procesos participativos, sustentado por las infraestructuras digitales y las plataformas creadas por la Administración pública.
- *Smart Living*. Se refiere a estilos de vida saludables y seguros, y también promover el bienestar de los ciudadanos sin menoscabo a su interacción con las nuevas tecnologías.

El modelo de Smart City exige una redefinición profunda de las formas de habitar, administrar, negociar, consumir y disfrutar el espacio público urbano, no es tan solo una mera implementación de sensores, redes de comunicación y análisis de datos. En consecuencia, el concepto tiende hacia una formulación expansiva, que abarca dimensiones transversales y que requiere, de manera ineludible, la participación de la ciudadanía y la cooperación entre los sectores público y privado (Ricoy Casas, 2017)¹.

Así, la Smart City representa un nuevo paradigma en la gestión del espacio público y en la prestación de servicios, alineado con los principios de participación abierta. Este enfoque promueve una gobernanza colaborativa, centrada en el ciudadano, sustentada en la transparencia, la rendición de cuentas y el aprovechamiento estratégico de las TICS (Carmona Garias, 2020).

¹ Desde que se constituyó la Red Española de Ciudades Inteligentes, España ocupa como país un puesto de liderazgo, destacando las ciudades de Madrid, Barcelona, Málaga o Valladolid (Telefónica, 2023).

A este concepto hay que añadirle una dimensión social fundamental, vinculada al concepto de Smart «Human» City, que enfatice la inclusión de la diversidad. Algunos autores señalan que esta noción surge de la necesidad de diseñar estrategias inclusivas que aseguren la integración de todas las personas en el entorno de la ciudad, evitando así desigualdades. La «Smart Human City» se configura como una evolución más humanizada del modelo de Smart City, centrada en el ejercicio de derechos y en la atención directa a los individuos como principales destinatarios de las políticas urbanas.

Este punto de vista demanda una colaboración aún más estrecha entre los sectores público y privado, las soluciones van a requerir la participación de otros actores, no solo a las administraciones públicas, sino también a los proveedores tecnológicos. En última instancia, se trata de repensar colectivamente la ciudad para que responda de manera efectiva a las necesidades reales de sus habitantes (Fuentes i Gasó, 2021).

3.2. La utilización de Inteligencia Artificial por la Administración pública

La IA es una aplicación tecnológica que emula el razonamiento humano mediante el aprendizaje y la formulación de una serie de reglas generales y algoritmos, en la actualidad, los programas de IA más extendidos operan mediante el análisis de enormes cantidades de datos (el Big Data), lo que les permite detectar patrones, identificar tendencias y generar predicciones de forma automática, con gran precisión y en tiempos muy reducidos (Solar Cayón, 2021).

Este avance representa una oportunidad significativa para su aplicación en el entorno urbano, pero es necesario que se rija por principios de transparencia, imparcialidad, privacidad y responsabilidad, de modo que se pueda aprovechar los beneficios de la IA sin poner en riesgo los derechos fundamentales de los ciudadanos (Galazarza Quinto et al., 2024).

La Administración pública ha ido evolucionando desde el modelo clásico del siglo XIX, en el cual la única «tecnología» era el uso del papel, la imprenta y la máquina de escribir. Ya en la Administración 2.0 se incorporan tecnologías como son los ordenadores, los procesadores de texto y la impresora (o fax). Con la irrupción de Internet, los smartphones y las redes sociales, la Administración pública se dirigió hacia un modelo 3.0 (más propio del siglo XXI), en el cual la inmediatez, agilidad, digitalización y automatización son sus principales características (Corvalán, 2018).

El futuro apunta a una nueva etapa, la de la Administración 4.0, cuya principal seña es la utilización de la IA. Por tanto, de la gestión del papel a una digitalización de la burocracia, obtenemos finalmente una burocracia «inteligente». Esto es, que la IA automatizará las tareas, acelerará los procesos documentales y facilitará las interacciones mediante sus algoritmos (Muñoz, 2020).

Este avance representa el punto de partida para la estandarización y automatización de procesos administrativos, especialmente aquellos que presentan alta demanda y uniformidad. Sin embargo, la IA no constituye el único recurso disponible, sino que es el primer paso hacia una gestión automatizada e instantánea. Existen múltiples técnicas basadas en algoritmos que permiten desarrollar capacidades cognitivas artificiales.

Los autores especializados en el estudio de la IA señalan que esta busca emular facultades cognitivas humanas, interpretando parámetros de forma flexible para aprender y aplicar el conocimiento adquirido en función de objetivos específicos. En un nivel más avanzado, el «machine learning», una rama de la IA, permite el aprendizaje genuino mediante el procesamiento de datos relacionados. Finalmente, el «deep learning» o aprendizaje profundo, como evolución del «machine learning», posibilita la creación de modelos abstractos que permiten tomar decisiones automatizadas basadas en el conocimiento previamente adquirido (Muñoz, 2020).

En cuanto a las posibilidades auténticas que tiene la Smart City para el uso de la IA destacan (Sánchez Bravo, 2022):

- Smart Grids. La gestión más eficiente de la energía mediante el desarrollo de redes eléctricas inteligentes, facilitando una gestión más eficiente del consumo energético gracias a una comunicación entre el usuario y el centro de control.

- Smart Metering. Sistemas de medición inteligente que permiten la lectura remota y en tiempo real del consumo energético.
- Smart Citizen. Aunque obviamente el ciudadano es el eje principal de la Smart City, este puede apoyarse en las aplicaciones de IA para aumentar su participación.
- Smart Sensors. Sensores inteligentes que recopilan datos esenciales para el funcionamiento coordinado del entorno urbano.

Precisamente es en torno a los «smart sensors» donde el estudio de la videovigilancia adquiere una relevancia particular, en tanto en cuanto, es una tecnología que no sólo se fundamenta en la captación de imágenes, sino también en sistemas de procesamiento de datos y detección.

3.3. La videovigilancia y la seguridad ciudadana. Perspectiva histórica y jurídica

El origen de la videovigilancia no está tan cercano en el tiempo como se pudiera pensar, sus antecedentes históricos se sitúan a principios de siglo XX en Francia, las primeras cámaras fotográficas tenían el objetivo de capturar las imágenes faciales de los ciudadanos que infringían la ley. Sin embargo, fue en Inglaterra, en la década de los 1930, cuando la videovigilancia comenzó a consolidarse como una herramienta sistemática, por aquel entonces se utilizaba para registrar quien vulneraba las normas de las señales de tráfico (Mena Bravo, 2021)

Con el tiempo, la utilización de cámaras de videovigilancia se extendió al ámbito privado, los primeros sectores fueron la banca, los comercios y el sanitario. El objetivo era reducir los índices de hurto y fraude, al principio la tecnología no era muy avanzada y requerían supervisión humana constante (no se podían almacenar las grabaciones).

Tras los atentados del 11 de septiembre en 2001, el uso de la videovigilancia aumentó exponencialmente, especialmente en Estados Unidos. Este evento marcó un punto de inflexión en la percepción de la seguridad pública, generando una demanda urgente de avances tecnológicos en materia de vigilancia. Con la capacidad de almacenar los datos y las tecnologías biométricas, la videovigilancia se incorporó a las instituciones educativas y a otros espacios urbanos para facilitar la identificación de ciudadanos que pudieran realizar actividades vandálicas (Nieto et al., 2002).

En la actualidad y con toda la experiencia que se ha generado con el uso de la videovigilancia en diferentes países se ha evidenciado que esta es altamente eficaz como método de seguridad. Tampoco es necesario que se utilice exclusivamente para actividades delictivas, sino que puede servir para identificar cuando alguna situación se sale de control o existe algún comportamiento anormal entre los ciudadanos (Galdon-Clavell, 2015).

Obviamente para la Smart City la seguridad ciudadana es un elemento que interesa abordar, pues hay conflictos que pueden incidir negativamente en la vida cotidiana de los ciudadanos. Por ejemplo, fenómenos que incluyen el robo de vehículos o a ciudadanos, desordenes públicos, vandalismo, y en los casos más extremos los asaltos a ciudadanos o actos de terrorismo. La seguridad es un elemento clave pues los estudios afirman que cuando se es víctima de un delito esto inmediatamente se asocia a la disminución del bienestar no sólo personal sino también colectivo y a una disminución de la calidad de vida.

La inseguridad tiene también repercusiones económicas significativas como son la reducción de inversiones, la depreciación de los bienes inmuebles y el gasto de recursos adicionales en medidas de protección. Aunque hay varias perspectivas sobre cómo abordar el fenómeno de la seguridad ciudadana, las más relevantes son aquellas que se orientan a la prevención, el monitoreo, la detección y la intervención, por lo que el papel de la videovigilancia es clave (Morales et al., 2023).

La seguridad automatizada tampoco es perfecta, de hecho, puede generar nuevas formas de discriminación. En el caso de que se utilice la IA puede surgir la denominada «discriminación algorítmica», la cual deriva los sesgos en el proceso de toma de decisiones, produciendo situaciones inéditas que no se relacionan tanto con las causas «humanas» y tradicionales de discriminación, sino con la posible falta de transparencia y opacidad de los entornos digitales (Huerdo Lora, 2020).

4. Implicaciones sociales, éticas y jurídicas en el uso de la videovigilancia «inteligente»

Para que un sistema de videovigilancia sea efectivo es necesario que se aplique en un espacio que posea visibilidad y accesibilidad suficiente, esto es, que la observación de las actividades que ocurren en el entorno facilite la identificación de los comportamientos sospechosos. También es necesario que exista una «legibilidad», es decir, una señalización suficiente, clara y coherente para que los ciudadanos conozcan las normas de uso esperadas en el espacio videovigilado.

Aunque desde esta perspectiva la videovigilancia se enfoca para que el espacio urbano sea concebido como una zona de seguridad y de protección, lo cierto es que su aplicación produce una serie de efectos sociales tal como el desplazamiento de las actividades delictivas a zonas que no poseen sistemas de videovigilancia. En lo que respecta a la ciudadanía existe un aumento de la percepción de la seguridad de los ciudadanos en las zonas videovigiladas, mientras que por otro lado, este aumento de protección también contrasta con la sensación de falta de privacidad y desconfianza (Pérez Macías, 2024).

En cualquier caso, la videovigilancia es una herramienta muy relevante para la estrategia de seguridad en la Smart City, no representa por supuesto una solución definitiva para frenar la criminalidad, sin embargo, con la utilización de la IA los efectos sociales van a reconfigurarse, por lo que es necesario analizar las posibilidades que plantea y el marco regulatorio.

4.1. Aplicaciones prácticas para la Inteligencia Artificial en la videovigilancia

En un sentido amplio cualquier modelo de IA que se aplique a la seguridad ciudadana va a incorporar el uso de algoritmos y modelos estadísticos. Estos algoritmos van a permitir realizar predicciones espacio-temporales sobre la ocurrencia de los delitos, facilitando por ejemplo la identificación de zonas en las cuales la criminalidad sea elevada o exista un patrón delictivo recurrente.

Esta aplicación de IA se tiene que complementar necesariamente con técnicas estadísticas y de prevención, pues si se analiza por ejemplo que en una zona concreta de la ciudad hay una mayor presencia de homicidios o tráfico de drogas, se pueden desarrollar otras herramientas para la prevención. También existe la capacidad para identificar los delitos y analizar su evolución en el tiempo para planificar estrategias de seguridad (Barragán-Huamán et al., 2023).

La implementación de la IA también contribuye a que se optimice el trabajo de los cuerpos y fuerzas de seguridad en cuanto a la distribución policial y la anticipación de los eventos delictivos, algunos de los problemas delictivos más «cotidianos» van a estar referidos a cuestiones de desorden público y la alteración de normas sociales (Elluri et al., 2019)

Mediante un sistema de predicción inteligente pueden identificarse las zonas en las cuales hay mayor probabilidad de que ocurra un futuro delito. Los datos recopilados pueden servir para analizar variables geográficas, demográficas y temporales no solo en la ocurrencia de delitos sino también en los accidentes de tráfico (Barragán-Huamán et al., 2023).

El uso de drones constituye otra manifestación del empleo de IA en tareas de vigilancia y control. Estos dispositivos presentan una amplia variedad de aplicaciones, desde fines comerciales, como la detección de enfermedades en cultivos, hasta usos militares. En este último ámbito, destaca el caso de Estados Unidos, cuya fuerza aérea dispone de más de 80.000 drones destinados a operaciones antiterroristas. La proliferación de estas tecnologías plantea la necesidad de establecer marcos normativos que regulen su uso, especialmente en lo que respecta a la recopilación de datos, la seguridad de las infraestructuras críticas y la protección de los derechos humanos (Malamud, 2018).

Una de las aplicaciones más destacadas de la videovigilancia «inteligente» es la detección y localización de disparos, esta utilización de la tecnología cobra mucha importancia porque en el ámbito de la ciudad probablemente el sonido de un disparo es de los factores que más percepción incrementa de la inseguridad, contando también las consecuencias sociales y económicas que supone para el entorno urbano.

Con la utilización de la IA se permite una respuesta más rápida y eficaz por parte de las autoridades, no sólo para una mejor atención a las posibles víctimas sino también para la identificación y captura de los responsables. Como se ha comentado anteriormente, los datos generados son muy valiosos para desarrollar algoritmos predictivos y analizar patrones de criminalidad (Morales et al., 2023).

Otra aplicación interesante, aunque con menor desarrollo, es la detección de armas en espacios públicos o privados, tanto armas de fuego como armas blancas que puedan producir lesiones, alteraciones de orden público y en el caso más grave un homicidio. La detección de armas por los sistemas de videovigilancia con IA ayudaría a cumplir dos funciones principales: la prevención de incidentes violentos y facilitar el seguimiento e identificación del portador de la misma, al margen de si el arma fuera utilizada o no (Hashmi et al., 2021).

Sin embargo, al contrario que la detección de disparos, la detección de armas (u otros objetos) en imágenes presenta dificultades más específicas porque son objetos pequeños que se mueven rápidamente y cuyos portadores pueden ocultar parcial o totalmente. Las futuras investigaciones se enfocarán no sólo al análisis de los videos grabados para facilitar esta detección, sino que esta se pueda producir a tiempo real mediante los algoritmos (Zhao et al., 2021).

Existen muchos enfoques basados en técnicas de IA que pueden mejorar la seguridad ciudadana, por lo que el interés técnico y científico irá en aumento con el paso del tiempo, también el estudio de los algoritmos, los sistemas de alto procesamiento y la recopilación de datos. En cualquier caso, todos los esfuerzos tienen que ir dirigidos hacia el diseño de soluciones que realmente sean eficaces (Morales et al., 2023).

4.2. Los derechos fundamentales ante los sistemas de videovigilancia «inteligentes»

Una vez desplegados los dispositivos tecnológicos necesarios, sensores, cámaras y otros componentes digitales, en el entorno urbano, estos comienzan a recoger datos en tiempo real, alimentando los sistemas de IA que procesan dicha información para generar respuestas automatizadas. Este escenario, que algunos autores se atreven a representar como una distopía tecnológica, facilita el control constante de la ciudadanía por parte de las autoridades. Por ejemplo, el caso de China, sirve como prototipo ilustrativo de Smart City en cuanto de los riesgos asociados a este tipo de vigilancia intensiva (Álvarez Pereira, 2019).

La interconexión de plataformas, el uso masivo de cámaras y la integración del Internet de las Cosas permiten capturar cómo las personas realmente viven, más allá de sus opiniones o autopercepciones. Esta idea ya siendo llevada a cabo por empresas como Netflix, Google y Amazon, de tal modo que se utiliza el análisis de datos de comportamiento para ofrecer productos y servicios ajustados a las preferencias reales de los usuarios, abriendo la puerta así a la individualización de los servicios. Aunque esta personalización sin duda puede mejorar la atención al cliente, también supone desafíos para los principios de equidad e igualdad (Velasco Rico, 2019).

La implementación de sistemas de videovigilancia en el entorno de la Smart City plantea un dilema fundamental entre la protección de las libertades individuales y el potencial de la tecnología para mejorar la seguridad pública. En este contexto, se requiere un equilibrio normativo y ético, sustentado en tres pilares fundamentales:

- Derecho a la privacidad. El equilibrio entre la seguridad en espacios públicos y el respeto a la intimidad de las personas debe ser garantizado por el marco legal. Las leyes deben regular el uso de videovigilancia en espacios públicos y privados con acceso público, y prohibirla en espacios estrictamente privados. La Declaración Universal de los Derechos Humanos, en su artículo 12, establece que ningún ciudadano debe ser objeto de vulneraciones en su vida privada, familia o domicilio.
- Protección de datos personales. La videovigilancia implica la captación de datos sensibles, como imágenes, voz y comportamiento, lo que exige una protección robusta. Desde el año 2018 con la aplicación del Reglamento General de Protección de Datos

de la Unión Europea el consentimiento se ha convertido en un factor muy relevante en cuanto a los principios de libertad, revocabilidad, informado y específico.

- No discriminación. El uso de videovigilancia también puede derivar en prácticas discriminatorias, especialmente cuando se realiza seguimiento a personas consideradas «sospechosas» por criterios subjetivos como el color de piel, la vestimenta o el origen étnico (Vizcaíno Zamora, 2021).

Como se ha señalado, las Smart Cities se fundamentan en una doble exigencia: por un lado, la inevitable modernización tecnológica de la gestión administrativa de los servicios municipales; por otro, la transformación institucional que demandan cada vez más los gobiernos, impulsada por el uso intensivo de las «TICS». En este marco, se plantea que las Smart Cities deben asumir un compromiso firme con la transparencia, entendida como un valor que debe ser promovido desde la innovación tecnológica.

Este planteamiento sitúa a los proyectos de Smart City, especialmente aquellos desarrollados en España, ante el reto de cumplir con un conjunto normativo administrativo que, en muchos casos, presenta incoherencias y falta de sistematicidad. Las normas que regulan estos procesos han sido aprobadas de forma fragmentada, lo que dificulta su integración como base sólida para la construcción de las ciudades del futuro.

Es necesario subrayar que el primer requisito para un buen gobierno de la Smart City debería ser el cumplimiento riguroso del ordenamiento jurídico vigente. Sin embargo, como se abordará más adelante, este cumplimiento no siempre se produce con el nivel de diligencia que sería deseable (Velasco Rico, 2019).

5. Modelos internacionales de videovigilancia «inteligente»

Uno de los retos más complejos en la implementación de la IA en el contexto de la Smart City es la gestión ética y legal de los datos generados por aplicaciones y dispositivos que están conectados a la red. La implicación de actores privados, como empresas de automoción y proveedores tecnológicos, introduce riesgos relacionados con el uso indebido de datos personales, especialmente si se realiza sin el pertinente consentimiento.

La diversidad de modelos refleja también distintas formas de concebir la relación entre tecnología y ciudadanía. Algunos enfoques priorizan la dimensión social, democrática y participativa, mientras que otros se centran casi exclusivamente en la infraestructura tecnológica y otros valores como la seguridad y la protección. Este último punto es precisamente una de las principales preocupaciones de tipo jurídico en el contexto de las Smart Cities (Ricoy Casas, 2017).

Un ejemplo paradigmático es el sistema de crédito social implementado en China, que asigna puntuaciones a los ciudadanos en función de sus comportamientos, hábitos de consumo y actividades en Internet. Este sistema, que se sustenta en tecnologías de vigilancia masiva y análisis de datos, condiciona el acceso a servicios públicos y derechos básicos, generando una serie de discriminaciones estructurales. Este sistema es claramente incompatible con los principios democráticos y las garantías jurídicas propias de los Estados occidentales (Durán Ruiz, 2020).

La eficacia de estos sistemas también va a depender en gran medida de la disponibilidad de la infraestructura tecnológica, ya que esta debe permitir como mínimo la captura, almacenamiento y procesamiento de imágenes de manera inmediata y segura. Esta capacidad técnica es fundamental para que las autoridades competentes puedan utilizar los registros audiovisuales en investigaciones penales, contribuyendo así al fortalecimiento de la justicia y al control de la delincuencia (Malamud, 2018).

A continuación se analizarán una serie de modelos que pueden ilustrar como de avanzado están los modelos de videovigilancia basados en IA. El análisis de estos modelos de países tan diferentes permitirá definir las implicaciones para los derechos fundamentales así como tras implicaciones en términos de seguridad y privacidad así como los desafíos éticos que plantean.

5.1. La eficiencia tecnológica frente a la privacidad ciudadana. El modelo chino y singapurense

Desde hace años China ha estado desarrollado uno de los sistemas de vigilancia más sofisticados del mundo, este está basado en una extensa red de más de veinte millones de cámaras de seguridad equipadas con tecnologías de IA capaces de identificar en tiempo real características individuales como el sexo, la edad, el color de piel y la vestimenta de las personas.

Además, el sistema permite también para cuestiones de tráfico el reconocimiento de vehículos por marca, modelo, color y tipo, así como su estado (en circulación o estacionado). Esta infraestructura realmente es una estrategia para combatir la corrupción y localizar a aquellos ciudadanos que estén implicados en alguna actividad delictiva, ya sea mediante el uso de reconocimiento facial y aprendizaje automático, conectados directamente con las bases de datos policiales.

La implementación de este sistema genera un intenso debate sobre las implicaciones que tiene para la privacidad y las libertades individuales, pues la capacidad del Estado para identificar y rastrear a los ciudadanos en tiempo real plantea interrogantes sobre el equilibrio que debe existir entre seguridad pública y respeto de los derechos fundamentales (Burgueño, 2025).

Una de las innovaciones más curiosas en China ha sido es la creación de una comisaría completamente automatizada, gestionada por IA, en la que no se requiere interacción humana. Este centro está diseñado para atender trámites relacionados con el ámbito automovilístico, como pruebas de conducción mediante simuladores y la gestión de documentación, la identificación de los usuarios se realiza exclusivamente mediante reconocimiento facial (Araujo y Mendes, 2025).

Por otro lado, Singapur se presenta también como un referente en la aplicación de tecnologías a la videovigilancia, una de sus aplicaciones más relevantes es el uso de drones equipados con sensores para el monitoreo del tráfico y la contaminación, así como androides dotados de visión nocturna y cámaras de 360 grados. Estos drones son capaces de emitir alertas visuales y sonoras, han sido diseñados para detectar comportamientos sociales no deseados. Los denominados robots «Xavier» desempeñaron un papel clave en el control del distanciamiento social durante la pandemia de COVID 19, actuando como asistentes tecnológicos de las fuerzas de seguridad (Bendel, 2022)

Este tipo de innovación representa un cambio radical en la forma en que se concibe la Administración pública, introduciendo un modelo de gestión automatizada que, si bien puede mejorar la eficiencia, también plantea serias preocupaciones sobre la deshumanización de los servicios públicos y la protección de los datos personales (Estévez Martín y Ramírez Barredo, 2018).

5.2. La seguridad inteligente frente a la alta criminalidad. El modelo colombiano y mexicano

La expansión de los sistemas de videovigilancia en las principales ciudades colombianas se plantea como una medida necesaria para mitigar los riesgos de las altas tasas de criminalidad y garantizar el derecho de los ciudadanos a transitar libremente por espacios públicos. Aunque no se trata de una solución definitiva, su implementación representa un avance significativo en la lucha contra la delincuencia (Manjarrés de Ávila y Baca Mejía, 2017).

Reducir la videovigilancia a una función meramente de seguridad sería sin duda una visión limitada, por ello estos sistemas también contribuyen al orden social y al desarrollo urbano mediante el apoyo «humano» de las fuerzas y cuerpos de seguridad, con este equilibrio se obtiene una gestión más eficiente de los espacios públicos. A medida que crece la población y se diversifican las tecnologías, es imprescindible que los sistemas de vigilancia se actualicen y se extiende a nuevos sectores.

Si de algo sirve el ejemplo de Colombia, es que el avance tecnológico ha transformado las tácticas tradicionales de las fuerzas policiales, permitiendo la persecución del delito mediante la captación de imágenes claras que facilitan la reconstrucción de hechos y el rastreo de personas u objetos. En consecuencia, los sistemas de videovigilancia ofrecen múltiples beneficios que van desde la prevención del delito hasta el fortalecimiento de la justicia y la cohesión social (Madrigal Chacón, 2019).

El ejemplo de México también es relevante, pues allí se ha desarrollado un sistema que emplea cámaras instaladas en la vía pública para identificar maniobras prohibidas de tráfico, como giros en sentido contrario o cruzar con el semáforo rojo. Esta tecnología resulta especialmente relevante, dado que una parte importante de las colisiones entre vehículos ocurren en intersecciones. En este caso el sistema permite una supervisión automatizada de estas zonas críticas, contribuyendo a la prevención de accidentes y al fortalecimiento de la seguridad vial (Guzmán Arenas, 2023).

Recientemente se han desarrollado otros sistemas que facilitan el seguimiento de personas en tiempo real mediante múltiples cámaras en espacios cerrados, este sistema tiene diversas aplicaciones en seguridad, como son el control de accesos, la vigilancia de multitudes y la búsqueda de personas, también se puede utilizar para realizar análisis predictivos con fines comerciales (Vizcaíno Zamora, 2021).

Los retos técnicos de esta tecnología se relacionan con la calidad y la sincronización de las imágenes, así como las condiciones de iluminación. La detección inicial de personas se realiza mediante el uso de redes informáticas, específicamente el modelo YOLO (You Only Look Once), que permite identificar objetos en imágenes en tiempo real. Este modelo utiliza tres funciones de pérdida: clasificación, localización y confianza, cuya suma determina la precisión del sistema (Guzmán Arenas, 2023).

5.3. Los sesgos algorítmicos frente a las garantías jurídicas y democráticas. El modelo estadounidense y europeo

El empleo de algoritmos y herramientas de IA en el ámbito jurídico y policial ha dejado de ser una hipótesis teórica para convertirse en una realidad con consecuencias tangibles, algunas de las cuales han sido objeto de litigios judiciales. Ejemplos paradigmáticos como el sistema COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) en Estados Unidos, cuestionado por sesgos raciales, y el sistema SyRI (Systeem Risico Indicatie) en Europa, por su impacto en las garantías procesales clásicas, han puesto de manifiesto los riesgos inherentes a estas tecnologías.

El caso de COMPAS merece especial atención, pues ha generado un amplio debate en la doctrina jurídica norteamericana y en medios de comunicación de referencia como The New York Times. Este sistema fue utilizado por jueces para determinar el riesgo de reincidencia de los acusados, lo que suscitó preocupaciones sobre la posible existencia de sesgos discriminatorios en sus predicciones (Cotino Hueso 2020).

Estas herramientas no constituyen, en modo alguno, soluciones infalibles: los algoritmos no pueden prever el futuro ni resolver por sí solos los problemas estructurales de la delincuencia. Además, con el tiempo se han detectado ciertas «trampas metodológicas» en el uso de los algoritmos, como son el uso de datos de baja calidad, la interpretación errónea de las variables, la falta de evaluación rigurosa o simplemente la ausencia de derechos fundamentales.

Ante estos desafíos, se han formulado recomendaciones para las Fuerzas y Cuerpos de Seguridad que emplean IA en los sistemas de videovigilancia. Recientemente, algunos departamentos de policía en Estados Unidos han comenzado a revisar de «cero» sus estrategias, sustituyendo progresivamente los sistemas algorítmicos por modelos en los que valore también la participación e la comunidad (Rivero Ortega, 2023).

Los sesgos algorítmicos deben entenderse como efectos secundarios de una transformación tecnológica no anticipada por sus creadores, pues como es lógico, ni los diseñadores de software ni los responsables de las administraciones públicas han podido prever completamente las implicaciones sociales de los algoritmos. No obstante, esto no significa tampoco la no utilización en absoluto de los algoritmos, pues incluso las decisiones humanas están contaminadas por sesgos y «ruido», lo que otorga a los algoritmos una ventaja relativa. Además, los algoritmos pueden ser modulados para corregir prejuicios, algo que resulta más complejo en el caso de los sesgos humanos (Sunstein, 2022).

Aunque algunos tribunales han exigido garantías en el uso de algoritmos, la Corte Suprema de Estados Unidos no ha declarado su inconstitucionalidad, lo que permite su aplicación actual y futura. Esta postura, siempre que se acompañe de medidas como la transparencia, la supervisión humana y filtros previos, no resulta desacertada. La IA puede contribuir a la realización del principio de legalidad en el Estado de Derecho, siempre que se utilice con responsabilidad (Rivero Ortega, 2023).

En la actualidad, más de la mitad de la población mundial reside en entornos urbanos, lo que genera profundas transformaciones en la cultura, los estilos de vida, las relaciones sociales y la espiritualidad. Algunas autoridades europeas, entre las que podemos destacar al reciente fallecido Papa Francisco han señalado que las ciudades pueden ser al mismo tiempo espacios de libertad y realización humana, pero también escenarios de deshumanización y sufrimiento. Esta dualidad revela la complejidad del fenómeno urbano contemporáneo (Europa Press Sociedad, 2021).

Incluso en las ciudades más desarrolladas y aparentemente ordenadas, persiste la existencia de lo que se denomina como una «anti-ciudad»: territorios simbólicos habitados por individuos invisibilizados, privados de vínculos sociales significativos y relegados a «no-lugares». Estas personas, excluidas del reconocimiento social, son descritas como «anti-hombres», en una denuncia que pone de relieve la radical deshumanización que puede producirse en el seno de la vida urbana.

Frente a esta realidad, se advierte sobre los riesgos que implica el uso de tecnologías como la IA, que pueden convertirse en instrumentos de discriminación y despersonalización si no se desarrollan bajo criterios que sean éticos. Francisco reconoció los avances tecnológicos como expresión de la creatividad humana, no obstante, subrayó que este potencial solo se materializa plenamente cuando quienes diseñan y aplican estas tecnologías lo hacen con responsabilidad social y coherencia moral (Sánchez Bravo, 2022).

6. Conclusiones

La ciudad se ha convertido en un espacio complejo donde convergen muchas dinámicas sociales, tecnológicas y políticas, cada vez que aparece una nueva innovación tecnológica, es necesario una revisión profunda del marco normativo que está vigente. El crecimiento de la población y la dificultad de satisfacer las nuevas necesidades de los ciudadanos están impulsando que cada vez más las nuevas tecnologías recopilen datos, se optimicen los procesos y, por ende, se mejore la gestión de la Administración pública.

La utilización de la IA en los sistemas de videovigilancia en el contexto de la Smart City plantea en primer lugar una transformación profunda de cómo gestionar la seguridad del ciudadano y a la vez respetar sus derechos fundamentales. El desarrollo de tecnologías nuevas aplicadas a la videovigilancia ha mostrado avances significativos y presenta una serie de oportunidades en cuanto al avance en la eficiencia de la Administración pública, y también nuevas técnicas para mejorar la seguridad pública, sin embargo, esto genera también una serie de desafíos sociales, éticos y jurídicos.

Dos de los aspectos clave de la utilización de la IA es la recopilación masiva de datos, y la automatización de decisiones. La videovigilancia es sin duda una herramienta clave que es capaz de realizar un análisis predictivo de los datos, detectar comportamientos, y en conjunción con el factor humano anticipar riesgos y realizar una intervención rápida si es necesario.

Por las posibilidades analizadas está claro que su implementación debe estar cuidadosamente regulada, pues los derechos de intimidad y privacidad pueden quedar vulnerados. Existen varios modelos actualmente acerca de cómo enfocar estas tecnologías, por ejemplo, los modelos chino y singapurense dan un predominio más alto a la eficiencia y el avance tecnológico por encima incluso de los derechos más personales, los modelos colombiano y mexicano aprovechan las ventajas de la IA para reducir las altas tasas delictivas, mientras que los modelos europeos y estadounidense prefieren un modelo más garantista en el que se aborden los conceptos de transparencia y el respeto riguroso de los derechos fundamentales.

Se ha puesto de relieve que la utilización de la IA necesitan unos mecanismos de supervisión y rendición de cuentas, especialmente ante los sesgos algorítmicos. La protección de los derechos fundamentales en la Smart City requiere unas normas claras y coherentes, pero es necesario también que la «cultura» institucional sea la del respeto de derechos.

Tampoco basta con establecer marcos jurídicos, es imprescindible promover una reflexión ética sobre el uso responsable de la tecnología, orientada al bienestar humano. Si el análisis se limita a indicadores como la eficiencia o la seguridad, se corre el riesgo de vulnerar derechos fundamentales tan importantes como la privacidad o la dignidad humana.

El desarrollo de la Smart City debe estar guiado por una visión más humanista de la tecnología, pues la innovación tecnológica no puede ser un fin en sí mismo, sino que debe ser un medio que se encuentre en equilibrio con la justicia, la libertad y las garantías democráticas. Sólo así será posible en un futuro crear verdaderas ciudades «inteligentes» respetuosas con sus ciudadanos.

Referencias

- Aguado i Cudolà, V. (2022). Ciudades inteligentes y tecnología de cadena de bloques. Hacia un ejercicio compartido de funciones públicas. En G. M. Díaz González (coord.), *Blockchain y Gobiernos locales*, 83-124.
- Aguado i Cudolà, V., Parisio, V., & Casanovas i Ibàñez, Ò. (2018). *El derecho a la ciudad: el reto de las smart cities*. Barcelona: Atelier.
- Álvarez Pereira, C.D. (2019). Ciudades Inteligentes: el dilema entre privacidad de datos o bien común. *Cuadernos UCAB*, 15, 5-19,
- Araujo, M., & Mendes, A. (2025). Cibersegurança como soberanía nacional? Perspectivas do Brasil e da China. *Liinc em Revista*, 21(1), 1-20. <https://doi.org/10.18617/liinc.v21i1.7548Resumo>
- Barragán-Huamán, Cataño-Añazco K., Sevincha-Chacabana M., & Vargas-Salas O. (2023). La inteligencia artificial y la video-vigilancia en la predicción y detección de delitos en espacio-tiempo: una revisión sistemática. *Revista Criminalidad*, 65(1), 11-25. <https://doi.org/10.47741/17943108.398>
- Bendel, O. (2022). Robots in policing. En R. Hakli, P. Mäkelä & J. Seibt (Eds.) *Social Robots in Social Institutions: Proceedings of Robophilosophy*, 135-144. <https://doi.org/10.3233/FAIA220612>
- Burgueño, M.R. (2025). El dato biométrico y la videovigilancia como herramientas de control social. *Revista Blockchain e Inteligencia Artificial*, 6(6), 31-76. [https://doi.org/10.22529/rbia.2025\(6\)03](https://doi.org/10.22529/rbia.2025(6)03)
- Carmona Garias, S. (2020). *Democracia y gobierno abierto: una nueva cultura administrativa*. Madrid: McGraw-Hill.
- Corvalán, J.G. (2018). Hacia una Administración Pública 4.0: digital y basada en inteligencia artificial. *La Ley*, 154, 1-12.
- Cotino Hueso, L (2018). La obligación de relacionarse electrónicamente con la Administración y sus escasas garantías. IDP. *Revista de Internet, Derecho y Política*, 26, 3-14. <https://doi.org/10.7238/idp.v0i26.3112>
- Cotino Hueso, L. (2020). SyRi, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. *La Ley privacidad*, 4.
- Durán Ruiz, F.J. (2020). Implicaciones jurídicas de la implementación de ciudades inteligentes en la Unión Europea y en España. *Revista internacional Consinter de direito*, 6(7), 108-132. <https://doi.org/10.19135/revista.consinter.00011.04>
- Elluri, L., Mandalapu, V., & Roy, N. (2019). Developing Machine Learning Based Predictive Models for Smart Policing. *IEEE International Conference on Smart Computing*, 198-204. <https://doi.org/10.1109/SMARTCOMP.2019.00053>
- Estévez Martín, A., & Ramírez Barredo, B. (2018). Smartcity: la inteligencia artificial en la ciudad del futuro: estudio del caso Amazon Go. *Actas Icono 14, VI Congreso Internacional Ciudades Creativas*, 199-215.
- Europa Press Sociedad (2021). *El Papa alerta de que los que viven en grandes ciudades «artificiales» pueden perder la capacidad de contemplación*. <https://www.europapress.es/sociedad/noticia-papa-alerta-viven-grandes-ciudades-artificiales-pueden-perder-capacidad-contemplacion-20210505130135.html>
- Font i Llove, t. (2021). La ciudad inteligente como actor global. *European review of digital administration & law*, 2(1), 19-32.
- Fuentes i Gasó, J.R. (2021). Patrimonio cultural y smart city: la transformación integral de la ciudad. *Cuadernos de derecho local*, 57, 124-171.
- Galarza Quinto, A.K., Ferruzola Gómez, E.C., Jativa Aguirre, S.E., Hernández Cordova, H.E. & Zambrano Muñoz, N.A. (2024). Inteligencia artificial y derecho: implicaciones éticas y

- normativas en la justicia digital. *Sinergia Académica*, 7(6), 491-510. <https://doi.org/10.51736/kvp2z718>
- Galdon-Clavell, G. (2015). Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas. *EURE (Santiago)*, 41(123), 81-101. <https://doi.org/10.4067/S0250-71612015000300004>
- Guzmán Arenas, A. (2023). Cámaras con Inteligencia Artificial para las vías públicas de la CdMx. *Revista de Administración Pública*, 161(2), 79-98.
- Hashmi, T.S.S., Ul Haq, N., Fraz, M.M., & Shahzad, M. (2021). Application of Deep Learning for Weapons Detection in Surveillance Videos. *International Conference on Digital Futures and Transformative Technologies*, 1-6.
- Huergo Lora, A.J. (2020). Una aproximación a los algoritmos desde el derecho administrativo. En G.M. Díaz González, & A.J. Huergo Lora, (dir.), *La regulación de los algoritmos*, 23-87.
- Madrigal Chacón, I. (2019). *El uso de los sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la protección de datos personales*. San José: Universidad de Costa Rica
- Malamud, S. (2018). Videovigilancia y privacidad. Consideraciones en torno a los casos «Globos» y «Drones». *Revista chilena de Derecho y Tecnología*, 7(2), 137-162. <https://doi.org/10.5354/0719-2584.2018.49097>
- Manjarrés de Ávila, W. & Baca Mejía, W. (2017). Victimización por crimen, percepción de seguridad y satisfacción con la vida en Colombia. *Revista de Economía Institucional*, 21(41), 133-160. <https://doi.org/10.18601/01245996.v21n41.06>
- Mena Bravo, C.R. (2021). *Sistemas de videovigilancia y su aporte a la evolución estratégica de la seguridad ciudadana*. Bogotá: Universidad Militar Nueva Granada.
- Morales, O.M., Fletscher Bocanegra, L.A., & Botero Vega, J.F. (2023). La Inteligencia Artificial como apoyo a la gestión de la seguridad ciudadana: un estado del arte. *Revista de Pensamiento Estratégico y Seguridad*, 8(2), 55-72.
- Muñoz, R. (2020). *Las TICS en la Administración pública. La inteligencia artificial ante una perspectiva de derechos*. Editorial Astrea.
- Nieto, M., Johnston-Dobbs, K., & Simmons, C. (2002). *Public and private applications of video surveillance and biometric technologies*. Sacramento California Research Bureau.
- Pérez Macías, E. (2024). Videovigilancia urbana: ¿Herramienta de prevención del delito o control social? *Revista Digital de Estudios Organizacionales*, 5, 200-207. <https://doi.org/10.69509/yy5r5975>
- Ricoy Casas, R.M. (2017). Protección de datos y E-Administración en las Smart Cities: ¿seguridad, igualdad y libertad? *XIII Congreso AECPA la Fortaleza de Europa: Vallas y Puentes. Santiago de Compostela*.
- Rivero Ortega, R. (2023). *Derecho e Inteligencia Artificial. Cuatro estudios*. Santiago de Chile: Ediciones Olejnik
- Sánchez Bravo, Á. (2022). Ciudades, TIC e inteligencia artificial. En Á. Sánchez Bravo, (dir.), *Intellegentiae artificialis, imperium et civitatem*, (175-200).
- Solar Cayón, J.I. (2021). Reflexiones sobre la aplicación de la inteligencia artificial en la administración de justicia. *Teoría Jurídica Contemporánea*, 6, 1-35. <http://hdl.handle.net/10902/24149>
- Sunstein, C.R. (2022). Governing by Algorithm? No Noise and (Potentially) Less Bias. *Duke Law Journal* 71, 1175-1205. <https://scholarship.law.duke.edu/dlj/vol71/iss6/1>
- Telefónica (2023). *Las smartcities españolas y el Plan Nacional de ciudades inteligentes*. <https://www.telefonica.com/es/sala-comunicacion/blog/las-smartcities-espanolas-y-el-plan-nacional-de-ciudades-inteligentes/>
- Velasco Rico, C. (2019). La ciudad inteligente: entre la transparencia y el control. *Revista General de Derecho Administrativo*, 50.
- Villarejo Galende, H. (2015). Smart Cities. Una apuesta de la Unión Europea para mejorar los servicios públicos urbanos. *Revista de Estudios Europeos*, 66, 25-51.

- Vizcaíno Zamora, Á. (2021). Videovigilancia e inteligencia artificial: entre la utopía y la distopía. *Revista Mexicana De Ciencias Penales*, 4(14), 8-38. <https://doi.org/10.57042/rmcp.v4i14.432>
- Zhao, F., Fashola, O.I., Olarewaju, T. & Onwumere, I. (2021). Smart city research: A holistic and state-of-the-arte literature review. *Cities*, 119.