UNIVERSIDAD MIGUEL HERNÁNDEZ

Facultad de Ciencias Sociales y Jurídicas de Elche
Grado en Seguridad Pública y Privada (SEPP)

VIDEOVIGILANCIA FRENTE A DERECHOS CIUDADANOS

TRABAJO FIN DE GRADO

CURSO ACADÉMICO 2025/2026

Autor: Antonio Lucerón Díez

Tutor: Javier Valero Sánchez

RESUMEN

Este Trabajo de Fin de Grado gira en torno a la **videovigilancia policial**, entendida no solo como una herramienta técnica, sino como un fenómeno que combina **dimensiones jurídicas, éticas y operativas**. En los últimos años, las cámaras fijas, móviles o instaladas en drones, se han consolidado como instrumentos fundamentales en la labor policial, contribuyendo a mejorar la seguridad ciudadana, prevenir delitos. Sin embargo, este avance tecnológico también abre un campo de debate en torno a los derechos fundamentales, especialmente la intimidad y la protección de datos personales.

El trabajo desarrolla un análisis del marco legal que regula esta materia, tomando como referencia el Reglamento General de Protección de Datos, la Ley Orgánica 7/2021 y el Real Decreto 517/2024, que adapta la normativa europea al uso de drones en España. A partir de este estudio, se identifican los principales límites y obligaciones que recaen sobre las Fuerzas y Cuerpos de Seguridad en el uso de sistemas de captación de imágenes, así como las zonas grises que aún requieren de análisis y estudio.

Más allá del enfoque jurídico, el proyecto incorpora una reflexión ética sobre la posición del agente ante el uso de la tecnología: su responsabilidad al manejar imágenes sensibles, la necesidad de actuar con proporcionalidad y respeto. Esta parte ética no se plantea como un complemento, sino como un eje transversal que conecta la normativa con la realidad del servicio.

Desde mi experiencia en la Unidad de Medios Aéreos de la Policía Local de Orihuela, he tratado de aportar una visión pragmática y aplicada, mostrando cómo la normativa se debe traducir en decisiones operativas diarias: desde la planificación de vuelos y la gestión del DRI hasta la custodia de las grabaciones. Esta vivencia profesional permite acercar el trabajo académico a la realidad de la calle.

En definitiva, el proyecto propone una videovigilancia más humana, basada en la eficiencia policial, pero también en el control ético y en el respeto por los derechos de las personas. Una forma de entender la seguridad pública que no renuncia a la tecnología, pero tampoco a los valores.

PALABRAS CLAVE: videovigilancia, drones, seguridad pública, privacidad, ética.

ABSTRACT

This Final Degree Project focuses on **police video surveillance**, understood not only as a technical tool but as a phenomenon that combines **legal, ethical, and operational dimensions**. In recent years, fixed, mobile, and drone-mounted cameras have become essential instruments in police work, helping to enhance public safety and prevent crime. However, this technological progress also opens a field of debate concerning fundamental rights, particularly privacy and the protection of personal data.

The project develops an analysis of the legal framework governing this matter, taking as references the General Data Protection Regulation, Organic Law 7/2021, and Royal Decree 517/2024, which adapts European regulations to the use of drones in Spain. From this study, the main limits and obligations imposed on Law Enforcement Agencies in the use of image-capturing systems are identified, as well as the gray areas that still require deeper analysis and discussion.

Beyond the legal perspective, the project incorporates an ethical reflection on the officer's role when using technology: their responsibility in handling sensitive footage and the need to act with proportionality and respect. This ethical dimension is not presented as a mere complement but as a transversal axis connecting legal norms with real-life policing.

Drawing from my experience in the Aerial Media Unit of the Local Police of Orihuela, I have sought to provide a pragmatic and applied view, showing how regulations must translate into daily operational decisions — from flight planning and DRI management to the custody of recordings. This professional perspective helps bridge academic analysis with on-the-ground reality.

Ultimately, the project advocates for a more human approach to video surveillance — one based on police efficiency but also on ethical control and respect for individual rights. A vision of public security that embraces technology without abandoning values.

KEYWORDS: video surveillance, drones, public security, privacy, ethics.

LISTADO DE ABREVIATURAS Y SIGLAS

ACLU: *American Civil Liberties Union* (EE. UU.).

AEPD: Agencia Española de Protección de Datos.

AES (AES-256): *Advanced Encryption Standard* (cifrado simétrico; 256 bits).

AESA: Agencia Estatal de Seguridad Aérea.

CCTV: *Closed-Circuit Television* (televisión de circuito cerrado).

CNIL: *Commission nationale de l'informatique et des libertés* (autoridad francesa de protección de datos).

CONOP: *Concept of Operations* (Concepto de Operaciones).

DC: *District of Columbia* (EE. UU.).

DJI: Da-Jiang Innovations (fabricante de drones).

DRI: *Direct Remote Identification* (identificación remota directa).

EASA: *European Union Aviation Safety Agency* (Agencia de la Unión Europea para la Seguridad Aérea).

ECLI: *European Case Law Identifier* (Identificador Europeo de Jurisprudencia).

EURE: *EURE (Santiago)* (revista científica).

FRA: *European Union Agency for Fundamental Rights* (Agencia de Derechos Fundamentales de la UE).

H1–H8: Hipótesis 1 a 8.

IA: Inteligencia Artificial.

JARUS: *Joint Authorities for Rulemaking on Unmanned Systems*.

LiDAR: *Light Detection and Ranging*.

LO: Ley Orgánica.

LOPDGDD: Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

NIST: *National Institute of Standards and Technology* (EE. UU.).

QR: *Quick Response* (código QR).

RD: Real Decreto.

RGPD: Reglamento General de Protección de Datos (UE 2016/679).

RTCC: *Real-Time Crime Center* (centro de crimen/seguridad en tiempo real).

RTK: *Real Time Kinematic* (posicionamiento cinemático en tiempo real).

SORA: *Specific Operations Risk Assessment* (evaluación específica del riesgo operacional).

STS: Sentencia del Tribunal Supremo.

TEDH: Tribunal Europeo de Derechos Humanos.

TS: Tribunal Supremo.

UAS: *Unmanned Aircraft System(s)* (sistema(s) de aeronaves no tripuladas).

UE: Unión Europea.

UK: *United Kingdom* (Reino Unido).

ÍNDICE GENERAL

1. Introducción

1.1 Delimitación del tema de investigación

La videovigilancia policial se ha convertido en una pieza clave dentro de las estrategias de seguridad pública. Lo que comenzó con cámaras fijas en calles o edificios municipales ha evolucionado hacia algo mucho más complejo, donde los drones y otros sistemas ofrecen una nueva forma de mirar, registrar y actuar.

Sin embargo, este avance tecnológico no solo ha transformado la manera de trabajar de las fuerzas policiales, sino que también ha abierto un debate profundo sobre los límites de la **privacidad**, la **protección de datos** y la **proporcionalidad**.

En España, las cámaras terrestres se regulan desde hace años por la Ley Orgánica 4/1997 y el Real Decreto 596/1999, pero el salto hacia la videovigilancia aérea ha desbordado ese marco legislativo. Con la entrada en vigor del Real Decreto 517/2024, por primera vez se establecen pautas claras para las operaciones policiales con drones, una herramienta que en pocos años ha pasado de ser de uso extraordinario a convertirse en habitual. Aun así, la norma no elimina las dudas ni los vacíos legales que aparecen cuando la tecnología va más rápido que la ley.

El trabajo se centra precisamente en ese punto de encuentro entre lo jurídico, lo técnico y lo humano: en cómo las policías locales, y las instituciones, gestionan el uso de la videovigilancia sin perder de vista los derechos fundamentales de la ciudadanía.

1.2 Planteamiento del problema

La cuestión principal que da origen a este trabajo es clara: **¿cómo puede la policía aprovechar todo el potencial de la videovigilancia sin poner en riesgo los derechos de las personas?**

El equilibrio entre seguridad y libertad siempre ha sido delicado, pero con la llegada de los drones el dilema se ha hecho más visible. Por un lado, se busca una mayor eficacia operativa y una respuesta más rápida ante emergencias o delitos. Por otro lado, surgen preguntas sobre hasta qué punto es legítimo grabar, almacenar o analizar imágenes de espacios públicos o privados.

La realidad demuestra que no siempre hay respuestas simples. Las normas no terminan de adaptarse al ritmo del avance tecnológico, y la aplicación práctica de los principios

de finalidad, necesidad y proporcionalidad depende en la mayoría de las veces del criterio y la formación de los agentes.

Además, la percepción ciudadana frente a las cámaras no es homogénea: algunos las ven como una garantía de seguridad, y otros las asocian a un control excesivo o a la pérdida de intimidad.

1.3 Justificación de la investigación

Este trabajo nace de la necesidad de reflexionar sobre un fenómeno que, más allá de las leyes o los titulares, forma parte del día a día policial. La mirada no es solo académica, sino también profesional y humana. Desde la experiencia directa como piloto de drones en una unidad de medios aéreos, he podido comprobar cómo cada vuelo implica decisiones operativas con responsabilidades legales y éticas.

La videovigilancia no es solo una cuestión técnica; es también una cuestión de responsabilidad. Captar imágenes desde el aire puede ayudar a resolver un delito o a coordinar un operativo de emergencia, pero siempre debe hacerse bajo un marco de respeto a los derechos fundamentales y con una conciencia clara de sus límites.

Por eso, el trabajo busca juntar tres puntos de vista que rara vez se unen de forma equilibrada: la jurídica, que marca los límites; la técnica, que define las posibilidades; y la ética o humana, que recuerda que detrás de cada cámara hay personas observando a otras personas.

El estudio pretende aportar una visión basada en la realidad, basada en la práctica, pero también crítica y con propuesta de soluciones. Analiza cómo se están aplicando las normas, qué carencias existen y qué mejoras podrían incorporarse.

1.4 Contenido y límites del trabajo

El desarrollo del trabajo combina tres enfoques complementarios: el **análisis normativo**, la **experiencia profesional** y el **estudio de casos reales**. Primero, se revisa la normativa que regula la videovigilancia en España, tanto terrestre como aérea, desde la Ley Orgánica 4/1997 hasta el reciente Real Decreto 517/2024, y con el marco europeo de protección de datos. Después, se examina la experiencia acumulada en el uso policial de drones, identificando las principales ventajas y riesgos que surgen en la práctica.

El alcance del trabajo se centra en el ámbito policial local y autonómico, dejando fuera la vertiente militar o de seguridad privada. Tampoco se aborda el análisis técnico de hardware o software de los drones, ya que el objetivo es comprender cómo se aplican y se controlan jurídicamente sus usos.

En definitiva, se trata de un estudio que busca responder, con mirada crítica y constructiva, a cómo puede articularse una videovigilancia policial eficaz, ética y respetuosa con los derechos fundamentales en una sociedad que ya convive con la tecnología.

2. Marco teórico: tecnología, derechos y videovigilancia aérea policial

2.1 Evolución tecnológica de la videovigilancia

Hablar de videovigilancia es hablar de una tecnología que ha crecido de un modo vertiginoso. Hoy nos resulta tan cotidiana que casi pasa desapercibida, una cámara en un semáforo, otra en la fachada del ayuntamiento, un domo giratorio en la esquina de una calle o un dron que sobrevuela un concierto. Sin embargo, detrás de cada una de esas imágenes hay una mezcla de progreso, control y responsabilidad.

La **primera generación** de videovigilancia, la de los sistemas analógicos, tenía gran parte de artesanal. Eran cámaras robustas, conectadas por cables coaxiales que terminaban en grabadoras VHS, y cada cinta duraba unas horas. Aquello obligaba a un control manual: etiquetar, archivar, rebobinar. Las imágenes eran borrosas, con suerte permitían reconocer siluetas o colores.

Imagen 1. Cámara de videovigilancia de primera generación.

Aun así, esas cámaras fueron un primer paso. En esos primeros compases se generó la idea de que el espacio público podía ser observado de forma permanente.

Con la llegada de la digitalización, todo cambió. Las cámaras IP trajeron consigo una mejora importante en calidad de imagen, la posibilidad de conectar dispositivos entre sí y, sobre todo, el salto al control remoto. Por primera vez, un operador podía vigilar decenas de cámaras desde una sala de control o incluso desde un portátil. Ya no hacía

falta rebobinar cintas: las imágenes se guardaban durante semanas en servidores y podían consultarse con un simple clic.

El cambio no fue solo técnico, sino cultural. La videovigilancia dejó de ser una herramienta auxiliar para convertirse en un elemento central de la gestión de la seguridad. Las ciudades comenzaron a integrar los sistemas en sus salas de control, los cuerpos policiales a coordinar sus recursos y las administraciones a invertir en redes de cámaras. En poco tiempo, la vigilancia dejó de ser un acto puntual para convertirse en una presencia constante.

Y entonces llegó el gran salto, la inteligencia artificial. Lo que antes era una cámara pasiva, que se limitaba a grabar lo que pasaba delante de su lente, se convirtió en una herramienta activa capaz de analizar comportamientos, reconocer patrones y tomar decisiones automáticas. La analítica de vídeo es hoy una de las áreas que más rápidamente está creciendo. Permite detectar aglomeraciones, identificar matrículas o localizar objetos abandonados sin intervención humana directa.

Imagen 2. Cámara domo de videovigilancia.

Pero, esta evolución ha traído también sus sombras. Cuanto más potente es la tecnología, más cuidado se debe poner en el equilibrio entre utilidad y riesgo. Los algoritmos no son neutrales: se entrenan con datos que, a menudo, reflejan los mismos sesgos que existen en la sociedad. Un error de lectura o una mala interpretación del algoritmo puede derivar en una identificación errónea o en una sospecha injustificada. No hablamos de un fallo técnico cualquiera, sino de una decisión que puede afectar a personas reales.

Aun así, la videovigilancia ha demostrado ser una aliada importante para mejorar la respuesta policial. La diferencia entre llegar a tiempo o no hacerlo puede depender de la rapidez con que se detecta una incidencia, y en este ámbito de actuación las cámaras marcan la diferencia. Pero de nada sirve tener un sistema sofisticado si no se gestiona con responsabilidad, si las grabaciones se acumulan sin control o si nadie revisa el uso que se hace de ellas.

El problema ya no es técnico. La tecnología funciona, y lo hace muy bien. El problema es ético y operativo: cómo usarla de forma legítima, proporcional y transparente. Esa es la verdadera asignatura pendiente.

2.2 Los drones como nueva herramienta policial

Si las cámaras fijas cambiaron la forma de mirar la ciudad, los drones han hecho lo mismo, pero desde el aire. Hoy ya no son una rareza tecnológica ni un capricho: son parte del equipamiento habitual de muchos cuerpos policiales. Y lo más interesante es que no se trata de una moda pasajera, sino de una transformación profunda en la manera de entender la vigilancia, la prevención y la respuesta ante emergencias.

El dron ha roto las barreras físicas del terreno. Permite observar desde el aire con una rapidez que ningún otro recurso iguala. Donde antes había que desplazar un helicóptero o montar un operativo entero, hoy basta con un despegue de treinta segundos para tener una imagen completa del escenario. En operaciones de rescate, búsqueda de personas, control de tráfico o gestión de aglomeraciones, esa rapidez marca la diferencia entre reaccionar a tiempo o llegar tarde.

Modelos más utilizados en cuerpos policiales

Imagen 3. Dron de ultima generación. Modelo DJI Mavic 4T.

En España, la implantación de drones en cuerpos policiales se ha apoyado, en términos generales, en soluciones comerciales ampliamente extendidas en el mercado profesional. En la práctica, esto ha favorecido una cierta homogeneidad tecnológica, especialmente en el ámbito municipal y autonómico, donde suele priorizarse la disponibilidad de equipos contrastados, la facilidad de mantenimiento y la existencia de un ecosistema de trabajo ya conocido por la mayoría de operadores. Dentro de ese panorama, DJI se ha consolidado como el fabricante más frecuente, no tanto por una cuestión de marca en sí, sino por su posición dominante en el sector y por la estandarización que aporta en formación, repuestos y procedimientos.

A partir de ahí, lo relevante para este trabajo no es describir cada modelo como si se tratara de un catálogo, sino entender qué explica su uso y qué implicaciones tiene desde el punto de vista de la gobernanza. Los equipos que más se repiten en unidades policiales suelen responder a una combinación de factores: portabilidad, fiabilidad, integración de sensores (visual y térmico), estabilidad de transmisión y capacidad de operar en escenarios diversos. Esa combinación ha hecho habituales determinadas plataformas en los servicios de apoyo policial, sin que ello signifique que el rendimiento

dependa del modelo concreto, sino de cómo se integra el recurso en procedimientos, formación y control.

Tecnología embarcada y sus utilidades operativas

Más allá del dron en sí, lo que marca la diferencia es la carga útil o carga de pago, es decir, los sensores que lleva a bordo. Las cámaras térmicas, ópticas, multiespectrales o de visión nocturna han abierto un abanico de posibilidades.

Las cámaras termográficas son, sin duda, una de las herramientas más útiles en el trabajo policial y de emergencias. Su funcionamiento se basa en detectar las variaciones de temperatura en el entorno y transformarlas en una imagen visible. Gracias a ellas, es posible localizar personas en la oscuridad, detectar fugas de calor en incendios, o identificar vehículos que acaban de ser utilizados.

En operaciones de búsqueda de personas desaparecidas, una cámara térmica puede detectar un cuerpo humano incluso entre la maleza. En incendios, permite a los equipos de emergencia identificar focos activos y zonas de riesgo antes de acceder. En la práctica policial, ayuda a detectar a los autores de hechos delictivos en la oscuridad de la noche, facilitando mucho la labor de búsqueda y detención.

Además de la térmica, los drones actuales combinan cámaras visuales de altísima resolución con zooms híbridos de hasta 200 aumentos, capaces de leer una matrícula a más de 800 metros sin pérdida de detalle. Esta capacidad es muy valiosa en operativos de observación discreta o control perimetral, donde acercarse físicamente sería contraproducente.

Otra innovación clave son los sensores LiDAR (Light Detection and Ranging), que emiten pulsos láser para crear nubes de puntos tridimensionales. Permiten cartografiar zonas de difícil acceso, calcular volúmenes o reconstruir escenas de accidentes de tráfico con precisión milimétrica. Cada vez más unidades comienzan a utilizar esta tecnología en atestados o informes periciales.

Por último, cabe mencionar los sistemas de altavoces direccionales y proyectores LED integrados en algunos modelos, que permiten emitir avisos, ordenar desalojos o señalizar zonas de peligro desde el aire.

Seguridad de vuelo y comunicaciones

Toda esta potencia tecnológica se sostiene sobre un principio básico: la seguridad. Los drones policiales actuales incorporan sistemas de posicionamiento RTK (Real Time Kinematic) que corrigen el GPS y ofrecen una precisión centimétrica. También incluyen sensores anticolisión de 360°, retorno automático en caso de pérdida de señal y baterías inteligentes que calculan la autonomía restante y proponen rutas de regreso seguras.

En cuanto a las comunicaciones, el estándar es el cifrado AES-256, que protege la transmisión de vídeo frente a interceptaciones. Algunos modelos, como el Matrice 350 RTK o el nuevo Mavic 4T, incluyen enlaces redundantes con cambio automático de frecuencia entre 2.4, 5.8 y 6 GHz para evitar interferencias. En el fondo supone una garantía jurídica y operativa.

Usos policiales más habituales

En el día a día, los drones se han integrado en tareas muy diversas. En eventos multitudinarios, permiten controlar flujos de personas y detectar puntos de riesgo antes de que se produzca una avalancha. En operaciones de tráfico, ayudan a valorar el estado de la vía o gestionar. En búsqueda y rescate, reducen drásticamente el tiempo de localización de personas desaparecidas, especialmente en zonas de montaña, costa o cauces de río.

En actuaciones nocturnas, la combinación de cámaras térmicas y luces auxiliares permite identificar movimientos sospechosos o localizar sujetos o vehículos ocultos sin necesidad de exponer a las patrullas. En investigaciones judiciales, las imágenes aéreas sirven como apoyo pericial para reconstruir escenas y elaborar informes visuales.

Lo más importante es que el dron no sustituye al agente, sino que lo amplía. Le ofrece un punto de vista imposible desde tierra y reduce riesgos innecesarios. Cada vuelo, sin embargo, debe estar justificado: no se trata de grabar por grabar, sino de volar con propósito.

El uso responsable es lo que da sentido a la herramienta. Un dron que despega con una misión clara es un recurso valioso. Pero un dron que se utiliza sin planificación ni control puede convertirse en una fuente de conflicto jurídico.

La tecnología y el factor humano

Por mucha inteligencia artificial que se integre, el factor humano sigue siendo esencial. Un piloto de drones no es solo un técnico; es un operador de seguridad con **responsabilidades legales y éticas**. Tiene que conocer la normativa aérea, la protección de datos y las limitaciones operativas. Cada decisión tiene implicaciones que van mucho más allá de la técnica.

En resumen, los drones han traído una nueva dimensión a la videovigilancia. Han ampliado la mirada policial y han demostrado que la tecnología puede salvar vidas, agilizar intervenciones y mejorar la eficacia operativa. Pero también han recordado algo fundamental: cuanta más tecnología se tiene, más responsabilidad exige su uso.

2.3 Marco jurídico de la videovigilancia policial. "*Ex lege libertas"*

Detrás de cada imagen captada por una cámara policial hay una cuestión que va más allá de la técnica. Porque grabar en el espacio público no es un acto neutro. Implica manejar información personal, interpretar conductas y, en muchos casos, tomar decisiones que afectan directamente a derechos fundamentales. De ahí que el marco jurídico no sea un simple acompañamiento, sino el eje que da legitimidad a todo el sistema.

En España, el punto de partida es la Constitución de 1978, concretamente su artículo 18.1, que protege el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Ese mismo artículo, en su apartado cuarto, advierte que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos". Lo que en su momento parecía una referencia abstracta a las bases de datos informáticas se ha convertido hoy en una cláusula fundamental (Constitución Española, 1978, art. 18.1 y 18.4).

Esa garantía se desarrolla en un conjunto de normas que delimitan con precisión el uso de cámaras y drones por parte de las Fuerzas y Cuerpos de Seguridad. La Ley Orgánica 4/1997 y su Reglamento de desarrollo (RD 596/1999) fueron los primeros textos que pusieron límites a la videovigilancia policial. Exigen que la instalación de cámaras fijas en lugares públicos cuente con autorización previa de la Comisión de Garantías de Videovigilancia y que el uso de las imágenes esté restringido a fines concretos: prevención del delito, mantenimiento de la seguridad y orden público, y persecución de

infracciones penales (Ley Orgánica 4/1997, de 4 de agosto; Real Decreto 596/1999, de 16 de abril).

La Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) incorporó al ordenamiento español el Reglamento General de Protección de Datos (RGPD, UE 2016/679), estableciendo principios esenciales como la licitud, la transparencia, la minimización y la limitación temporal del tratamiento. El artículo 22 regula expresamente la videovigilancia, imponiendo la obligación de señalizar las zonas grabadas, restringir la conservación de imágenes a un máximo de 30 días y asegurar que las grabaciones solo se utilicen para los fines previstos (Ley Orgánica 3/2018, de 5 de diciembre, art. 22; Reglamento (UE) 2016/679).

La videovigilancia policial, sin embargo, tiene una característica particular: se vincula a finalidades propias de seguridad pública e investigación penal. Por eso, desde 2021, el tratamiento de datos en este contexto se rige también por la Ley Orgánica 7/2021, que adapta la Directiva (UE) 2016/680 al ordenamiento nacional. Esta norma especifica que los cuerpos policiales pueden tratar datos personales con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales, pero siempre bajo el principio de proporcionalidad y supervisión. También limita las decisiones basadas exclusivamente en tratamientos automatizados, cuestión crucial cuando se emplean herramientas de analítica avanzada o reconocimiento biométrico (Ley Orgánica 7/2021, de 26 de mayo; Directiva (UE) 2016/680).

El siguiente gran bloque normativo lo constituye la regulación del espacio aéreo. El Real Decreto 1036/2017 fue durante años la norma básica sobre utilización civil de drones en España, pero el avance tecnológico lo dejó pronto desfasado. En 2024 entró en vigor el Real Decreto 517/2024, que actualiza la normativa y adapta el marco europeo (Reglamento de Ejecución (UE) 2019/947) al contexto nacional. Esta norma refuerza obligaciones de registro, planificación y control, con especial atención a operaciones sensibles (Real Decreto 1036/2017; Real Decreto 517/2024; Reglamento de Ejecución (UE) 2019/947).

- Cada operador debe estar registrado cuando la normativa lo exige y operar conforme a los deberes de identificación y responsabilidad previstos en el marco europeo (Reglamento de Ejecución (UE) 2019/947).
- En determinadas operaciones, especialmente en entorno urbano o sobre reuniones de personas, se prevén exigencias reforzadas, incluida comunicación previa en los supuestos previstos por la norma nacional (Real Decreto 517/2024).

- Se exige documentación suficiente para asegurar trazabilidad y control a posteriori, de forma que la actuación pueda justificarse y auditarse con criterios objetivos (Real Decreto 517/2024).

La jurisprudencia también ha ido marcando límites relevantes. En el ámbito penal, el Tribunal Supremo ya ha abordado la captación de imágenes con dron como elemento de investigación, vinculando su validez a un juicio estricto de necesidad y proporcionalidad, y a la adecuada motivación y control de la injerencia cuando la captación afecta a expectativas razonables de privacidad (Tribunal Supremo, Sala Segunda, STS 797/2025, ECLI:ES:TS:2025:4225).

Y en el ámbito europeo, el Tribunal Europeo de Derechos Humanos (TEDH), en el caso *Big Brother Watch and Others v. Reino Unido* (2021), reafirmó que los Estados no pueden justificar una vigilancia masiva con el argumento genérico de la seguridad nacional: cualquier intromisión debe estar prevista por la ley, responder a una necesidad real y ser proporcional al fin perseguido (Big Brother Watch and Others v. the United Kingdom, 2021).

En resumen, el marco jurídico actual no prohíbe la videovigilancia; la ordena y condiciona. Reconoce su utilidad, pero impone garantías: justificación, limitación, transparencia y supervisión (Constitución Española, 1978; Ley Orgánica 4/1997; Ley Orgánica 3/2018; Ley Orgánica 7/2021; Real Decreto 517/2024).

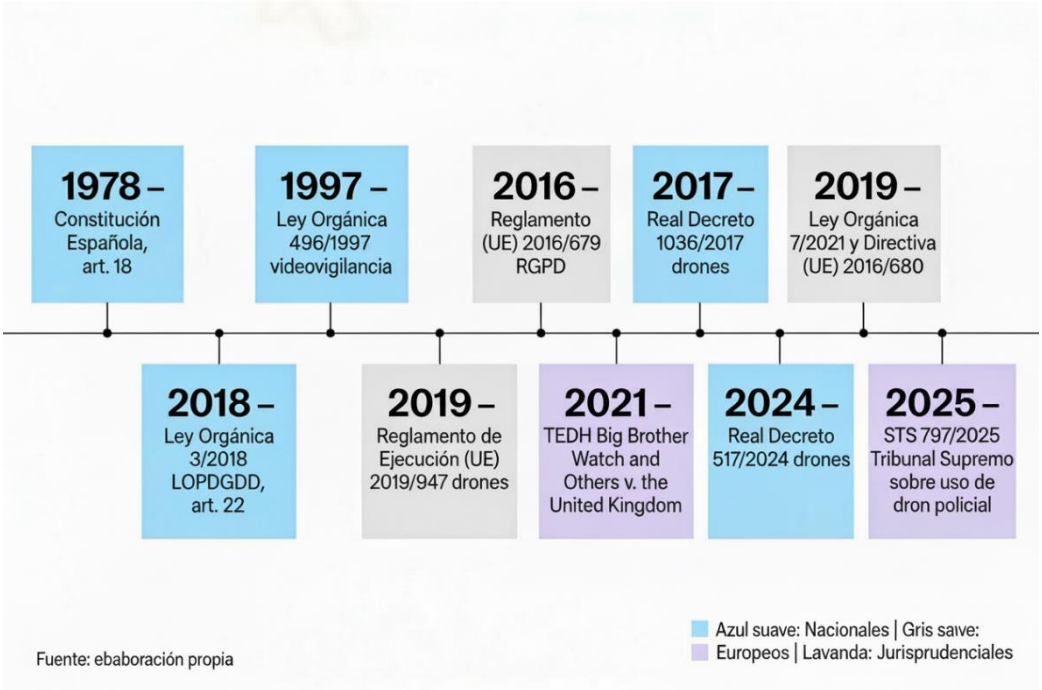


Grafico 1. Evolución de la normativa UAS.

2.4 Impacto en los derechos fundamentales

Cada vez que una cámara se enciende o un dron despega, se pone en tensión el equilibrio entre intimidad y seguridad. Es una frontera difusa, pero decisiva, porque condiciona el tipo de sociedad en la que vivimos. No se trata de oponerse a la tecnología, sino de garantizar que su uso no erosione los derechos que precisamente debe proteger (Constitución Española, 1978, arts. 18 y 21).

El primer derecho afectado es la privacidad y la protección de datos personales. Aunque la vía pública no es un espacio de intimidad "plena", eso no significa que todo valga: el principio de proporcionalidad obliga a que la captación se limite al tiempo, el espacio y la finalidad estrictamente necesarios (Ley Orgánica 7/2021, 2021; AEPD, 2019). Una cámara o un dron que graba "por si acaso" durante largos periodos no solo es discutible en términos de eficacia; también incrementa el riesgo de injerencia ilegítima, porque amplía el rastro de datos y su posible reutilización fuera de contexto (AEPD, 2019).

Este conflicto se vuelve más intenso con vigilancia aérea, porque la movilidad y la altura dificultan la percepción inmediata por parte del ciudadano, y con ello se resiente la transparencia material del tratamiento. La propia AEPD ha advertido que la captación mediante drones exige extremar la minimización, ajustar la finalidad y reforzar medidas organizativas y de seguridad, precisamente por su capacidad de registrar imágenes en espacios y ángulos no previsibles (AEPD, 2019). En paralelo, la jurisprudencia reciente ya está marcando líneas rojas: el Tribunal Supremo ha analizado supuestos de captación con dron en entornos residenciales, vinculando la observación dirigida e intensa con límites derivados del derecho fundamental y de la exigencia de proporcionalidad y control (STS 797/2025, ECLI:ES:TS:2025:4225).

El segundo bloque sensible es la libertad de circulación y, sobre todo, la libertad de reunión. En contextos de protesta o concentración, la vigilancia audiovisual puede generar un efecto inhibidor (chilling effect), porque introduce la percepción de identificación y seguimiento. Este riesgo ha sido reconocido en la jurisprudencia comparada: en *Bridges v. Chief Constable of South Wales Police* se cuestionó la proporcionalidad y la calidad de las salvaguardas en el uso policial de tecnologías biométricas en espacios públicos (Court of Appeal, 2020). Y, desde un plano más general, el TEDH ha insistido en que las injerencias intensas en privacidad y comunicaciones requieren base legal clara, necesidad real y salvaguardas eficaces, precisamente para evitar derivas de vigilancia masiva (Big Brother Watch and Others v. the United Kingdom, 2021).

Un tercer ámbito especialmente delicado es la presunción de inocencia cuando entran en juego analítica avanzada y reconocimiento facial. Sin controles sólidos, estas tecnologías pueden desplazar el foco desde conductas a “perfiles” y aumentar el riesgo de falsos positivos. La literatura técnico-institucional ha documentado diferencias de rendimiento por grupos demográficos en sistemas de reconocimiento facial, con implicaciones directas en sesgos y errores (NIST, 2019). En la misma línea, organismos europeos han advertido sobre riesgos de discriminación, proporcionalidad y gobernanza en el uso de biometría e IA en espacios públicos (FRA, 2025).

Frente a ese escenario, el marco español marca un límite relevante: en el tratamiento de datos con fines policiales, no puede descansarse en decisiones basadas únicamente en tratamientos automatizados cuando produzcan efectos adversos significativos, exigiendo intervención y control humano efectivo (Ley Orgánica 7/2021, 2021, art. 14).

En definitiva, el impacto de la videovigilancia sobre derechos fundamentales no es una discusión teórica: se traduce en cómo nos movemos, cómo participamos en el espacio público y qué nivel de confianza otorgamos a la institución. Por eso, además de legalidad, hacen falta límites comprensibles, controles verificables y una ética operativa real que se note en la práctica diaria (AEPD, 2019; Big Brother Watch, 2021).

2.5 Balance riesgo-beneficio

Hablar de riesgo y beneficio en videovigilancia es hablar de equilibrios. Toda herramienta de seguridad implica un intercambio entre eficacia y privacidad, entre control y confianza. El objetivo no es eliminar el riesgo, sino gestionarlo con inteligencia.

Los beneficios son evidentes. Las cámaras y los drones han demostrado su utilidad en prevención del delito, búsqueda de personas, gestión de emergencias e investigación judicial. En operaciones reales, han permitido acortar tiempos de reacción, documentar escenas antes de que se alteren y recoger pruebas con valor procesal. En casos de incendios, accidentes o rescates, los drones se han convertido en aliados, reduciendo riesgos para los propios agentes.

Pero los riesgos también son claros: la vigilancia desproporcionada, la retención excesiva de imágenes, la falta de transparencia y el uso inadecuado de la tecnología pueden minar la confianza ciudadana. Cuando la gente siente que se le observa sin saber por qué, la relación entre policía y comunidad se resiente.

Hay, sin embargo, modelos que demuestran que se puede hacer bien. El ejemplo del dron de rescate marítimo en Barcelona Marítim 2024 es paradigmático: se activa únicamente cuando hay aviso, graba solo el área del incidente, no almacena imágenes y no invade espacios privados. Resultado: vidas salvadas sin vulnerar derechos. Ese es el camino.

Para mantener ese equilibrio, es necesario aplicar una serie de **garantías operativas**:

- **Justificación previa**: toda instalación de cámara o vuelo con dron debe basarse en un objetivo concreto, documentado y verificable.
- **Limitación temporal y espacial**: grabar solo lo necesario, durante el tiempo estrictamente imprescindible.
- **Transparencia**: informar a la ciudadanía mediante cartelería, códigos QR o portales web sobre quién graba, con qué fin y durante cuánto tiempo.
- **Auditorías externas**: revisar periódicamente el cumplimiento normativo, los accesos a las grabaciones y la eliminación de los datos.
- **Formación continua**: asegurar que los agentes que operan cámaras o drones conocen la legislación vigente y las implicaciones éticas de su trabajo.

En definitiva, el verdadero desafío no está en la tecnología, sino en el uso que hacemos de ella. Una cámara puede ser una herramienta de seguridad o un instrumento de control; un dron puede salvar una vida o vulnerar un derecho.

3. Objetivos e hipótesis

3.1 Objetivo general.

El objetivo general de este Trabajo Fin de Grado es **analizar de manera crítica y reflexiva el uso de la videovigilancia en el ámbito policial**, con especial atención a la progresiva incorporación de los drones como herramienta operativa, desde una perspectiva jurídica, ética y funcional, con el fin de valorar si su utilización actual permite alcanzar un equilibrio real y sostenible entre la mejora de la seguridad ciudadana y la protección efectiva de los derechos fundamentales.

Este objetivo parte de la constatación de que la videovigilancia se ha consolidado en las últimas décadas como un elemento estructural de las políticas de seguridad pública. Lo que en sus inicios se concibió como un apoyo puntual a la prevención y a la investigación del delito, fundamentalmente a través de cámaras fijas instaladas en espacios

concretos, ha evolucionado hacia sistemas cada vez más complejos y tecnológicamente avanzados, capaces de ampliar de forma significativa el alcance de la vigilancia. En este proceso, la incorporación de drones en el ámbito policial supone un cambio cualitativo relevante, al permitir una observación más flexible, móvil y adaptada a contextos operativos diversos.

No obstante, este desarrollo tecnológico no siempre ha ido acompañado de una reflexión proporcional sobre sus implicaciones jurídicas y éticas. En el ámbito policial, la adopción de nuevas herramientas suele estar impulsada por su potencial operativo, como la mejora de la visión del terreno, el acceso a zonas de difícil alcance o el refuerzo de la seguridad en intervenciones complejas. Sin embargo, estas ventajas deben ser analizadas conjuntamente con el impacto que dichas prácticas pueden tener sobre derechos fundamentales, en particular el derecho a la intimidad y la protección de los datos personales. Existe así el riesgo de que la tecnología se integre en la práctica policial de forma progresiva y normalizada, sin un análisis crítico suficiente sobre los límites que deben regir su uso.

Desde esta perspectiva, el objetivo general del trabajo no consiste en determinar si la videovigilancia policial es intrínsecamente positiva o negativa, sino en examinar bajo qué condiciones puede considerarse legítima dentro de un Estado social y democrático de Derecho. Para ello, resulta necesario analizar tanto el marco normativo que regula estas prácticas como la manera en que dicho marco se traduce en la actuación cotidiana de las Fuerzas y Cuerpos de Seguridad, donde intervienen factores como la urgencia de la intervención, el margen de discrecionalidad policial y el grado de formación especializada del personal.

Asimismo, el trabajo sitúa al agente policial en el centro de la reflexión, no como un mero operador de dispositivos tecnológicos, sino como un garante directo de los derechos fundamentales. Las decisiones que se adoptan en el ejercicio diario de la función policial, como la activación de un dron, la finalidad de la grabación o el tratamiento posterior de las imágenes obtenidas, poseen una relevancia jurídica y ética que trasciende el plano puramente técnico. En este sentido, la experiencia profesional se incorpora al análisis como una fuente de conocimiento aplicada que permite contrastar la regulación vigente con la realidad operativa.

En definitiva, este Trabajo Fin de Grado tiene como finalidad contribuir a una comprensión más equilibrada y responsable de la videovigilancia policial, entendida no solo como un instrumento de eficacia operativa, sino como una práctica institucional que debe desenvolverse dentro de límites claros y principios bien definidos. Solo desde este

enfoque resulta posible avanzar hacia un modelo de videovigilancia legítimo, proporcionado y compatible con una concepción garantista y humana de la seguridad pública.

3.2 Objetivos específicos.

A partir del objetivo general planteado, este Trabajo Fin de Grado se articula en torno a una serie de objetivos específicos que permiten concretar el análisis y orientar de manera sistemática el desarrollo de la investigación. Estos objetivos buscan descomponer el planteamiento general en ámbitos de estudio más delimitados, facilitando así la coherencia entre el marco teórico, la metodología empleada y los resultados obtenidos.

En primer lugar, se pretende **analizar la evolución tecnológica** de la videovigilancia policial, identificando los principales cambios que han marcado su desarrollo desde los sistemas tradicionales de cámaras fijas hasta la incorporación de dispositivos móviles y plataformas aéreas no tripuladas. Este objetivo permite contextualizar el uso actual de la videovigilancia y comprender cómo el avance tecnológico ha ampliado progresivamente las capacidades de observación y control en el ámbito policial.

En segundo lugar, se establece como objetivo **examinar el marco jurídico** que regula la videovigilancia policial y el uso de drones, prestando especial atención a los principios que deben regir la actuación de las Fuerzas y Cuerpos de Seguridad, tales como la legalidad, la necesidad, la proporcionalidad y la minimización de datos. El análisis normativo resulta esencial para determinar los límites formales dentro de los cuales puede desarrollarse una actuación legítima.

Asimismo, se plantea como objetivo **evaluar el impacto** de la videovigilancia sobre los derechos fundamentales, con especial referencia al derecho a la intimidad y a la protección de datos personales. Este análisis permite valorar en qué medida las prácticas de vigilancia pueden afectar a la esfera privada de la ciudadanía y cuáles son los riesgos asociados a un uso extensivo o poco controlado de estas tecnologías.

Otro de los objetivos específicos consiste en **analizar experiencias y modelos comparados**, tanto a nivel internacional como nacional, con el propósito de identificar buenas prácticas, carencias y contradicciones en la regulación y aplicación de la

videovigilancia policial. La comparación entre distintos contextos permite enriquecer el análisis y extraer conclusiones que trasciendan el ámbito estrictamente local.

Igualmente, se persigue valorar la utilidad operativa real de la videovigilancia aérea mediante drones, atendiendo a su aplicación en situaciones concretas de seguridad pública, prevención del delito o apoyo a intervenciones policiales. Este objetivo se apoya tanto en el estudio de casos como en la experiencia profesional acumulada, entendida como un elemento que aporta una visión práctica y contextualizada del fenómeno analizado.

Por último, se establece como objetivo reflexionar sobre la dimensión ética del uso de la videovigilancia policial, poniendo el foco en la responsabilidad del agente y en la necesidad de integrar criterios de prudencia, transparencia y respeto a los derechos fundamentales en la toma de decisiones operativas. A partir de esta reflexión, el trabajo aspira a formular propuestas de mejora y recomendaciones orientadas a una utilización más legítima, proporcionada y socialmente aceptable de la videovigilancia en el ámbito policial.

3.3 Hipótesis de partida.

La hipótesis de partida de este Trabajo Fin de Grado sostiene que el desarrollo y la implantación de la videovigilancia policial, y de manera especialmente relevante el uso de drones como herramienta de captación de imágenes, han avanzado a un ritmo superior al de la construcción de un marco integral que combine protocolos operativos claros, sistemas de control efectivos y una reflexión ética plenamente incorporada a la práctica policial. Esta carencia conjunta genera un escenario en el que la tecnología se integra con rapidez, mientras que los criterios que deberían orientar su uso responsable permanecen insuficientemente definidos.

Desde el plano operativo, la videovigilancia ofrece ventajas evidentes para la gestión de la seguridad pública, la prevención del delito y el apoyo a intervenciones complejas. No obstante, la hipótesis plantea que estas ventajas se ven acompañadas de riesgos relevantes cuando no existen protocolos detallados que regulen aspectos esenciales como los supuestos de activación, los límites espaciales y temporales de la vigilancia, el tratamiento posterior de las imágenes o los criterios de cancelación y destrucción de datos. En ausencia de estas directrices, la utilización de la tecnología queda excesivamente condicionada por prácticas informales o por decisiones individuales, lo que dificulta una aplicación homogénea y garantista.

A esta falta de protocolos se suma la insuficiencia de mecanismos de control y supervisión, tanto internos como externos. La hipótesis sostiene que la debilidad de los sistemas de fiscalización impide verificar de forma sistemática si el uso de la videovigilancia se ajusta a los principios de necesidad y proporcionalidad. Incluso cuando las actuaciones persiguen fines legítimos, la ausencia de controles visibles y efectivos favorece la normalización de prácticas de vigilancia que pueden resultar difíciles de justificar desde el punto de vista jurídico y social.

Junto a estas carencias normativas y organizativas, el trabajo parte de la idea de que existe también un déficit ético en la integración de la videovigilancia policial. La hipótesis plantea que la ética suele quedar relegada a un plano secundario, tratada como un elemento abstracto o meramente declarativo, sin una traducción real en la toma de decisiones operativas. La falta de espacios de reflexión ética, de formación específica y de criterios compartidos sobre el impacto social de la vigilancia tecnológica contribuye a que el uso de estas herramientas se valore principalmente en términos de eficacia, dejando en segundo plano su repercusión sobre la dignidad, la privacidad y la confianza ciudadana.

Esta situación sitúa al agente policial en una posición especialmente compleja. En ausencia de protocolos claros, controles efectivos y referencias éticas sólidas, la responsabilidad recae de forma desproporcionada sobre el criterio individual del operador. La hipótesis de partida asume que este escenario incrementa la inseguridad jurídica, favorece decisiones dispares ante situaciones similares y dificulta la construcción de una cultura profesional basada en la prudencia y la rendición de cuentas.

Por último, la hipótesis sostiene que la falta de una integración efectiva entre técnica, control y ética institucional debilita la legitimidad del uso de la videovigilancia policial. Cuando la ciudadanía percibe que estas tecnologías se emplean sin reglas claras, sin supervisión suficiente y sin una reflexión ética visible, incluso los usos legítimos pueden interpretarse como formas de vigilancia excesiva. En consecuencia, el trabajo parte de la idea de que el verdadero reto no reside únicamente en disponer de tecnología avanzada, sino en dotarla de **principios éticos operativos, controles efectivos y protocolos claros** que permitan un uso verdaderamente legítimo y compatible con un modelo garantista y humano de la seguridad pública.

3.4 Hipótesis específicas.

A partir de la hipótesis de partida, este Trabajo Fin de Grado formula una serie de hipótesis específicas destinadas a analizar de manera detallada los factores que influyen en el uso de la videovigilancia policial y, de forma particular, en la utilización de drones como herramienta de captación de imágenes. Estas hipótesis se construyen desde una perspectiva integral, que combina el análisis jurídico, organizativo, ético, operativo y social, con el objetivo de evaluar no solo la eficacia técnica del recurso, sino también su legitimidad democrática y su impacto en la relación entre policía y ciudadanía.

Hipótesis específica 1. Protocolos operativos insuficientes y aplicación desigual

Se plantea que la inexistencia o insuficiente desarrollo de protocolos operativos claros, detallados y homogéneos provoca una aplicación desigual de la videovigilancia policial. En la práctica cotidiana, esta carencia se traduce en que aspectos fundamentales de la actuación, como los supuestos que justifican la activación de un sistema de grabación, el alcance espacial de la vigilancia, su duración temporal o los criterios para la conservación y destrucción de las imágenes, quedan excesivamente abiertos a la interpretación individual del personal o a pautas informales consolidadas en cada unidad. Esta situación dificulta la aplicación uniforme de los principios de necesidad y proporcionalidad, incrementa la discrecionalidad operativa y genera un marco de actuación poco previsible, tanto para los profesionales como para la ciudadanía, lo que debilita la seguridad jurídica y la coherencia institucional.

Hipótesis específica 2. Debilidad de los mecanismos de control y supervisión

La hipótesis sostiene que la insuficiencia de mecanismos efectivos de control y supervisión limita de manera significativa la capacidad institucional para garantizar un uso responsable y ajustado de la videovigilancia policial. La ausencia de procedimientos sistemáticos de revisión, auditorías periódicas, controles externos o sistemas claros de trazabilidad de las actuaciones dificulta verificar si cada intervención concreta responde a una finalidad legítima y proporcionada. Esta debilidad estructural no implica necesariamente la existencia de usos abusivos intencionados, pero sí favorece dinámicas de normalización del recurso tecnológico y reduce la capacidad de detectar desviaciones, corregir prácticas inadecuadas y ofrecer una rendición de cuentas clara ante la ciudadanía y los órganos de control.

Hipótesis específica 3. Subordinación del criterio ético a la eficacia operativa

En contextos policiales caracterizados por la urgencia, la presión del servicio y la necesidad de respuesta inmediata, se plantea que la reflexión ética tiende a quedar

subordinada a criterios de eficacia operativa. La hipótesis sostiene que, en ausencia de una ética aplicada integrada en la práctica profesional, la activación de sistemas de videovigilancia puede convertirse en una decisión rutinaria o preventiva, adoptada por inercia o por simple disponibilidad tecnológica, más que como resultado de una valoración consciente del impacto sobre los derechos fundamentales. La falta de formación específica, de espacios de reflexión y de referencias éticas compartidas contribuye a que la ética se perciba como un elemento teórico o abstracto, desconectado de la toma de decisiones reales en el ámbito operativo.

Hipótesis específica 4. Mayor intrusividad percibida en el uso de drones

Se plantea que el empleo de drones introduce un nivel adicional de intrusividad percibida respecto a otros sistemas de videovigilancia policial. Su movilidad, capacidad de aproximación, versatilidad técnica y posibilidad de operar desde ángulos no habituales generan una sensación de vigilancia más intensa y menos predecible para la ciudadanía. La hipótesis sostiene que esta percepción de intrusividad se incrementa cuando el uso del dron no va acompañado de límites visibles, explicaciones claras o criterios de actuación transparentes. En estos casos, incluso intervenciones con una finalidad legítima pueden ser interpretadas como formas de control excesivo, afectando negativamente a la confianza social en la actuación policial.

Hipótesis específica 5. Brecha entre potencial técnico y utilidad real

El trabajo plantea la existencia de una brecha relevante entre el potencial técnico atribuido a la videovigilancia policial y su utilidad real en términos de prevención del delito, apoyo a la investigación o eficacia probatoria. La hipótesis sostiene que, en determinados contextos, la implantación de estos sistemas responde más a procesos de modernización institucional, presión tecnológica o expectativas políticas que a un análisis riguroso de la necesidad real del recurso y de los beneficios contrastables que aporta. Esta sobrevaloración del potencial tecnológico puede conducir a un uso extensivo que no siempre se traduce en mejoras efectivas de la seguridad ciudadana y que, en cambio, incrementa los riesgos asociados a la afectación de derechos fundamentales.

Hipótesis específica 6. Influencia de la formación y del criterio profesional

Se sostiene que la legitimidad del uso de la videovigilancia policial depende en gran medida del nivel de formación especializada del personal operador, de su conocimiento del marco jurídico aplicable y de su capacidad de juicio profesional. Una formación adecuada permite comprender los límites legales, interiorizar criterios éticos y adoptar

decisiones ajustadas a los principios de minimización, focalización y proporcionalidad. Por el contrario, una capacitación insuficiente o desigual incrementa la inseguridad jurídica, amplía el margen de error y favorece actuaciones discutibles que pueden comprometer tanto la eficacia operativa como la confianza ciudadana. La hipótesis subraya que la tecnología no es neutra y que su uso responsable depende, en última instancia, del criterio de quien la opera.

Hipótesis específica 7. Protocolos, controles y ética como factores de legitimidad institucional

La hipótesis plantea que la implantación de protocolos claros, mecanismos de control efectivos y criterios éticos integrados en la práctica policial no solo no reduce la eficacia operativa de la videovigilancia, sino que contribuye a reforzar su legitimidad institucional. Un modelo basado en reglas claras, supervisión, trazabilidad y rendición de cuentas permite compatibilizar el uso de tecnologías avanzadas con el respeto a los derechos fundamentales. Además, este enfoque favorece una actuación más coherente, protege al profesional frente a la inseguridad jurídica y fortalece la sostenibilidad del recurso a medio y largo plazo.

Hipótesis específica 8. Percepción ciudadana y confianza institucional

Finalmente, se sostiene que la percepción ciudadana del uso de la videovigilancia policial constituye un elemento central para su legitimidad social. Incluso cuando una actuación se ajusta formalmente a la legalidad, la falta de información accesible, transparencia y controles visibles puede generar desconfianza, sensación de vigilancia permanente o resignación social. La hipótesis plantea que la aceptación ciudadana de estas tecnologías no depende únicamente de su eficacia, sino de la percepción de que existen límites claros, garantías reales y un compromiso ético por parte de la institución policial. Cuando estos elementos son visibles, la confianza institucional se refuerza y la videovigilancia es percibida como una herramienta al servicio de la seguridad colectiva y no como un mecanismo de control indiscriminado.

4. Metodología

4.1 Enfoque y diseño de la investigación

El presente Trabajo Fin de Grado se fundamenta en un **enfoque metodológico cualitativo**, de carácter descriptivo, analítico y crítico, adecuado para el estudio de un fenómeno complejo y multidimensional como es el uso de la videovigilancia policial. La

elección de este enfoque responde a la naturaleza del objeto de estudio, que no puede ser comprendido de forma adecuada mediante la simple cuantificación de datos, sino que requiere un análisis interpretativo capaz de integrar dimensiones jurídicas, organizativas, éticas, operativas y sociales que se encuentran estrechamente interrelacionadas.

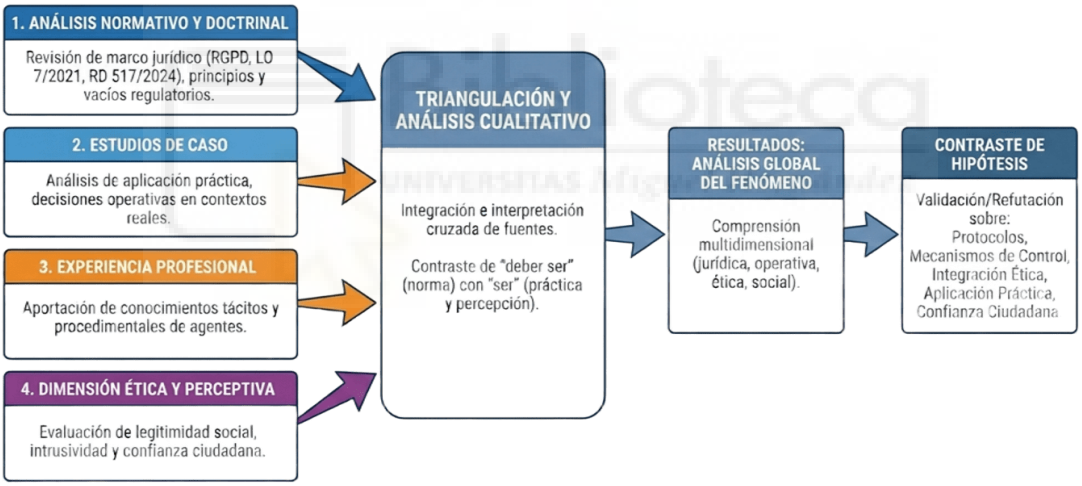
El objetivo principal de la investigación no es la comprobación empírica de hipótesis en términos estadísticos, sino su **contraste razonado y fundamentado**, atendiendo al contenido normativo, a las prácticas institucionales y a los criterios de actuación que rigen el uso de la videovigilancia policial. Las hipótesis formuladas en este trabajo plantean cuestiones relativas a la existencia de protocolos, la suficiencia de los mecanismos de control, la integración del componente ético, la aplicación práctica de la normativa y la percepción ciudadana de la vigilancia tecnológica. Todas estas cuestiones se sitúan en un plano cualitativo, ya que no dependen tanto de la frecuencia de uso de la tecnología como de **cómo, por qué y bajo qué condiciones se emplea**. Por este motivo, un enfoque cuantitativo resultaría insuficiente para captar la complejidad del fenómeno analizado, mientras que el enfoque cualitativo permite examinar los significados, las decisiones y las consecuencias asociadas al uso de la videovigilancia en contextos reales.

El diseño de la investigación se articula como un estudio documental y aplicado, estructurado en varias fases interrelacionadas. En una primera fase, se lleva a cabo un análisis del marco normativo y doctrinal que regula la videovigilancia policial y el uso de drones, con el objetivo de identificar los principios jurídicos que deben orientar la actuación policial, así como los posibles vacíos, ambigüedades o insuficiencias regulatorias. Esta fase resulta esencial para contrastar las hipótesis relativas a la falta de protocolos operativos claros, la debilidad de los mecanismos de control y la distancia existente entre el desarrollo tecnológico y su adaptación normativa.

En una segunda fase, el diseño incorpora el análisis de la aplicación práctica de la videovigilancia a través de estudios de caso y de la experiencia profesional. Este nivel de análisis permite observar cómo los principios normativos se traducen, o no, en decisiones operativas concretas, y hasta qué punto factores como la urgencia del servicio, la disponibilidad tecnológica o la formación del personal influyen en la activación y el uso de estos sistemas. De este modo, se pueden contrastar hipótesis relacionadas con la aplicación desigual de la videovigilancia, la carga de responsabilidad que recae sobre el agente y la subordinación del criterio ético a la eficacia operativa.

Asimismo, el diseño metodológico incorpora de manera explícita una dimensión ética y perceptiva, orientada a analizar tanto los procesos de toma de decisiones dentro de la organización policial como la percepción social del uso de la videovigilancia. Esta dimensión resulta clave para abordar hipótesis vinculadas a la legitimidad del recurso, la intrusividad percibida, especialmente en el uso de drones, y la influencia de la confianza ciudadana en la aceptación de estas tecnologías. El análisis ético se concibe como un componente transversal que atraviesa todas las fases de la investigación, y no como un apartado aislado o meramente teórico.

En conjunto, el diseño de la investigación se concibe como un proceso progresivo, coherente e integrado, en el que cada técnica metodológica empleada responde a una finalidad concreta y se vincula directamente con una o varias hipótesis específicas. Esta coherencia interna permite que la metodología no se limite a describir las fuentes utilizadas, sino que justifique de manera razonada su elección y su contribución al análisis global del fenómeno estudiado.



Fuente: elaboración propia

Grafico 2. Diseño del método de investigación.

4.2 Revisión documental y análisis normativo

La revisión documental y el análisis normativo constituyen uno de los pilares metodológicos de este Trabajo Fin de Grado, al tratarse de un estudio que examina el uso de la videovigilancia policial desde una perspectiva jurídica y garantista. Esta fase metodológica se orienta a contrastar las hipótesis relacionadas con la insuficiencia de protocolos operativos, la debilidad de los mecanismos de control y supervisión, la integración limitada del componente ético y la distancia existente entre el desarrollo tecnológico y su adaptación normativa.

El análisis normativo se ha centrado en el estudio sistemático del marco jurídico que regula la videovigilancia policial y el uso de drones, tanto en el ámbito europeo como en el nacional. No se ha limitado a una descripción literal de las normas, sino que ha atendido especialmente a los principios que las inspiran, como la legalidad, la necesidad, la proporcionalidad, la minimización de datos, la transparencia y la rendición de cuentas. Este enfoque permite identificar no solo qué está formalmente regulado, sino también qué aspectos quedan abiertos a interpretación o presentan lagunas relevantes desde el punto de vista de la protección de los derechos fundamentales.

La revisión documental ha incluido igualmente el análisis de doctrina jurídica, estudios académicos, informes institucionales y literatura especializada sobre videovigilancia, tecnologías de control y derechos fundamentales. Esta revisión ha resultado fundamental para contextualizar el debate teórico y empírico existente en torno a la eficacia real de la videovigilancia, los riesgos asociados a su normalización y la importancia de los controles y garantías en su aplicación práctica. A través de estas fuentes, se ha podido contrastar la hipótesis relativa a la brecha entre el potencial técnico atribuido a estas herramientas y su utilidad real, así como aquellas vinculadas a la percepción social y a la legitimidad institucional.

Un aspecto central del análisis normativo ha sido la identificación del grado de concreción de las normas en materia de **protocolos operativos y mecanismos de control**. Se ha prestado especial atención a la existencia, o ausencia, de directrices claras sobre los supuestos de activación de los sistemas de videovigilancia, los límites espaciales y temporales de la captación de imágenes, el tratamiento posterior de los datos obtenidos y los procedimientos de supervisión. Este análisis permite evaluar hasta qué punto el marco jurídico proporciona pautas suficientes para una actuación homogénea y garantista, o si, por el contrario, traslada un amplio margen de discrecionalidad al nivel operativo.

Asimismo, la revisión documental ha permitido incorporar una **dimensión ética** al análisis normativo, examinando en qué medida las normas y los documentos institucionales integran referencias explícitas a principios éticos o a criterios de responsabilidad en el uso de tecnologías de vigilancia. Esta aproximación resulta clave para contrastar la hipótesis según la cual la ética suele quedar relegada a un plano secundario, sin una traducción efectiva en protocolos y prácticas concretas.

En conjunto, la revisión documental y el análisis normativo han servido como base para establecer un marco de referencia sólido desde el que evaluar la aplicación práctica de la videovigilancia policial. Esta fase metodológica no solo permite identificar avances y

carencias en la regulación vigente, sino que proporciona los criterios necesarios para interpretar críticamente los estudios de caso, la experiencia profesional y los resultados que se presentan en los capítulos posteriores.

4.3 Experiencia profesional como piloto de drones.

Mi experiencia profesional como piloto de drones en el ámbito policial constituye una de las bases metodológicas de este Trabajo Fin de Grado. No se trata de un elemento accesorio ni de un relato autobiográfico, sino de una fuente de conocimiento aplicada que me permite analizar el uso de la videovigilancia aérea desde dentro, contrastando de manera directa el marco normativo, los principios teóricos y la realidad operativa cotidiana.

A lo largo de mi trayectoria profesional, he participado de forma activa en la planificación y ejecución de vuelos policiales con drones en distintos contextos operativos, lo que me ha permitido observar cómo se toman realmente las decisiones relacionadas con la activación de estos sistemas. En la práctica diaria, el uso del dron no responde únicamente a criterios técnicos o normativos, sino que se ve condicionado por factores como la urgencia de la intervención, la presión del servicio, la coordinación con otras unidades, la disponibilidad de medios y, en muchas ocasiones, la ausencia de protocolos suficientemente detallados que orienten la actuación con claridad. Esta realidad operativa constituye un punto de partida fundamental para contrastar las hipótesis planteadas en este trabajo, especialmente aquellas relativas a la aplicación desigual de la videovigilancia y a la falta de estandarización de criterios.

Desde mi experiencia como piloto, he podido constatar que buena parte de las decisiones clave sobre el uso del dron recaen directamente sobre el operador en tiempo real. Decisiones como cuándo resulta realmente necesario desplegar el dispositivo, qué espacio debe ser observado, durante cuánto tiempo debe mantenerse la vigilancia o qué tipo de imágenes resulta legítimo captar no siempre cuentan con una respuesta clara en la normativa o en los documentos internos. En este contexto, el criterio profesional, la formación previa y la experiencia acumulada adquieren un peso determinante, lo que pone de manifiesto la carga de responsabilidad que asume el agente cuando los marcos procedimentales son imprecisos o incompletos.

Esta experiencia directa me ha permitido identificar de forma clara la **distancia existente entre la norma y la práctica**. Si bien el marco jurídico establece principios generales como la proporcionalidad, la necesidad o la minimización de datos, su

traducción en decisiones operativas concretas no siempre resulta sencilla. En muchas situaciones reales, la actuación se desarrolla en escenarios cambiantes, con información incompleta y bajo una presión temporal considerable, lo que obliga al operador a interpretar esos principios de forma inmediata. Esta circunstancia refuerza la hipótesis de que, en ausencia de protocolos claros y controles efectivos, el margen de discrecionalidad aumenta y con él la inseguridad jurídica.

Mi experiencia profesional también ha sido determinante para analizar la dimensión ética del uso de la videovigilancia aérea. En la práctica policial cotidiana, la ética no siempre aparece formalizada en procedimientos escritos ni integrada de manera explícita en la toma de decisiones. Con frecuencia, la reflexión ética queda vinculada a la sensibilidad individual del agente y a la cultura profesional de la unidad. Decidir si una captación de imágenes es estrictamente necesaria, si puede afectar de forma desproporcionada a la privacidad de terceros o si existen alternativas menos intrusivas son cuestiones que, en muchos casos, se resuelven sobre el terreno, sin un respaldo ético institucional claramente definido. Esta vivencia directa refuerza la hipótesis relativa a la subordinación del componente ético frente a criterios de eficacia inmediata.

Asimismo, el ejercicio profesional como piloto de drones me ha permitido observar de primera mano la **reacción y percepción de la ciudadanía** ante el uso de estos dispositivos. La presencia de un dron en un espacio público genera un impacto visual evidente y provoca respuestas diversas, que van desde la sensación de mayor seguridad hasta la incomodidad o el rechazo. He podido comprobar que estas reacciones no siempre guardan relación con la legalidad de la actuación, sino con la forma en que el uso del dron se percibe, se comunica y se contextualiza. La falta de información visible o de explicaciones claras puede alimentar una sensación de vigilancia excesiva, incluso cuando la intervención tiene una finalidad legítima.

En conjunto, mi experiencia profesional como piloto de drones se integra en este trabajo como un instrumento metodológico de contraste crítico, que permite enriquecer el análisis normativo y teórico con una visión realista y contextualizada del uso de la videovigilancia aérea. Lejos de restar objetividad, esta aproximación aporta profundidad analítica y credibilidad al estudio, al evidenciar cómo las carencias en protocolos, controles y formación ética se traducen en tensiones reales en la práctica policial. Esta perspectiva resulta esencial para comprender los retos actuales de la videovigilancia policial y para formular propuestas de mejora ajustadas a la realidad operativa.

4.4 Estudios de casos y encuestas

El análisis de estudios de caso constituye un elemento central dentro de la metodología de este Trabajo Fin de Grado, al permitir contrastar las hipótesis planteadas a partir de **situaciones concretas y experiencias reales** en las que se ha aplicado la videovigilancia policial. Este enfoque resulta especialmente adecuado para un objeto de estudio que no puede comprenderse únicamente desde la norma o la teoría, sino que exige observar cómo se utilizan estas herramientas en contextos específicos y qué consecuencias prácticas generan.

Los estudios de caso seleccionados, tanto a nivel internacional como nacional, se han empleado como una herramienta analítica que permite identificar patrones de actuación, similitudes y diferencias en el uso de la videovigilancia, así como los efectos derivados de la existencia o ausencia de protocolos claros, mecanismos de control y criterios éticos explícitos. A través de estos casos, se ha podido contrastar especialmente las hipótesis relacionadas con la aplicación desigual de la videovigilancia, la brecha entre el potencial técnico y su utilidad real, y el impacto del uso de drones en la percepción ciudadana.

El análisis comparado de experiencias internacionales resulta útil para observar cómo distintos países han abordado la regulación y el uso operativo de la videovigilancia policial, identificando modelos más estructurados, con mayores niveles de control y supervisión, frente a otros más flexibles o fragmentados. Esta comparación permite contextualizar la situación nacional y valorar hasta qué punto determinadas carencias no son exclusivas de un ámbito concreto, sino que forman parte de un debate más amplio sobre la incorporación de tecnologías de vigilancia en sociedades democráticas.

En el ámbito nacional, los estudios de caso permiten descender a un nivel más próximo a la realidad operativa, analizando situaciones concretas en las que la videovigilancia ha sido utilizada con fines de prevención, control de espacios públicos, gestión de eventos o apoyo a intervenciones policiales. Estos casos resultan especialmente relevantes para contrastar las hipótesis relativas a la falta de estandarización, a la carga de responsabilidad que recae sobre el agente y a la influencia de la formación y del criterio profesional en la toma de decisiones.

El uso combinado de estudios de caso y encuestas permite, por tanto, contrastar de manera sólida las hipótesis relacionadas con la legitimidad social de la videovigilancia policial. No se trata únicamente de evaluar si una actuación es legal o técnicamente eficaz, sino de analizar cómo es percibida y qué efectos tiene sobre la confianza institucional. Este enfoque refuerza la idea de que la eficacia operativa no puede desvincularse de la percepción ciudadana ni de la existencia de garantías visibles.

En conjunto, los estudios de casos y las encuestas se integran en la metodología como instrumentos de contraste empírico cualitativo, que permiten observar cómo las carencias normativas, la falta de protocolos, la debilidad de los controles y la escasa integración del componente ético se manifiestan en situaciones reales. Esta aproximación aporta profundidad al análisis y refuerza la coherencia entre las hipótesis formuladas, la metodología empleada y los resultados que se expondrán en el capítulo siguiente.

4.5 Limitaciones del estudio

Como todo trabajo de investigación, el presente Trabajo Fin de Grado presenta una serie de limitaciones que deben ser tenidas en cuenta a la hora de interpretar sus resultados y conclusiones. La identificación explícita de estas limitaciones no pretende restar valor al estudio, sino situarlo con claridad dentro de su alcance real y de las posibilidades metodológicas disponibles.

En primer lugar, la adopción de un enfoque cualitativo implica que las conclusiones obtenidas no pueden generalizarse en términos estadísticos al conjunto de las Fuerzas y Cuerpos de Seguridad ni a todos los contextos territoriales. El trabajo no persigue medir la frecuencia de uso de la videovigilancia ni cuantificar su impacto de forma empírica, sino analizar críticamente las condiciones, los límites y las implicaciones de su utilización. Esta limitación resulta coherente con los objetivos planteados y con la naturaleza jurídica, ética y operativa del objeto de estudio.

En segundo lugar, el análisis se apoya en una revisión documental, normativa y de estudios de caso, así como en la experiencia profesional del autor, sin incorporar un trabajo de campo propio basado en encuestas o entrevistas directas a ciudadanos o profesionales. Si bien esta circunstancia limita la posibilidad de recoger datos primarios, se ha optado por integrar testimonios y entrevistas procedentes de fuentes secundarias contrastadas, lo que permite abordar la dimensión perceptiva y social de la videovigilancia sin desvirtuar el enfoque del trabajo.

Otra limitación relevante deriva de la heterogeneidad normativa y organizativa existente en el uso de la videovigilancia policial. Las diferencias entre países, cuerpos policiales y contextos locales dificultan la formulación de conclusiones plenamente homogéneas. No obstante, esta diversidad ha sido asumida como parte del objeto de estudio, permitiendo precisamente identificar contradicciones, carencias y buenas prácticas a través del análisis comparado.

Asimismo, la incorporación de la experiencia profesional del autor como piloto de drones introduce una perspectiva interna que, si bien aporta un valor añadido evidente al análisis, puede estar condicionada por el contexto concreto en el que se ha desarrollado dicha experiencia. Para minimizar este riesgo, dicha experiencia se ha utilizado con un enfoque reflexivo y crítico, contrastándola de forma sistemática con la normativa vigente, la literatura académica y los estudios de caso analizados.

Por último, debe tenerse en cuenta que el marco normativo y tecnológico en materia de videovigilancia y drones se encuentra en constante evolución, lo que implica que algunas conclusiones pueden verse afectadas por futuras modificaciones legales o por el desarrollo de nuevas capacidades técnicas. Esta circunstancia no invalida el análisis realizado, pero sí pone de manifiesto la necesidad de entender este trabajo como una aportación situada en un momento concreto, abierta a futuras líneas de investigación y actualización.

En conjunto, estas limitaciones no comprometen la coherencia interna ni la validez del estudio, sino que delimitan con precisión su alcance y refuerzan la honestidad metodológica del trabajo. Al mismo tiempo, permiten identificar posibles vías de ampliación y profundización que podrían abordarse en investigaciones posteriores.

5. Análisis y resultados

El presente capítulo expone los resultados obtenidos a partir del análisis de estudios de caso y situaciones reales en las que se ha aplicado la videovigilancia policial, tanto en el ámbito internacional como en el nacional. Estos resultados no se presentan como una mera descripción de experiencias, sino como un **contraste analítico de las hipótesis específicas** formuladas en el capítulo 7, a la luz de los criterios metodológicos establecidos en el capítulo 8.

El análisis de estos casos permite identificar patrones recurrentes, avances significativos, carencias estructurales y contradicciones en la aplicación práctica de la videovigilancia policial. En particular, los resultados obtenidos ofrecen evidencias relevantes en relación con la falta de protocolos operativos claros, la debilidad de los mecanismos de control y supervisión, la subordinación del componente ético a la urgencia operativa, la brecha entre el potencial técnico atribuido a estas herramientas y su utilidad real, así como la influencia determinante de la percepción ciudadana en la legitimidad del recurso.

Con el fin de facilitar una lectura ordenada y coherente, los resultados se presentan en dos bloques principales. En primer lugar, se exponen los resultados derivados del análisis comparado internacional, que permiten situar el caso español en un contexto más amplio y observar cómo distintos países han afrontado los retos asociados a la videovigilancia policial. En segundo lugar, se analizan casos nacionales, más próximos a la realidad operativa, que permiten profundizar en la aplicación práctica de estas tecnologías y en las dinámicas reales de toma de decisiones. Finalmente, se ofrece una síntesis de los principales hallazgos en relación con las hipótesis planteadas.

5.1 Análisis y resultados comparados del ámbito internacional del uso de la videovigilancia policial

5.1.1 Caso 1: Reino Unido

El caso del Reino Unido resulta especialmente relevante para este trabajo porque permite analizar un modelo de videovigilancia policial altamente consolidado y normalizado en el espacio público. Desde hace décadas, el uso extensivo de sistemas de CCTV forma parte de las políticas ordinarias de seguridad urbana, hasta el punto de constituir una infraestructura permanente en ciudades y municipios. Este contexto convierte al modelo británico en un referente idóneo para examinar los efectos reales de la videovigilancia cuando deja de ser una medida excepcional y se integra como una herramienta cotidiana de control y prevención (College of Policing, 2015).

Lejos de ofrecer una respuesta simple, la experiencia británica muestra un escenario complejo, en el que la utilidad operativa de la videovigilancia convive con limitaciones estructurales, tensiones éticas y debates persistentes sobre su legitimidad social. Precisamente por ello, este caso permite contrastar de forma directa varias de las hipótesis del trabajo, especialmente las relativas a la brecha entre potencial técnico y utilidad real, la necesidad de protocolos y controles internos, y la influencia de la percepción ciudadana.

A) Eficacia real del CCTV y dependencia del contexto

Uno de los resultados más consistentes del caso británico es que la eficacia del CCTV en la reducción del delito es limitada y altamente dependiente del contexto. Las evaluaciones institucionales y los estudios de síntesis coinciden en que su impacto no es uniforme ni automático, sino condicionado por factores operativos y ambientales. La evidencia empírica muestra mejores resultados en delitos contra la propiedad, especialmente en espacios cerrados o semi-cerrados como aparcamientos, donde la

vigilancia actúa como elemento disuasorio y facilita la identificación posterior. Por el contrario, el impacto es mucho más reducido en delitos violentos o impulsivos, que suelen producirse sin una evaluación racional del riesgo de ser observado (College of Policing, 2015; Piza et al., 2019).

Asimismo, el entorno físico y social resulta determinante. El CCTV tiende a ser más eficaz en espacios delimitados y con flujos previsibles, mientras que en entornos urbanos abiertos y complejos la capacidad disuasoria y probatoria disminuye de forma notable. A ello se suma la integración del sistema en la estrategia de seguridad: las cámaras generan resultados más consistentes cuando se combinan con monitorización activa, protocolos claros y capacidad de respuesta, y pierden eficacia cuando funcionan como un recurso pasivo de acumulación de imágenes (Piza et al., 2019).

B) De la captación de imágenes al valor operativo

El caso británico pone de relieve que la eficacia del CCTV depende en mayor medida de factores organizativos que de la tecnología en sí. Estudios clásicos muestran que muchos sistemas generan grandes volúmenes de imágenes con un valor operativo limitado si no existen procedimientos claros para su gestión, análisis y uso probatorio (Gill & Spriggs, 2005). La ausencia de protocolos sobre monitorización, selección de imágenes relevantes y coordinación con las unidades operativas reduce la capacidad preventiva del sistema y lo relega a un uso principalmente reactivo.

Estos hallazgos refuerzan las hipótesis del trabajo relativas a la importancia de la formación y del criterio profesional de los operadores. Incluso en un entorno con larga experiencia en CCTV, la utilidad del sistema sigue dependiendo de cómo se organiza su uso y de la capacidad para integrar la información visual en la toma de decisiones policiales.

C) Normalización de la vigilancia y necesidad de gobernanza

La normalización del CCTV en Reino Unido ha desplazado el debate desde la eficacia técnica hacia la gobernanza del sistema. Cuando la vigilancia se convierte en una presencia constante en el espacio público, la cuestión central pasa a ser cómo se controla, quién decide sobre su uso y qué garantías existen para evitar abusos o derivas funcionales. Este enfoque se refleja en la adopción y actualización del *Surveillance Camera Code of Practice*, que insiste en principios como finalidad legítima, proporcionalidad, transparencia y revisión periódica de la necesidad de las cámaras (Home Office, 2021).

Del mismo modo, los informes del *Biometrics and Surveillance Camera Commissioner* evidencian una preocupación institucional creciente por la rendición de cuentas, la supervisión independiente y la confianza pública (Biometrics and Surveillance Camera Commissioner, 2024). Estos elementos refuerzan la hipótesis de que la legitimidad de la videovigilancia no puede sostenerse solo en su legalidad formal o en su utilidad operativa.

D) Evolución tecnológica y riesgo de expansión funcional

La incorporación de analítica avanzada e inteligencia artificial ha reactivado debates que parecían parcialmente estabilizados. La ampliación de capacidades mediante reconocimiento de patrones o integración de bases de datos plantea nuevos interrogantes sobre los límites del sistema y el riesgo de expansión funcional. Estos desarrollos muestran cómo los marcos normativos y éticos pueden quedar rápidamente tensionados por la evolución tecnológica, intensificando además la percepción de vigilancia si no se acompaña de transparencia y garantías claras (London Borough of Hammersmith & Fulham, 2025).

Síntesis del caso de Reino Unido

En conjunto, el caso británico confirma que la eficacia del CCTV es limitada y contextual, lo que cuestiona enfoques basados en el despliegue masivo de tecnología sin una estrategia definida (College of Policing, 2015; Piza et al., 2019). Asimismo, evidencia que la utilidad real de la videovigilancia depende más de protocolos, procedimientos y formación que de la mera presencia de cámaras (Gill & Spriggs, 2005). Finalmente, muestra que la normalización de la vigilancia exige reforzar los mecanismos de gobernanza, control y rendición de cuentas para sostener la legitimidad social del sistema, especialmente ante el riesgo permanente de expansión funcional asociado a la evolución tecnológica.

5.1.2 Caso 2: Francia

El caso francés constituye un ejemplo especialmente ilustrativo para analizar el uso de drones policiales en un contexto democrático caracterizado por una **fuerte intervención del control judicial y constitucional**, así como por una progresiva construcción normativa específica. A diferencia del modelo británico, donde la videovigilancia terrestre se ha normalizado durante décadas, en Francia el despliegue de drones policiales ha seguido un recorrido más conflictivo y discontinuo, marcado por suspensiones judiciales, correcciones legislativas y una posterior expansión cuantitativa del uso.

Este recorrido convierte al modelo francés en un caso idóneo para contrastar varias de las hipótesis planteadas en este trabajo, en particular las relativas a la falta inicial de protocolos y controles, la centralidad del control externo, la tensión entre eficacia operativa y ética, y la percepción ciudadana ante la normalización de una herramienta altamente intrusiva.

A) Origen del conflicto: uso operativo sin base suficiente y reacción judicial

El punto de partida del caso francés se sitúa en el uso de drones por las fuerzas de seguridad durante el periodo de desconfinamiento derivado de la pandemia de COVID-19. En este contexto, la Prefectura de Policía de París empleó drones equipados con cámaras para vigilar el cumplimiento de las restricciones de movilidad. Esta práctica fue rápidamente impugnada y dio lugar a una decisión clave del Conseil d'État**,** que ordenó el cese del uso de drones al considerar que la captación de imágenes constituía un tratamiento de datos personales y que no existía una base legal suficiente ni garantías adecuadas para la protección de la vida privada (Conseil d'État, 2020).

Este primer resultado es especialmente relevante porque pone de manifiesto un patrón que se repite en otros contextos tecnológicos: la tecnología se despliega antes de que existan protocolos claros y un marco jurídico específico, lo que desplaza el ajuste hacia el control judicial a posteriori. En términos de las hipótesis del presente trabajo, este episodio confirma que la ausencia de reglas claras y controles previos incrementa la inseguridad jurídica y obliga a que sean los tribunales quienes delimiten los límites del uso legítimo.

B) Corrección constitucional del marco legal

Tras la intervención del Conseil d'État, el legislador francés intentó dotar de cobertura legal al uso de drones policiales a través de la denominada ley de "sécurité globale". Sin embargo, este intento de consolidación normativa fue parcialmente frenado por el Conseil constitutionnel, que declaró inconstitucionales varios preceptos al considerar que el legislador no había conciliado de forma suficientemente equilibrada las exigencias de seguridad con el respeto a la vida privada (Conseil constitutionnel, 2021).

En particular, el órgano constitucional reprochó la falta de delimitación clara de elementos esenciales como los supuestos de uso, la duración de las autorizaciones, los perímetros de vigilancia y el número de drones desplegables. Este segundo hito confirma que el problema no residía únicamente en la ausencia de ley, sino en la calidad normativa del marco propuesto. Para este trabajo, este episodio refuerza la hipótesis de

que la mera legalización formal de una tecnología no garantiza su legitimidad si no se acompaña de límites precisos y garantías efectivas.

C) Reconstrucción normativa

Tras estos correctivos, Francia consolidó un marco jurídico específico para el uso de drones policiales mediante su incorporación al Code de la sécurité intérieure, en los artículos L. 242-1 y siguientes, y su desarrollo reglamentario a través del Décret n° 2023-283, que regula las condiciones de tratamiento de las imágenes captadas por aeronaves utilizadas para misiones de policía administrativa (Décret n° 2023-283, 2023).

El elemento central de este modelo es la arquitectura formal de control, basada en varios niveles. En primer lugar, el uso de drones requiere una autorización escrita y motivada del prefecto, lo que introduce un control administrativo previo. En segundo lugar, se establecen límites materiales explícitos, como la prohibición de captar imágenes del interior de domicilios, la ausencia de captación de sonido y la limitación de la conservación de imágenes, generalmente fijada en un máximo de siete días salvo excepciones justificadas (CNIL, 2025; Vie-publique, 2023).

Desde el punto de vista de las hipótesis del presente trabajo, este resultado muestra un avance significativo en términos de control formal y protocolización. No obstante, también plantea una cuestión central que atraviesa todo el análisis: hasta qué punto estos controles se traducen en protocolos operativos efectivos, o si, por el contrario, tienden a convertirse en autorizaciones de carácter rutinario en determinados contextos, especialmente en manifestaciones y grandes eventos.

D) Normalización, litigios y tensión ética

Un resultado especialmente relevante del caso francés es que, una vez consolidado el marco normativo, el uso de drones policiales ha experimentado una rápida expansión cuantitativa. Datos recientes indican que en 2024 se concedieron más de 1.800 autorizaciones prefecturales para el uso de drones en todo el territorio francés, en contextos que incluyen manifestaciones, eventos multitudinarios y operaciones de seguridad preventiva (Le Monde, 2025).

Esta normalización operativa no ha eliminado, sin embargo, los conflictos jurídicos y éticos. En 2024 y 2025, diversos tribunales administrativos han suspendido autorizaciones concretas al apreciar deficiencias en la motivación, falta de acreditación de la inexistencia de medios menos intrusivos o delimitaciones excesivamente amplias

de los perímetros vigilados (Tribunal administratif d'Orléans, 2025). Estos pronunciamientos ponen de manifiesto que, incluso dentro de un marco legal aparentemente sólido, persisten problemas en la aplicación práctica de los principios de necesidad y proporcionalidad.

Desde una perspectiva ética y de percepción ciudadana, la expansión del uso de drones ha reactivado el debate sobre la normalización de la vigilancia aérea y su impacto sobre libertades como la de reunión y manifestación. La CNIL ha insistido de forma reiterada en la necesidad de transparencia, información al público y control efectivo para evitar que el uso de drones derive en una vigilancia sistemática incompatible con la confianza social (CNIL, 2025).

Síntesis analítica del caso francés

El análisis del caso francés permite extraer varios resultados relevantes para este trabajo.

-En primer lugar, confirma que el uso de drones policiales sin protocolos ni base legal clara conduce a una judicialización inmediata de la práctica (Conseil d'État, 2020).

-En segundo lugar, muestra que la legalización apresurada, sin delimitación precisa de garantías, resulta insuficiente desde el punto de vista constitucional (Conseil constitutionnel, 2021).

-En tercer lugar, evidencia que la construcción de una arquitectura formal de control representa un avance significativo, pero no elimina por sí sola los riesgos de uso rutinario y desproporcionado (Décret n° 2023-283, 2023; CNIL, 2025).

Finalmente, pone de relieve que la normalización cuantitativa del uso reabre de forma constante el debate ético y la preocupación ciudadana por la vigilancia aérea en el espacio público (Le Monde, 2025; Tribunal administratif d'Orléans, 2025).

5.1.3 Caso 3: Estados Unidos

El caso de Estados Unidos ofrece un escenario particularmente relevante para este Trabajo Fin de Grado debido a la **ausencia de un modelo nacional homogéneo de videovigilancia policial**. A diferencia del Reino Unido o Francia, donde existen marcos estatales relativamente coherentes, en Estados Unidos la regulación y el uso de tecnologías de vigilancia dependen de una compleja combinación de normas constitucionales, legislación estatal, ordenanzas municipales y políticas internas de cada departamento policial. Este modelo profundamente descentralizado convierte al

contexto estadounidense en un ejemplo paradigmático de los riesgos y oportunidades asociados a la expansión tecnológica sin una gobernanza uniforme (U.S. Department of Justice, Office of Legal Policy, 2024).

Este marco fragmentado permite contrastar con especial claridad varias de las hipótesis planteadas en este trabajo, en particular aquellas relativas a la aplicación desigual de la videovigilancia, la debilidad estructural de los controles, la priorización de la eficacia operativa sobre la reflexión ética y la influencia decisiva de la percepción ciudadana en la legitimidad institucional.

A) Eficacia real y resultados operativos: efectos heterogéneos y dependientes del contexto

Uno de los principales resultados que se desprenden del análisis del caso estadounidense es que los efectos de la videovigilancia policial son **altamente heterogéneos** y dependen de múltiples variables contextuales. La evidencia empírica disponible, especialmente en relación con las cámaras corporales y los sistemas de videovigilancia integrados, muestra resultados mixtos que impiden extraer conclusiones uniformes sobre su eficacia (National Institute of Justice, 2021).

En el caso de las cámaras corporales, diversos estudios han observado reducciones en las quejas ciudadanas y mejoras en la percepción de transparencia en determinados departamentos, mientras que otros análisis no detectan cambios significativos en variables clave como el uso de la fuerza o la criminalidad (National Institute of Justice, 2021). Estos resultados sugieren que la tecnología puede aportar beneficios concretos, pero solo cuando se inserta en un marco organizativo y procedimental adecuado.

Desde la perspectiva de este trabajo, estos hallazgos refuerzan la hipótesis de que la videovigilancia no genera efectos automáticos ni universales. Al igual que en el caso británico, la eficacia del sistema depende del tipo de delito, del entorno vigilado y, especialmente, de su integración dentro de una estrategia de seguridad coherente, lo que confirma la existencia de una brecha entre el potencial técnico atribuido a estas herramientas y sus resultados reales.

B) Integración y procedimientos

Un segundo resultado relevante del modelo estadounidense es que el valor operativo de la videovigilancia depende menos de la disponibilidad de tecnología y más de su integración funcional dentro de los procesos policiales. Esta lógica se aprecia con claridad en el desarrollo de los denominados Real-Time Crime Centers (RTCC), concebidos como plataformas para centralizar cámaras, bases de datos y herramientas

analíticas con el objetivo de acelerar la toma de decisiones en tiempo real (Bureau of Justice Assistance, 2019).

Los documentos técnicos sobre RTCC insisten en que su eficacia está condicionada por la existencia de procedimientos claros de acceso, priorización de incidentes, coordinación interunidades y tratamiento posterior de la información visual. En ausencia de estos elementos, los centros de crimen en tiempo real tienden a convertirse en meros nodos tecnológicos con escaso impacto real en la prevención o investigación del delito (Bureau of Justice Assistance, 2019).

Este resultado conecta directamente con las hipótesis relativas a la **falta de protocolos operativos claros** y a la dependencia del criterio profesional. En un contexto tan descentralizado como el estadounidense, la ausencia de estándares comunes provoca que tecnologías similares generen resultados muy distintos según el departamento que las gestione, reforzando la idea de que la tecnología, por sí sola, no garantiza eficacia ni legitimidad.

C) Marco normativo desigual

En materia de controles, el caso estadounidense se caracteriza por un **mosaico normativo** en el que coexisten límites constitucionales generales, legislación estatal diversa y políticas locales muy dispares. La Cuarta Enmienda de la Constitución establece el marco básico de protección frente a registros y vigilancias irrazonables, pero su aplicación a nuevas tecnologías ha requerido una interpretación progresiva por parte del Tribunal Supremo.

Un hito clave en este sentido es la sentencia *Carpenter v. United States*, en la que el Tribunal Supremo reconoció que determinadas tecnologías de seguimiento masivo generan un nivel de intrusión cualitativamente distinto, lo que exige garantías reforzadas, como la autorización judicial previa (U.S. Supreme Court, 2018). Esta doctrina resulta relevante para el análisis de la videovigilancia avanzada, incluidos drones y sistemas automatizados de seguimiento.

No obstante, más allá de estos principios generales, la regulación concreta varía enormemente entre estados y municipios. El propio Departamento de Justicia ha reconocido la existencia de grandes diferencias en ámbitos como el uso del reconocimiento facial, la conservación de datos o los mecanismos de auditoría y transparencia, lo que genera un escenario de **aplicación desigual y controles inconsistentes** (U.S. Department of Justice, Office of Legal Policy, 2024).

Frente a esta fragmentación, algunas ciudades han desarrollado modelos más garantistas, como la exigencia de informes de impacto en derechos civiles y aprobación política previa para nuevas tecnologías de vigilancia. Sin embargo, estas prácticas no son generalizadas y dependen en gran medida de la voluntad política local (City of Seattle, 2024).

D) Expansión reciente, conflicto ético y percepción ciudadana

Un cuarto resultado significativo del caso estadounidense es que la expansión acelerada de tecnologías de vigilancia ha ido acompañada de un **incremento del conflicto ético y social**. En particular, el uso de drones policiales en protestas, eventos públicos y labores de vigilancia preventiva ha generado una fuerte reacción por parte de organizaciones de derechos civiles, que advierten del riesgo de vigilancia masiva y del efecto disuasorio sobre derechos como la libertad de reunión (Stanley, 2024).

Asimismo, la proliferación de sistemas automatizados, como los lectores automáticos de matrículas o las redes privadas de cámaras integradas con fuerzas policiales, ha intensificado el debate público sobre la proporcionalidad, la finalidad del tratamiento de datos y la falta de transparencia en el acceso y uso de la información (U.S. Department of Justice, Office of Legal Policy, 2024).

Desde la perspectiva de este trabajo, estos elementos refuerzan la hipótesis de que la percepción ciudadana desempeña un papel central en la legitimidad del uso de la videovigilancia. En contextos donde los controles son poco visibles o inconsistentes, incluso actuaciones formalmente legales pueden ser percibidas como intrusivas o abusivas, erosionando la confianza en la institución policial.

Síntesis del caso de Estados Unidos

El análisis del caso estadounidense permite extraer varias conclusiones relevantes.

-En primer lugar, confirma que la eficacia de la videovigilancia policial es profundamente dependiente del contexto y del diseño organizativo, lo que refuerza la idea de que la tecnología no produce efectos uniformes (National Institute of Justice, 2021).

-En segundo lugar, evidencia que el valor operativo real depende de la integración procedimental y de la existencia de protocolos claros, más que de la mera acumulación de infraestructuras tecnológicas (Bureau of Justice Assistance, 2019).

-En tercer lugar, pone de relieve que la fragmentación normativa y la ausencia de estándares homogéneos incrementan el riesgo de aplicación desigual y debilitan los mecanismos de control (U.S. Department of Justice, Office of Legal Policy, 2024).

Finalmente, muestra que la expansión tecnológica sin una reflexión ética visible intensifica el conflicto social y afecta negativamente a la percepción ciudadana y a la legitimidad institucional (Stanley, 2024).

En conjunto, el caso de Estados Unidos ofrece un contrapunto esencial a los modelos británico y francés, y permite comprender cómo la descentralización extrema y la gobernanza fragmentada condicionan de manera decisiva el uso, los límites y la aceptación social de la videovigilancia policial.

5.1.4 Caso 4: Alemania

El caso alemán constituye un referente especialmente relevante para el análisis de la videovigilancia policial desde una perspectiva garantista. A diferencia de otros modelos donde el debate se ha centrado en la eficacia operativa o en la expansión tecnológica, en Alemania la videovigilancia se concibe prioritariamente como una **injerencia en derechos fundamentales** que debe ser objeto de una justificación estricta. Este enfoque condiciona tanto el diseño normativo como la práctica policial, y convierte al modelo alemán en un contrapunto idóneo para contrastar las hipótesis planteadas en este trabajo, especialmente aquellas relativas a la necesidad de protocolos claros, controles efectivos y una integración real del componente ético.

La tradición constitucional alemana, profundamente marcada por la protección de la dignidad humana y la experiencia histórica de regímenes de vigilancia intensiva, ha dado lugar a una cultura jurídica en la que la seguridad no se concibe como un valor absoluto, sino como un interés que debe armonizarse cuidadosamente con la libertad y la privacidad.

A) Fundamento doctrinal

Uno de los pilares del modelo alemán es la doctrina de la autodeterminación informativa, formulada por el Tribunal Constitucional Federal en su conocida sentencia sobre el censo de población. En ella se establece que toda persona debe conservar un control efectivo sobre el uso de sus datos personales, y que la recopilación masiva de información por parte del Estado puede generar un efecto disuasorio sobre el ejercicio de libertades fundamentales (Bundesverfassungsgericht, 1983).

Esta doctrina ha tenido una influencia decisiva en el desarrollo posterior de la videovigilancia policial. Desde esta perspectiva, la captación sistemática de imágenes en espacios públicos no se considera una medida neutra, sino una actuación que

requiere una **base legal clara**, una finalidad concreta y garantías suficientes para evitar usos expansivos o acumulativos. En consecuencia, el principio de proporcionalidad, desglosado en idoneidad, necesidad y proporcionalidad en sentido estricto, actúa como criterio central para evaluar la legitimidad de cualquier sistema de videovigilancia.

Este marco doctrinal resulta especialmente relevante para este trabajo, ya que conecta directamente con la hipótesis de que la eficacia técnica no puede justificar por sí sola el uso de tecnologías altamente intrusivas si no existen límites normativos y controles operativos bien definidos.

B) Uso práctico y delimitación de supuestos

En la práctica, la videovigilancia policial en Alemania se caracteriza por una delimitación estricta de los supuestos de uso. La normativa policial de los distintos Länder permite la instalación de cámaras en espacios públicos únicamente en contextos específicos, como la protección de infraestructuras especialmente sensibles o la prevención de delitos graves en zonas con riesgo acreditado de reiteración delictiva. Además, la vigilancia preventiva debe realizarse de **forma abierta y reconocible**, de modo que la ciudadanía pueda identificar la existencia del sistema (Sächsische Datenschutz- und Transparenzbeauftragte, s. f.).

Este requisito de "publicidad" de la vigilancia adquiere una especial relevancia en el caso de tecnologías menos visibles, como los drones. Cuanto mayor es la dificultad para que el ciudadano perciba la captación de imágenes, mayor es la exigencia de justificar su uso y de establecer medidas compensatorias de información y control. En contextos como eventos multitudinarios o manifestaciones, la captación de imágenes suele limitarse a planos generales destinados a la gestión del dispositivo, con restricciones claras sobre la grabación y la identificación individual.

Asimismo, existen límites específicos en situaciones especialmente sensibles. Por ejemplo, cuando una concentración o manifestación tiene lugar en un espacio habitualmente vigilado por razones de criminalidad, la doctrina y la supervisión administrativa han señalado que la videovigilancia debe interrumpirse o someterse a reglas específicas vinculadas al derecho de reunión, reforzando así la protección de las libertades públicas (Sächsische Datenschutz- und Transparenzbeauftragte, s. f.).

C) Controles y supervisión

El modelo alemán destaca por una **arquitectura de control robusta**, en la que confluyen el control constitucional, la supervisión judicial ordinaria y el papel activo de las autoridades de protección de datos. El Tribunal Constitucional Federal ha intervenido

en múltiples ocasiones para corregir habilitaciones legales consideradas excesivamente amplias o imprecisas, especialmente cuando la tecnología permite un seguimiento sistemático de las personas.

Un ejemplo paradigmático es la jurisprudencia sobre el reconocimiento automático de matrículas, en la que el Tribunal declaró inconstitucionales determinados preceptos por no establecer límites suficientemente claros y por permitir una recogida de datos desproporcionada (Bundesverfassungsgericht, 2018). Este razonamiento resulta plenamente trasladable a la videovigilancia avanzada, incluidos los sistemas de análisis automatizado o de seguimiento persistente.

A nivel normativo, Alemania ha incorporado la Directiva (UE) 2016/680 al ordenamiento interno mediante disposiciones específicas del Bundesdatenschutzgesetz para el tratamiento de datos por autoridades policiales, estableciendo obligaciones estrictas en materia de finalidad, minimización, conservación y seguridad de la información (Deutscher Bundestag, 2021). Este marco se ve reforzado por la actuación de la autoridad federal de protección de datos y de las autoridades regionales, que ejercen una supervisión activa sobre el uso policial de tecnologías de vigilancia.

Desde la óptica de este trabajo, este entramado de controles evidencia un modelo en el que la videovigilancia no se legitima únicamente por su utilidad, sino por su sujeción efectiva a reglas, auditoría y supervisión externa.

D) Evolución y tensiones

En los últimos años, Alemania se enfrenta, como otros países europeos, a la presión para incorporar nuevas capacidades tecnológicas, como la analítica avanzada o el reconocimiento biométrico. Sin embargo, estas propuestas suelen generar un intenso debate jurídico y social, precisamente por el estándar elevado de protección de derechos fundamentales que caracteriza al sistema alemán.

Las autoridades de protección de datos y los tribunales han insistido en que cualquier ampliación de capacidades debe venir acompañada de una habilitación legal específica y de garantías reforzadas, especialmente cuando existe el riesgo de vigilancia masiva o de identificación sistemática de personas. Esta resistencia institucional a la expansión tecnológica sin controles claros refuerza la idea de que la ética y la proporcionalidad no se conciben como elementos accesorios, sino como límites estructurales del uso policial de la videovigilancia.

Síntesis analítica del caso alemán

El análisis del caso alemán permite extraer varias conclusiones relevantes para este trabajo.

-En primer lugar, muestra un modelo en el que la videovigilancia se concibe como una injerencia que exige **justificación y proporcionalidad reforzadas**, y no como un recurso operativo neutro (Bundesverfassungsgericht, 1983).

-En segundo lugar, evidencia que el uso práctico de estas tecnologías está estrictamente delimitado por supuestos habilitantes, exigencias de vigilancia abierta y límites claros en contextos sensibles (Sächsische Datenschutz- und Transparenzbeauftragte, s. f.).

-En tercer lugar, pone de relieve la importancia de una arquitectura de control sólida, basada en la intervención judicial y la supervisión de autoridades independientes (Bundesverfassungsgericht, 2018; Deutscher Bundestag, 2021).

Finalmente, muestra que la presión tecnológica actual reabre de forma constante el debate ético y jurídico, reforzando la necesidad de controles efectivos para preservar la legitimidad del uso policial de la videovigilancia.

En conjunto, el modelo alemán aporta un contrapunto garantista que permite comprender hasta qué punto la existencia de protocolos claros, controles robustos y una cultura ética institucionalizada condiciona el alcance y la aceptación social de la videovigilancia policial.

5.1.5 Comparativa transversal de resultados internacionales (Reino Unido, Francia, Estados Unidos y Alemania)

El análisis comparado de los cuatro casos internacionales permite identificar patrones comunes y diferencias estructurales que resultan especialmente útiles para interpretar el caso español. Aunque cada país presenta un marco jurídico y una cultura institucional distinta, los resultados convergen en una idea central: la eficacia y la legitimidad de la videovigilancia dependen menos de la tecnología disponible que de la calidad de los protocolos, los controles y la gobernanza.

A) Grado de normalización y lógica de despliegue

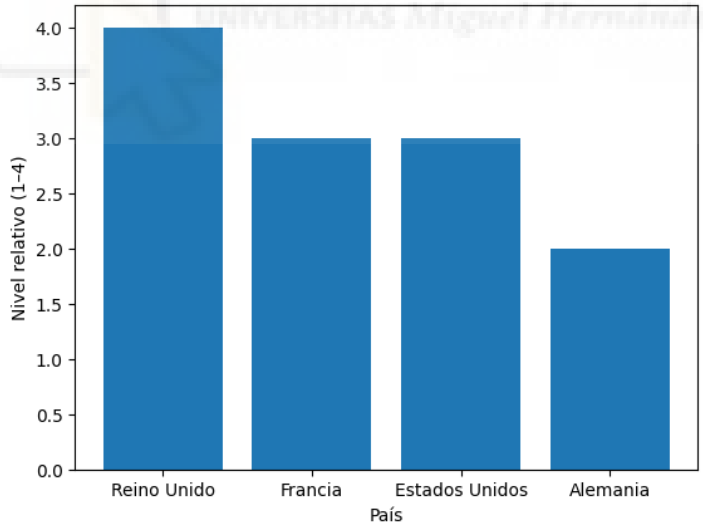
En **Reino Unido**, la videovigilancia (especialmente CCTV) constituye una infraestructura de seguridad consolidada y socialmente asumida en muchos entornos urbanos, lo que permite observar los límites del modelo cuando la vigilancia se convierte

en rutina. La expansión tecnológica se produce desde una lógica de sistema: la cuestión no es si se usa, sino cómo se gestiona y con qué garantías (College of Policing, 2015; Gill & Spriggs, 2005).

En **Francia**, la normalización es más reciente en el ámbito de drones, pero se acelera tras un periodo inicial de conflictividad. El despliegue ha evolucionado desde un uso operativo adelantado al marco legal hacia un modelo de autorización administrativa previa, con fuertes intervenciones correctoras del control judicial y constitucional (Conseil d'État, 2020; Conseil constitutionnel, 2021; Décret n° 2023-283, 2023).

En **Estados Unidos**, la lógica dominante es la descentralización: no existe un modelo unificado, sino un mosaico de soluciones tecnológicas y políticas internas por agencia y jurisdicción. Esto genera una normalización desigual, donde la vigilancia puede ser muy intensa en algunas ciudades y más limitada en otras, con gran variabilidad en estándares y controles (U.S. Department of Justice, Office of Legal Policy, 2024).

En **Alemania**, la normalización se contiene mediante un estándar garantista elevado. La videovigilancia tiende a justificarse como medida delimitada por supuestos habilitantes y bajo una cultura jurídica que parte de la vigilancia como injerencia que debe ser estrictamente proporcionada (Bundesverfassungsgericht, 1983).



Fuente: elaboración propia.

Grafica 3. Grado de normalización de la videovigilancia

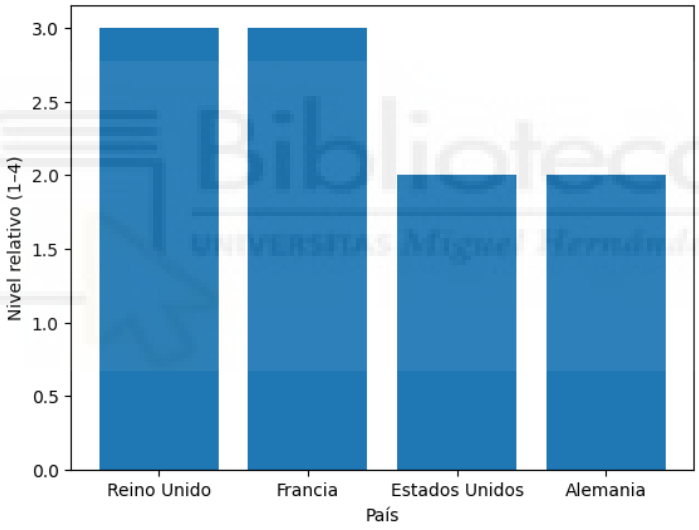
B) Eficacia real vs expectativas: el peso del contexto y la integración operativa

En **Reino Unido**, la evidencia muestra que el CCTV presenta impactos limitados y dependientes del contexto. Su rendimiento aumenta cuando se integra en estrategias operativas concretas y con gestión adecuada; disminuye cuando opera como

infraestructura pasiva o simbólica (College of Policing, 2015; Piza et al., 2019; Gill & Spriggs, 2005).

En **Estados Unidos**, los resultados tienden a ser todavía más heterogéneos: tecnologías como cámaras corporales o RTCC pueden aportar beneficios, pero la evidencia es mixta y depende del diseño procedimental, la formación y el control. La utilidad no reside en "tener tecnología", sino en cómo se inserta en una cadena operativa y probatoria (National Institute of Justice, 2021; Bureau of Justice Assistance, 2019).

En **Francia** y **Alemania**, el análisis comparado sugiere que la discusión pública se centra menos en medir eficacia cuantitativa general y más en la legitimidad y los límites. En Francia, el foco ha sido ajustar la autorización y el uso a la proporcionalidad, especialmente en contextos sensibles como manifestaciones. En Alemania, el estándar de proporcionalidad condiciona desde el inicio el alcance, lo que limita la expansión y reduce el riesgo de vigilancia rutinaria amplia.



Fuente: elaboración propia.

Grafica 4. Integración operativa y eficacia.

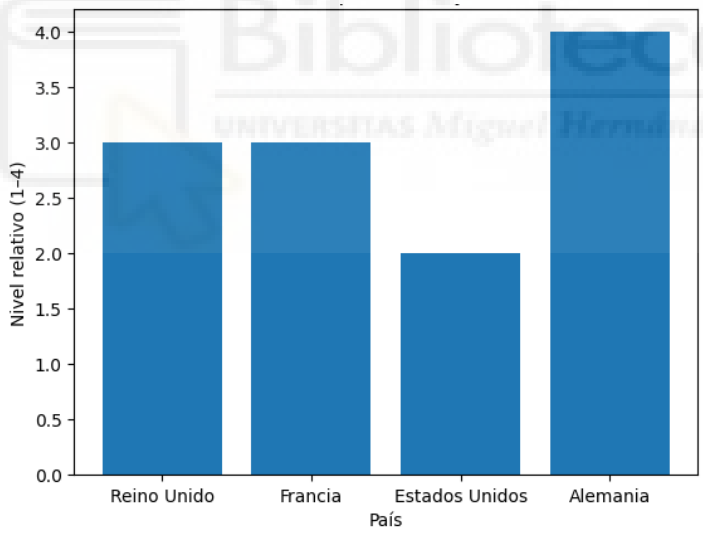
C) Protocolos y controles: de la formalidad al control efectivo

En **Francia** se aprecia un modelo de control previo administrativo (autorización prefectural) complementado por control judicial, constitucional y supervisión de protección de datos. Sin embargo, la persistencia de suspensiones judiciales por deficiencias de motivación o por perímetros excesivos evidencia que los controles formales no garantizan siempre un control material eficaz si la práctica deriva hacia autorizaciones de baja calidad argumentativa (Conseil d'État, 2020; Tribunal administratif d'Orléans, 2025).

En **Estados Unidos**, la fragmentación normativa genera un riesgo mayor: los controles dependen de políticas internas y decisiones locales, lo que puede producir "zonas de baja gobernanza" en las que la tecnología crece más rápido que las salvaguardas. Frente a ello, algunas ciudades han desarrollado marcos de evaluación de impacto y control público, pero no constituyen un estándar general (U.S. Department of Justice, Office of Legal Policy, 2024; City of Seattle, 2024).

En **Reino Unido**, la existencia de códigos y comisionados muestra un intento de mantener legitimidad mediante principios de transparencia y gobernanza; sin embargo, el despliegue masivo hace que el reto se traslade a la calidad del uso: gestión efectiva, auditoría y control de nuevas capacidades (Home Office, 2021; Biometrics and Surveillance Camera Commissioner, 2024).

En **Alemania**, los controles se apoyan en una arquitectura especialmente fuerte: base legal estricta, límites jurisprudenciales y supervisión de protección de datos, lo que actúa como freno estructural frente a la expansión sin garantías (Bundesverfassungsgericht, 2018; Deutscher Bundestag, 2021).



Fuente: elaboración propia.

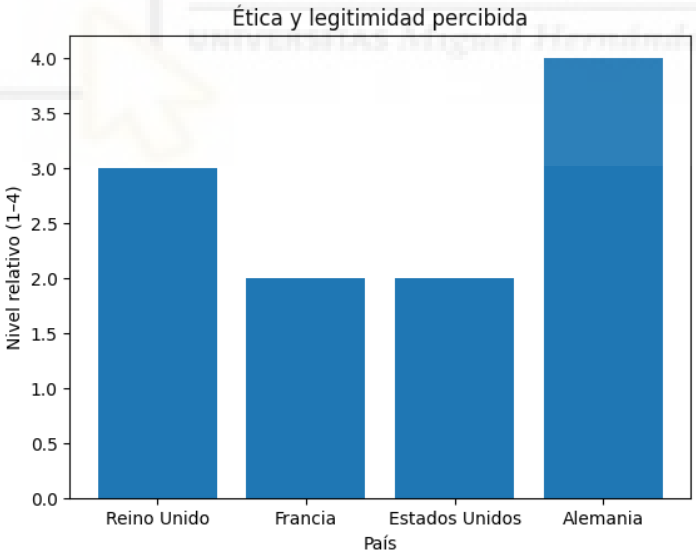
Grafica 5. Fortaleza de protocolos y controles.

D) Ética, legitimidad y percepción ciudadana

En los cuatro casos aparece una conclusión transversal: **la legitimidad social no se sostiene solo con legalidad**. Cuando la ciudadanía percibe opacidad, expansión

funcional o ausencia de límites, el uso de la videovigilancia se problematiza incluso si la herramienta aporta valor operativo.

- En **Reino Unido**, la incorporación de capacidades "inteligentes" reabre el debate sobre expansión funcional y confianza pública (London Borough of Hammersmith & Fulham, 2025).
- En **Francia**, la normalización cuantitativa de drones intensifica el debate sobre vigilancia aérea en manifestaciones y espacios públicos (Le Monde, 2025; CNIL, 2025).
- En **Estados Unidos**, el conflicto social se acentúa en tecnologías de seguimiento automatizado y en vigilancia de reuniones públicas, donde la percepción de vigilancia masiva afecta directamente a la confianza (Stanley, 2024; U.S. Department of Justice, Office of Legal Policy, 2024).
- En **Alemania**, la ética aparece institucionalizada como límite estructural: la vigilancia debe ser excepcional, justificada y estrictamente proporcionada, en parte por sensibilidad histórica y por estándares constitucionales reforzados (Bundesverfassungsgericht, 1983).



Fuente: elaboración propia.

Grafica 6. Ética y legitimidad percibida.

5.1.6 Contraste con las hipótesis formuladas. Ámbito internacional.

La comparación entre Reino Unido, Francia, Estados Unidos y Alemania deja una idea clara: **no importa tanto tener más tecnología, sino cómo se gestiona**. Lo decisivo es el modelo de gobernanza: qué reglas hay, quién controla, cómo se usa en la práctica y cómo se explica a la ciudadanía. Desde ahí, la evidencia comparada apoya cuatro conclusiones que encajan con hipotesis formuladas:

1) La videovigilancia funciona mejor cuando está bien integrada (H4; H1)

La eficacia no es automática. Depende del lugar, del tipo de delito y, sobre todo, de si el sistema está conectado a una forma real de trabajar: monitorización, patrullas, respuesta y uso de las imágenes como prueba. En Reino Unido, las cámaras rinden más cuando hay vigilancia activa y capacidad de actuar; si solo "graban", su efecto baja (College of Policing, 2015). En Estados Unidos se repite lo mismo: cámaras corporales o centros de control pueden ayudar, pero solo si hay procedimientos, formación y control, y si están integrados en la cadena operativa (National Institute of Justice, 2021). Esto confirma que el valor está en la organización, no en acumular dispositivos.

2) Sin protocolos claros, sube la discrecionalidad y el problema acaba fuera (H5; H1)

Cuando no existen reglas internas claras y verificables, el uso de la tecnología se decide "sobre la marcha". Eso aumenta la inseguridad jurídica y hace que el sistema termine corrigiéndose desde fuera: jueces, autoridades de control o conflictos públicos. En Reino Unido ya se vio que muchos sistemas generan muchas imágenes, pero sirven poco si no hay procedimientos sólidos para gestionar, seleccionar y usar ese material como prueba (Gill & Spriggs, 2005). En Francia, el control judicial ha intervenido cuando las garantías o la justificación no eran suficientes, mostrando que si el control interno falla, el ajuste lo impone el control externo (Conseil d'État, 2020).

3) Los países con controles fuertes frenan mejor el "uso por inercia" (H6; H1)

La tecnología tiende a expandirse cuando está disponible: si se puede usar, se usa más. Por eso, los modelos con controles estructurales fuertes contienen mejor el riesgo de que se amplíen finalidades sin darse cuenta. Alemania es un ejemplo de enfoque muy garantista: la vigilancia se trata como una injerencia que exige base legal clara y proporcionalidad estricta, lo que frena la expansión rutinaria (Bundesverfassungsgericht, 2018). En Reino Unido existen marcos y códigos de gobernanza, pero el reto está en controlar bien el uso diario y las nuevas capacidades (Home Office, 2021). La lección es clara: los límites deben estar diseñados "de serie", no depender solo del criterio individual.

4) La confianza depende de transparencia y control, no solo de que sea "legal" (H7; H8; H6)

Aunque algo sea legal, puede ser socialmente frágil si la gente lo percibe como opaco, excesivo o sin límites. En Francia, el debate sobre drones y vigilancia aérea se activa cuando se sospecha expansión o falta de garantías (CNIL, 2025). En Estados Unidos, el uso de tecnologías de vigilancia en contextos sensibles ha generado conflictos por su impacto en la confianza pública (Stanley, 2024). Esto conecta con la vigilancia aérea: el dron es menos visible y más impredecible, y por eso necesita controles más claros, criterios de activación más estrictos y una explicación institucional comprensible.

5.2 Analisis de modelo nacional de videovigilancia policial

Tras el análisis comparado internacional, resulta imprescindible centrar el estudio en el contexto español, ya que es en este ámbito donde se aprecia con mayor claridad la relación entre el marco normativo y la práctica cotidiana. Los casos nacionales permiten observar cómo se aplica realmente la videovigilancia policial en escenarios concretos, qué decisiones se adoptan en situaciones reales de servicio y cómo se materializan los principios legales cuando la intervención deja de ser teórica y se convierte en operativa.

Este bloque no se limita a describir los distintos usos de cámaras o drones, sino que tiene como finalidad identificar patrones recurrentes en la práctica policial. Se analizan las condiciones en las que la tecnología aporta un valor preventivo o probatorio efectivo y aquellas en las que, por el contrario, genera expectativas que no siempre se traducen en resultados. Asimismo, se examina el papel de los protocolos, los mecanismos de control y la supervisión posterior, atendiendo a las carencias que surgen cuando estos elementos no están suficientemente definidos o no se aplican de forma homogénea.

El análisis de los casos nacionales pone también el foco en una característica específica del modelo español: la coexistencia de múltiples sistemas de videovigilancia y niveles competenciales. Cámaras municipales, dispositivos en grandes eventos, actuaciones preventivas en espacios públicos y el uso creciente de drones configuran un escenario complejo, en el que la eficacia y la legitimidad dependen en gran medida de la coordinación institucional, del diseño de procedimientos claros y del respeto a los límites legales.

5.2.1 Videovigilancia fija en espacios urbanos

La videovigilancia fija constituye en España el componente más estable y extendido del sistema de captación de imágenes en seguridad pública. Su implantación responde a dos lógicas complementarias: una red permanente en entornos urbanos con alta densidad de tránsito o zonas sensibles, y el refuerzo puntual en grandes eventos y celebraciones multitudinarias. Esta doble lógica permite analizar un aspecto central del trabajo: la tecnología no aporta valor por sí misma, sino en función de cómo se gobierna, se integra operativamente y se somete a garantías y controles.

Desde el plano jurídico, el marco básico se articula en torno a la Ley Orgánica 4/1997 y su desarrollo reglamentario mediante el Real Decreto 596/1999, que configuran un sistema de autorización y garantías inspirado en el principio de proporcionalidad, con exigencias de motivación, delimitación espacial y control institucional a través de las Comisiones de Garantías (Ley Orgánica 4/1997, 1997; Real Decreto 596/1999, 1999).

A) La normalización de la vigilancia

En la práctica, el primer fenómeno relevante es la normalización. Un sistema fijo tiende a permanecer y, con el tiempo, a integrarse en el paisaje urbano. Esta normalización puede desplazar la carga justificativa, reduciendo la evaluación periódica de la necesidad real de la captación en un punto concreto. El riesgo no es solo jurídico, sino institucional: la videovigilancia puede mantenerse por inercia y por su valor simbólico, aun cuando su rendimiento operativo sea irregular.

Este fenómeno conecta directamente con el principio de proporcionalidad exigido por el ordenamiento. La Ley Orgánica 7/2021 incorpora expresamente el tratamiento de datos mediante sistemas de grabación por Fuerzas y Cuerpos de Seguridad y obliga a vincularlo a finalidades concretas de seguridad pública e investigación penal, reforzando la exigencia de proporcionalidad y justificación continuada (Ley Orgánica 7/2021, 2021).

B) Relación: entre grabar y producir un resultado útil

Un análisis riguroso de la videovigilancia fija obliga a distinguir entre la mera captación de imágenes y la generación de valor operativo. Entre ambos extremos existe una cadena con eslabones críticos: diseño del sistema, monitorización efectiva, capacidad de respuesta y uso probatorio con garantías de custodia y trazabilidad.

Esta perspectiva coincide con la evidencia acumulada sobre CCTV, que muestra efectos modestos y dependientes del contexto. Las revisiones indican que la reducción del delito, cuando existe, es limitada y más consistente en determinados entornos como

aparcamientos, especialmente cuando hay monitorización activa y una estrategia operativa coherente (College of Policing, 2015; Piza et al., 2019).

Aplicado a España, esto implica que aumentar el número de cámaras no equivale automáticamente a mejorar resultados. En grandes eventos, la cámara fija aporta una visión panorámica útil para la gestión del dispositivo, pero esa utilidad no siempre se traduce en valor probatorio individualizable. La obtención de evidencias claras exige sistemas bien diseñados, protocolos de explotación de imágenes y coordinación real con las unidades en calle.

C) Gobernanza, autorizaciones y el punto crítico de los controles

El tercer nivel de análisis es la gobernanza del sistema, especialmente relevante cuando intervienen cámaras municipales y centros de control. El Reglamento de desarrollo de la Ley Orgánica 4/1997 establece que, cuando las Fuerzas y Cuerpos de Seguridad ejercen control efectivo sobre la captación, visionado y custodia de imágenes, resulta aplicable el régimen completo de la Ley y su Reglamento, con independencia de la titularidad formal de la instalación (Real Decreto 596/1999, 1999).

Aquí surge un riesgo práctico central: la existencia de autorización formal no garantiza por sí sola un control material homogéneo. Sin protocolos operativos claros sobre accesos, finalidades, extracción y documentación, la trazabilidad se debilita. La trazabilidad no es un aspecto técnico menor, sino un indicador directo de legitimidad. Cuando falla, aumentan la discrecionalidad y la vulnerabilidad a usos expansivos, incluso sin mala fe.

En este punto, las guías de la Agencia Española de Protección de Datos insisten en principios como la limitación de finalidad, la minimización de datos y la necesidad de una base jurídica clara, aplicables de forma específica a la actuación de las Fuerzas y Cuerpos de Seguridad (AEPD, 2025).

D) Conservación, supresión y uso posterior de las imágenes

Otro plano crítico es la gestión posterior de las imágenes. En videovigilancia, el "después" es tan relevante como el "durante". La AEPD recuerda el criterio general de conservación máxima de un mes y la obligación de supresión posterior, salvo cuando las imágenes deban conservarse para acreditar hechos relevantes, conforme al régimen específico de la Ley Orgánica 4/1997 (AEPD, 2025).

En grandes eventos, este aspecto adquiere especial sensibilidad por el volumen de personas captadas. Sin reglas internas claras sobre conservación y finalidad, el sistema

puede derivar hacia una lógica de acumulación preventiva incompatible con la minimización. Además, el uso ulterior de imágenes en contextos distintos al que motivó la captación genera riesgos jurídicos y de legitimidad si no existe una justificación clara y documentada.

E) Dimensión ética

Aunque este apartado se centra en resultados, la práctica de la videovigilancia fija revela con claridad una dimensión ética aplicada. La legitimidad no se sostiene solo en la legalidad formal, sino en cómo la institución gestiona el poder de observar. En términos operativos, la ética se concreta en decisiones sobre qué se vigila, con qué intensidad, durante cuánto tiempo se conserva la información y qué controles existen para evitar desbordamientos de finalidad.

En síntesis, el caso español de videovigilancia fija muestra un sistema ampliamente implantado y útil en determinados contextos, pero cuyo rendimiento y legitimidad dependen de factores que no siempre reciben la misma atención que el despliegue tecnológico: protocolos operativos detallados, controles verificables, trazabilidad, políticas claras de conservación y una gobernanza coherente cuando intervienen distintos niveles institucionales. Es en ese punto donde la videovigilancia deja de ser "tener cámaras" y pasa a ser "saber gobernarlas" conforme a los principios de proporcionalidad y finalidad que exige el propio marco legal (Ley Orgánica 4/1997, 1997; Real Decreto 596/1999, 1999; Ley Orgánica 7/2021, 2021; AEPD, 2025).

5.2.2 Uso de drones por fuerzas policiales en España

La incorporación progresiva de drones al ámbito policial español ha supuesto un cambio cualitativo en la forma de concebir la vigilancia, la prevención y el apoyo operativo en seguridad pública. Frente a la videovigilancia fija, basada en dispositivos estables e integrados en el espacio urbano, el dron introduce una vigilancia móvil y flexible, capaz de adaptarse con rapidez a escenarios cambiantes y de aportar información operativa allí donde la patrulla tradicional presenta limitaciones. En términos institucionales, supone una nueva forma de presencia policial sustentada en la observación y la gestión del espacio desde una plataforma tecnológica.

Esta capacidad operativa explica su expansión, pero también incrementa de manera inevitable las exigencias jurídicas, éticas y organizativas. El dron no es una cámara más:

su movilidad y alcance hacen que la captación de imágenes sea más difícil de delimitar y justificar, y menos predecible para la ciudadanía. A diferencia de la videovigilancia fija, visible y localizada, la vigilancia aérea puede ser intermitente y potencialmente más intrusiva, lo que desplaza el debate desde la mera legalidad formal hacia la legitimidad material del uso. La cuestión central deja de ser si el dron puede volar o grabar y pasa a ser si debe hacerlo en un momento, lugar y finalidad concretos, con un control institucional suficiente.

Por ello, el uso policial de drones no puede analizarse únicamente desde la habilitación legal. Su legitimidad se construye en la interacción entre la normativa aeronáutica, el régimen de videovigilancia policial, la protección de datos y, de forma decisiva, la capacidad de autorregulación interna mediante protocolos claros y verificables. El dron se convierte así en un indicador de madurez institucional: cuando faltan reglas internas sólidas, la tecnología tiende a imponer su propia lógica, un riesgo que suele hacerse visible ante incidentes, quejas ciudadanas o procedimientos judiciales.

Desde una perspectiva ética aplicada, el problema no es el dron, sino su uso sin límites internos consistentes. La ética se concreta en decisiones operativas: cuándo desplegarlo, si es necesario, qué se graba, cuánto tiempo se conserva la información y qué controles existen. En ausencia de protocolos, estas decisiones dependen del criterio individual o de la urgencia del momento, difuminando la frontera entre un uso legítimo y uno excesivo.

Además, la falta de protocolos afecta también a la eficacia y a la seguridad jurídica. Sin trazabilidad, cadena de custodia y reglas claras de conservación, imágenes potencialmente relevantes pueden perder su valor probatorio. Sin límites claros y garantías visibles, la confianza se erosiona con facilidad. Por ello, el dron exige algo más que capacidad técnica: exige gobernanza, basada en protocolos internos coherentes, aplicados de forma consistente y revisables cuando la práctica lo exige.

El encaje normativo no es garantía suficiente

Desde el punto de vista jurídico, el uso del dron policial se articula sobre una doble base normativa. En primer lugar, el marco aeronáutico europeo y nacional define las condiciones de seguridad aérea y gestión del riesgo operacional. En segundo lugar, la normativa de videovigilancia y protección de datos establece los límites y garantías cuando la operación implica captación de imágenes con finalidad de seguridad pública.

El Reglamento de Ejecución (UE) 2019/947 introduce un modelo de regulación basado en el riesgo, que se concreta en categorías de operación con exigencias crecientes

según el impacto potencial sobre terceros. Este enfoque es especialmente relevante para el ámbito policial, ya que muchas operaciones reales se desarrollan en entornos urbanos, con presencia de personas no participantes y necesidad de respuesta inmediata. En estos contextos, el marco normativo no prohíbe la operación, pero exige planificación, análisis del entorno y medidas de mitigación.

En España, el Real Decreto 517/2024 desarrolla este marco y regula específicamente las actividades o servicios no EASA, entre los que se incluyen las operaciones policiales. Este régimen introduce una flexibilidad aparente al excluir determinadas misiones del sistema clásico de autorización aeronáutica, pero en realidad desplaza el centro del control hacia la organización que opera el dron. La legalidad deja de descansar en un permiso externo individualizado y pasa a depender del cumplimiento estricto de condiciones operativas, escenarios estándar y análisis de riesgo previamente definidos.

Esta estructura normativa tiene una consecuencia directa: la ley presupone que la organización policial dispone de capacidad interna para planificar, decidir, documentar y auditar sus propias operaciones. El marco legal no sustituye a los protocolos internos, sino que los exige implícitamente. Sin autorregulación operativa, la flexibilidad normativa se convierte en una fuente de inseguridad jurídica y de riesgo reputacional.

El dron como sistema de videovigilancia móvil y el salto cualitativo en la intrusión

Cuando el dron incorpora cámara, entra en juego el régimen de videovigilancia policial. La Ley Orgánica 4/1997 establece los principios básicos para la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, extendiendo su ámbito a cualquier medio técnico análogo. El dron encaja sin dificultad en esta categoría, pero con una particularidad relevante: su movilidad aérea amplifica el alcance de la captación y reduce la capacidad del ciudadano para percibir de forma inmediata que está siendo grabado.

Este factor incrementa la intensidad de la injerencia y, con ello, la exigencia de proporcionalidad. La captación aérea no es equivalente a una cámara fija visible en una fachada. Supone una observación dinámica, potencialmente amplia y difícil de anticipar por parte de quienes se encuentran en el espacio público. Por este motivo, el uso del dron exige una justificación más robusta, tanto en términos de necesidad como de delimitación de la finalidad.

La Ley Orgánica 7/2021 refuerza esta lógica al integrar la videovigilancia dentro del régimen de tratamiento de datos personales con fines policiales. La norma desplaza el foco desde el dispositivo hacia el dato, obligando a analizar no solo la captación, sino

todo el ciclo de vida de la información. El uso de dispositivos móviles de grabación, categoría en la que se sitúa el dron, queda sujeto a autorización administrativa, con una cláusula de urgencia que permite la actuación inmediata cuando concurran razones operativas, pero impone una posterior rendición de cuentas.

Este diseño normativo es revelador: el legislador asume que la urgencia es consustancial a la función policial, pero no renuncia al control. La urgencia habilita la actuación, no la exime de justificación. De nuevo, el sistema presupone la existencia de procedimientos internos capaces de documentar, evaluar y, en su caso, corregir la actuación.

La autorregulación como pilar

Es en este punto donde emerge con claridad el concepto de autorregulación institucional. El marco legal español no define con detalle cómo debe organizarse una unidad policial de drones, pero sí establece obligaciones que solo pueden cumplirse mediante una arquitectura interna sólida. La normativa presupone que existen protocolos que determinan cuándo se activa el dron, quién adopta la decisión, con qué finalidad se vuela, si se graba o no, qué se hace con las imágenes y cómo se documenta todo el proceso.

La trazabilidad no es un requisito accesorio, sino el núcleo de la legitimidad operativa. Un sistema trazable permite reconstruir la cadena completa de decisiones y actuaciones. Permite saber quién autorizó la misión, bajo qué criterio, qué imágenes se captaron, quién accedió a ellas y con qué finalidad. Sin esta trazabilidad, la legalidad formal se vuelve frágil y la institución queda expuesta a cuestionamientos jurídicos y éticos, incluso aunque no exista una voluntad abusiva.

En el ámbito del dron, esta exigencia es aún mayor que en la videovigilancia fija. La facilidad de despliegue, la rapidez de activación y la versatilidad técnica aumentan el riesgo de decisiones improvisadas si no existen reglas claras. La autorregulación mediante protocolos internos no es, por tanto, una opción organizativa, sino una condición para que la herramienta sea sostenible en el tiempo.

El CONOP como herramienta de control del dron policial

En este contexto adquiere una relevancia central el **CONOP (Concept of Operations)** como herramienta clave para la gobernanza del uso policial de drones. El CONOP no es un procedimiento técnico ni un manual de vuelo, sino un documento estratégico-operativo que define cómo una organización concibe y controla el empleo de esta capacidad. Delimita escenarios de uso, finalidades, límites operativos y jurídicos y

mecanismos de supervisión, permitiendo transformar una capacidad técnica en una capacidad institucional gobernada y compatible con los principios de legalidad, proporcionalidad y rendición de cuentas (EASA, s. f.; JARUS, 2023).

Desde una perspectiva técnico-regulatoria, el CONOP encaja en el modelo europeo de gestión del riesgo operacional. La metodología SORA sitúa la definición del concepto de operación como punto de partida del análisis de riesgos, exigiendo describir la operación, el sistema utilizado, el entorno y la organización interna antes de evaluar mitigaciones (JARUS, 2019; JARUS, 2023). Esta lógica evidencia que la seguridad y la legitimidad dependen de la gobernanza de la operación en su conjunto.

El Reglamento de Ejecución (UE) 2019/947 refuerza este enfoque al exigir, en la categoría específica, una evaluación del riesgo basada en las características concretas de cada operación. En la práctica, el CONOP actúa como soporte documental de esta exigencia, describiendo misión, entorno, riesgos previsibles y medidas de mitigación. Sin un concepto de operación definido, la evaluación pierde solidez técnica y defensabilidad jurídica (Reglamento de Ejecución (UE) 2019/947, 2019; EASA, s. f.).

En España, la relevancia del CONOP se intensifica con el Real Decreto 517/2024, que flexibiliza trámites administrativos pero refuerza la responsabilidad de las organizaciones operadoras en planificación, control y documentación. La aprobación de escenarios estándar no elimina la planificación interna, sino que exige Manuales de Operaciones con anexos de CONOP específicos (Real Decreto 517/2024, 2024; AESA, 2024).

Desde el punto de vista operativo, el CONOP conecta el nivel estratégico, definiendo finalidad y límites; el nivel operativo, estableciendo roles y procedimientos; y el nivel informacional, regulando el tratamiento de imágenes y datos captados durante todo su ciclo de vida, aspecto especialmente relevante en el ámbito policial (Ley Orgánica 4/1997, 1997; Ley Orgánica 7/2021, 2021).

Un CONOP policial eficaz debe diferenciar perfiles de misión y criterios de activación, ya que el apoyo a emergencias, la búsqueda de personas, los grandes eventos o las intervenciones urgentes presentan niveles distintos de riesgo e intrusión. El CONOP permite adaptar los umbrales de autorización y control a cada escenario, evitando patrones operativos uniformes (EASA, s. f.; JARUS, 2019).

Asimismo, debe incorporar la geografía operacional de la misión, delimitando áreas de vuelo y volúmenes de contingencia, lo que cumple una función de legitimación

institucional al demostrar identificación previa de riesgos y medidas de minimización del impacto sobre terceros (AESA, 2025; EASA, s. f.).

El CONOP debe definir con claridad la estructura organizativa y las responsabilidades, reduciendo la discrecionalidad individual y reforzando el control institucional (Ley Orgánica 7/2021, 2021). Finalmente, integra la gobernanza de los datos y de las imágenes captadas, traduciendo las obligaciones legales en reglas operativas claras sobre grabación, acceso, custodia, conservación y destrucción (Ley Orgánica 4/1997, 1997; Ley Orgánica 7/2021, 2021; AEPD, 2019).

Desde una perspectiva de gobernanza, la implantación del CONOP supone un avance cualitativo. Obliga a planificar antes de actuar, facilita la supervisión y permite defender la actuación ante órganos de control. En ausencia de un CONOP real, aumentan la discrecionalidad y el riesgo de expansión funcional; concebido como instrumento vivo y revisable, se consolida como pilar esencial para un uso legítimo y defendible del dron policial (Real Decreto 517/2024, 2024; EASA, s. f.).

Riesgo de expansión funcional

Uno de los riesgos más relevantes asociados al dron es la expansión funcional. Una herramienta inicialmente concebida para búsquedas o emergencias puede terminar utilizándose de forma rutinaria en vigilancia preventiva amplia si no existen límites claros. Este fenómeno no requiere mala fe; basta con la disponibilidad del recurso y la presión operativa cotidiana.

La autorregulación mediante protocolos y CONOP actúa como barrera frente a este riesgo. Al definir de forma explícita los escenarios legítimos de uso y exigir una justificación documentada para cada misión, se dificulta la deriva hacia usos no previstos. Además, se refuerza la capacidad de la organización para explicar y defender sus decisiones ante la ciudadanía, los tribunales o los órganos de control.

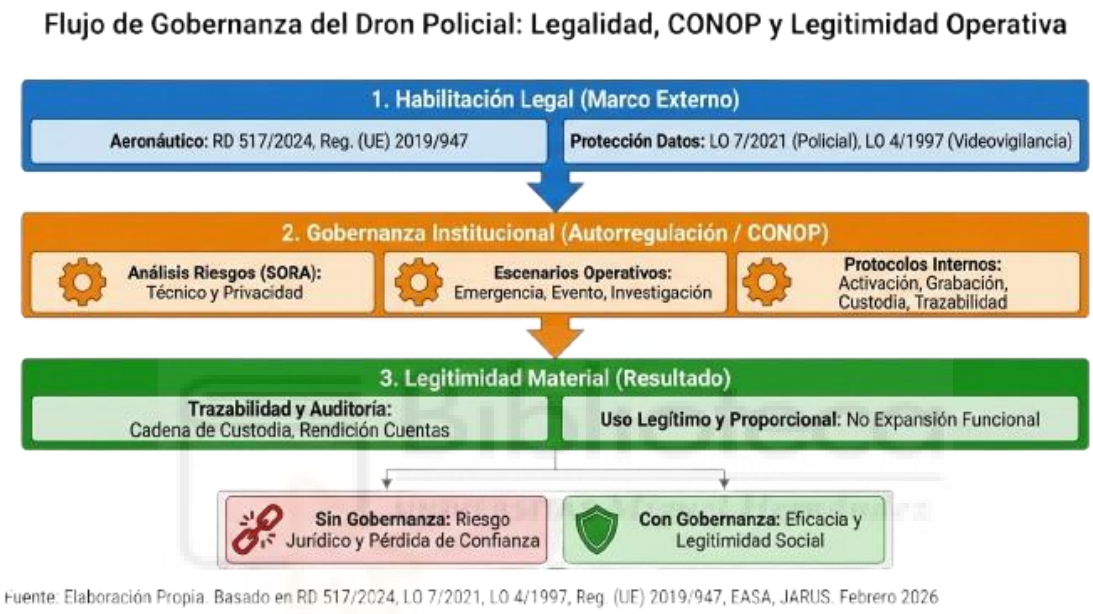
Síntesis final: del cumplimiento normativo a la gobernanza responsable

El análisis del uso de drones por fuerzas policiales en España pone de manifiesto que el ordenamiento jurídico ofrece un marco suficiente para su utilización, pero exige a cambio un alto nivel de responsabilidad institucional. La normativa aeronáutica y de videovigilancia no elimina la discrecionalidad, pero la encauza hacia un modelo de autorregulación basada en protocolos, trazabilidad y planificación previa.

En este contexto, la capacidad de una unidad policial para diseñar y aplicar CONOP claros, coherentes y revisables se convierte en un indicador clave de legitimidad. Allí

donde existen estos instrumentos, el dron se integra como una herramienta eficaz y socialmente defendible. Allí donde faltan, la tecnología corre el riesgo de adelantarse a la gobernanza, generando tensiones jurídicas, éticas y de confianza ciudadana.

Desde la óptica de este trabajo, el dron no es solo un medio técnico, sino un test de madurez institucional. Su uso responsable depende menos de la plataforma y más de la capacidad de la organización para autorregularse, anticipar riesgos y demostrar que la seguridad puede gestionarse con eficacia sin renunciar a las garantías propias de un Estado de Derecho.



Grafica 7. Flujo de gobernanza del dron policial.

5.2.3 Drones y prueba penal

La incorporación del dron como herramienta policial no plantea únicamente un debate técnico o aeronáutico, sino que adquiere una dimensión especialmente relevante en el plano probatorio. En el contexto español, la validez de las imágenes obtenidas mediante drones en una investigación penal depende de que su captación respete los límites constitucionales y procesales, y de que pueda justificarse conforme a criterios de necesidad, proporcionalidad y control. Este aspecto conecta de forma directa con las hipótesis del trabajo relativas a la gobernanza del uso tecnológico, la importancia de los protocolos internos y el riesgo de una vigilancia expansiva carente de límites claros (H1, H5 y H8).

En este sentido, la jurisprudencia reciente del Tribunal Supremo aporta un marco interpretativo especialmente útil para aterrizar el debate. La **STS 797/2025, de 2 de octubre** (ECLI:ES:TS:2025:4225), aborda de manera expresa la impugnación de una prueba obtenida mediante dron por presunta vulneración de derechos fundamentales. El Alto Tribunal sitúa el análisis en el marco del artículo 588 quinquies a) de la Ley de Enjuiciamiento Criminal, que habilita a la Policía Judicial para la captación y grabación de imágenes por cualquier medio técnico en espacios o lugares públicos, siempre que resulte necesario para fines legítimos de investigación penal.

La sentencia resulta relevante porque clarifica que la cobertura procesal para el uso de drones no se basa en una habilitación genérica, sino en la delimitación precisa del ámbito espacial y de la finalidad de la captación. El Tribunal establece una distinción nítida entre la observación en espacios públicos, donde la expectativa de privacidad es menor y la captación puede acordarse por iniciativa policial dentro de los límites legales, y aquellos ámbitos protegidos por el derecho a la inviolabilidad del domicilio o por una expectativa reforzada de privacidad, en los que la autorización judicial resulta imprescindible. Esta distinción es especialmente significativa en operaciones con drones, ya que su posición aérea puede facilitar la captación de imágenes en zonas limítrofes o ambiguas desde el punto de vista jurídico.

El Supremo reconoce, además, la dificultad de fijar reglas rígidas aplicables a todos los supuestos, subrayando que el análisis debe realizarse caso por caso. Para ello, se apoya en la doctrina constitucional que ha advertido de los riesgos de extender de forma automática el concepto de “espacio público” a lugares de acceso restringido, como determinadas zonas comunes de edificios o recintos privados. Esta advertencia tiene una clara proyección operativa: el uso del dron exige una especial cautela en la delimitación del encuadre y del perímetro de observación, ya que una captación aparentemente incidental puede convertirse en una injerencia ilegítima si afecta a ámbitos protegidos.

Desde la perspectiva del presente trabajo, el valor principal de esta jurisprudencia no reside únicamente en confirmar la licitud o ilicitud de una actuación concreta, sino en reforzar la idea de que la prueba obtenida mediante dron es especialmente sensible a la calidad de la gobernanza interna. El Tribunal Supremo diferencia expresamente entre el plano administrativo y el plano procesal: cumplir con la normativa aeronáutica, actualmente desarrollada por el Real Decreto 517/2024, no garantiza por sí solo la validez probatoria de las imágenes si no se respetan los requisitos propios de la

investigación penal. Esta distinción refuerza la tesis de que el uso policial del dron requiere un doble nivel de control: técnico-administrativo y jurídico-procesal.

En términos prácticos, la jurisprudencia analizada pone de relieve que la legitimidad probatoria del dron no depende solo de la captación de imágenes, sino de la capacidad de la organización para explicarla y documentarla. Para que una grabación aérea sea defendible en sede judicial, resulta imprescindible acreditar, de forma verificable, la finalidad concreta de la operación, la necesidad del uso del dron frente a otras alternativas menos intrusivas, la delimitación espacial de la captación, la evitación de ámbitos de privacidad reforzada y la correcta gestión posterior de las imágenes, incluida la cadena de custodia y el control de accesos.

Este criterio conecta de forma directa con las hipótesis del trabajo sobre la insuficiencia de la mera habilitación legal y la centralidad de los protocolos internos. La ausencia de reglas claras de activación, documentación y cierre de misión incrementa el riesgo de nulidad probatoria y traslada el ajuste al control externo, ya sea judicial o a través de autoridades de garantía. En cambio, cuando la unidad dispone de procedimientos definidos y coherentes con el marco normativo, el dron puede integrarse como una herramienta legítima y eficaz, capaz de aportar información relevante sin desbordar los límites constitucionales.

En síntesis, la jurisprudencia reciente del Tribunal Supremo refuerza la idea central de este trabajo: el dron no es problemático por sí mismo, sino por la forma en que se gobierna su uso. La vigilancia aérea intensifica la exigencia de proporcionalidad y control, y convierte la autorregulación institucional en un elemento clave para garantizar tanto la validez de la prueba como la legitimidad social de la actuación policial.

5.2.4 Cuestionario planteado a profesionales policiales

Con el objetivo de reforzar el contraste empírico del trabajo y complementar el análisis documental y de casos, se incorporó una encuesta dirigida a responsables de unidades de drones de los principales cuerpos de policía local de la provincia de Alicante. La finalidad fue captar, desde una perspectiva profesional y de gestión operativa, el grado real de madurez organizativa en torno a tres ejes que atraviesan este estudio: protocolos y controles internos, componente ético aplicado y percepción ciudadana.

Características de la muestra y alcance interpretativo

La encuesta obtuvo resultado cualitativamente significativo por el perfil de los participantes, todos ellos con responsabilidad directa sobre la activación, el uso y el control del recurso UAS. Por la naturaleza del colectivo encuestado, los resultados deben interpretarse con prudencia desde un punto de vista estadístico, pero resultan especialmente valiosos como herramienta de triangulación, al permitir contrastar si las tensiones detectadas en la literatura y en los casos analizados se reproducen en la práctica cotidiana de unidades reales de policía local.

Resultados principales por dimensiones

1) Protocolos: existencia, aplicabilidad y accesibilidad

Los resultados apuntan a una presencia formal de protocolos que no siempre se traduce en operatividad real. Un 75 % de los encuestados considera que existen protocolos, pero los percibe como genéricos o poco concretos, mientras que un 25 % afirma que no existen o apenas se conocen. Esta conclusión se refuerza al analizar su aplicación práctica: el 62,5 % señala que los protocolos solo se tienen en cuenta en determinadas situaciones, frente a un 25 % que indica una aplicación habitual y un 12,5 % que afirma que rara vez influyen en la actuación real.

En cuanto a su accesibilidad, el patrón es coherente con la idea de un protocolo "existente pero poco operativo". El 62,5 % indica que los protocolos existen, pero no son fácilmente accesibles, y el 37,5 % considera que no están claramente disponibles para los operadores. Desde una perspectiva de gobernanza interna, esto sugiere que la norma interna no siempre funciona como instrumento de homogeneización, sino como un marco difuso que deja margen a interpretaciones dispares.

2) Activación, discrecionalidad y cadena de decisión

Respecto a quién decide habitualmente la activación del dron, la opción mayoritaria es que depende del contexto, sin un criterio fijo, lo que alcanza al 62,5 % de las respuestas. También aparecen modelos en los que la decisión corresponde de forma expresa a un mando, con un 25 %, y otros en los que recae en el propio agente operador según la situación, igualmente con un 25 %. En algunos casos se señalaron varias opciones, lo que refuerza la idea de que la cadena decisional no siempre está claramente cerrada.

Este resultado se ve reflejado en la percepción de discrecionalidad. El 50 % describe un margen moderado, dentro de ciertos límites, mientras que el 37,5 % lo considera amplio

y muy dependiente del criterio personal del operador. Solo un 12,5 % percibe un margen muy limitado por normas claras. En conjunto, el modelo que se dibuja es uno en el que la decisión se apoya con frecuencia en el contexto inmediato y en la experiencia individual, más que en un circuito institucional plenamente estandarizado.

3) Controles posteriores y trazabilidad

En relación con los mecanismos de supervisión posterior, el 50 % afirma que existen, pero se aplican de manera irregular, y el 37,5 % considera que no existen o son meramente formales. Solo un 12,5 % describe un control sistemático y consolidado. Este dato resulta especialmente relevante, ya que la supervisión ex post es el elemento que permite verificar si la autorregulación es efectiva o únicamente declarativa.

La trazabilidad presenta un escenario dividido. El 50 % sostiene que siempre se deja constancia documental del uso del dron, mientras que el otro 50 % indica que dicha constancia solo se genera en algunos casos. Esta división apunta a un nivel de madurez desigual entre unidades y refuerza la necesidad de estandarizar los procedimientos de documentación y cierre de misión.

4) Formación y actualización

La formación aparece como una de las carencias más claras detectadas en la encuesta. El 87,5 % considera que la formación recibida en materia de videovigilancia, en sus dimensiones legal, operativa y ética, es básica o parcial, mientras que solo un 12,5 % la califica como suficiente y actualizada. En coherencia con ello, el 75 % señala que la actualización formativa se produce únicamente de forma puntual, frente a un 25 % que la describe como regular.

Este resultado es especialmente relevante, ya que en sistemas complejos la eficacia y la legitimidad no dependen solo del marco normativo, sino de la capacidad de los operadores para interiorizar criterios, aplicarlos de forma consistente y justificar sus decisiones bajo presión operativa.

5) Ética aplicada y urgencia operativa

En la dimensión ética, las respuestas indican una integración limitada. Un 50 % afirma que la ética se menciona, pero no se desarrolla de forma operativa, y un 37,5 % considera que no se aborda de manera expresa. Solo un 25 % sostiene que la ética está integrada de forma clara en la formación y en los procedimientos. En algunos casos se seleccionaron varias opciones, lo que refleja la coexistencia de discurso ético general con una falta de operativización concreta.

El análisis de la urgencia operativa refuerza esta percepción. El 50 % considera que, en situaciones urgentes, la dimensión ética queda claramente relegada frente a la eficacia, mientras que el otro 50 % entiende que se tiene en cuenta solo de forma secundaria. En conjunto, los resultados sugieren que, en contextos de presión, la ética depende en exceso de la voluntad individual del operador, en ausencia de protocolos suficientemente interiorizados.

6) Utilidad operativa, adecuación y regulación del dron

Pese a las carencias señaladas, la percepción de utilidad operativa del dron es elevada. El 75 % considera que la videovigilancia aporta resultados reales de forma frecuente, mientras que el 25 % estima que solo lo hace en contextos concretos. Sin embargo, al valorar la adecuación del uso, aparece una tensión significativa. El 50 % cree que, en general, el uso se ajusta a la necesidad, aunque a veces se sobredimensiona; el 37,5 % sostiene que en muchos casos se utiliza sin una necesidad claramente definida; y el 25 % considera que se ajusta bien a la finalidad perseguida. En algunos casos se marcaron varias opciones, lo que refuerza la percepción de ambivalencia.

En relación con el marco regulador del dron, el 75 % considera que está aceptablemente definido, aunque es mejorable, mientras que el 25 % lo percibe como bien delimitado y justificado. Este resultado es coherente con la tesis central del trabajo: existe un marco formal, pero su efectividad depende de la traducción operativa y del desarrollo de protocolos internos sólidos.

7) Percepción ciudadana, transparencia y legitimidad

La percepción ciudadana del uso de drones se describe como variable y muy dependiente del contexto. Un 37,5 % señala reacciones mayoritariamente positivas o neutras, otro 37,5 % describe percepciones mixtas, y un 25 % identifica reacciones frecuentemente negativas o de incomodidad. A este escenario se suma un déficit claro en materia de transparencia: el 50 % considera insuficiente la información ofrecida a la ciudadanía sobre por qué y para qué se utilizan estas tecnologías, y el otro 50 % la valora como parcial y limitada a determinados contextos.

En cuanto a la legitimidad, el 62,5 % opina que el uso actual de drones refuerza la confianza ciudadana, mientras que un 25 % advierte que puede generar desconfianza si no se controla mejor, y un 12,5 % considera que no influye de forma clara. Esta distribución apunta a un apoyo condicionado, que depende de la percepción de control, proporcionalidad y transparencia.

5.2.5 Contraste con las hipótesis formuladas. Ámbito nacional.

El análisis del modelo español, construido a partir de la videovigilancia fija en espacios urbanos y grandes eventos, el uso policial de drones desde una perspectiva normativa y operativa, la jurisprudencia reciente sobre validez probatoria y los resultados del cuestionario a profesionales policiales, permite realizar un contraste integrado con las hipótesis formuladas en este trabajo. La convergencia de estas fuentes ofrece una visión especialmente sólida, al combinar marco jurídico, práctica operativa real, control judicial y percepción profesional interna.

H1. Brecha entre avance tecnológico y capacidad organizativa para gobernarlo

El modelo español confirma con claridad que la expansión tecnológica (cámaras fijas, sistemas municipales, despliegues en grandes eventos y, más recientemente, drones) avanza a un ritmo superior al de la consolidación organizativa necesaria para gobernarla de forma homogénea. En la videovigilancia fija se aprecia que el marco existe, pero el rendimiento y la legitimidad dependen de cómo se aplica en la práctica: revisión periódica, control de accesos, trazabilidad y coordinación entre titulares y operadores. Con drones, esta brecha se amplifica, porque la capacidad de despliegue rápido y la movilidad exigen un nivel superior de planificación, documentación y límites operativos. La jurisprudencia penal refuerza esta idea al exigir que la captación sea justificable y delimitada, y el cuestionario muestra que, en términos profesionales, persisten diferencias relevantes en protocolos y controles internos. En conjunto, la hipótesis se confirma: el problema no es la ausencia de norma, sino la dificultad de convertirla en una práctica uniforme y verificable. **Resultado: confirmada (alto grado).**

H2. Suficiencia limitada del marco clásico (LO 4/1997) ante el ecosistema actual

El análisis nacional muestra que la LO 4/1997 mantiene utilidad como base garantista en videovigilancia fija —especialmente en proporcionalidad, autorización y control—, pero resulta insuficiente para describir por sí sola el escenario actual, donde la vigilancia se integra en un ciclo de tratamiento de datos más complejo y donde la movilidad tecnológica introduce nuevas tensiones. En España, la gestión real del sistema depende tanto de la instalación como del “después”: acceso, conservación, extracción, cesión y supresión, lo que sitúa el foco en el régimen de tratamiento de datos con fines policiales. En drones, la propia lógica operativa y la necesidad de gobernanza mediante CONOP refuerzan que el marco clásico necesita complementarse con normas que atiendan a trazabilidad y responsabilidad organizativa. Además, la discusión probatoria confirma que no basta con encajar en un régimen de videovigilancia: la validez de la captación exige justificación procesal y límites espaciales. La percepción profesional recogida en

el cuestionario refuerza esta necesidad de complementariedad normativa y procedimental. **Resultado: confirmada parcialmente.**

H3. El marco del dron mejora la seguridad jurídica, pero exige capacidad organizativa real

La hipótesis se confirma en el caso español: el marco aeronáutico vigente aporta orden y criterios de seguridad, pero su eficacia práctica depende de que las unidades tengan capacidad de gestión documental, formación y control operativo. En la práctica, la diferencia entre un uso defendible y un uso frágil no está solo en "poder volar", sino en operar bajo procedimientos claros y coherentes con el conjunto normativo. En este punto, la gobernanza mediante CONOP adquiere un papel central: permite fijar escenarios, umbrales de activación, niveles internos de autorización y obligaciones de cierre de misión. La jurisprudencia penal contribuye a reforzar la misma idea desde otro ángulo: aunque la captación pueda ser lícita, su validez probatoria dependerá de la delimitación, la finalidad y la trazabilidad. Y el cuestionario sugiere que, en la realidad policial, la aplicación de estas exigencias es desigual, lo que confirma que el marco mejora la seguridad jurídica "sobre el papel", pero requiere estructura interna para materializarse. **Resultado: confirmada.**

H4. La eficacia depende más de la integración institucional que del dispositivo

El análisis conjunto muestra que la eficacia real en España no se explica por la cantidad de cámaras o la disponibilidad de drones, sino por la integración de la tecnología en una cadena operativa completa. En videovigilancia fija, los sistemas aportan valor cuando conectan captación, monitorización y respuesta, y cuando el uso probatorio está previsto (extracción y custodia). En grandes eventos, la utilidad es alta para la gestión del dispositivo, pero no siempre se traduce en prueba individualizable si no existe diseño técnico adecuado y coordinación táctica. En drones, la lógica es la misma: el recurso rinde cuando está integrado en la toma de decisiones y coordinación de unidades, no cuando se limita a observar. La dimensión probatoria refuerza que incluso una captación útil puede perder valor si no es defendible y trazable. Y el cuestionario consolida esta lectura desde la práctica profesional: la tecnología funciona cuando hay procedimientos, formación y coordinación real. **Resultado: confirmada (alta consistencia).**

H5. Protocolos y controles internos como condición de legitimidad y valor probatorio

Esta hipótesis aparece como una de las más robustas en el modelo nacional. La videovigilancia fija muestra que los puntos críticos no son solo la instalación o la cobertura, sino quién accede, cómo se documenta la extracción, cuánto se conserva y cómo se asegura la trazabilidad, especialmente cuando existen sistemas municipales o centros de control compartidos. Con drones, la necesidad de protocolos se vuelve aún más intensa por la rapidez de despliegue y la facilidad de ampliar el perímetro de captación; aquí el CONOP funciona como mecanismo de autorregulación que traduce principios legales en reglas operativas concretas. La jurisprudencia penal evidencia que, si no se puede demostrar finalidad, delimitación y respeto a ámbitos de privacidad, el riesgo probatorio aumenta. Los resultados del cuestionario, además, reflejan que los protocolos no siempre son homogéneos, lo que incrementa discrecionalidad y fragilidad jurídica. En síntesis, el control efectivo depende de que el sistema esté gobernado por procedimientos verificables y auditables. **Resultado: confirmada (muy alto grado).**

H6. Déficit de ética aplicada y riesgo de expansión funcional

El análisis nacional respalda que el riesgo principal no suele ser el abuso deliberado, sino la expansión progresiva de usos por disponibilidad y normalización. En videovigilancia fija, la permanencia del sistema puede desplazar la carga justificativa: lo que fue excepcional pasa a asumirse como estructural si no hay revisión real de necesidad. En drones, este riesgo se intensifica porque la herramienta permite observar más, más rápido y con menor previsibilidad, lo que facilita que un uso pensado para apoyo puntual derive hacia vigilancia preventiva amplia sin criterios de activación claros. La dimensión probatoria actúa como freno cuando hay conflicto, pero llega tarde si la ética aplicada no se traduce previamente en limitación de finalidad, minimización, control de accesos y documentación. El cuestionario apunta, precisamente, a esa necesidad de convertir la ética en reglas operativas concretas, no en declaraciones generales. **Resultado: confirmada.**

H7. Transparencia y comunicación como condición de aceptación social

La evidencia nacional respalda que la aceptación social es condicional: la ciudadanía tiende a aceptar la videovigilancia si percibe finalidades claras y garantías creíbles. En el caso de cámaras fijas, la señalización y la estabilidad del dispositivo hacen que la vigilancia sea más “predecible”, pero la legitimidad depende de controles reales sobre acceso, conservación y difusión. Con drones, la necesidad de transparencia aumenta porque el sistema es menos visible y más difícil de anticipar, lo que eleva el riesgo de percepción de opacidad. La jurisprudencia y los estándares de proporcionalidad muestran que la legalidad formal no es suficiente sin capacidad de justificación y

rendición de cuentas. El cuestionario refuerza esta lectura al señalar la importancia de reglas claras y explicables para sostener confianza institucional. **Resultado: confirmada.**

H8. La vigilancia aérea incrementa la percepción de intrusión y eleva la exigencia de control

La hipótesis se confirma de forma parcial pero consistente en la dimensión jurídico-operativa. Frente a la cámara fija, visible y localizada, el dron introduce movilidad, imprevisibilidad y una captación potencialmente más amplia, lo que aumenta la exigencia de proporcionalidad, delimitación espacial y control del dato. La jurisprudencia penal refuerza que la frontera entre espacio público y ámbitos de privacidad puede volverse problemática en captación aérea, de modo que la operación debe planificarse y documentarse con especial cuidado. La gobernanza mediante CONOP resulta clave para fijar umbrales de activación, perímetros, límites técnicos y obligaciones de cierre de misión. En la percepción profesional reflejada por el cuestionario aparece también esta sensibilidad: el dron se reconoce como útil, pero especialmente delicado en legitimidad si no se acompaña de controles estrictos. La confirmación es parcial porque la percepción social concreta depende del contexto y de la calidad de la comunicación institucional, pero el aumento de exigencia de control es claro. **Resultado: confirmada parcialmente.**

6. Conclusiones

6.1 Síntesis de resultados y aprendizajes

El desarrollo del presente trabajo ha permitido analizar el uso policial de la videovigilancia desde una perspectiva integral, combinando el estudio normativo, la revisión de literatura científica, el análisis comparado internacional, los casos nacionales y la evidencia empírica obtenida a través de entrevistas a responsables de unidades de drones. Esta aproximación múltiple ha puesto de manifiesto que la videovigilancia policial no puede entenderse únicamente como una herramienta técnica, sino como un sistema complejo que afecta de forma directa a derechos fundamentales, a la organización interna de los cuerpos policiales y a la percepción social de la seguridad.

Uno de los principales aprendizajes es que el problema central no reside en la ausencia de regulación. Tanto en el ámbito español como en el europeo existe un marco jurídico

amplio y garantista que establece principios claros de legalidad, necesidad, proporcionalidad y control. Sin embargo, el análisis demuestra que la verdadera dificultad aparece en la traducción práctica de esos principios en procedimientos operativos claros, homogéneos y verificables. La brecha entre norma y práctica emerge como un patrón constante a lo largo del trabajo.

Asimismo, los resultados confirman que la eficacia de la videovigilancia, ya sea mediante cámaras fijas o drones, no es automática ni uniforme. Su impacto depende en gran medida del contexto, del tipo de delito, del entorno vigilado y, sobre todo, de la forma en que la tecnología se integra en una estrategia de seguridad más amplia. Allí donde existe planificación, monitorización activa, capacidad de respuesta y aprovechamiento probatorio, la tecnología aporta valor. Cuando estos elementos faltan, el sistema tiende a generar captación sin retorno proporcional.

Otro aprendizaje relevante es la constatación de un déficit estructural en materia de protocolos internos, formación y controles posteriores. La encuesta realizada a responsables de unidades de drones confirma que, en muchos casos, los protocolos existen de forma formal, pero no siempre son accesibles, aplicables o interiorizados. Esta debilidad organizativa incrementa la discrecionalidad individual y dificulta la rendición de cuentas, especialmente en contextos de urgencia operativa.

Finalmente, el trabajo pone de relieve que la percepción ciudadana constituye un elemento clave del sistema. La aceptación social de la videovigilancia es real, pero claramente condicionada. La ciudadanía tiende a apoyar estas herramientas cuando las percibe como necesarias, proporcionadas y controladas, pero manifiesta preocupación cuando la vigilancia se presenta como difusa, poco transparente o carente de límites comprensibles.

6.2 Propuesta de mejora y regulación

A la luz de los resultados obtenidos y del contraste con las hipótesis planteadas, resulta evidente que las principales áreas de mejora en el uso policial de la videovigilancia no se sitúan tanto en la necesidad de nuevas prohibiciones o restricciones generales, sino en el refuerzo de los mecanismos de gobernanza interna, estandarización operativa y control efectivo. La propuesta que se plantea a continuación parte de una idea central: la legitimidad de la videovigilancia se construye más desde dentro de la organización que desde la mera acumulación normativa.

a) Reforzamiento de la autorregulación mediante protocolos operativos claros

La primera mejora debe centrarse en crear y consolidar **protocolos internos claros, accesibles y realmente aplicables**. No basta con enunciar principios generales: los protocolos deben traducir el marco jurídico en **reglas operativas concretas** que guíen la actuación diaria. Esto implica definir con precisión los supuestos de activación, los criterios de necesidad y proporcionalidad, la cadena de decisión (quién autoriza y en qué condiciones), los roles y responsabilidades de cada interviniente, y los procedimientos de cierre: documentación de la operación, registro de accesos y trazabilidad de lo actuado.

En el caso de los drones, esta protocolización debe articularse mediante **CONOP diferenciados por escenarios**, evitando aplicar un único patrón a situaciones distintas. Separar de forma expresa misiones como apoyo a emergencias, dispositivos preventivos, búsquedas de personas o intervenciones urgentes permite ajustar el nivel de exigencia y control a cada contexto. Con ello se reduce la discrecionalidad individual, se homogeneiza la actuación entre operadores y se refuerza la rendición de cuentas, haciendo el uso del dron más defendible tanto operativa como jurídicamente.

b) Integración real de la ética en la práctica operativa

Una mejora clave es incorporar la ética como parte del trabajo diario, no como un principio abstracto. En videovigilancia y, especialmente, en drones, el riesgo no suele ser el abuso deliberado, sino la normalización: que, por disponibilidad, se amplíen usos y perímetros sin una justificación clara. Por eso, la ética debe traducirse en criterios operativos simples y verificables que funcionen incluso en situaciones de urgencia.

En la práctica, esto implica aplicar un **doble filtro**. Antes de activar el sistema, debe exigirse una justificación mínima: finalidad concreta, necesidad y ausencia de alternativa menos intrusiva. Durante la operación, la ética se materializa en **minimización real**: acotar tiempo y perímetro de grabación, establecer zonas excluidas cuando proceda y usar de forma restrictiva capacidades de alta intrusión como el zoom o determinados sensores. Después de la intervención, debe garantizarse la **gobernanza del dato**: accesos limitados y registrados, extracción justificada, conservación solo de lo relevante y supresión del resto conforme a criterios y plazos, evitando usos secundarios no previstos.

Finalmente, las actuaciones más intrusivas deberían someterse a una revisión breve y periódica, no punitiva, orientada a aprender y corregir: ajustar umbrales de activación, mejorar protocolos y actualizar el CONOP. De este modo, la ética deja de ser una reflexión ex post y se convierte en una herramienta de control preventivo y de legitimidad, que protege tanto la eficacia operativa como la confianza ciudadana.

c) Mejora de la formación y la cultura de cumplimiento

La formación aparece como uno de los elementos clave para cerrar la brecha entre norma y práctica. Resulta necesario avanzar hacia modelos de formación continua que integren de forma equilibrada los aspectos técnicos, jurídicos y éticos del uso de la videovigilancia. No se trata solo de capacitar para volar o manejar un sistema, sino de formar en criterios de activación, proporcionalidad, documentación y responsabilidad.

Asimismo, la formación debería extenderse más allá de los operadores directos y alcanzar a mandos intermedios y responsables de la toma de decisiones. De este modo, se refuerza una cultura organizativa en la que el cumplimiento normativo y la reflexión ética no se perciben como obstáculos, sino como elementos que protegen tanto al ciudadano como al propio profesional.

d) Fortalecimiento de los mecanismos de control y supervisión

Otra línea de mejora imprescindible es el refuerzo de los controles internos y de la supervisión posterior. La existencia de registros claros de activación, uso y cierre de misión, así como de sistemas de auditoría interna, permite detectar desviaciones, corregir prácticas y mejorar procedimientos. La supervisión no debe concebirse como una herramienta sancionadora, sino como un instrumento de aprendizaje organizativo.

En este sentido, la estandarización de la documentación y la trazabilidad de las actuaciones resulta esencial para proteger el valor probatorio de las imágenes y para garantizar la rendición de cuentas. La ausencia de controles sistemáticos no solo incrementa el riesgo jurídico, sino que debilita la confianza institucional y la percepción de legitimidad.

e) Transparencia y comunicación con la ciudadanía

Finalmente, cualquier propuesta de mejora debe incorporar una dimensión externa orientada a la ciudadanía. La transparencia no implica revelar detalles operativos sensibles, sino explicar de forma comprensible por qué se utilizan determinadas tecnologías, con qué finalidades, bajo qué límites y qué garantías existen para proteger los derechos. Una comunicación clara y coherente contribuye a reducir la percepción de vigilancia opaca y a reforzar la aceptación social del sistema.

La experiencia comparada muestra que la legitimidad de la videovigilancia aumenta cuando la ciudadanía percibe que existen reglas claras, controles efectivos y voluntad institucional de rendir cuentas. En este sentido, la transparencia actúa como un

complemento indispensable de la regulación y de los protocolos internos, cerrando el círculo entre legalidad, ética y operatividad.

6.3 Reflexión final: hacia una videovigilancia legítima y humana

Si algo me deja claro este trabajo es que la videovigilancia no es un debate puramente técnico. No es solo elegir cámaras mejores, drones más capaces o software más "inteligente". En el fondo, es una pregunta sobre **qué tipo de policía queremos ser** y qué relación queremos construir con la ciudadanía. Y esa pregunta obliga a mirar más allá del "funciona o no funciona" para entrar en la legitimidad, que es el terreno donde todo se sostiene… o se rompe.

Yo llevo muchos años en la calle y he visto cómo cambia la delincuencia, cómo cambia la ciudad y cómo cambia la mirada de la gente hacia nosotros. En ese contexto, el dron y la cámara no son neutros. Pueden ser una herramienta útil, incluso decisiva, pero también pueden convertirse en un símbolo. Un dron puede ayudarte a coordinar mejor, a ganar tiempo en una emergencia, a buscar a una persona desaparecida o a dar seguridad en un dispositivo complejo. Pero también puede proyectar la sensación de que "se vigila demasiado". Y esa tensión no se resuelve con discursos: se resuelve con límites claros, control real y una forma de trabajar que sea defendible sin excusas.

Cuando me metí de lleno en el trabajo con drones lo hice con mentalidad de servicio: si la herramienta mejora la respuesta y reduce riesgos, tiene sentido. Sin embargo, este TFG me ha hecho entender algo con más fuerza: **cuanto más potente es una herramienta, más necesario es saber cuándo no usarla**. La tecnología tiene una inercia natural: si está disponible, tiende a desplegarse. A veces por eficacia, a veces por costumbre, a veces por presión operativa. No hace falta mala intención para que aparezcan excesos; basta con falta de estructura.

Por eso, la idea que atraviesa todo el trabajo es muy clara: la clave no es la tecnología, es la gobernanza. Protocolos que existan de verdad y se apliquen, no solo documentos genéricos. Formación continua que integre lo técnico, lo jurídico y lo ético. Trazabilidad y supervisión posterior, para poder justificar decisiones y corregir desviaciones. Y una cultura interna que entienda que grabar no es "un detalle", sino el inicio de responsabilidades.

Además, hay algo que como policía creo que es fundamental asumir: el ciudadano no vive la videovigilancia como la vivimos nosotros. Nosotros pensamos en operatividad, prevención, pruebas, coordinación. El ciudadano piensa en intimidad, límites y control.

Y ambas miradas son legítimas. La brecha aparece cuando nosotros nos refugiamos en el “si es legal, ya está”, pero la ciudadanía percibe “si no lo entiendo, me inquieta”. Con drones esa brecha puede ser mayor, porque su presencia es menos predecible y la captación puede parecer más invasiva, incluso cuando se usa correctamente.

En este sentido, el concepto de CONOP encaja con la forma en que yo entiendo la profesionalidad. Un CONOP bien hecho te obliga a pensar antes de actuar: escenarios, límites, roles, criterios de activación, cierre de misión y control del dato. No te quita rapidez; te da estructura. Y con estructura puedes ser eficaz sin improvisar, proporcional sin perder capacidad operativa, y transparente sin comprometer el servicio.

Termino este trabajo con una convicción: **la tecnología no nos hace mejores policías por sí sola; nos hace más responsables**. Y esa responsabilidad no puede recaer solo en la buena voluntad individual, sino en un sistema interno sólido. Yo quiero una videovigilancia que sirva para proteger, prevenir, coordinar y llegar antes. Pero la quiero con garantías, con límites y con humanidad. Porque lo que está en juego no es solo la eficacia de una herramienta: es la confianza que sostiene la relación entre la policía y la sociedad a la que sirve.

Referencias bibliográficas

- España. (1997). *Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*. Boletín Oficial del Estado.
- España. (1999). *Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997*. Boletín Oficial del Estado.
- España. (2021). *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*. Boletín Oficial del Estado.
- España. (2024). *Real Decreto 517/2024, por el que se regula el uso civil de sistemas de aeronaves no tripuladas y se desarrolla el régimen aplicable a actividades o servicios no cubiertos por la normativa europea*. Boletín Oficial del Estado.
- Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos)*. Diario Oficial de la Unión Europea.
- Unión Europea. (2019). *Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas*. Diario Oficial de la Unión Europea.
- Agencia Estatal de Seguridad Aérea. (2023). *Guía sobre el contenido del Manual de Operaciones (categoría específica), incluyendo anexos de ConOps*. AESA.
- Agencia Estatal de Seguridad Aérea. (2024). *Operaciones con UAS/drones: Categoría específica*. AESA.
- European Union Aviation Safety Agency. (2025). *Guidelines on operations in the open and specific category* (Issue 03). EASA.
- Joint Authorities for Rulemaking on Unmanned Systems. (2023). *Guidelines on Specific Operations Risk Assessment (SORA) (Version 2.5)*. JARUS.
- Agencia Española de Protección de Datos. (2019). *Drones y protección de datos*. AEPD.

- Agencia Española de Protección de Datos. (2025). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. AEPD.
- College of Policing. (2015). *Closed-circuit television (CCTV)*. Authorised Professional Practice.
- Home Office. (2021). *Surveillance Camera Code of Practice*. UK Government.
- Biometrics and Surveillance Camera Commissioner. (2024). *Annual Report and Accounts 2023–2024*. UK Government.
- Cebrián Beltrán, S. (2022). Nuevos desafíos en el ámbito de la videovigilancia por las Fuerzas y Cuerpos de Seguridad desde la perspectiva de la LO 7/2021: El difícil equilibrio entre la seguridad y la protección de datos. *Estudios de Deusto, 70*(1), 221–251.
- Galdón Clavell, G. (2015). Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas. *EURE (Santiago), 41*(123), 81–101.
- Gill, M.., & Spriggs, A. (2005). *Assessing the impact of CCTV* (Home Office Research Study 292). Home Office.
- Piza, E. L.., Welsh, B. C.., Farrington, D. P.., & Thomas, A. L.. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy, 18*(1), 135–159.
- Conseil constitutionnel. (2021). *Décision n° 2021-817 DC (Loi pour une sécurité globale préservant les libertés)*. République française.
- République française. (2023). *Décret n° 2023-283 du 19 avril 2023 (tratamiento de datos por aeronaves para misiones de policía administrativa)*. République française.
- Bundesverfassungsgericht. (1983). *Census Act decision (informationelle Selbstbestimmung / informational self-determination)*. Federal Republic of Germany.
- Supreme Court of the United States. (2018). *Carpenter v. United States*, 585 U.S. (2018).
- U.S. Department of Justice, Office of Legal Policy. (2024). *Artificial Intelligence and Criminal Justice: Final report*. U.S. Department of Justice.

- ACLU. (2024). Stanley, J. *Police drone surveillance and civil liberties* (análisis y posicionamiento institucional). ACLU.
- City of Seattle. (2017). *Ordinance 125376: Acquisition and use of surveillance technologies*. Seattle City Council.
- Tribunal Supremo (Sala de lo Penal). (2025, 2 de octubre). *Sentencia núm. 797/2025* (ECLI:ES:TS:2025:4225). Centro de Documentación Judicial (CENDOJ).