Estudios de Deusto

Revista de Derecho Público

Vol. 70/1 enero-junio 2022

DOI: https://doi.org/10.18543/ed7012022

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

New challenges in the field of video surveillance by the security forces under Organic Law 7/2021: The difficult balance between security and data protection

Selena Cebrián Beltrán
Investigadora doctoral
Universitat de València

https://doi.org/10.18543/ed.2501

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

New challenges in the field of video surveillance by the security forces under Organic Law 7/2021: The difficult balance between security and data protection

Selena Cebrián Beltrán
Investigadora doctoral
Universitat de València

https://doi.org/10.18543/ed.2501

Recibido: 15.02.2022
Aceptado: 14.06.2022
Publicado en línea: junio 2022

Resumen

El presente trabajo pretende analizar el tratamiento de datos personales por parte de las Fuerzas y Cuerpos de Seguridad en el ámbito de la videovigilancia, realizado con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública: a) Un análisis de la regulación de esta materia en relación a la nueva Ley Orgánica 7/2021, de 26 de mayo; b) Examinar cómo se compatibiliza el derecho fundamental a la protección de datos con la seguridad pública; c) Profundizar en los límites del tratamiento de los datos personales por los sistemas de videovigilancia.

Palabras clave

Ley Orgánica 7/2021, videocámaras, Fuerzas y Cuerpos de Seguridad, protección de datos personales, derecho a la intimidad, seguridad pública.

Abstract

This essay intends to analyze the processing of personal data by the Security Forces a in the field of video surveillance, carried out for the purposes of prevention, detection, investigation and prosecution of criminal offenses or the execution of criminal sanctions, including protection and prevention in the face of threats against public security: a) An analysis of the regulation of this matter in relation to the new Organic Law 7/2021, of May 26; b) Examine how the fundamental right to data protection is compatible with public security; c) Delve into the limits of the processing of personal data by video surveillance systems.

Keywords

Organic Law 7/2021, video surveillance, Security Forces, data protection, privacy, public security.

Sumario: I. Origen y antecedentes de la regulación de los sistemas de videovigilancia de las Fuerzas y Cuerpos de Seguridad: adaptación de la legislación española al entorno normativo europeo. II. Videovigilancia en el ámbito de las Fuerzas y Cuerpos de Seguridad: uso de cámaras fijas y dispositivos móviles. 1. Definición de videocámaras fijas y dispositivos móviles. 2. ¿Dónde se instalarán las videocámaras fijas y los dispositivos móviles y quién será el órgano competente para permitir su instalación o uso?. 3. ¿Se debe informar acerca de su instalación o uso?. 4. Duración de la instalación o uso de los sistemas de videovigilancia. 5. Especial referencia a la captación de imágenes y a la inviolabilidad del domicilio. 6. Datos captados por los dispositivos electrónicos. Especial referencia a los datos biométricos. III. Equilibrio en el uso de la videovigilancia: derecho a la protección de datos y derecho a la seguridad. 1. Principio de legalidad de la injerencia. 2. Principio de proporcionalidad. 3. Principio de adecuación. 4. Principio de necesidad. IV. Límites al uso de los sistemas de videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad: protección de datos personales. 1. Aspecto subjetivo. 2. Periodo de conservación de las imágenes. 3. Conservación de la integridad y autenticidad de las grabaciones. Cadena de custodia. 4. Responsabilidad de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado. 5. Ejercicio de los derechos por parte de los interesados. 6. El derecho fundamental a la presunción de inocencia. V. Consideraciones finales y perspectivas futuras. VI. Biblografía.

I. ORIGEN Y ANTECEDENTES DE LA REGULACIÓN DE LOS SISTEMAS DE VIDEOVIGILANCIA DE LAS FUERZAS Y CUERPOS DE SEGURIDAD: ADAPTACIÓN DE LA LEGISLACIÓN ESPAÑOLA AL ENTORNO NORMATIVO EUROPEO

La aceleración del fenómeno de la globalización en estas últimas décadas ha provocado un desarrollo sin parangón de las tecnologías digitales que han ido "permeando las diversas esferas de la vida social, política, económica y cultural en las distintas sociedades de nuestro tiempo".[1]

Pese a las mejoras evidentes que nos ha proporcionado esta tecnología, también han traído nuevas implicaciones en el ámbito del Derecho.[2] En

[1] Gendler, M.A.: "Globalización y tecnología digitales: Un estado de situación", *Unidad Sociológica I* Número 6 Año 2, Buenos Aires, 2016.
https://ri.conicet.gov.ar/bitstream/handle/11336/105689/CONICET_Digital_Nro.d20fd533-eddd-4f24-afaa-8b946e5e9cf6_A.pdf?sequence=2&isAllowed=y

[2] Alegría, H.: "Globalización y Derecho" http://repositoriouba.sisbi.uba.ar/gsdl/collect/pensar/index/assoc/HWA_3114.dir/3114.PDF

particular, ha representado un auténtico desafío para la efectividad del derecho a la protección de datos.

Este derecho, sin perjuicio del debate acerca de su configuración dogmática en clave de habeas data, ha sido objeto de un extenso desarrollo normativo en las últimas décadas para dar respuesta a los nuevos retos que se le planteaban.[3]

En el año 2016, el Parlamento Europeo y el Consejo de la Unión Europea aprobaron sendas normas que asentarían el marco normativo actual de la protección de datos de las personas físicas.

La primera norma, fue el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Posteriormente, en el año 2018, España adaptó el Reglamento General de Protección de Datos al ámbito interno mediante la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.[4]

La segunda norma, fue la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Al tratarse de una Directiva, España quedaba ligada en cuanto a la finalidad, pero no en cuanto a los medios para su transposición[5].

Así lo hacía constar la citada Directiva, que en su artículo 63 apartado 1 indicaba que "Los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva.

---

[3] Al respecto, léase Martínez López-Sáez, M.: *Una revisión del derecho fundamental a la protección de datos de carácter personal. un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea,* Tirant lo Blanch, Valencia, 2018.

[4] Un reciente análisis exhaustivo y detallado de dicha adaptación puede encontrarse en la obra colectiva Tomás Mallén, B., García Mahamut, R., y Pauner Chulvi, C. (Eds.): *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo*, Valencia, Tirant lo Blanch, 2021.

[5] El Tratado de Funcionamiento de la Unión Europea indica en su artículo 288 que "La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios."

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del 6 de mayo de 2018."

Esta previsión fue incumplida por España, que a dicha fecha límite no había incorporado la Directiva (UE) 2016/680 en su ordenamiento jurídico. Este hecho conllevó que el Tribunal de Justicia de la Unión Europea mediante la Sentencia de 25 de febrero de 2021 (Comisión Europea/España, asunto C-658/19), emitiera el siguiente pronunciamiento: "Habida cuenta de la gravedad y de la duración de la infracción, el Tribunal de Justicia condena a España a abonar a la Comisión una suma a tanto alzado de 15 000 000 de euros y, si el incumplimiento declarado persiste en la fecha en que se dicte la sentencia, una multa coercitiva diaria de 89 000 euros desde esa fecha y hasta que se haya puesto fin al incumplimiento declarado."

Esta condena fue innovadora porque era la primera en la que el Tribunal de Justicia imponía, con arreglo al artículo 260 TFUE, apartado 3, los dos tipos de sanciones económicas al mismo tiempo.

Finalmente, España traspuso la Directiva mediante la adopción de la 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.[6]

Entre su regulación se encuentra en la Sección 2ª el Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad. [7]

Esta previsión de la videovigilancia no aparece desarrollada en la Directiva, sino solamente mencionada sucintamente en el Considerando 26[8]; pero España ha creído necesario incluirla dentro de esta norma.

Esta regulación no debe confundirse con la que realiza la 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 y el reglamento de desarrollo a la misma, el Real Decreto 596/1999, de 16 de abril.

---

[6] 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. (2021) (de ahora en adelante se mencionará como LO 7/2021).

[7] Para determinar qué son las Fuerzas y Cuerpos de Seguridad debemos acudir a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que en su artículo 2 incluye:

a) Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la Nación.
b) Los Cuerpos de Policía dependientes de las Comunidades Autónomas.
c) Los Cuerpos de Policía dependientes de las Corporaciones Locales.

[8] Todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con las personas físicas afectadas, y únicamente podrá llevarse a cabo con los fines específicos previstos en la ley. Ello no impide, per se, que las autoridades policiales puedan llevar a cabo actividades tales como las investigaciones encubiertas o la videovigilancia.

En efecto, la LO 4/1997 indica que su regulación va orientada a grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública. Por su parte, la LO 7/2021 va orientada a la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.[9]

La instalación de videocámaras u otros dispositivos son medidas de tipo predelictual utilizadas por el Estado a través de los agentes de la autoridad con la finalidad de garantizar la seguridad general que también contienen datos personales y, por lo tanto, necesitadas de la protección que se otorga a los datos de carácter personal.[10]

Por ello y aunque la finalidad por la que se recaban estas imágenes sean las que hemos referido, en su implementación debe tenerse en cuenta los derechos y libertades individuales, para garantizar, especialmente, el derecho a la intimidad y a la protección de datos personales.[11]

A continuación, se realizará un análisis de los sistemas de videovigilancia, así como se indicará cuándo pueden ser utilizados y qué limitaciones debemos tener en cuenta para conciliar el derecho fundamental a la intimidad y a la protección de datos con el objetivo de garantizar la seguridad pública.

II. VIDEOVIGILANCIA EN EL ÁMBITO DE LAS FUERZAS Y CUERPOS DE SEGURIDAD: USO DE CÁMARAS FIJAS Y DISPOSITIVOS MÓVILES

1. *Definición de videocámaras fijas y dispositivos móviles*

Comenzado por las videocámaras fijas, "se entenderá por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección."[12]

[9] Artículo 1 de la LO 7/2021.

[10] Pérez Estrada, M.J.: "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, pp. 1297-1330.

[11] Aba Catoira, A.: "La videovigilancia y la garantía de los derechos individuales: su marco jurídico", Anuario da Facultade de Dereito da Universidade da Coruña, n. 7, 2003, pp. 13-36.

[12] Artículo 16.1 de la LO 7/2021.

Un "dispositivo móvil" se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales.[13]

Estos dispositivos no solo podrán captar imágenes sino también sonidos como indica el artículo 17.1 de la LO 7/2021.

Bajo el vocablo "dispositivos", por tanto, se deja constancia de que no solo abarca a videocámaras sino a otros elementos tecnológicos como podrían ser PDAs, teléfonos móviles, smartphones u otros elementos más recientes como el uso de cámaras móviles personales tipo "bodycam"[14][15] o uso de drones.

Estos elementos podrán estar ubicados en todos los instrumentos, objetos o medios de transporte utilizados por las Fuerzas y Cuerpos de Seguridad, como puede ser el coche patrulla, el helicóptero, una embarcación o incluso, las cámaras que llevan incorporadas las pistolas táser.[16]

En cuanto a los requisitos a los que están sometidos estos dispositivos, deben ser los necesarios para garantizar la seguridad de los datos, por lo que no se podrían utilizar cámaras o teléfonos personales de los agentes de las Fuerzas y Cuerpos de Seguridad.

Respecto de esto se ha pronunciado la Agencia Española de Protección de Datos (en adelante, AEPD) en una consulta que planteaba si la policía local, en el ejercicio de sus funciones de policía judicial en sentido genérico y en casos excepcionales de máxima urgencia, pudiera captar imágenes por

[13] Véase el interesante análisis que realiza Fernández Sánchez, R.: *El uso policial de la bodycam y sus propuestas de mejora*, Madrid, Ed. Reus, 2019.

[14] Fernández Sánchez, P.: *El uso policial de las bodycam y su propuesta de mejor*a, Madrid, Editorial Reus, 2019, pp. 15-21.

[15] "Anuncio de formalización de contratos de: Subdirección General de Gestión Económica y Patrimonial. Objeto: Suministro de un mínimo de 300 cámaras personales para su uso en diversas unidades del Cuerpo Nacional de Policía y de la Guardia Civil. Expediente: 00000018M089, *Boletín Oficial del Estado, 242*, de 8 de octubre de 2019, páginas 54366 a 54367. La Subdirección General de Gestión Económica y Patrimonial del Ministerio del Interior adquirió en octubre del año 2019 un *suministro mínimo de 300 cámaras personales para su uso en diversas unidades del Cuerpo Nacional de Policía y de la Guardia Civil,* por lo que podemos entender que su uso ya se está extendiendo.

[16] Véase las siguientes noticias: J.C.A.; "Marbella compra videocámaras para las pistolas táser de la Policía Local" en *Marbella 24 horas,* 2021 https://www.marbella24horas.es/local/marbella-compra-videocamaras-para-las-pistolas-taser-de-la-policia-local-29836;

AGENCIAS; "Pistolas táser con cámara de vídeo para la Policía Municipal" en *Madrid es Noticia,* 2020 https://www.madridesnoticia.es/2020/12/pistolas-taser-camara-video-policia-municipal/

cualquier medio a su alcance (videocámaras domésticas y teléfonos móviles) dando cuenta en el plazo de 72 horas mediante informe motivado al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y la Comisión constituida por la Ley Orgánica 4/1997 al efecto con la entrega de dichas imágenes cuando la Comisión lo solicite. A lo que la AEPD contestó que el uso de los dispositivos privados no garantiza la seguridad de los datos; por tanto, rechazó su uso.[17]

Sin embargo, la previsión más interesante la hace al finalizar el análisis: "en el caso de que se utilizasen dispositivos inteligentes que se hayan entregado con carácter oficial para su uso con fines policiales, éstos deberán adoptar todas las precauciones para impedir accesos indebidos a los datos que con ellos se capten."

Por tanto, la AEPD deja claro que los dispositivos personales no pueden ser usados, mientras que los dispositivos que se hayan entregado por las propias Fuerzas y Cuerpos de Seguridad para los fines oficiales sí son admisibles, siempre y cuando se guarden las medidas de seguridad adecuadas.

En lo referente a los drones y si se pueden considerar sistemas de videovigilancia a efectos de la aplicación de la norma específica de protección de datos, debemos acudir a la consulta planteada a la AEDP en la que se pretendía saber si a los drones, en su función de captación de imágenes, les era aplicable la regulación establecida por LO 4/1997[18]. La AEPD respondió afirmativamente a esta cuestión, lo que nos lleva a hacerla extensible a la LO 7/2021 cuando su finalidad fuere la recogida en el artículo 1 de dicha norma.

[17] Véase el Informe Jurídico de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS sobre el uso de cámaras privadas por parte de la Policía Local https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-uso-camaras-privadas-por-la-policia.pdf

[18] "Con igual reiteración la AEPD ha dictaminado que la 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, atribuye a las Fuerzas y Cuerpos de Seguridad la competencia exclusiva para la instalación de videocámaras fijas o móviles en lugares públicos. Por ello la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito de aplicación que "Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal.

Así pues, podemos decir que la ley no permite con carácter general, sin cumplir los requisitos previstos en la legislación citada, la instalación de cámaras de videovigilancia en lugares públicos, ya sean fijas o móviles, lo que en consecuencia y por extensión cabe aplicar a la captación de imágenes de personas en la vía pública a través de sistemas de captación de datos instalados en un dron." https://www.aepd.es/es/documento/informe-juridico-rgpd-drones.pdf

2. *¿Dónde se instalarán las videocámaras fijas y los dispositivos móviles y quién será el órgano competente para permitir su instalación o uso?*

Nos indica la LO 7/2021 que la instalación de las videocámaras fijas será en vías o lugares públicos y que para llevarla a cabo se deberá tener en cuenta el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima, así como realizar un análisis de riesgos y una evaluación de impacto [19].

Ello lleva a extraer por una parte que, su colocación no es libre y, por otra, que solo podrá realizarse en las vías o lugares públicos.

Esta disposición es aplicable no solo a las videocámaras propias de las Fuerzas y Cuerpos de Seguridad, sino que se hace extensiva a aquellas de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento.[20]

Esto se relaciona con el ámbito de la cesión de imágenes que pudiera hacerse desde la seguridad privada a la seguridad pública.[21] Pues, obviamente, los mecanismos de colaboración entre la seguridad pública y la seguridad privada no pueden quedar exentos de la debida ponderación de los derechos fundamentales en juego.[22]

---

[19] Artículo 16.1 LO 7/2021 "1. En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida".

[20] Artículo 16.2 de la LO 7/2021.

[21] Ley 5/2014, de 4 de abril, de Seguridad Privada.

Artículo 15. "1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales."

[22] En el plano doctrinal, una minuciosa ponderación de los derechos fundamentales en juego en el marco de la conciliación y colaboración entre seguridad pública y seguridad priva-

No se podrá, por tanto, instalar en lugares privado ni en domicilios particulares, para lo cual debemos acudir al régimen establecido en la la Ley de Enjuiciamiento Criminal, cuando menciona en sus artículos 588 quater al 588 quinquies c la colocación de estos dispositivos autorizados por la autoridad judicial como medios de investigación dentro de un procedimiento judicial. [23]

Resulta novedosa, por otra parte, la inclusión de una obligación con respecto a los ciudadanos que sean los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, ya que están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.[24]

El procedimiento para la instalación de estas videocámaras fijas no estará sujeto al control preventivo de las entidades locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.[25]

En el ámbito de los dispositivos móviles, en lo que atañe a su uso -repárese que, como las cámaras pueden ir variando de lugar o ser portadas por las Fuerzas y Cuerpos de Seguridad, debemos hablar de un uso y no de una instalación que implicaría la idea de permanencia[26], las autoridades competentes serán:[27]:

1. La persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y de proporcionalidad.
2. En el caso de los Cuerpos de Policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas y bienes y para el mantenimiento del orden público, serán sus órganos correspondientes los que autorizarán este tipo de actuaciones para sus fuerzas policiales, así como para las dependientes de las Corporaciones locales radicadas en su territorio.
3. En casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al

da, puede encontrarse en la obra de Ridaura Martínez, M.J.: *Seguridad privada y derechos fundamentales: la nueva Ley 5/2014, de Seguridad Privada*, Valencia, Tirant lo Blanch, 2015.

[23] Estas disposiciones fueron añadidas mediante la Ley Orgánica 13/2015, de octubre, en vigor desde el 6 de diciembre de 2015.

[24] Artículo 16.4 de la LO 7/2021.

[25] Artículo 16.3 de la LO 7/2021.

[26] Artículo 17.1 de la LO 7/2021.

[27] Artículo 16.1 de la LO 7/2021.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

> Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.[28]

Como ilustración de derecho autonómico comparado, cabe mencionar que la Agencia Catalana de Protección de Datos, a través de la Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, introdujo una regulación del uso de ambos tipos de sistemas de videovigilancia y hace especial referencia a cómo debe ser el uso de videocámaras personales por parte de su policía autonómica, indicando que "la utilización de cámaras o sistemas de videovigilancia por parte de la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña requiere la autorización correspondiente en los supuestos previstos en su normativa específica."[29]

Como ejemplo del uso de estos dispositivos móviles, tenemos el operativo del 1-O por la Unidad de Intervención Policial en el que se captó imágenes con "cámaras Gopro" instaladas en sus cascos y mediante otros dispositivos de grabación. Estas imágenes están en manos del Tribunal Superior de Justicia de Cataluña que va a proceder a analizar los posibles delitos cometidos por los participantes.[30]

En cuanto al lugar de instalación, la LO 7/2021 no hace en su artículo 17 la misma acotación que efectúa el artículo 16 cuando habla de la instalación de sistemas fijos, que es "vías o lugares públicos", por tanto, el uso de los dispositivos móviles debería ser acotado en un futuro.

3. *¿Se debe informar acerca de su instalación o uso?*

La LO 7/2021 indica con respecto a la instalación de sistemas fijos que "los ciudadanos serán informados de manera clara y permanente de la existencia de

---

[28] Artículo 17.3 de la LO 7/2021.

[29] Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia (2009), *Diari Oficial de la Generalitat de Catalunya, 5322*, 13258 -13272. https://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/686.pdf

[30] Véase los siguientes artículos periodísticos: Olmo, J.M.: "Golpes, mossos pasivos, falsos heridos: el 1-O desde las cámaras 'GoPro' de la Policía" en *El Confidencial,* 2018 https://www.elconfidencial.com/espana/2018-04-28/imagenes-gopro-policia1-o-mossos-golpes-falsos-heridos_1556347/

EUROPA PRESS: "La Policía aportó al TSJC 8 horas de grabaciones realizadas el 1-O por agentes con cámaras 'GoPro'·en *Europapress,* 2019 https://www.europapress.es/nacional/noticia-policia-aporto-tsjc-horas-grabaciones-realizadas-agentes-camaras-gopro-20190402193017.html

las videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos".[31]

Evidentemente si el fin perseguido mediante la colocación de las videocámaras fijas es la prevención de la delincuencia, el hecho de mencionar la ubicación exacta pondría en peligro su consecución. Pero, a falta de desarrollo normativo posterior, se debería entender que se tendría que dar una relativa cercanía entre la ubicación del aviso de que hay una instalación fija y la ubicación de la instalación en sí.

Esta misma previsión de información no aparece realizada acerca de los dispositivos móviles.

4. *Duración de la instalación o uso de los sistemas de videovigilancia*

Con relación a las instalaciones fijas, la normativa no indica ningún límite, por lo que podrán colocarse de manera permanente.

En cuanto al uso de dispositivos móviles sí se hace una previsión y es que las autorizaciones "no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro."[32]

Por tanto, que se pueda hacer uso de ellas depende de la existencia de un análisis previo de peligro o la existencia de un evento concreto, como podría ser el caso comentado del 1-O.

5. *Especial referencia a la captación de imágenes y a la inviolabilidad del domicilio*

Como se ha indicado anteriormente, el uso de dispositivos móviles no queda circunscrito a un espacio concreto como sí queda realizado con las videocámaras fijas –vía pública–, por lo que esto lleva a plantearnos un hipotético uso de los sistemas móviles en los lugares cerrados o en el ámbito del domicilio.

Es bien sabido, que la inviolabilidad del domicilio es un derecho fundamental recogido por la Constitución española y que los límites a este derecho según el artículo 18.3 serían la autorización judicial, el consentimiento del titular y, en última instancia, la flagrancia delictiva. También se recogen otros límites en el artículo 55.1 CE, cuando se menciona los supuestos del estado de excepción y de sitio.

La autorización para la captación de imágenes y/o sonidos que contiene la LO 7/2021 proviene de la autorización de las autoridades a nivel

[31] Artículo 16.5 de la LO 7/2021.

[32] Artículo 17. 2 de la LO 4/2021.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

administrativo, por lo que no están comprendidas dentro de los límites que la Constitución española establece para este derecho.

Pero, como se ha indicado, la LO 7/2021 cuando regula los dispositivos móviles, no hace ninguna acotación en este sentido, por lo que quedan varias cuestiones en el aire como, ¿qué ocurre si se está produciendo una grabación en una zona pública y por cuestiones del servicio se debe entrar en un lugar cerrado o, incluso, en el domicilio de una persona? ¿Estas imágenes podrían ser tenidas en cuenta o, por el contrario, deberíamos eliminar cualquier grabación de imagen y sonido que no contase con el consentimiento del titular o una autorización judicial?

O, es más, ¿no se podrían llevar estos dispositivos cuando se va a proceder a realizar una actuación en alguno de estos lugares mencionados?

Por tanto, es claro que la tecnología plantea otras cuestiones que no aparecen recogidas en la legislación vigente. Consecuentemente habrá que ponderar las coordenadas prácticas en las que se va a desenvolver la LO 7/2021 para dar respuesta a estos planteamientos, dado que los supuestos limitativos previstos en el artículo 18.3 de la Constitución son "taxativos", como se encargó de subrayar nuestra Jurisdicción Constitucional en la crucial STC 341/1993, de 18 de noviembre (FJ 8º). Esto ayudaría a mejorar la seguridad jurídica y a garantizar con más éxito el derecho fundamental a la inviolabilidad domiciliaria y, en consecuencia, a la intimidad personal y familiar. De igual manera, esos imperativos de la seguridad jurídica (en términos de accesibilidad y de previsibilidad) fueron destacados por la jurisprudencia del TEDH en un asunto importante de 1998 contra España relacionado con la regulación de las escuchas telefónicas, y por el que nuestro país fue condenado (artículo 8 CEDH) como consecuencia de la insuficiencia normativa e inseguridad jurídica que genera el régimen de dichas escuchas en las previsiones entonces vigentes de la Ley de Enjuiciamiento criminal.[33]

[33] Se trata de la STEDH *Valenzuela Contreras c. España* de 30 de julio de 1998, en cuyo párrafo 46 se señala: "El peligro de arbitrariedad resulta especialmente evidente en los casos en que existe un ejercicio en secreto de facultades discrecionales. Cuando se trata de medidas secretas de vigilancia o de interceptación de las comunicaciones por las autoridades públicas, la exigencia de previsibilidad significa que el Derecho interno debe usar términos suficientemente claros para indicar a todos de manera adecuada en qué circunstancias y bajo qué condiciones se autoriza a los poderes públicos a tomar tales medidas (Sentencia Malone antes citada, págs. 31-32, 66-67; Kruslin antes citada, págs. 22-23, §30; Halford contra el Reino Unido, de 25 de junio de 1997. *Recueil,* 1997-111, pág. 1017, §49, y Kopp antes citada, pág. 541, §64). La existencia de reglas claras y detalladas en la materia es indispensable, tanto más cuanto que los procedimientos técnicos no cesan de perfeccionarse (Sentencias Kruslin y Huvig antes citadas, pág. 23, §33, y pág. 55, §32, respectivamente, y Kopp antes citada, págs. 542-543, §72)".

6. *Datos captados por los dispositivos electrónicos. Especial referencia a los datos biométricos*

Estos instrumentos posibilitan la captación de datos personales más allá de los considerados como "usuales", permitiendo el tratamiento de aquellos datos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física." [34]. Como se apreciará, se trata de datos sumamente sensibles, por lo que habrá que tomar en consideración los principios de protección de tales datos previstos en la legislación española y, por supuesto, en la europea, tanto de la UE (Reglamento General de Protección de Datos y normativa concordante relativa al espacio de libertad, seguridad y justicia) como del Consejo de Europa (especialmente, el Convenio 108 y su versión modernizada -conocido como Convenio 108+-, esta última ratificada recientemente por España, a finales de enero de 2021)[35] .Lógicamente, las sinergias entre las normativas de ambas organizaciones europeas se revelan fundamentales, para evitar distorsiones y dilemas aplicativos en el ámbito interno.[36]

En concreto, se destaca la posibilidad de tratar datos biométricos que van destinados a identificar de manera inequívoca a una persona.

¿Qué debemos incluir bajo el vocablo "datos biométricos"? La propia LO 7/2021 nos indica que son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Como indica la definición, los datos biométricos no se consiguen con la simple captación de imágenes de una persona, sino que se precisa que dichas imágenes posteriormente sean tratadas técnicamente para contribuir a la identificación de la persona.[37]

---

[34] Artículo 13.1 de la LO 7/2021.

[35] Véase Martínez López-Sáez, M.: "La ratificación española del Convenio 108+: consideraciones jurídicas básicas del nuevo marco Paneuropeo de protección de datos", *Revista General de Derecho Europeo*, n. 54, 2021.

[36] La necesidad de esa interacción entre los estándares europeos para conjurar el riesgo de disfunciones en el terreno doméstico ha sido destacada por Tomás Mallén, B.: "Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el convenio 108+ del Consejo de Europa", en García Mahamut, R. y Tomás Mallén, B. (Eds).: *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales*, Valencia, Tirant Lo Blanch, 2019, pp. 57-89.

[37] Se recoge así en el dictamen del 12/2009 del GT 29, p. 19 https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

Por ello, a priori, las imágenes captadas por las Fuerzas y Cuerpos de Seguridad no desvelarían por sí mismas datos biométricos, pero sí se abre la posibilidad a, mediante el desarrollo y aplicación de programas informáticos, proceder a utilizar el reconocimiento biométrico con la finalidad de identificar unívocamente a una persona.

Ahora bien, para utilizarlos debe darse alguna circunstancia justificativa, que en el ámbito de las Fuerzas y Cuerpos de Seguridad constituye la indicada en el artículo 13 en su apartado 2 de la LO 7/2021, esto es, las autoridades competentes podrán tratar dichos datos biométricos cuando lo crean necesario para sus actividades que persigan fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Otro aspecto a tener en cuenta es que la propia Agencia Española de Protección de Datos destaca que los sistemas de identificación/autentificación biométrica, deben ser más seguros para los ciudadanos[38] que otros sistemas de tratamiento de datos.

Por el contrario, la LO 7/2021 no parece seguir dicho enfoque, ya que en su contenido no hay una previsión específica que refuerce este tratamiento en el caso de llevarse a cabo.

III. EQUILIBRIO EN EL USO DE LA VIDEOVIGILANCIA: DERECHO A LA PROTECCIÓN DE DATOS Y DERECHO A LA SEGURIDAD

La Constitución española de 1978 dedica su artículo 18 a la regulación de la intromisión en la esfera de los derechos personalísimos y hace especial referencia al derecho que nos asiste a la protección de datos.

El texto fundamental fue pionero entre los de su entorno al incorporar en el artículo 18.4 que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Desde esta perspectiva, se ha observado que dicha incorporación al Texto Constitucional apuntaba a hacer frente al enorme desafío de "constitucionalizar nuevos derechos que satisfagan la demanda social de protección frente a riesgos y amenazas [sociodigitales] presentes y futuras".[39]

[38] Agencia Española de Protección de Datos "14 equívocos con relación a la autentificación e identificación biométrica" https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf

[39] Rallo Lombarte, A.: "Del Derecho a la Protección de Datos a la Garantía de Nuevos Derechos Digitales" en García Mahamut, R. y Tomás Mallén, B. (Eds).: *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales*, *op.cit*., 2019, p. 137.

Posteriormente, en el año 1982 se aprobó la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

La propia LO 7/2021 en su artículo 15 indica que "La captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen."

Con estas referencias, para poder restringir tales derechos personalísimos de la esfera privada, en favor de la seguridad ciudadana, se deben cumplir una serie de requisitos. Para ello tomaremos como referencia aquellos que indica Agustín-Jesús Pérez-Cruz Martín [40] que podemos considerar el estándar mínimo exigible.[41]

1. *Principio de legalidad de la injerencia*

El Convenio Europeo de Derechos Humanos se refiere al principio de la legalidad de la injerencia en estos términos en su artículo 8.2 "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

El propio Tribunal Europeo de Derechos Humanos ha establecido que la videovigilancia de lugares públicos entra dentro del alcance del artículo 8

[40] Pérez-Cruz Martín, A.J.: "Videovigilancia y derecho a la intimidad: ¿un nuevo ejemplo de conflicto entre el derecho a la seguridad pública y el derecho fundamental a la intimidad?" en *Anuario de la Facultad de Derecho*, pp. 401-412 https://ruc.udc.es/dspace/bitstream/handle/2183/1942/AD-1-21.pdf

[41] Freixes San Juan, T.: *Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos. El standard mínimo exigible a los derechos internos de derechos en Europa.*

El Tribunal parte del carácter del Convenio Europeo como "standard" mínimo previsto para los estados signatarios, todos ellos en línea de la tradición política propia de los sistemas democráticos.

https://personal.us.es/juanbonilla/contenido/CM/TRIBUNAL%20EUROPEO%20DE%20DERECHOS%20HUMANOS/JURISPRUDENCIA%20TEDH/PRINCIPALES%20CRITERIOS%20JURISPRUDENCIALES%20DEL%20TEDH.pdf

cuando los datos visuales se graban, se almacenan y se hacen públicos (Peck c. Reino Unido, §§ 57-63).[42]

Según Teresa Freixes Sanjuán las condiciones impuestas por el Tribunal Europeo para que las injerencias o límites sean compatibles con el Convenio, pueden reconducirse a tres: [43]

1. Que los límites estén previstos en la ley.
2. Que los límites sean necesarios en una sociedad democrática para conseguir un interés legítimo.
3. Que los límites sean proporcionales con relación al fin legítimo perseguido.

En relación con los límites previstos en la ley, el artículo 18 de la Constitución española que reconoce los citados derechos de la esfera privada, y en particular su apartado 4, deben ser desarrollados en nuestro ordenamiento jurídico a través de una ley orgánica que en todo caso deberá respectar su contenido esencial. En efecto, esta materia está sometida a reserva de ley orgánica a la luz del artículo 53.1[44] CE en conjunción con el artículo 81 CE.[45]

El inconveniente viene cuando los frenéticos cambios y mejoras tecnológicas no van acompasadas con los cambios legislativos, surgiendo nuevas formas de garantizar la seguridad pública que intentan encajarse en una legislación desfasada.

En cuanto a sus fines, están dentro de los recogidos en el artículo 104 de la Constitución española "1. Las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana."

Como es lógico, la acción administrativa de las fuerzas y los cuerpos de seguridad del Estado, a efectos de asegurar ese orden público, no se concreta únicamente en medidas de represión de las posibles perturbaciones de esos

[42] Análisis contenido en la Guía sobre el artículo 8 del Convenio Europeo de Derechos Humanos de la Corte Europea de Derechos Humanos https://www.echr.coe.int/Documents/Guide_Art_8_SPA.pdf

[43] Freixes San Juan, T.: *Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos. El standard mínimo exigible a los derechos internos de derechos en Europa.*

[44] "Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a)."

[45] El artículo 81 CE al indicar que "1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales…" incluye en ellos al artículo 18 situado en la Sección 1ª del Capítulo Segundo del Título I "De los derechos fundamentales y de las libertades públicas".

derechos, sino que también incluye medidas de prevención, y dentro de dichas medidas se incluye el uso de los sistemas de videovigilancia.[46] En otras palabras, es obvio que las eventuales extralimitaciones en el ejercicio de la libertad deben corregirse introduciendo medidas compensatorias del potencial déficit de seguridad.

Nos restaría incidir en el último aspecto, ya mencionado, para asegurar la compatibilidad de la acción policial con el CEDH, que sería su proporcionalidad con el fin perseguido, lo cual será analizado a continuación.

2. *Principio de proporcionalidad*

El principio de proporcionalidad está orientado a resolver conflictos entre derechos, intereses o valores en concurrencia, atendido a su grado de injerencia en un ámbito protegido, así como al carácter y alcance del sacrificio que impone sobre los derechos o intereses afectados.[47]

Pero el principio de proporcionalidad, en palabras del Tribunal Constitucional en la Sentencia 55/1996, no es un principio único y aislado, sino que debe ponerse en valor junto con otros principios:

"[e]s, si quiere decirse así, un principio que cabe inferir de determinados preceptos constitucionales … y, como tal, opera esencialmente como un criterio de interpretación que permite enjuiciar las posibles vulneraciones de concretas normas constitucionales. Dicho con otras palabras, desde la perspectiva del control de constitucionalidad que nos es propio, no puede invocarse de forma autónoma y aislada el principio de proporcionalidad, ni cabe analizar en abstracto si una actuación de un poder público resulta desproporcionada o no. Si se aduce la existencia de desproporción, debe alegarse primero y enjuiciarse después en qué medida ésta afecta al contenido de los preceptos constitucionales invocados: sólo cuando la desproporción suponga vulneración de estos preceptos cabrá declarar la inconstitucionalidad."

Por tanto, el análisis del principio de proporcionalidad es indispensable para saber si una medida restrictiva de un derecho fundamental "es susceptible de conseguir el objetivo propuesto (juicio de idoneidad): si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más

[46] De la Serna Bilbao, M.N. "Seguridad ciudadana y los sistemas de videovigilancia. Límites, garantías y regulación en *Iusta*, 45. 2016, pp. 129-163.

[47] "XV Conferencia Trilateral 24-27 de octubre 2013: *Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española,* Roma, p.2 https://www.tribunalconstitucional.es/es/trilateral/documentosreuniones/37/ponencia%20espa%C3%91a%202013.pdf

beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad, en sentido estricto)".[48]

La LO 7/2021 especifica que las Fuerzas y Cuerpos de Seguridad deben seguir el principio de proporcionalidad, en relación con los siguientes criterios para la instalación de sistemas de grabación de imágenes y sonidos:[49]

a) asegurar la protección de los edificios e instalaciones propias;
b) asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia;
c) salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Por otra parte, el artículo 16.1 ahonda en la cuestión señalando que "en las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima" y así también lo señala el artículo 17.1 "(…) adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad."

La norma es consciente del reto que es conciliar las dos esferas- protección de datos y seguridad pública- y, por ello, nos indica que hay que poner en relación el principio de proporcionalidad con el de idoneidad del instrumento utilizado y el principio de intervención mínima.

El Tribunal Constitucional considera idónea la medida cuando es susceptible de conseguir el objetivo propuesto (STC 207/1996, de 16 de diciembre), considerando la idoneidad como una de las tres exigencias del principio de proporcionalidad: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto (SSTC 173/2011, de 7 de noviembre y 115/2013, de 9 de mayo).[50]

En cuanto al principio de intervención mínima, este es más seguido en el ámbito del Derecho Penal, y como indica la STC 26/2018, de 5 de marzo [51] queda caracterizado de la siguiente manera:

> "Debe recordarse también que, según expresó la STC 229/2003, de 18 de diciembre, en materia penal rige el denominado principio de intervención mínima, conforme al cual la intromisión del Derecho Penal debe

[48] STC 66/1995, de 8 de mayo; 55/1996, de 28 de marzo; 207/1996, de 16 de diciembre.

[49] Artículo 15.2 de la LO 7/2021.

[50] Circular 1/2019, de 6 de marzo, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.

[51] https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25597

> *quedar reducida al mínimo indispensable para el control social*. De modo tal que la sanción punitiva, como mecanismo de satisfacción o respuesta, se presenta como *ultima ratio,* reservada para aquellos casos de mayor gravedad y siempre sometida a las exigencias de los principios de legalidad y tipicidad. (…)"

Aplicando este análisis al supuesto que estamos estudiando, la instalación de videocámaras fijas y dispositivos móviles se ceñirán a la afectación mínima indispensable de los derechos de los ciudadanos para proceder a satisfacer los fines indicados en el artículo 1 de la norma.

3. *Principio de adecuación*

Indica Robert Alexy que "el principio de adecuación excluye el empleo de medios que perjudican la realización de al menos un principio, sin promover al menos un principio o meta a cuya realización sirven". [52]

Esta adecuación puede ser *ex ante*, es decir, si la medida legislativa es adecuada para lograr el fin que se propone, considerada en el momento que se ordenó; pero también puede ser ex post, que llegue a ser adecuada posteriormente gracias a los cambios científicos, tecnológicos o sociales.[53]

Desde esta perspectiva varios autores, entre ellos Juan Manuel López[54] o Samuel Parra[55], han sostenido que la regulación contenida en la LO 7/2021 constituye una suerte de justicia preventiva, por lo que no se estaría haciendo un tratamiento conveniente de la videovigilancia.

En palabras de Emiliano Borja Jiménez la justicia preventiva penal es un concepto proveniente del Derecho anglosajón utilizado para "designar un conjunto de instituciones del Derecho Penal, del Derecho Procesal, del Derecho sancionador, e incluso del Derecho Civil, que tienen en común su carácter coactivo y restrictivo de bienes y libertades de los sujetos afectados con el fin de perseguir intereses generales de mayor relevancia (justicia, seguridad ciudadana, salud pública y otros similares). Se trata, por tanto, de justicia preventiva porque abarca una serie de medidas legales, de naturaleza coercitiva

---

[52] Alexy, R.: *Derechos Fundamentales, ponderación y racionalidad,* p. 8 https://www.corteidh.or.cr/tablas/r25294.pdf

[53] Sánchez Gil, R.: *Principio de proporcionalidad,* México, 2007, pp. 36-59. https://archivos.juridicas.unam.mx/www/bjv/libros/5/2422/8.pdf

[54] Alías, M.:"Polémica por la nueva ley del Gobierno para proteger datos en las causas penales" en *Voz pópuli*, 2021 https://www.vozpopuli.com/espana/ley-datos-proteccion.html

[55] Infantes, G. "Nos preguntáis si una "nueva ley" permite al Gobierno recabar información sobre sexualidad o ideología: es para proteger datos en investigaciones policiales", en *Newtra*l, 2021, https://www.newtral.es/gobierno-datos-geneticos-sexualidad-biometricos/20210603/

con las que cuenta el Estado para evitar en el futuro el menoscabo de intereses colectivos o ataques a bienes jurídicos de la comunidad."[56]

Por tanto, este sistema iría orientado, en un primer momento, preventivo, a la evitación del delito y, posteriormente, represivo, a la posible identificación de los culpables a través de las imágenes captadas por las videocámaras fijas o los dispositivos móviles. [57]

Centrándonos en la disuasión delictiva, José Luis Díez Ripollés y Ana Isabel Cerezo Domínguez realizaron un trabajo en el que sintetizan los primeros resultados de un estudio empírico pionero en España[58], desarrollado en la ciudad de Málaga y mediante el que se ha pretendido verificar la eficacia de la instalación de videocámaras en lugares públicos en la prevención de la delincuencia y en la creación de sentimientos de seguridad en los ciudadanos.

En sus conclusiones alcanzadas indican lo siguiente: "Los resultados provisionales acabados de recoger avalan en gran medida la primera hipótesis de nuestro trabajo. En efecto, la instalación de videocámaras ha reducido el crecimiento de la tasa de delitos en la zona en la que están operativas, en comparación con la zona de control. En términos de representatividad sobre el conjunto de delitos producidos, la mayoría de los delitos patrimoniales han reducido su porcentaje en la zona de tratamiento, en sentido contrario a lo que ha sucedido en la zona de control."

En cuanto a la posibilidad de identificación del delito mediante el uso de estos instrumentos, debemos plantearnos cómo se tratan los datos resultantes de la videovigilancia por las Fuerzas y Cuerpos de Seguridad, en especial cuando las imágenes y/o los sonidos contienen hechos presuntamente delictivos.

La LO 7/2021 responde a esta cuestión en su artículo 18: "las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación (…). En el caso de que las cámaras no hubiesen captada nada de esto, la eliminación de las imágenes y/o sonidos será realizada a los tres meses."[59]

---

[56] Borja Jiménez, E.: "Justicia penal preventiva y Derecho penal de la globalización: proyecciones en el ámbito del terrorismo", *Estudios jurídico penales y criminológicos*, Vol. 1, 2018, págs. 803-837

[57] Lechner, M.: *Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social* http://ridaa.unq.edu.ar/handle/20.500.11807/264

[58] Díez Ripollés, J.L y Cerezo Domínguez, A.I.: *La prevención de la delincuencia callejera mediante videocámaras. Regulación jurídica y eficacia* https://scielo.conicyt.cl/scielo.php?pid=S0718-33992009000100006&script=sci_arttext

[59] 1. Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de

Pongámonos en el supuesto de que se han captado hechos antijurídicos, ¿qué valor procesal le otorgaríamos a ese material?

La LO 7/2021 no se pronuncia acerca de este valor procesal.[60]

Para la incorporación en el proceso penal de estas grabaciones obtenidas de modo extrajudicial se debe cumplir una serie de requisitos señalados por la jurisprudencia que, dado el vacío legal al respecto (al efecto la Sentencia del Tribunal Supremo (Sala 2ª, Sección 1ª) nº 1517/2006 (recurso nº 1577/2004) de 17 de marzo de 2006 y la STS (Sala 2ª, Sección 1ª) nº 4822/1998 (recurso nº 4018/1998) de 17 de julio de 1998), se basan en el control, a posteriori, de la autoridad judicial:[61]

En primer lugar, es importante que las grabaciones hayan sido obtenidas de manera legítima, teniendo en cuenta que, si la intromisión es ilegítima a la hora de obtener la prueba, vulnera el principio de presunción de inocencia recogido por el art. 24 CE, y si así se declarase en sede judicial, la consecuencia será el dictado de una sentencia absolutoria (siempre y cuando no existan otras pruebas de cargo de entidad suficiente). [62]

La STS (Sala 2ª, Sección 1ª) nº 503/1999 (recurso nº 3185/1997) de 30 de enero de 1999, la STS (Sala 2ª, Sección 1ª) nº 558/2014 (recurso nº 10645/2013) de 28 de enero de 2014 y la STS (Sala 2ª, Sección 1ª) nº 80/2017 (recurso nº 643/2016) de 12 de enero de 2017 declaran que "la eficacia probatoria de la filmación videográfica está subordinada a su visualización en el acto del juicio oral, para que tengan realidad los principios procesales de contradicción e igualdad inmediación y publicidad. Así la doctrina jurisprudencial, sentencias citadas anteriormente, exigen que el material videográfico haya sido visionado en juicio oral con plenas garantías de contradicción y publicidad."

De hecho, a esta vulneración del derecho fundamental a la presunción de inocencia también se refiere la LO 7/2021 cuando indica en su artículo 9 que el hecho de que se establezcan diferentes categorías de interesados "no debe

infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

[60] Pajares Montolio, E.: "Videovigilancia y Constitución" en *Cuadernos de Derecho Público*, n. 26, 2006, pp. 173-216.

[61] Suárez-Quiñones y Fernández, J.C.: *Las video-grabaciones como prueba en el proceso penal* file:///C:/Users/selen/Downloads/Dialnet-LasVideograbacionesComoPruebaEnElProcesoPenal-2149959.pdf

[62] Durán Alonso, S., y Aranda Serna, F. J.: "Videovigilancia en lugares públicos: su utilización como prueba en el proceso penal español", *Estudios en Seguridad y Defensa,* n. 16 (31), pp. 115-135. https://doi.org/10.25062/1900-8325.298

impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución."[63]

En segundo lugar, para que estas grabaciones sean tenidas en cuenta sería necesario la realización de un control de integridad de la video-grabación mediante una cadena de custodia, que trataremos en el punto siguiente.

En tercer lugar, debería atenderse al control de autentificación de la filmación, de lo que ya es consciente la propia LO 7/2021 cuando indica que [las Fuerzas y Cuerpos de Seguridad] pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible.

En cuarto lugar, se deberían respetar los principios procesales de contradicción, igualdad e inmediación, por ello será necesario volver a visionar las imágenes obtenidas una vez concluya la fase de instrucción; concretamente, en el momento de practicar la prueba en el acto del juicio oral.[64]

4. *Principio de necesidad*

La jurisprudencia se ha pronunciado en el sentido de que "el subprincipio de necesidad, requiere que la medida dictada por la Autoridad Judicial sea necesaria en el sentido de que no exista la posibilidad de adoptar otra medida más moderada para la consecución del tal propósito con igual eficacia" (STC 207/1996 F.J. 4).

Por tanto, se debe acreditar que la instalación de videocámaras fijas y el uso de dispositivos móviles es indispensable para el objetivo perseguido y que no hay otro mecanismo alternativo menos gravoso o intromisivo contra los derechos fundamentales a la intimidad y a la protección de datos.

---

[63] Artículo 9 de la LO 7/2021. Distinción entre categorías de interesados.

El responsable del tratamiento, en la medida de lo posible, establecerá entre los datos personales de las distintas categorías de interesados, distinciones tales como:

a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
b) Personas condenadas o sancionadas por una infracción penal.
c) Víctimas o afectados por una infracción penal o que puedan serlo.
d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución.

[64] Suárez Quiñones y Fernández, J.C.: "Las video-grabaciones como prueba en el proceso penal" en *Boletín del Ministerio de Justicia*, n- 60, 2006, pp. 4515-4543.

IV. LÍMITES AL USO DE LOS SISTEMAS DE VIDEOVIGILANCIA POR PARTE DE LAS FUERZAS Y CUERPOS DE SEGURIDAD: PROTECCIÓN DE DATOS PERSONALES

La LO 7/2021 es sabedora de que, aunque su objeto sea la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, deben existir límites a la transgresión de la intimidad y a los datos personales objeto de tratamiento.

1. *Aspecto subjetivo*

El primer límite impuesto es que la instalación y utilización de estos sistemas de videovigilancia solo puede realizarse por las Fuerzas y Cuerpos de Seguridad.

No se permite su uso o instalación por particulares o por otro tipo de funcionarios públicos.

Esto viene referido a que la finalidad de proteger la seguridad ciudadana se le otorga en exclusiva por la Constitución española en el artículo 104 a las Fuerzas y Cuerpos de Seguridad.

2. *Periodo de conservación de las imágenes*

El segundo límite tiene que ver con el periodo de conservación de las imágenes, distinguiendo si contienen la comisión de hechos que pudiesen ser constitutivos de infracciones penales o no.

En referencia a las videocámaras fijas, no hay ninguna previsión al respecto.

En cuanto a los dispositivos móviles, si las imágenes y/o sonidos captados pudieran constituir una infracción penal las Fuerzas y Cuerpos de Seguridad deberán ponerlos a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.[65]

En caso contrario, las imágenes deberán ser destruidas en un plazo máximo de tres meses.[66]

[65] Artículo 18.1. de la LO 7/2021.

[66] Artículo 18.3 de la LO 7/2021.

3. *Conservación de la integridad y autenticidad de las grabaciones. Cadena de custodia*

Si bien la LO 7/2021 ordena que las imágenes sean trasladadas a sede judicial, no se hace ninguna previsión acerca de su cadena de custodia, que podría plantear problemas en un futuro.

Este punto es necesario para salvaguardar la integridad y la autenticidad de las imágenes captadas y, además, que puedan ser usadas en un posible procedimiento judicial y que puedan ser consideradas como una prueba válida.

El Tribunal Supremo se ha pronunciado al respecto en la sentencia (Sala 2º) nº 299/2006, de 17 de marzo (nº recurso 1577/2004), indicando que para considerar el videograma como prueba de cargo se requieren las siguientes exigencias:

a) el primer condicionamiento está integrado por la supervisión judicial de las condiciones de la captación de imágenes, que en todo caso han de ser respetuosas con el derecho a la intimidad personal y a la inviolabilidad domiciliaria;
b) comunicación o puesta a disposición judicial del material videográfico grabado en evitación de manipulaciones;
c) aportación de los soportes originales en los que se incorporan las imágenes captadas;
d) aportación íntegra de lo filmado (lógicamente que tenga relación con la investigación del delito), a fin de posibilitar la selección judicial de las imágenes relevantes para la causa.

El procedimiento de recogida, traslado y custodia de las evidencias adquiere un especial relieve en tanto que se debe garantizar la autenticidad, inalterabilidad e indemnidad de la prueba pericial que se realice sobre las muestras e indicios obtenidos en la investigación criminal. La cadena de custodia es el nombre que recibe ese conjunto de actos que, en definitiva, garantizan la verosimilitud de la prueba.[67]

La transgresión de la cadena de custodia afectaría a varios de los principios constitucionalmente previstos en el artículo 24, como es el derecho a un juicio justo y con todas las garantías, así como podría significar una afectación indebida al principio de presunción de inocencia.

En este mismo sentido se ha pronunciado el Tribunal Supremo en sentencias como la STS (Sala 2ª, Sección 1ª) nº 2250/2013 (recurso nº 1179/2012)

[67] Richard González, M.;"La cadena de custodia en el proceso penal español" en *La Ley,* nº 8187, 2013, http://www.gabineteorellana.com/articulos/LA%20LEY%20Especial%20probatica%2012.pdf

de 26 de marzo de 2013 o el Tribunal Constitucional en sentencias como la STC 199/2013, de 5 de diciembre, la STC 43/2014, de 27 de marzo o la STC 189/2016, de 14 de noviembre. Y, por supuesto, debe tenerse en cuenta la interpretación (por mandato del artículo 10.2 de la Constitución) o el control subsidiario operado eventualmente por el TEDH (tras el agotamiento de los recursos judiciales internos) sobre la base del derecho a un proceso equitativo del artículo 6 CEDH.

Por tanto, será indispensable para la celebración de un procedimiento judicial sin mácula que el material captado a través de las videocámaras fijas y otros dispositivos guarde una adecuada cadena de custodia y que misma sea desarrollada por legislación ad hoc aplicable a la materia.

4. *Responsabilidad de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado*

Por otra parte, si los miembros de las Fuerzas y Cuerpos de Seguridad no guardan la diligencia debida en el ejercicio de las funciones que tienen asignadas respecto de los sistemas de videovigilancia estarán sujetos a responsabilidad disciplinaria de carácter administrativo y, en su caso, a la penal.

El artículo 19 de la LO 7/2021, señala que, "sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica".[68]

Por otra parte, el mismo artículo regula los supuestos en los que los miembros de las Fuerzas y Cuerpos de Seguridad habrán cometido una infracción administrativa. Se debe destacar que la consideración que se les da a las faltas en el ámbito de la videovigilancia es de muy graves, y son las siguientes:

a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.
b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.
c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.
d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.

[68] Artículo 19.1 de la LO 7/2021.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

5. *Ejercicio de los derechos por parte de los interesados*

La norma hace referencia a la posibilidad de que los interesados ejerciten los derechos de acceso (art. 22), rectificación, supresión y limitación de su tratamiento (at. 23) – obsérvese que esta norma no contempla la portabilidad de los datos como sí hace la LO 3/2018-.

Para poder desgranar este límite debemos abordar quién será interesado a efectos de esta norma.

El artículo 9 nos indica que las categorías de interesados son:

a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
b) Personas condenadas o sancionadas por una infracción penal.
c) Víctimas o afectados por una infracción penal o que puedan serlo.
d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución.

6. *El derecho fundamental a la presunción de inocencia.*

El hecho de ser interesado de las cuestiones que regula la norma no elimina el derecho a la presunción de inocencia.

Esta previsión va orientada a que, por ejemplo, el hecho de que una cámara fija instalada por la Policía Nacional captase a una persona que presuntamente ha cometido un hecho delictivo, no es suficiente para considerarlo culpable ni mucho menos porque siempre debemos de recurrir al principio de presunción de inocencia.

Al interpretar este artículo junto con la regulación del tratamiento de datos personales en el ámbito de la videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad, adquiere más importancia todavía el alcance restrictivo de esa potencial limitación de los derechos fundamentales. Ese es el sentido, por ejemplo, del artículo 18 CEDH (limitación de la aplicación de las restricciones de derechos) cuando dispone que "las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual hayan sido previstas". En otros términos, como es sabido, las restricciones a los derechos y libertades deben ser objeto de interpretación restrictiva.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 70/1, enero-junio 2022, págs. 221-251
https://doi.org/10.18543/ed.2501 • http://www.revista-estudios.deusto.es/

De ahí que si se captase alguna imagen de un acto presuntamente delictivo no son las Fuerzas y Cuerpos de Seguridad las que tendrían un papel clave, sino que las imágenes deberán ser puestas a disposición judicial y de no poder ser así, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

V. CONSIDERACIONES FINALES Y PERSPECTIVAS FUTURAS

La tecnología se desarrolla a un ritmo superior al que se elabora y se actualiza la legislación nacional e internacional. Piénsese que son miles de compañías especializadas las que trabajan para hallar el mejor instrumento posible pero que en las institucionales internacionales o en España solo tenemos un respectivo foco de producción normativa con proyección más general, que consiguientemente debe lidiar con una multitud de asuntos.

A ello debe sumarse que estos nuevos cambios han provocado que haya que perfeccionar los límites que deben establecerse para proteger a los derechos fundamentales de las nuevas injerencias.

El tratamiento de datos mediante el uso de videocámaras contiene implicaciones para la intimidad y para la protección de datos personales, por lo que hay que equilibrar la difusa barrera entre sentirse protegido y sentirse observado y esto es lo que ha constituido el objetivo de la 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.

Esta norma ha detallado las condiciones de instalación y uso de la videovigilancia y ha determinado las salvaguardias indispensables que se deben asignar a los mismos para limitar sus efectos. También ha puesto especial énfasis al uso del principio de proporcionalidad y otros principios subsidiarios con relación a los utilizados para consolidar las cautelas necesarias cuando los derechos fundamentales se pueden ver limitados o transgredidos.

Aun así, y dada la variedad de técnicas que tenemos al alcance actualmente, quedan elementos por configurar con un impacto directo en cuestiones fundamentales.

Una de esas cuestiones es la diversidad de datos que pueden ser captados a través de esos instrumentos y la ausencia de protecciones específicas para las categorías consideradas especiales.

Otro aspecto merecedor de una mejor disciplina sería contemplar cómo proteger de manera más férrea las imágenes captadas de menores o personas discapacitadas necesitadas de especial protección.

Por otro lado, se debería tratar la posible colisión con otros derechos fundamentales como es el de inviolabilidad domiciliaria durante el uso

específico de dispositivos móviles o las posibles consecuencias en relación al principio de presunción de inocencia.

Por añadidura, se deberían constreñir los límites que impone la Ley Orgánica, a fin de concretarlos más y de evitar recovecos que pudieran plantear problemas de difícil resolución. Y dentro de esto, con carácter más específico, ser más exhaustivos acerca de cómo realizar una cadena de custodia que permita la conservación de las imágenes íntegras y sin atisbo de duda acerca de su autenticidad.

Por ello, también debería hacerse especial hincapié en la necesidad de aplicar un sistema de seguridad que protegiera el almacenamiento de las imágenes y/o sonidos y que asegurara su completo borrado una vez pasado el tiempo legislativamente indicado, o una vez hayan quedado desvinculadas de los procedimientos en los que hayan formado parte.

Sin duda, todo lo anterior persigue el objetivo que indica la norma específica que nos ocupa en relación con la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Pero ello abre el debate acerca de si la seguridad pública es suficiente para la limitación de determinados derechos fundamentales, como los que nos ocupan en este análisis. En otras palabras, el inseparable binomio libertad-seguridad adquiere una nueva dimensión con la nueva normativa adoptada en España.

La seguridad pública, como competencia exclusiva del Estado (art. 149.1. 29ª CE), es uno de los elementos indispensables de toda nación, tanto en el ámbito internacional como en el ámbito nacional. Y es objetivo de todo poder público tener un ambiente seguro, lo que genera sentimientos positivos a la ciudadanía y lo que tiene un impacto directo en la política, la economía o, incluso, el turismo.

Por ello, ser considerado un país, un territorio o una zona como espacios seguros adquiere tanta importancia que es necesario utilizar todos los recursos disponibles. O sea, garantizar los dictados de la seguridad conciliándolos con los imperativos de la libertad constituye un enfoque de orden público no restrictivo, sino orientado a la defensa de los derechos fundamentales y las libertades públicos.

La instalación de videocámaras fijas y el uso de dispositivos móviles corresponde a la puesta al servicio del Estado de medios técnicos para conseguir este objetivo de seguridad pública. Y, consecuentemente, proteger a toda la ciudadanía mediante este sistema preventivo.

Ahora bien, como se ha comentado, estas videocámaras tienen efectos directos sobre la intimidad de las personas (art. 18.1) y sobre su protección de datos personales (art. 18.4) o, incluso podrían llegar a afectar a su

inviolabilidad domiciliara (art. 18.2). Esto implica que su utilización deba estar sobradamente justificada y que se haga de la forma menos invasiva posible a los derechos anteriormente mencionados.

Pero también implica la puesta a disposición del ciudadano de mecanismos de limitación y restauración de los derechos, como es un tiempo máximo de conservación de las imágenes, o igualmente los derechos de acceso, rectificación, oposición o limitación de los datos, sin olvidar el debido respeto y consideración al principio de presunción de inocencia (art. 24 CE).

La compaginación de seguridad pública e intimidad y protección de datos constituye una tarea harto complicada que solo puede resultar efectiva mediante un escrupuloso desarrollo normativo, que deberá ser interpretado y resuelto en última instancia a través de la labor desempeñada por los órganos jurisdiccionales.

Expresado lo cual no debemos ser pesimistas en exceso, en la medida en que de unas décadas a esta parte hemos conseguido poner en la agenda de todas las organizaciones internacionales y nacionales el asunto de la protección de datos y se ha recorrido un exitoso camino para su delimitación y protección.

En los próximos años asistiremos a un desarrollo similar en materia del tratamiento que de estos datos realicen las autoridades policiales y a través de ello conseguiremos una sociedad con mayores cotas de seguridad y libertad en todos los aspectos.

VI. BIBLIOGRAFÍA

Aba Catoira, A.: "La videovigilancia y la garantía de los derechos individuales: su marco jurídico", *Anuario da Facultade de Dereito da Universidade da Coruña*, n. 7, 2003, pp. 13-36.

Ajares Montolio, E.: "Videovigilancia y Constitución", *Cuadernos de Derecho Público*, n. 26, 2006, pp. 173-216.

Alegría, H.: "Globalización y Derecho".

Alexy, R.: *Derechos Fundamentales, ponderación y racionalidad.*

De la Serna Bilbao, M.N. "Seguridad ciudadana y los sistemas de videovigilancia. Límites, garantías y regulación", *Iusta*, 45. 2016, pp. 129-163.

Díez Ripollés, J.L y Cerezo Domínguez, A.I.: *La prevención de la delincuencia callejera mediante videocámaras. Regulación jurídica y eficacia.*

Durán Alonso, S., y Aranda Serna, F. J.: "Videovigilancia en lugares públicos: su utilización como prueba en el proceso penal español", *Estudios en Seguridad y Defensa,* n. 16 (31), pp. 115-135.

Fernández Sánchez, R.: *El uso policial de la bodycam y sus propuestas de mejora*, Madrid, Ed. Reus, 2019.

Freixes San Juan, T.: *Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos. El standard mínimo exigible a los derechos internos de derechos en Europa.*

García Mahamut, R. y Tomás Mallén, B. (Eds).: *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales*, Valencia, Tirant Lo Blanch, 2019, pp. 57-89.

Gendler, M.A.: "Globalización y tecnología digitales: Un estado de situación", *Unidad Sociológica I* Número 6 Año 2, Buenos Aires, 2016.

Lechner, M.: *Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social.*

Martínez López-Sáez, M.: "La ratificación española del Convenio 108+: consideraciones jurídicas básicas del nuevo marco Paneuropeo de protección de datos", *Revista General de Derecho Europeo*, n. 54, 2021.

Pérez Estrada, M.J.: "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, pp. 1297-1330.

Pérez-Cruz Martín, A.J.: "Videovigilancia y derecho a la intimidad: ¿un nuevo ejemplo de conflicto entre el derecho a la seguridad pública y el derecho fundamental a la intimidad?", *Anuario de la Facultad de Derecho*, pp. 401-412.

Rallo Lombarte, A.: "Del Derecho a la Protección de Datos a la Garantía de Nuevos Derechos Digitales" en García Mahamut, R. y Tomás Mallén, B. (Eds).: *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales*, 2019, pp. 137 y ss.

Richard González, M.: "La cadena de custodia en el proceso penal español" en *La Ley,* nº 8187, 2013,

Ridaura Martínez, M.J.: *Seguridad privada y derechos fundamentales: la nueva Ley 5/2014, de Seguridad Privada*, Valencia, Tirant lo Blanch, 2015.

Sánchez Gil, R.: *Principio de proporcionalidad,* México, 2007, pp. 36-59.

Suárez-Quiñones y Fernández, J.C.: *Las video-grabaciones como prueba en el proceso penal,* n- 60, 2006, pp. 4515-4543.

Tomás Mallén, B., García Mahamut, R., y Pauner Chulvi, C. (Eds.): *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo*, Valencia, Tirant lo Blanch, 2021.