



**ACREDITACIÓN  
INSTITUCIONAL EN  
ALTA CALIDAD**  
Resolución 008607 de mayo 16 de 2022

## **Las cámaras de videovigilancia y la vulneración del derecho a la intimidad de los ciudadanos en la ciudad de Medellín**

Autor(es)

Wilmer Arvey Sánchez Agudelo

Carlos Alberto Arcila Valencia

Carlos Mauricio Restrepo Galeano

Monografía de investigación presentado para optar por el título de Magíster en Derecho  
Procesal Penal y Teoría del Delito

Asesor

Fernando León Tamayo Arboleda, Doctor en Derecho

Universidad Autónoma Latinoamericana (UNAULA)  
Escuela de Posgrados  
Maestría en Derecho Procesal Penal y Teoría del Delito  
Medellín, Antioquia, Colombia

2022

**José Rodrigo Flórez Ruiz**

Rector

Universidad Autónoma Latinoamericana

**Mónica Cecilia Montoya Escobar**

Decana (e) de Escuela de Posgrados

**Luis Eduardo Agudelo Suárez**

Coordinador(a) de la Maestría en Derecho Procesal Penal y Teoría del Delito

**Federico Londoño Mesa**

**Juan Camilo Muñetón Villegas**

Evaluadores

El trabajo de grado fue sustentado el 02 de julio de 2022 y obtuvo una aprobación unánime de conformidad con el Acuerdo 195 del Consejo Académico de 2016, lo cual quedó en el consignado en el acta de evaluación de trabajos de grado # 08 de 2022.

### **Agradecimientos y dedicatoria**

Lo más importante de cualquier logro, no es solo el cumplimiento del deber o el esfuerzo y la disciplina que cimentó hacerlo, lo que más debe hacernos conscientes es el hacer notorio los cambios generados en nuestra vida para ser mejores seres humanos.

Dedicamos este trabajo a nuestras familias, compañeros, compañeras, amigos y amigas y somos conscientes de que esas transformaciones personales, también tienen un impacto en la sociedad.

## Resumen

Los gobiernos en el mundo han encontrado en los avances tecnológicos, como las cámaras de videovigilancia, un aliado competente para salvaguardar la seguridad ciudadana en sus territorios. En Colombia, la ciudad de Medellín no ha sido ajena a la instalación, en años recientes, de estos dispositivos para optimizar su gestión en la disminución en la comisión de ciertas conductas delictivas; aunque estos resultados han generado consecuencias adversas en los derechos fundamentales y las libertades individuales de su población, entre otros factores por el tratamiento generalizado, indiscriminado y masivo de datos personales por entidades públicas y privadas. En este orden de ideas, el propósito con el presente texto es analizar la vulneración del derecho a la intimidad con las cámaras públicas de videovigilancia implementadas en la ciudad de Medellín. Se concluye que la seguridad ciudadana prevalece en el territorio nacional y local por ser un asunto de interés general; lo que deriva en la limitación y vulneración del derecho a la intimidad con las cámaras de videovigilancia instaladas en la ciudad, debido principalmente, a la ausencia de los criterios de idoneidad, necesidad y proporcionalidad, así como la existencia de una normatividad insuficiente para el tratamiento y autorización en el uso de datos sensibles y biométricos.

**Palabras clave:** Cámaras de Videovigilancia, Derecho a la Intimidad, Seguridad Ciudadana, Sistema de Seguridad.

## Abstract

Governments in the world have found in technological advances, such as video surveillance cameras, a tool for safeguarding citizen security in their territories. In Colombia, the city of Medellin has not been immune to the installation of these devices to optimize their management in reducing the commission of certain criminal behaviors; although these results have generated adverse consequences on the fundamental rights and individual freedoms of its population, among other factors due to the generalized, indiscriminate and massive treatment of personal data by public and private entities. In this order of ideas, the purpose of this text is to analyze the violation of the right to privacy by the public video surveillance cameras implemented in the city of Medellín. It is concluded that citizen security prevails in the national and local territory, as it is a matter of general interest; which derives in the limitation and violation of the right to privacy by the video surveillance cameras installed in the city, mainly due to the absence of the criteria of suitability, necessity and proportionality, as well as the existence of insufficient regulations for the treatment and authorization in the use of sensitive and biometric data.

**Keywords:** Video surveillance cameras, Right to Privacy, Citizen Security, Security System.

## Contenido

1. Introducción .....	9
2. El derecho a la intimidad, desde sus concepciones doctrinales, normativas y jurisprudenciales .....	13
2.1. El delgado hilo entre la intimidad y la privacidad.....	13
2.2. El derecho a la intimidad en el marco normativo nacional e internacional. ....	15
2.3. El derecho a la intimidad: entre lo constitucional y penal.....	20
3. Uso y regulación de las cámaras de videovigilancia en el contexto nacional y local ..	25
3.1. Herramientas tecnológicas usadas en Colombia para el monitoreo de la seguridad. ....	25
3.2. Regulación de los sistemas de videovigilancia en Colombia .....	29
3.3. Uso de las cámaras de videovigilancia en la ciudad de Medellín.....	34
3.4. Política Publica de Seguridad y Convivencia de Medellín, 2015.....	37
4. La prevalencia de la seguridad ciudadana, vulnera el goce efectivo del derecho a la intimidad.....	40
4.1. Registro y tratamiento indiscriminado de los datos personales.....	42
4.2. De los datos sensibles y biométricos recopilados con cámaras analíticas y de reconocimiento fácil .....	42
4.3. Inobservancia de los principios de idoneidad, necesidad y proporcionalidad ..	47
4.4. Invasión ilegal en el domicilio de los ciudadanos .....	49
5. Conclusiones .....	51
Referencias .....	54

## Lista de Tablas

Tabla 1. Principales tecnologías de sistemas de videovigilancia .....	26
---	----

## Lista de Figuras

Figura 1. Principios rectores que rigen el derecho a la intimidad y su conexidad con el derecho de habeas data.....	19
Figura 2. Clasificación y tipos de cámaras de video de seguridad.....	28
Figura 3. Comparativo de los resultados operativos en Medellín con el CCTV y S. Situacional, según los delitos priorizados.....	36

## 1. Introducción

El gobierno colombiano, reconociendo y aprovechando los beneficios que se derivan de las nuevas tecnologías y con el fin de potenciar su gestión pública, ha instalado cámaras de videovigilancia en todo el territorio nacional. Esta instalación ha tenido lugar en mayor medida a partir del año 2014, conforme con lo planteado en el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país” (Departamento Nacional de Planeación [DNP], 2015); esto con el objetivo primordial de fortalecer la seguridad ciudadana en el país. En este sentido, Medellín se ha destacado en el país, por ser una de las pocas ciudades en haber implementado las cámaras de videovigilancia con recursos propios y por arrojar resultados positivos en el monitoreo y la atención efectiva de determinadas conductas delictivas registradas con estos sistemas, a través de las intervenciones de la Alcaldía de Medellín, junto con la Policía Metropolitana; logrando así, entre otros resultados, la recuperación de 813 motocicletas y 328 celulares hurtados en la ciudad y la ejecución de 1.167 capturas durante el año 2021 (Arboleda, 2021).

Aunque estos resultados son alentadores en cuanto a la seguridad ciudadana en Medellín, se identifica que algunas disposiciones legales promulgadas con el denominado Código de Policía (Ley 1801 de 2016), como el artículo 237, promueven el monitoreo indiscriminado de la población, no solo porque permite convertir los datos personales en datos públicos cuando estos son recolectados o almacenados por sistemas de vigilancia oficiales, sino también porque con esta norma se “establecen mecanismos de vigilancia masiva que por su ausencia de definiciones y límites y por su falta de ponderación entre medios y fines, resultan violatorios de los derechos [de los ciudadanos]” (Centro de Estudios de Derecho, Justicia y Sociedad [Dejusticia], 2016, p. 1). Entre estos, se encuentra el derecho a la intimidad, el cual cumple con la función de “proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad” (Megías, 2002, p. 530).

Desde esta perspectiva, con esta monografía se pretende responder a la siguiente pregunta de investigación: ¿En qué medida las cámaras públicas de videovigilancia instaladas en la ciudad de Medellín afectan el goce efectivo del derecho a la intimidad de la población? En este orden de ideas, la tesis defendida en este estudio es que la implementación y uso de las cámaras públicas de videovigilancia en la ciudad de Medellín favorece la recolección indiscriminada de grandes volúmenes de información, imágenes y datos de cualquier índole de la población en general, sin las garantías constitucionales suficientes. Lo que, por ende, vulnera el derecho a la intimidad, entre otros motivos, porque condiciona su ejercicio a los espacios privados. Se trata de una temática que invita a reflexionar acerca de los efectos producidos con los sistemas de videovigilancia en la ciudad de Medellín, en relación con el derecho a la intimidad y se convierte en un material de consulta para quienes se interesen en el desarrollo de nuevas investigaciones sobre este asunto, de corte nacional e internacional.

Ahora bien, de conformidad con lo planteado en acápite previos, el propósito con la presente monografía de investigación es analizar la vulneración del derecho a la intimidad, con las cámaras públicas de videovigilancia implementadas en la ciudad de Medellín; por lo tanto, para el cumplimiento de dicho objetivo, se inicia el desarrollo de esta tesis con la presente introducción. Después se continúa con el primer capítulo de resultados, mediante el cual, se efectúa la delimitación del derecho a la intimidad, conforme con la doctrina y la normatividad nacional e internacional al respecto, así como la jurisprudencia de la Corte Constitucional; teniendo en cuenta, entre otras, las disposiciones legislativas consagradas con la Convención Americana de Derechos Humanos (art. 11), el Pacto Internacional de Derechos Civiles y Políticos (art. 17), la Carta Magna Nacional (art. 15), así como la jurisprudencia de la Corte Constitucional proferida con la finalidad de establecer el concepto de privacidad (sentencia T-787/04), argumentar sobre el derecho a la intimidad (sentencia T-552/97), definir la finalidad de protección con este derecho (sentencia T-414/92) y plantear algunas características del derecho a la intimidad (sentencia T-413/93).

Adicionalmente, se explica el régimen legal que regula el uso de las cámaras públicas de videovigilancia como mecanismo de seguridad ciudadana en Colombia y Medellín; comenzando este capítulo con una breve caracterización de estos dispositivos tecnológicos, de acuerdo con su funcionamiento y los diferentes tipos de tecnologías en materia de videovigilancia, principalmente. Después, se continúa con los referentes normativos en la materia, teniendo especial consideración con los preceptos regulatorios del Decreto Ley 356 de 1994, la Ley 1581 de 2012, el Código de convivencia ciudadana (Ley 1801 de 2016) y el Decreto Reglamentario 1377 de 2013, etc.

Sumado a esto, se clarifica el alcance de las siguientes expresiones: espacios públicos, semipúblicos, áreas comunes, lugares abiertos al público o que, siendo privados, trasciendan a lo público; y se traen a colación los pronunciamientos de la Corte Constitucional al respecto, entre los cuales se encuentra la Sentencia T-407/2012. También, se tiene en cuenta la información suministrada por la Secretaría de Seguridad y Convivencia de Medellín como respuesta al derecho de petición presentado por los autores en el año 2021, información que corresponde al impacto en cifras estadísticas que han tenido en los años 2020 y 2021, las cámaras de videovigilancia instaladas en Medellín, con respecto a las acciones reactivas y de prevención efectuadas por la Policía Metropolitana contra determinadas conductas punibles cometidas en la ciudad, junto con la cantidad y el tipo de cámaras disponibles en el contexto local para este propósito.

Se finaliza esta tesis con el tercer capítulo de resultados, enfocado en realizar una reflexión analítica y comparativa entre la seguridad ciudadana y el derecho a la intimidad, según los elementos característicos presentes en su desarrollo normativo, jurisprudencial y legal. En este caso, se explican particularmente, la prevalecía de la seguridad ciudadana y los factores que dan lugar a la limitación y vulneración del derecho a la intimidad por los habitantes de Medellín, con las cámaras públicas de videovigilancia, tales como: el registro y tratamiento discriminados de los datos personales generales, sensibles y biométricos, la inobservancia de los criterios de

proporcionalidad, idoneidad y necesidad y la invasión de los espacios íntimos de los ciudadanos.

Se termina la tesis con las respectivas conclusiones, las cuales establecen la vulneración del derecho a la intimidad, por el uso desproporcionado de las cámaras de videovigilancia, ya que las mismas tienen alcance, incluso hasta en los espacios físicos intermedios, donde aún se conserva, una expectativa legítima del ejercicio y goce efectivo de este derecho.

## **2. El derecho a la intimidad, desde sus concepciones doctrinales, normativas y jurisprudenciales**

Para continuar con el desarrollo de la presente investigación se realiza una delimitación del derecho a la intimidad, a partir de los referentes doctrinales, normativos y jurisprudenciales que lo fundamentan, teniendo en cuenta su relación constitucional y penal; así como, su aproximación con el derecho a la privacidad.

### **2.1. El delgado hilo entre la intimidad y la privacidad**

Desde la literatura se identifica con frecuencia una confusión en la utilización de los conceptos de intimidad y privacidad, la cual ha sido originada porque, incluso, “la jurisprudencia ha tratado en ocasiones como sinónimos a los conceptos de ‘intimidad’ y ‘privacidad’” (Bautista, 2015, p. 30) y también, debido a la complejidad de plantear las significativas divergencias existentes entre ambos constructos; no obstante, en esta sección se intenta establecer las diferencias doctrinales y jurisprudenciales entre lo íntimo y lo privado.

Etimológicamente, Rebollo (2005) explica que el concepto de intimidad se deriva de la expresión latina *intimus*, superlativo del vocablo *interus*, *de inter*, cuyo significado hace referencia a la zona espiritual reservada de una persona, un grupo o una familia. Se trata de una concepción que, si bien ha sido ampliamente utilizada en la literatura jurídica, también revela una connotación reduccionista, en términos del espacio en el cual los individuos son soberanos para decidir acerca de su comportamiento social y privado; ya que de acuerdo con el doctrinante Toscano (2017), la intimidad corresponde con el interior de cada persona, “radica en su fuero interno, por lo que nadie más que el propio sujeto tiene acceso a él. No hacen falta pestillos ni puertas que impidan la intromisión de otros como en el espacio privado” (p. 542). Aunado con lo anterior, la jurisprudencia de la honorable Corte Constitucional concibe la intimidad, como:

Un espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto (Corte Constitucional. Sentencia T-552/97, 1997, p. 5).

Desde esta perspectiva, es posible afirmar que la intimidad es un constructo inherente a la personalidad y esfera interna de cada persona, un espacio interno, oculto de los demás y profundo de su ser; mediante el cual puede gozar de su soledad, hasta que decide compartir y exteriorizar sus sentimientos y pensamientos, con otras personas definidas por cada individuo; pero teniendo en cuenta que la proyección externa de sus actuaciones íntimas y su esfera interna dejan sin efecto la condición, por la cual son consideradas como intrínsecamente inaccesibles, renunciando en este caso, a lo íntimo y trasladando dichas actuaciones hacia la esfera privada, concepto explicado a continuación.

Ahora bien, de acuerdo con las raíces etimológicas de la acepción de privacidad, esta palabra se origina en dos componentes léxicos latinos, a saber: *privatus* (propio, particular, prohibido al público) y el sufijo *-dad* (cualidad); por lo tanto, dicha expresión alude a las concepciones quitar, despojar, desposeer o prohibir (Vítóres, 2018), así como al “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión” (Real Academia Española [RAE], 2021, párr. 2). En este sentido, Fernández -Barbudo (2019) agrega que lo privado “[cumple] con una función mediadora entre la publicidad y el secreto, pues reconoce la existencia de *algo* que debe mantenerse al margen del circuito público de información y que, en consecuencia, debe gozar de confidencialidad” (p. 144) (cursiva en texto original). Al respecto, Warren y Brandeis (1890) citados por Toscano (2017), consideran que “la privacidad se refiere al grado de accesibilidad, o al control que ejercemos sobre el acceso de otros, a nuestra esfera íntima, cuyo núcleo está formado por pensamientos, sentimientos, etc.” (p. 543). Sumado a esto, la Corte Constitucional (2004), a través de la Sentencia T-787/04, arguye que:

El concepto de '*privacidad*' o '*de lo privado*', corresponde a los asuntos que en principio tocan exclusivamente con los intereses propios y específicos de la persona humana, sin que afecten o se refieran a los demás miembros de la colectividad; razón por la cual, sobre estos asuntos la sociedad a través del ordenamiento jurídico, no le exige o les impone a las personas el deber de informar o comunicar (p. 22).

De esta manera es posible dilucidar que el concepto de privacidad guarda relación con el control que ejerce sobre los pensamientos, sentimientos y la información que cada individuo posee en su esfera íntima y que, a través de lo privado, pone a disponibilidad y accesibilidad a una persona, un grupo de individuos o de su familia; aunque no por ello sus intereses propios y específicos se conviertan en asuntos que deba informar o comunicar, lo que si sucede con aquellas cuestiones definidas por el derecho como común o general, ya que estas pasan de lo privado a lo público.

En esencia, los conceptos de intimidad y privacidad difieren entre sí en la medida en que el primero está orientado a excluir a los extraños del conocimiento de los asuntos íntimos de una persona y la privacidad corresponde con el respeto y el control que ejercen las personas sobre su información y sus asuntos personales, los mismos que no tienen el deber de transmitir a otros por la ausencia de una exigibilidad al respecto, desde el derecho. Una vez delimitados estos conceptos, se procede con la explicación del derecho a la intimidad propiamente dicho, desde los preceptos normativos que lo respaldan en el contexto nacional e internacional, hasta llegar a su concepción actual centrada en una intimidad informacional.

## **2.2. El derecho a la intimidad en el marco normativo nacional e internacional.**

*Grosso modo*, lo íntimo está catalogado como un derecho fundamental de todas las personas, cuya función en palabras de Megías (2002), “es proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad” (p. 530). Se trata de una prerrogativa irrenunciable, inalienable e

imprescriptible, como se evidencia, desde el marco legislativo nacional e internacional promulgado al respecto.

En el ámbito mundial, la Declaración Universal de los Derechos Humanos, la Convención Americana de Derechos Humanos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, concuerdan en establecer que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” (Asamblea General de las Naciones Unidas. Resolución 217 (III), 1948, art. 12; Organización de los Estados Americanos [OEA], 1969, art. 11; Asamblea General de las Naciones Unidas. Resolución 2200 A (XXI), 1966, art. 17).

De conformidad con el precitado texto, se comprende el derecho a la intimidad, en virtud del marco normativo internacional, como una prerrogativa *iusfundamental* que tienen todas las personas de disfrutar a plenitud sus espacios privados, su entorno familiar y su lugar de domicilio, sin irrupciones o embates deliberados en su contra; es así como se ordena que la invasión del ámbito privado de los ciudadanos sólo es posible según las formalidades de ley, mediante orden judicial.

En el contexto nacional, la Constitución Política de 1991, en su artículo 15 delimita taxativamente el derecho a la intimidad en conexión con el derecho al *habeas data*, como se expone a continuación.

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (Constitución Política de Colombia, 1991).

De la parte conducente del artículo 15 de la Constitución Política nacional, antes transcrita, es posible identificar la estrecha relación entre el derecho a la intimidad y el derecho al *habeas data*, a raíz de las facultades reconocidas a todos los ciudadanos del país para que las dimensiones de su vida personal (circunstancias, pensamientos, sentimientos, experiencias y conductas), puedan ser conservadas en un plano reservado para sí mismo, para decidir con libertad las personas que quisiera excluir sobre el conocimiento de esta vida personal; y que además, la información existente sobre ellos pueda ser solicitada, corregida, actualizada o eliminada, si así lo demandasen las personas implicadas.

Al retomar los aportes doctrinales y jurisprudenciales referenciados en acápites previos sobre los conceptos de intimidad y privacidad, se evidencia entonces que el derecho a la intimidad conjuga ambas acepciones, dado que permite garantizar esa esfera personalísima y profunda de su ser que solo admite la injerencia de los demás, en casos justificados, cuando el fin perseguido es legal; junto con la facultad para determinar a quienes se le da a conocer o no su vida personal, momento en el cual, lo íntimo pasa a ser privado y conocido por otras personas.

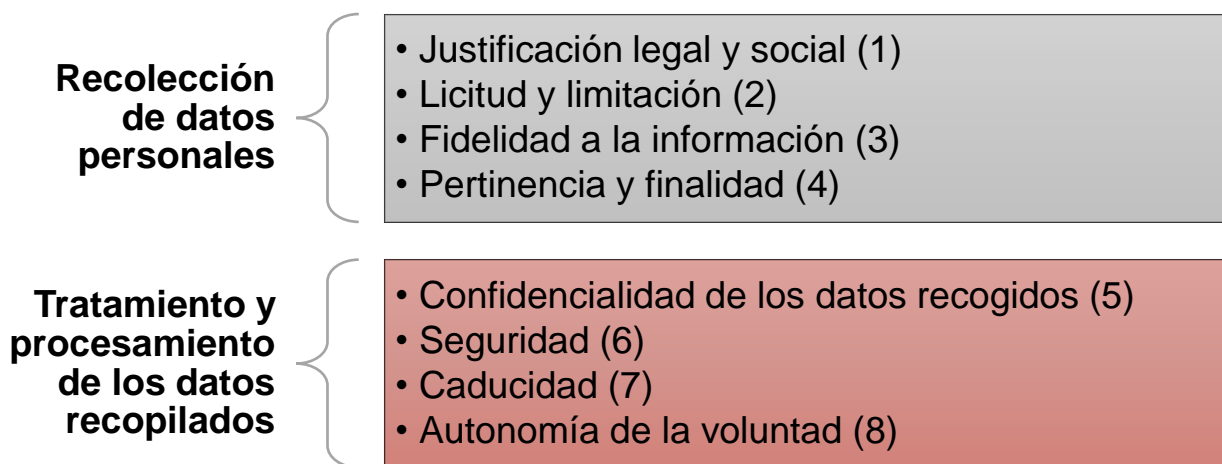
En esta misma línea argumentativa, Moreno (2003), señala que el derecho a la intimidad centra su contenido positivo del derecho en el control de los datos personales de cada individuo, por lo tanto, se trata de un derecho fundamental pero no autónomo ni absoluto, ya que se apoya y guarda conexidad con otras prerrogativas, como el derecho a la vida, la libertad y el derecho a la dignidad humana y se prioriza con respecto a asuntos de interés general, como la seguridad ciudadana. Desde esta perspectiva, esta autora reconoce la dualidad del contenido del derecho a la intimidad y explica:

A partir de este planteamiento, el derecho a la intimidad, tendría un doble contenido: uno negativo, de exclusión, que impediría determinadas intromisiones ajenas y, otro positivo, el control por parte del titular de los datos personales que le permita conocer y controlar la información que sobre él se encuentran en soportes o archivos informáticos y convencionales.

Desde esta perspectiva, el derecho a la intimidad se presenta como el derecho de una persona no sólo a reservar un ámbito de su vida como secreto e intangible para los demás sino también a ostentar la capacidad y medios para evitar su manipulación por otros. Esta es la posición que nos parece más correcta, ya que facilita la extensión de la protección de la intimidad a los datos que se encuentran en archivos o registros no automatizados, así como a cualquier otro tipo de tecnología presente (p.ej. cintas magnetofónicas, cámaras de video, etc.) y futura que permita la recogida y tratamiento de información de las personas (Moreno, 2003, p. 73).

Si bien en el capítulo dos de la presente monografía, se especifica la regulación formulada en el país en relación con el uso y el tratamiento de la información personal, de las cámaras de videovigilancia y el desarrollo tecnológico implicado con las mismas; también, se evidencia con el precitado texto que, el desarrollo jurídico del derecho a la intimidad, no solo se adelanta a la realidad tecnológica y social que prima en las sociedades actuales, caracterizada por el acceso a grandes volúmenes de datos e información, a través de numerosos mecanismos informáticos; sino que además se expone la conexión existente con el derecho de *habeas data*, reconocido en la actualidad en el territorio nacional con la Ley Estatutaria 1266 de 2008 y que en conjunto, le permiten a las personas garantizar y proteger, tanto su derecho a preservar una parte de su vida personal intangible ajena a las injerencias de otras personas, como el derecho a tener un mayor control de la información situada en su esfera privada y de aquellos datos que por decisión propia determina mostrar a otras personas naturales o jurídicas.

Con la finalidad de lograr una protección efectiva del derecho a la intimidad y evitar que la misma pueda resultar afectada por la injerencia de otros, se ha establecido una serie de principios que rigen el uso y el tratamiento de la información personal de los individuos, es decir que reglamentan el derecho de *habeas data*; el mismo que, de acuerdo con la información de la figura 1, se aplica a partir de dos acciones en particular, a saber: la recolección de los datos y el tratamiento de la información, cada una de estas regida por cuatro principios rectores, los cuales se proceden a explicar a continuación.



*Figura 1.* Principios rectores que rigen el derecho a la intimidad y su conexión con el derecho de *habeas data*.

*Fuente:* adaptado de Megías (2002).

A tenor de lo planteado con la figura 1, se encuentra que el proceso de recolección de la información personal debe llevarse a cabo con base en una finalidad lícita (1), a través de medios legales y consentidos por las personas y solo con los datos netamente necesarios para cumplir con el fin lícito perseguido con dicha recolección (2), datos que deben ser completos, exactos y actualizados, pero con la posibilidad de rectificarlos en un momento dado (3) y que además, solo pueden ser conservados para la finalidad perseguida (4) (Megías, 2002).

Prosiguiendo con la información de la figura 1, se tiene que un segundo proceso asociado con el derecho a la intimidad y de *habeas data* hace referencia al tratamiento y procesamiento de los datos recopilados, lo cual debe salvaguardar la confidencialidad

de los mismos, por parte de las entidades y empleados responsables (5), así como su preservación del conocimiento ajeno, a través de los medios idóneos para ello (6). De igual forma, los datos recolectados deben ser eliminados de las bases de datos, una vez se cumple con la finalidad lícita perseguida (7), teniendo en cuenta que, independientemente de las acciones adelantadas al respecto, el tratamiento de los datos debe ser consentido previamente por los titulares de los datos (8).

Se evidencia entonces que a través de los derechos a la intimidad y de *habeas data*, junto con los principios rectores que los rigen, se busca proteger y salvaguardar la integridad de las personas, en relación con la garantía de conservar su información íntima (pensamientos, ideologías, sentimientos, etc.) en secreto y alejado de injerencias de terceros y también de decidir acerca de los datos que desea exteriorizar y con quiénes pretende hacerlo. Todo esto, siempre y cuando la recolección, tratamiento y procesamiento de los mismos sea consentido previamente por las personas y se cumpla conforme con lo dispuesto por las normas que regulan la materia, la cual para efectos de la presente monografía es abordada en el capítulo dos. Sin embargo, para continuar con el desarrollo de esta sección, en las siguientes líneas se plantea la relación entre el carácter constitucional y penal del derecho a la intimidad.

### **2.3. El derecho a la intimidad: entre lo constitucional y penal.**

Según se referenciaba en acápites anteriores, el derecho fundamental a la intimidad es protegido y garantizado en el territorio nacional, a través de una serie de instrumentos normativos internacionales que hacen parte del bloque de constitucionalidad del Estado colombiano; aunque más importante es su reconocimiento explícito con el artículo 15 de la Carta Magna nacional, teniendo en cuenta los tres elementos clave que lo componen: la intimidad, el *habeas data* y el respeto por la correspondencia. Desde esta perspectiva, la Corte Constitucional en nutrida jurisprudencia, ha confirmado y estudiado el alcance y las limitaciones de esta prerrogativa, como se ha desarrollado con la Sentencia T-552 de 1997 citando la Sentencia T-530 de 1992, mediante la cual asegura que:

El derecho a la intimidad implica la facultad de exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas (...). La Corte Constitucional, (...) ha definido el núcleo esencial del derecho fundamental a la intimidad como “el espacio intangible, inmune a las intromisiones externas del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto” (Corte Constitucional. Sentencia T-552/97, 1997, p. 5).

Para complementar el precitado contenido jurídico del derecho a la intimidad, esta Corporación también advirtió que la finalidad de la protección de este derecho es:

Es [resguardar] la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer “erga omnes”, vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta (Corte Constitucional. Sentencia T-414/92, 1992, p. 17) (subrayado texto original).

Ahora bien, en reiterada jurisprudencia se ha validado el contenido jurídico del derecho a la intimidad. Es así como, recientemente, con la Sentencia C-094/20 la Corte Constitucional realizó un análisis de constitucionalidad contra los artículos 32, 95 (parcial), 139 (parcial), 146 (parcial) y 237 (parcial) de la Ley 1801 de 2016 “*por la cual*

se expide el Código Nacional de Seguridad y Convivencia Ciudadana”. En esta ocasión, la honorable Corte declaró la exequibilidad de los artículos 32 y 146 (parcial) y la exequibilidad condicionada del artículo 237 de la ley en mención y aseveró el derecho a la intimidad en los siguientes términos:

La Corte Constitucional ha definido el derecho a la intimidad como aquel derecho que *“garantiza en los asociados, el poder contar con una esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas”*. Igualmente, ha señalado que la intimidad comprende *“el espacio exclusivo de cada uno, (...) aquella órbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo frente a la necesaria injerencia de los demás, dada la sociabilidad natural del ser humano”*. Adicionalmente, ha destacado que el derecho a la intimidad tiene dos dimensiones: (i) la negativa, como secreto de la vida privada; y (ii) la positiva, como libertad. En su *dimensión negativa*, prohíbe cualquier injerencia arbitraria en la vida privada e impide la divulgación ilegítima de hechos o documentos privados. En su *dimensión positiva*, protege el derecho de toda persona a tomar las decisiones que conciernen a la esfera de su vida privada (Corte Constitucional. Sentencia C-094, 2020, p. 23) (subrayado fuera del texto original, cursiva original).

De acuerdo con el anterior pronunciamiento de la Corte Constitucional, particularmente, los apartes subrayados, exponen los criterios esenciales determinados por esta Corporación que permiten comprender su delimitación y alcance; por lo tanto, se establece que el derecho fundamental a la intimidad, según las intervenciones de esta Corte es una prerrogativa reconocida a todos los colombianos, sin excepción, dado su carácter inalienable e imprescriptible y teniendo en cuenta que el ejercicio del mismo se efectúa *“erga omnes”*. Es un derecho que rechaza la injerencia arbitraria de otros en su espacio privado e íntimo, así como la publicación y divulgación de sus datos íntimos, personales y privados, por parte de una persona natural o jurídica que haya sido previamente autorizada por el titular de la información e incluso, se trata de un derecho

con el que se reconoce el control que tienen las personas sobre sus datos e información personal, para que no sean divulgados sin su consentimiento previo.

Ahora bien, aunque para el año 2004 existía un marco constitucional y jurisprudencial que reconocía y garantizaba el derecho a la intimidad de todos los colombianos; se carecía de una figura en el derecho penal que penalizara la contravención de estos preceptos normativos y jurisprudenciales. Es así como a través del Código de Procedimiento Penal (Ley 906 de 2004), se efectúan los primeros avances en el tema, mediante la promulgación de los principios rectores y garantías procesales que rigen este derecho, cuya defensa fue consagrada explícitamente con el artículo 14 de este Código.

En la actualidad, dicho precepto determina que, originado en el derecho a la intimidad, ninguna persona puede ser afectado en su vida privada por las injerencias de un tercero. Por lo tanto, el allanamiento, el registro de su domicilio, residencia o lugar de trabajo o el acceso a bases de datos, debe efectuarse con orden escrita del Fiscal General de la Nación con arreglo de las formalidades y motivos de ley, excluyendo las situaciones de flagrancia y demás contempladas en la ley (Congreso de la República de Colombia. Ley 906, 2004). Adicional a lo anterior, el Estado colombiano modificó el Código Penal con la promulgación de la Ley 1273 de 2009, mediante la cual se creó la protección de la información y de los datos como un nuevo bien jurídico tutelado, junto con la preservación de los mismos en sistemas informáticos basados en las Tecnologías de la Información y la Comunicación (TIC). En esta oportunidad, se tipificó una serie de delitos informáticos, algunos de ellos, estrechamente implicados con la protección del derecho a la intimidad, como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación y la interceptación de datos informáticos, entre otros; siendo este último el de mayor incidencia con respecto al derecho a la intimidad, toda vez que amplía el espectro en cuanto al tipo de comunicaciones con las cuales se puede dar la comisión de este delito y que se encuentran por fuera del presupuesto normativo contemplado para su sanción.

En definitiva, existe una relación de complementariedad entre el marco constitucional y legal con el desarrollo penal del derecho a la intimidad; ya que, con los primeros, se pretende proteger la información y los datos personales y los espacios íntimos y privados de todos los colombianos, considerando los nuevos avances tecnológicos y con el marco penal establecido en el país al respecto, se busca limitar las injerencias en las bases de datos y en los sistemas informáticos por parte de terceros no autorizados o que no tengan la custodia de los mismos. Lo que, por ende, permite defender y salvaguardar el derecho a la intimidad de los ciudadanos colombianos; teniendo en cuenta que un elemento clave en el análisis jurídico, frente a la vulneración o no de este derecho, hace referencia a la autorización y/o voluntad del titular del derecho de poner a disposición la información protegida con esta prerrogativa.

### **3. Uso y regulación de las cámaras de videovigilancia en el contexto nacional y local**

A tenor del objetivo propuesto con la presente investigación, en este capítulo se efectúa un acercamiento al régimen constitucional y legal que regula las cámaras de videovigilancia en Colombia, con énfasis en la ciudad de Medellín. Se inicia esta sección con la descripción de las tecnologías usadas en el país para el monitoreo de la seguridad, teniendo en cuenta la titularidad de las cámaras de videovigilancia y clarificando los diferentes espacios de vigilancia. Se continúa con la explicación del marco normativo que reglamenta el uso de estas herramientas tecnológicas en el territorio nacional y se finaliza este capítulo con la caracterización del uso de las cámaras de videovigilancia en la ciudad de Medellín.

#### **3.1.Herramientas tecnológicas usadas en Colombia para el monitoreo de la seguridad.**

No es una novedad que, los vertiginosos avances de las TIC han propiciado cambios de fondo en cada una de las esferas de desarrollo de las personas y de la sociedad en general; por medio de la creación e implementación de herramientas tecnológicas más sofisticadas para el mejoramiento, entre otros asuntos, de la comunicación, la promoción y comercialización de productos y servicios, así como para fortalecer la gestión en seguridad de las entidades públicas y privadas.

Uno de los avances al respecto ha sido la modernización de los sistemas para el control y monitoreo de seguridad, como los sistemas de videovigilancia, los cuales son implementados con el propósito de “garantizar la seguridad de bienes o personas en un lugar determinado (...), incrementando su presencia al ser considerados como un medio idóneo para realizar el monitoreo y la observación de actividades en escenarios domésticos, empresariales, laborales y públicos” (Superintendencia de Industria y Comercio [SIC], 2016, p. 5); teniendo en cuenta que su uso ha implicado una masiva recopilación de diversos tipos de datos personales, como imágenes, audios, videos,

etc. Aunado con lo anterior, García del Valle (2013), explica de forma amplia y clara que:

Los sistemas digitales basados en Videovigilancia-IP, en términos generales, permiten la captación/tratamiento, o la grabación de imágenes y sonido, de forma digital ya sea de lugares públicos o privados. Estos sistemas de Videovigilancia-IP, se basan a nivel general en el componente principal, las Cámaras-IP, que son cámaras con tecnología digital utilizando el protocolo-IP (Internet Protocol), para comunicarse entre sí. Estas digitalizan las imágenes y sonido (si fuera necesario) que captan de forma autónoma, y las emiten a través del protocolo de comunicación-IP, mediante una red Ethernet (LAN), lo que permite ver en tiempo real lo que está pasando, tanto en un lugar cercano, a través de un PC o Tablet conectado a dicha red o, aunque estén a miles de kilómetros de distancia, cuando estas se conectan a internet o a una Red de Área extendida (WAN), mediante algún sistema-IP, digital (p. 10).

Complementando lo anterior, se ha identificado la existencia de diversos tipos de sistemas de videovigilancia, los cuales difieren entre sí, por sus características –las cuales dependen de las necesidades del usuario–, los costos de implementación y las tecnologías empleadas para su uso. Con respecto a este último asunto, en la tabla 1, se referencian los sistemas de videovigilancia más empleados en años recientes y sus características más relevantes, con la finalidad de tener una mejor comprensión acerca de su evolución en el contexto nacional y mundial.

Tabla 1.

*Principales tecnologías de sistemas de videovigilancia*

<b>Nombre del sistema</b>	<b>Circuito Cerrado de Televisión (CCTV)</b>	<b>Power over Ethernet (PoE, Energía Eléctrica por Ethernet)</b>
<b>Tipo de tecnología usada</b>	Tecnología visual	Tecnología que integra energía eléctrica y datos a través de un mismo cableado.

<b>Principal objetivo</b>	Supervisar las actividades en distintos ambientes	Instalar equipos externos o remotos sin tener que conectarse a la alimentación de Corriente Alterna o CA
---------------------------	---	--

*Fuente:* adaptado de Rivas y Velázquez (2011).

Tabla 1.

*Principales tecnologías de sistemas de videovigilancia (continuación)*

<b>Nombre del sistema</b>	<b>Circuito Cerrado de Televisión (CCTV)</b>	<b>Power over Ethernet (PoE, Energía Eléctrica por Ethernet)</b>
<b>Elementos que lo integran</b>	Cámaras de video (algunas con micrófono) Monitores. Grabadoras de Lapso de Tiempo (VCR): casetes tipo VHS, DVR y enrutadores (router) Routers de distribución: WAN	Equipo de Alimentación Eléctrica (PSE, Power Sourcing Equipment), v.gr. End-span Dispositivo Alimentado (PD, Powered Device), v.gr. teléfono IP, punto de acceso LAN inalámbrico, etc.
<b>Características de uso</b>	Se usan preferiblemente, fijas para mejorar la captación de imágenes.  Pueden ser controladas remotamente.	Elimina la necesidad de disponer de corriente eléctrica en todos lados. El cableado soporta la categoría 5/5e hasta 100 metros. Asegura el funcionamiento, entre otros dispositivos, de cámaras de seguridad IP, por ser usados con una fuente de alimentación eléctrica ininterrumpida (UPS) centralizada.

*Fuente:* adaptado de Rivas y Velázquez (2011).

Se deduce, de acuerdo con la información de la tabla 1, que los sistemas de videovigilancia pueden estar integrados por tecnologías visuales apoyadas en ciertas ocasiones en la grabación de audios y también en los dispositivos tecnológicos integradores que combinan datos y energía eléctrica, con la finalidad de optimizar la captación y recopilación de los datos, cuando la alimentación eléctrica es interrumpida. Si bien puede resaltar por su obviedad, el elemento esencial en los sistemas de videovigilancia son las cámaras videograbadoras, siendo las más relevantes las de red, llamadas también IP. En palabras de Rivas y Velázquez (2011), son aquellas

videocámaras diseñadas para enviar señales de video y audio digitales, las cuales, unidas a un ordenador, forman una única unidad, y que, además, poseen una serie de componentes en común entre los diferentes tipos existentes al respecto, los cuales son, según Báez (2019), los siguientes: Lente, circuitos, chipset y carcasa.

A grandes rasgos, de conformidad con la información de la figura 2, las cámaras de seguridad para los sistemas de videovigilancia, son clasificadas en la actualidad, en dos grandes grupos, las cámaras análogas y las digitales IP.



*Figura 2. Clasificación y tipos de cámaras de video de seguridad.  
Fuente: tomado de Todoelectrónica (2019)*

En virtud de los aportes de la figura 2 y de Báez (2019), se encuentra que las cámaras de seguridad análogas son aquellas que poseen un conector BNC utilizado con las antenas de televisión convencionales y con un cable coaxial; características que, en conjunto, representan una alternativa económica para la implementación del sistema de videovigilancia. Por su parte, las cámaras digitales se enfocan en realizar una conexión IP, a través de internet o directamente a un router; esto con el propósito de que puedan ser controladas continuamente desde un computador o un dispositivo móvil; teniendo en cuenta que su funcionamiento se puede potenciar con una conexión a un grabador de video NVR (*Network Video Recorder*), de forma tal que la información captura sea almacenada directamente en un disco duro.

Una vez, se ha efectuado un breve acercamiento con respecto al desarrollo tecnológico de los sistemas de videovigilancia, a continuación, en la siguiente sección, se describen

los preceptos legislativos que reglamentan en Colombia, el uso de videograbadoras, clarificando con mayor interés, su uso privado, público, semipúblico y semiprivado, y exponiendo datos sobre el uso de estos dispositivos en la ciudad de Medellín.

### **3.2. Regulación de los sistemas de videovigilancia en Colombia**

Para el año 2020, Jasso-López (2020), reseñó la existencia de programas nacionales de seguridad pública y tecnología en la mayoría de los países latinoamericanos, aunque no en todos estos programas se reglamentaban explícitamente las acciones en materia de videovigilancia ni existía una planeación gubernamental al respecto. No obstante, lo anterior, uno de los países que ha integrado programas nacionales y locales con estrategias, objetivos y acciones sobre videovigilancia, ha sido Colombia; gracias a la política de defensa y seguridad anunciada con los planes de desarrollo del país y aprobados, a su vez, por el gobierno nacional para cada nuevo período presidencial, en este caso en específico este autor hacía referencia al documento “Política de Defensa y Seguridad. Todos por un nuevo país”. De igual forma, estos avances se dan gracias a la promulgación de diversos instrumentos jurídicos para la regulación de los sistemas de seguridad y de los datos recopilados, a través de los mismos; los cuales se referencian en las siguientes líneas, no solo para tener una mejor comprensión sobre el tema, sino también para delimitar su uso en el territorio nacional.

En este orden de ideas, se traen a colación los preceptos normativos de la Ley 1581 de 2012, enfocada en la protección de datos personales, los cuales son definidos en dicho cuerpo normativo como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Congreso de Colombia. Ley 1581, 2012, art. 3, lit. c); y que, además, sea registrada en cualquier base de datos que haga a esta información susceptible de tratamiento por entidades públicas o privadas. En correlación con esta definición, es posible establecer que, en el caso de las cámaras de videovigilancia, los datos susceptibles de tratamiento, son las imágenes –y en ciertas ocasiones los audios–, captados con estos dispositivos, los mismos que

permiten asociar la información recopilada a una persona o varias personas de forma explícita o identificable.

Ahora bien, con el propósito de salvaguardar los datos personales de los colombianos y de garantizar sus derechos, libertades y garantías constitucionales, así como el derecho a la intimidad, de *habeas data* y el derecho a la información consagrado con el artículo 20 superior; el legislador establece en el artículo 4 del Título II de la Ley 1581 de 2012, una serie de principios rectores para el tratamiento de los datos personales, los cuales ha sido abordados en acápites previos; sin embargo, es pertinente señalar que con base en el principio de libertad, el tratamiento de los datos personales solo puede efectuarse con la autorización previa, expresa e informada del titular, mediante los mecanismos establecidos para ello y, bien sea por escrito, de forma oral o a través de conductas inequívocas (Congreso de Colombia. Ley 1581, 2012).

Cabe clarificar que la autorización del titular para el tratamiento de sus datos personales no es necesaria cuando se trata de información solicitada por entidades públicas o administrativas en el ejercicio de sus funciones legales o por orden judicial; cuando son datos de naturaleza pública, los casos de urgencia médica o sanitaria y cuando el tratamiento de la información es autorizado por la ley para fines históricos, estadísticos o científicos y en el caso de los datos relacionados con el Registro Civil de las Personas (Congreso de Colombia. Ley 1581, 2012).

Corolario con lo anterior, el Código de Policía y Convivencia (Ley 1801 de 2016), también contiene una serie de disposiciones legislativas para la reglamentación del uso de mecanismos tecnológicos por la Policía Nacional, con el propósito de salvaguardar la seguridad de los ciudadanos. En este orden de ideas, esta norma establece en su artículo 237 la integración de sistemas de vigilancia, mediante la cual se regula que son considerados datos públicos y de libre acceso todos los datos captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, así como aquellos que se encuentren instalados en espacio público, áreas comunes, lugares abiertos al público o

que siendo privados trasciendan a lo público; exceptuando la información amparada por reserva legal y aquellos datos destinados para la Defensa y Seguridad Nacional (Congreso de la República de Colombia. Ley 1801, 2016).

Por otra parte, el Código de Procedimiento Penal, en materia de vigilancia preceptúa, particularmente en el artículo 239 que, sin afectar la expectativa razonable de la intimidad de los indiciados, imputados o de terceros, las autoridades competentes pueden tomar fotografías, grabar videos y en general, efectuar las actividades y usar los medios técnicos aceptados por la ley, con el fin de recaudar los datos relevantes que permitan la identificación o individualización de los autores o partícipes en la comisión de una conducta punible (Congreso de la República de Colombia. Ley 906, 2004). Por lo tanto, dentro de las posibilidades técnicas para ejecutar dicha recaudación, es procedente la utilización de diversos medios tecnológicos, incluyendo, las cámaras de videovigilancia.

De conformidad con el contenido de este precepto normativo, las autoridades públicas competentes, junto con la Policía Nacional, no solo están facultadas para la implementación de cámaras de videovigilancia en determinados espacios, sino que, además, amparadas en la integración de los sistemas de vigilancia, también pueden acceder y/o utilizar los datos registrados con cámaras de seguridad privadas; siendo clave en este asunto, las limitaciones de cada uno de estos espacios.

Así las cosas, aunque el Estado colombiano ha realizado un esfuerzo significativo en la regulación del tratamiento de los datos personales de sus ciudadanos y el uso en el territorio nacional de las cámaras de videovigilancia, también se encuentra que uno de los principales debates jurídicos al respecto, se ha dado en torno a los límites en el uso de los datos privados, públicos y semipúblicos, así como la delimitación de los espacios públicos, los lugares abiertos al público (semipúblicos) y los espacios que siendo privados trasciendan a lo público; frente a lo cual, el legislador y la Corte Constitucional realizan un acercamiento considerable sobre este asunto, como se explica a continuación.

En este orden de ideas, con relación a la clasificación de los datos según su naturaleza, la Ley Estatutaria 1266 de 2008, dictamina que los datos públicos son todos aquellos que no son semiprivados o privados, según la ley en mención y que, además, por mandato legal o constitucional tiene dicha cualidad, como en el caso de los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas, etc. Por otra parte, los datos semiprivados son aquellos que carecen de naturaleza íntima, reservada, pública y que, además, su conocimiento o publicación solo puede interesar al titular de la información o a un sector en específico, como se sucede con los datos financieros y crediticios, entre otros. Sumado a esto, los datos privados son de naturaleza íntima o reservada, por lo tanto, solo son relevantes para el titular de la información (Congreso de la República de Colombia. Ley Estatutaria 1266, 2008).

En esta misma línea argumentativa, la honorable Corte Constitucional en la Sentencia T-574 de 2017 precisó acerca de la clasificación de los datos personales, para efectos normativos y jurisprudenciales en el país. En este sentido, esta Corporación efectuó la siguiente delimitación de la naturaleza de la información:

La información *pública* es aquella que se puede obtener y es entregada sin ningún tipo de restricción o cumplimiento de requisitos. La *semi-privada* tiende a ser personal o impersonal y para acceder a ella existen grados de limitación, es decir que para obtenerla se necesita de una autoridad administrativa que esté en ejercicio de sus funciones. La *privada* hace referencia a datos que corresponden al ámbito privado de la persona y sólo puede ser obtenida a través de autoridad judicial en cumplimiento de sus funciones. Finalmente, la *reservada* se encuentra constituida por información personal que atañe directamente a los derechos fundamentales del titular, como la intimidad, libertad, dignidad y habeas data y que no puede ser obtenida ni siquiera por autoridad judicial en el ejercicio de sus funciones (Corte Constitucional. Sentencia T-574/17, 2017, p. 12).

Según el precitado texto, es posible dilucidar que, aunque la Corte en esa ocasión plantea una clasificación superflua de los datos conforme con su naturaleza jurídica, teniendo en cuenta que los datos públicos carecen de restricción en cuanto a su acceso y tratamiento, los datos semiprivados se ubican en la personalidad de los individuos y el acceso a los mismos, se adecua conforme con la autorización administrativa previa para ello. Adicionalmente, los datos privados están asociados con los datos situados en la esfera privada de las personas, por lo tanto, para su acceso, se requiere autorización judicial previa y los datos reservados, como su nombre lo indica, están relacionados con los datos personales del titular de la información que guardan relación con sus derechos fundamentales, entre otros, a la dignidad humana, derecho de *habeas data* y a la intimidad, etc.; teniendo en consideración que el acceso a dicho datos no es posible ni siquiera con autorización proferida por las autoridades competentes.

Por su parte, la Corte Constitucional en la Sentencia T-364 de 2018 en consideración con el contenido de la Sentencia T-407 de 2012, fijó la existencia de cuatro espacios en torno a la recopilación y tratamiento de datos personales, a saber: públicos, privados, intermedios (semiprivados) y los espacios semipúblicos.

[Existen] espacios públicos, en los que el interés general prima sobre el particular y por tanto la intimidad se ve ciertamente menguada; espacios privados en los que el carácter personalísimo del entorno hace que la protección de la intimidad presente un estándar ciertamente más estricto; espacios intermedios, como lo son los semiprivados y otros semi-públicos, que integran características tanto públicas como privadas, los primeros, respectivamente, relacionados con escenarios “cerrados en los que un conjunto de personas comparten una actividad y en los que el acceso al público es restringido” y los segundos, con “acceso relativamente abierto en los que diferentes personas se encuentran en determinado momento para realizar cierta actividad puntual

dentro de un espacio compartido: un cine, un centro comercial, un estadio” (Corte Constitucional. Sentencia T-364/18, 2018, p. 14).

De conformidad con el anterior texto, se encuentra que la clasificación de los espacios en función de la intimidad espacial consagrada por la Corte Constitucional permite determinar el alcance de los mismos, comenzando con los espacios públicos donde se da relevancia al interés general, sobre el interés particular, por lo tanto, es de acceso abierto. Los espacios privados, por su parte, protegen la intimidad de una forma estricta, de acuerdo con el carácter personalísimo de los datos. De igual forma, los espacios semipúblicos, hacen referencia a aquellos espacios abiertos al público y compartidos por las personas para efectuar una actividad en concreto. Y los espacios son semiprivados, cuando el acceso de las personas se da en un escenario cerrado, donde se reúnen con otras personas, hasta que cumplen con el propósito definido para dicha acción. En suma, Galindo y Ramírez (2021), reconocen que “si bien aún en estos espacios las personas cuentan con el derecho a la intimidad, es evidente que la expectativa de privacidad va disminuyendo entre más abierto al público sea el lugar donde ocurren las acciones humanas” (p. 12).

Sin duda, establecer los límites del derecho a la intimidad, en los términos de la naturaleza de los datos y los espacios, es una tarea compleja que deben asumir las autoridades competentes, conforme con las particularidades de cada caso, ya que, si bien se disponen de normas y pronunciamientos jurisprudenciales al respecto, algunos de los mismos también carecen de la especificidad requerida para caracterizar de forma amplia y precisa el alcance de cada uno de ellos.

### **3.3. Uso de las cámaras de videovigilancia en la ciudad de Medellín.**

Para culminar el desarrollo de este capítulo, se procede con la caracterización del uso de las cámaras de videovigilancia en Medellín, con la información recibida el pasado cuatro de noviembre de 2021, como respuesta a un derecho de petición presentado previamente ante la Secretaría de Seguridad y Convivencia por los autores de la presente monografía.

A la fecha, la Secretaría de Seguridad y Convivencia informó acerca de la existencia de 2.886 cámaras de videovigilancia en su dominio, entre las cuales se encontraban cámaras multisensor (cobertura hasta de 360°), cámaras analíticas y de reconocimiento facial, cámaras analíticas de placas de vehículos y motocicletas (LPR), y cámaras fijas de alto alcance; todos estos dispositivos conectados y visualizados, a través de un sistema de videovigilancia CCTV, es decir, un Circuito Cerrado de Televisión, el cual tiene como encargado del tratamiento de los datos a los operadores del CCTV y a la Policía Metropolitana, quienes mediante la implementación de planes estratégicos de visualización y teniendo en cuenta el trabajo reactivo y preventivo que se realiza de manera permanente y que se ve reflejado en los indicadores oficiales reportados por el SISC; efectúan el mapeo de los casos relacionados con hurtos, homicidios, lesiones, extorsiones entre otros delitos priorizados, cuyos resultados impactan los indicadores de gestión de estas entidades y que son referenciados en secciones subsiguientes.

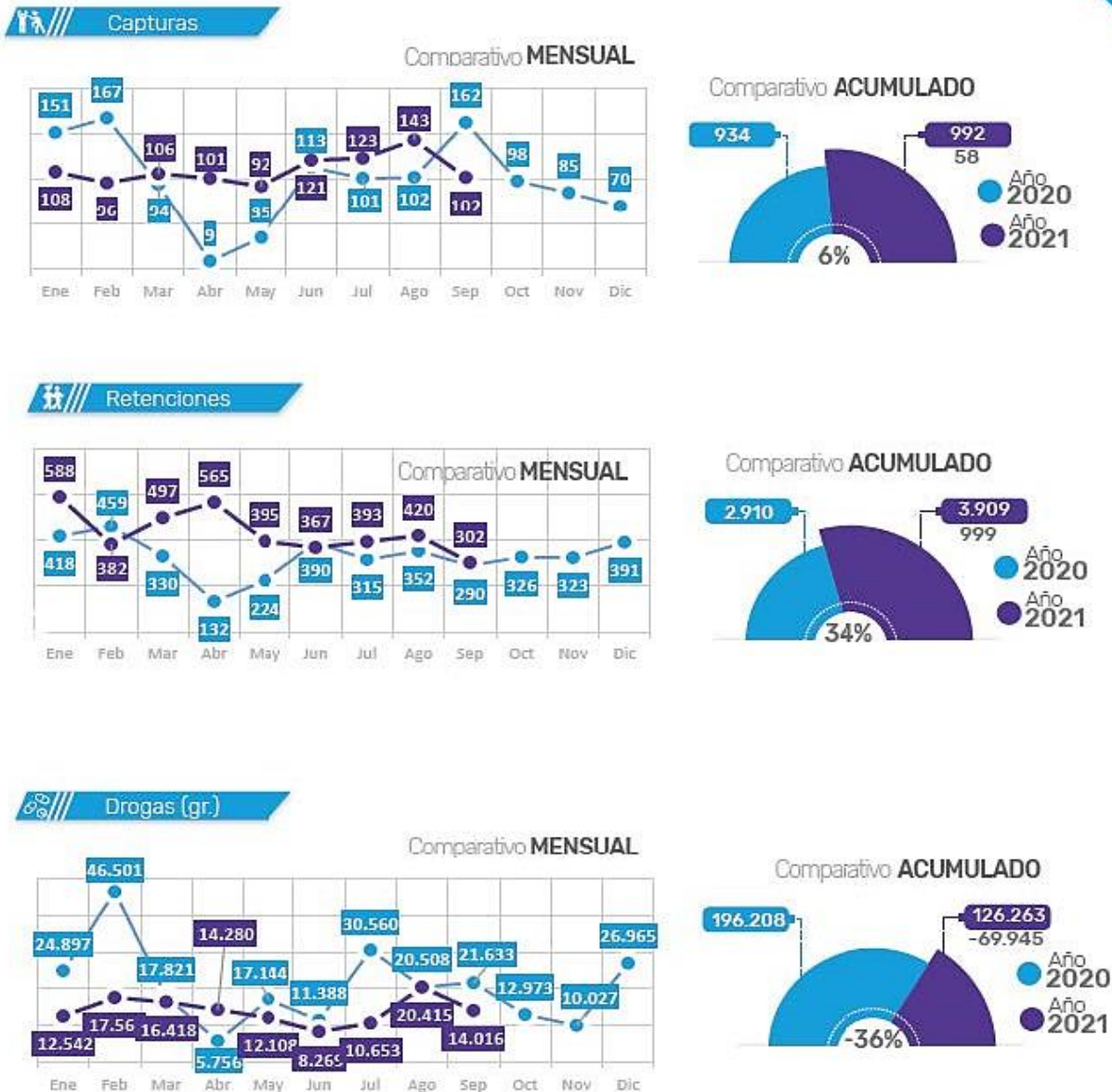


Figura 3. Comparativo de los resultados operativos en Medellín con el CCTV y S. Situacional, según los delitos priorizados. Fuente: tomado de la Secretaría de Seguridad y Convivencia (2021).

Si bien la Secretaría de Seguridad y Convivencia no fue enfática en aseverar acerca del impacto que han tenido las cámaras de videovigilancia en la ciudad de Medellín, con respecto a la disminución en la comisión de ciertas conductas delictivas en este territorio; es posible señalar conforme con los datos de la figura 3 que, durante los meses de enero a septiembre de los años 2020 y 2021, gracias al trabajo articulado del

equipo de visualizadores de la Secretaría de Seguridad en conjunto con la Policía Metropolitana se logró capturar en el año 2021 (Enero a Septiembre) a 992 individuos y en el año 2020 en el mismo periodo de tiempo a 934 individuos, de acuerdo a lo anterior se lograron 58 capturas más que el año anterior. Frente a las retenciones realizadas, se logró conducir a 3909 individuos en el 2021 y 910 individuos en el año 2020 desde el mes de enero a septiembre. Las cámaras de ciudad operadas por el personal de la Secretaría de Seguridad y la Policía Nacional propician una mejor percepción de seguridad a la ciudadanía y un respaldo permanente, ya que son monitoreadas las 24 horas del día, además de apoyar, tanto actividades preventivas como reactivas.

Otro aspecto importante de articulación pública está relacionado con las investigaciones realizadas por estas entidades, las cuales se apoyan en las grabaciones que son utilizadas en procesos de desarticulación de bandas delincuenciales, esclarecimiento de homicidios y de hurto en todas las modalidades que se realizan de manera permanente en conjunto con los operadores de videovigilancia de la Secretaría de Seguridad, la Policía Nacional y entidades de Seguridad y Justicia.

#### **3.4. Política Pública de Seguridad y Convivencia de Medellín, 2015**

En esta instancia es pertinente indicar que los resultados referenciados en la sección anterior, así como las acciones de vigilancia adelantadas por las autoridades competentes locales, se fundamentan no solo en los preceptos normativos constitucionales y legales dictaminados en el ámbito nacional; sino que también se rigen a la luz de las disposiciones legislativas promulgadas en la ciudad de Medellín, en este caso con la Política Pública de Seguridad y Convivencia, consagrada con un horizonte temporal de 10 años, a través del Acuerdo Municipal 021 de 2015, con el cual se evidencia el uso intensificado de estrategias de videovigilancia, por medio de su Sistema Integrado de Emergencias y Seguridad de Medellín (SIES-M), un proyecto de integración tecnológica con escalabilidad, integridad y gobernabilidad tecnológica

centrado en la optimización de la información y la atención a los reportes generados (Alcaldía de Medellín, 2015a).

Esta política pública junto con el SIES-M están fundamentados en la Constitución Política de 1991 (artículos 2, 315 y 189 con sus numerales 4 y 11); el documento CONPES 3437 de 2006 con el que se fijan los parámetros generales para la operación de dicho sistema, el Decreto Presidencial 4366 de 2006, con el que se regula la operatividad de los Sistemas Integrados de Emergencias y Seguridad y además, prevé los subsistemas que los conforman y también se sustenta en el Decreto Municipal 0495 de 2012, por el cual se modifica la estructura administrativa de la Secretaría de Gobierno y se crea la Secretaría de Seguridad (Alcaldía de Medellín, 2015b).

La Política Pública de Seguridad y Convivencia, se origina con la finalidad de atender de una forma continuada y efectiva las problemáticas en materia de seguridad presentadas en la ciudad desde muchas décadas atrás y que han derivado en la violación de los Derechos Humanos de sus habitantes, la inobservancia de diversos Derechos Sociales, Económicos y Culturales y la comisión sistemática de numerosos delitos, como el desplazamiento forzado (Alcaldía de Medellín, 2015a).

Ante esta alarmante realidad, se propuso la presente política pública en el Plan de Desarrollo 2012-2015: Medellín, un hogar para la vida, teniendo como principios esenciales y generales el Desarrollo Humano Integral y la Seguridad Humana. El primer concepto se adopta conforme con la definición consolidada desde la década de los años noventa del siglo anterior, el cual se centra en el bienestar de la población en cada una de las esferas en que se desenvuelve y no solo en su contexto económico; y la Seguridad Humana se concibe como la protección de las libertades fundamentales en los ámbitos económicos y sociales de la población (Alcaldía de Medellín, 2015a).

Así las cosas, el eje central de la Política Pública de Seguridad y Convivencia, corresponde con el diseño y la implementación del Modelo Integral de Gestión Local de la Seguridad y Convivencia, el cual se fundamenta en la Seguridad Ciudadana, la

misma que concibe desde una perspectiva multidimensional, ya que transversaliza la seguridad personal, política y la seguridad humana. En este sentido, la seguridad personal se enfoca en la protección de los habitantes, principalmente, con respecto a la violencia física; la seguridad política reside en que las personas puedan vivir en una sociedad donde se respetan sus derechos humanos fundamentales y se fortalece su tejido social, dos aspectos que dan lugar a la seguridad comunitaria (Alcaldía de Medellín, 2015a).

De esta forma, el Modelo Integral de Gestión Local de la Seguridad y Convivencia, se consolida la seguridad ciudadana, reposicionando a los ciudadanos como el principal objeto de la protección estatal contra actos violentos o criminales, mediante la formulación de políticas de seguridad centradas en el bienestar de la población y los derechos humanos. De igual forma, se sustenta y desarrolla conforme con diversos enfoques teóricos y empíricos, entre los cuales se encuentra el enfoque de derechos. Se trata de un modelo conformado por diversos subsistemas, dentro de los cuales se destacan el Subsistema de Videovigilancia y Subsistema de Alarmas Comunitarias y está constituido por tres componentes principales: lineamientos estratégicos, instrumentos y escenarios (Alcaldía de Medellín, 2015a).

En línea con el primer componente y con la presente investigación, se tiene que una de las estrategias propuestas con esta política pública está orientada hacia la implementación de tecnología para la gestión de la seguridad y la convivencia, para la optimización de la información y la atención a los reportes generados con respecto a la seguridad de la ciudadanía; lo cual se ha efectuado, mediante la incorporación de “aplicaciones web como seguridad en línea, App 123, CAI Móvil y (...) Patrullas Inteligentes que permite localizar geográficamente las patrullas en servicio para una reacción más oportuna” (Alcaldía de Medellín, 2015a, p. 81). Además, el componente de los instrumentos, se concreta con “la elaboración y efectiva implementación de programas, proyectos y planes de acción para la intervención de problemáticas prioritizadas” (Alcaldía de Medellín, 2015a, p. 82).

#### **4. La prevalencia de la seguridad ciudadana, limita y vulnera el goce efectivo del derecho a la intimidad**

De conformidad con el desarrollo de la presente monografía, en este capítulo se efectúa una reflexión analítica con respecto a la seguridad ciudadana y al derecho a la intimidad, desde sus perspectivas doctrinales, normativas y jurisprudenciales, haciendo énfasis en las implicaciones que tiene el uso de las cámaras de videovigilancia en el ejercicio efectivo de este derecho.

En este orden de ideas, para el cumplimiento de los fines esenciales consagrados con el artículo 2 de la Constitución Política de 1991, entre estos, la garantía y protección de los derechos y principios fundamentales de sus ciudadanos, como la vida y el respeto de su honra y bienes; el Estado colombiano, en su calidad de Estado Social de Derecho procura su intervención, a través de sus cuerpos y fuerzas de seguridad, para asegurar el goce efectivo de estas prerrogativas a todos los ciudadanos del territorio nacional. Para garantizar la seguridad nacional, el Estado colombiano se ha apoyado en la implementación de diversas estrategias y mecanismos de política de defensa y seguridad, mediante los cuales se busca fortalecer la legitimidad estatal y el régimen democrático, el respeto por los derechos humanos y la construcción de legalidad.

Para la observancia de estos objetivos, junto con la prevención y represión en la comisión de delitos en general, el gobierno nacional y municipal ha fortalecido en años recientes su aparato de seguridad pública con la incorporación y el uso intensivo de las TIC, encontrando en las cámaras de videovigilancia un conjunto de dispositivos idóneos para estos fines, porque, entre otras ventajas, permiten la captación en tiempo real de datos de diversa tipología que favorecen la prevención del delito, la reacción temprana ante hechos que afectan la seguridad ciudadana y posibilitan la toma de decisiones informadas en la materia (Grisales & Bustamante, 2020; Nájera, 2015).

En el marco de los avances tecnológicos empleados en el país y en la ciudad de Medellín para resguardar la seguridad ciudadana, esta ha sido concebida desde una

perspectiva punitiva y represiva, considerando que para responder de forma efectiva con la seguridad pública, es suficiente con la atención y reducción de las problemáticas de criminalidad originadas en el territorio nacional y con un mayor control de los espacios donde estos asuntos se materializan; un discurso utilizado para argumentar la necesidad de tener este tipo de cámaras y de incrementarlas paulatinamente, aunque en realidad lo que por lo general se logra es desplazar las actividades ilegales a otros lugares (Londoño, 2021).

Sin duda, la seguridad ciudadana es fundamental en los Estados democráticos como Colombia, porque favorece la protección integral de sus administrados y también contribuye con la garantía del ejercicio y goce efectivo de sus derechos humanos y fundamentales; de ahí que se concibe como un asunto de interés general con prevalencia en el territorio nacional para garantizar el orden público. Sin embargo, diversos autores aseveran que el uso generalizado de las cámaras de videovigilancia en los espacios públicos de las ciudades para la atención de la seguridad ciudadana limita e, incluso, vulnera los derechos de la población, entre estos, el derecho a la intimidad y el *habeas data*; una situación que desde el ámbito doctrinal, normativo, jurisprudencial y empírico implica sacrificar hasta cierta medida esta prerrogativa, así como la invasión a su vida privada y libertades personales (Grisales & Bustamante, 2020; Osorio & Perozzo, 2016), lo que a su vez, es justificada y reconocida por la Corte Constitucional, por la finalidad legítima que persigue, es decir, conservar la tranquilidad y seguridad del pueblo en general (Corte Constitucional. Sentencia C-881/14, 2014).

Especialmente, en ciudades como Medellín, donde sus habitantes continúan sufriendo los estragos de la violencia e inseguridad urbana, estas se buscan contrarrestar con la instalación de cámaras de videovigilancia y el monitoreo masivo de la población (Delgado, 2019); un mecanismo que si bien recopila información gráfica que puede ser utilizada para adelantar una investigación criminal, esclarecer y buscar el autor de un determinado delito, también se evidencia que dicho procedimiento produce el desconocimiento del derecho a la intimidad y la recolección indiscriminada y masiva de datos personales sensibles que afectan el desarrollo libre de su personalidad, todo ello

“para que prevalezca la seguridad (...) una tara de los tiempos tecnológicos modernos, pero [que] en la práctica no resuelve crímenes y sí deja a la toda la ciudadanía expuesta y sin protección” (León, 2020, párr. 5); dado que los estudios referidos a su efectividad en la lucha contra la delincuencia, no logran demostrar la reducción en la comisión de conductas punibles.

Así las cosas, se ha identificado que la limitación y vulneración del derecho a la intimidad, para salvaguardar la seguridad ciudadana mediante la implementación de cámaras de videovigilancia en la ciudad de Medellín; se configura por la confluencia de una serie de factores que dan lugar a esta situación, los cuales se explican en las siguientes líneas.

#### **4.1. Registro y tratamiento indiscriminado de los datos personales**

Según se ha referenciado en acápites anteriores, las cámaras de videovigilancia son dispositivos tecnológicos de uso masivo que integran un CCTV y han sido instaladas en la ciudad de Medellín, entre otros propósitos, para mejorar la seguridad y defensa local, a través de la captación de una significativa cantidad de imágenes y videos en tiempo real en numerosos lugares de la ciudad.

Se trata de una recopilación y tratamiento indiscriminados y generalizados de grandes volúmenes de datos personales de la población que, junto con un régimen general de protección de datos personales inconstante, insuficiente e incongruente para responder con la rápida evolución de la tecnología y con la instauración de parámetros que condicionen la instalación de las cámaras de videovigilancia; generan que mientras el legislador reacciona y se adapta a estas nuevas circunstancias, el derecho a la intimidad de las personas quede expuesto a posibles abusos y atropellos de todo tipo, por parte de quienes monitorean las cámaras y que además, los datos recopilados puedan ser utilizados para fines diferentes a la seguridad ciudadana (Delgado, 2019).

#### **4.2. De los datos sensibles y biométricos recopilados con cámaras analíticas y de reconocimiento fácil**

A tenor de lo planteado en breve, la limitación y vulneración del derecho a la intimidad frente a la seguridad ciudadana, también se puede presentar con respecto al tratamiento de los datos biométricos obtenidos en la ciudad de Medellín, con las cámaras de videovigilancia analíticas y de reconocimiento facial instaladas desde el año 2021, los cuales se encuentran catalogados como datos personales sensibles, ya que la Ley de *habeas data* (Ley 1581 de 2012) en su artículo 5, los define así:

Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Congreso de Colombia. Ley 1581, 2012).

Según el precitado texto, se evidencia explícitamente que los datos biométricos (v.gr. huellas dactilares, lectura fácil, etc.) son de carácter sensible, no solo porque el uso indebido de los mismos puede dar lugar a hechos de discriminación contra sus titulares, sino también porque son datos de las personas derivados de sus rasgos únicos e intransferibles, los cuales facilitan su identificación y asociación con determinados aspectos políticos, religiosos, sociales, ideológicos, entre otros, de la vida íntima y privada de las personas.

En términos generales, por la naturaleza de los datos sensibles, las disposiciones normativas referidas en la Ley de *habeas data* prohíben el tratamiento de los mismos, aunque también preceptúa una serie de excepciones a la regla, lo que sucede cuando “el titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización” (Congreso de Colombia, Ley 1581, 2012, art. 6, lit. a). Es así como el tratamiento de los datos personales es legitimado cuando existe la autorización por parte de su titular, la cual se fundamenta en el principio de libertad y se materializa con el “consentimiento previo,

expreso e informado del titular” (Congreso de Colombia. Ley 1581, 2012, art. 3, lit, a), un procedimiento fundamental para la defensa del derecho a la intimidad.

Por este motivo, el tratamiento de los datos solo puede darse cuando la autorización por parte del titular es otorgada antes de dicho tratamiento (previo), de forma inequívoca y con absoluta claridad (expreso y no admite consentimiento tácito) y teniendo pleno conocimiento de los asuntos implicados con dicho procedimiento para que pueda tomar una decisión a conciencia (informado); estos tres requisitos en conjunto configuran un ejercicio efectivo de la libertad de los colombianos en la administración de sus datos personales y de decidir qué hacer con su información personal. Es preciso clarificar que la ausencia de alguno de estos tres requisitos rescinde el tratamiento de los datos y puede dar lugar a sanciones por parte de la Superintendencia de Industria y Comercio.

No obstante, el legislador también determina algunas excepciones para las cuales no se requiere la autorización del titular de los datos personales para efectuar su tratamiento, entre los que se tiene en cuenta, para efectos de la presente investigación, el literal (a) del artículo 10, el cual establece que se omita dicha autorización cuando la “información [es] requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial”; lo que es aplicable con respecto a las acciones implementadas en este caso, por la Alcaldía de Medellín para salvaguardar la defensa municipal y la seguridad ciudadana, a través de las cámaras de videovigilancia, siendo esta entidad en últimas, según lo proferido por la Corte Constitucional (Sentencia C-748/11, 2011), el Responsable del tratamiento de los datos en el orden municipal del Ejecutivo y por lo tanto, quien tendría la obligación de recoger la autorización de los ciudadanos, en especial cuando de datos sensibles y biométricos se trata.

En el marco de la seguridad ciudadana con cámaras de videovigilancia y para evitar la dificultad logística que conlleva la recopilación de las autorizaciones de quienes constitucionalmente, la Alcaldía de Medellín está llamado a proteger y con la finalidad de garantizar el derecho a la intimidad y su principio de libertad, se ha estipulado desde el gobierno nacional, conforme con la figura de las conductas inequívocas, la

posibilidad de obtener dicha autorización, según las disposiciones legislativas del Decreto compilatorio 1074 de 2015, mediante la ubicación de avisos o carteles de privacidad con las políticas de tratamiento de información de los lugares donde se operan este tipo de cámaras de seguridad. Se trata de un aviso que pueden ser difundido por medio de “documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular” (Presidente de la República de Colombia. Decreto 1074, 2015, art. 2.2.2.25.3.5.). De esta forma, entre otros elementos, estos avisos deben tener los datos de identificación del responsable del tratamiento de los datos recopilados, el tratamiento a realizar y los derechos del titular, etc.; además, se especifica con respecto a la recolección de datos personales sensibles que, en este caso, “el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos” (Presidente de la República de Colombia. Decreto 1074, 2015, art. 2.2.2.25.3.3.).

En teoría, se presume que las personas, antes de trasladarse en un espacio donde existen cámaras de videovigilancia instaladas, se han encontrado con el aviso de privacidad y han tomado una decisión informada sobre el tratamiento de los datos personales recopilados con aquellas. A simple vista, la ubicación de los avisos de privacidad pueden solucionar las dificultades logísticas que se derivan con la recopilación de las autorizaciones de los ciudadanos para que la Alcaldía de Medellín realice el tratamiento de sus datos sensibles y biométricos, con la finalidad de mantener la seguridad ciudadana; sin embargo, la efectividad de esta solución es parcial, porque limita y vulnera el derecho a la intimidad de las personas, toda vez, que las autoridades competentes o terceros, en especial el responsable del tratamiento puede utilizar los datos biométricos, sin haber confirmado que el tratamiento a efectuar es legítimo, porque en muchos casos las personas no muestran interés por leer estos avisos, son analfabetas o tienen limitaciones físicas o cognitivas que dificultan la comprensión de su contenido; lo que daría lugar a la falta de autorización en el tratamiento de datos realizado por la Alcaldía de Medellín.

Si bien con estos avisos de privacidad, se logra obtener hasta cierto punto y en determinados casos, el consentimiento del titular de los datos sensibles y biométricos de las personas que circulan por las zonas vigiladas, también se evidencia que, en reiteradas circunstancias, las personas autorizan el tratamiento de sus datos personales, con la aceptación de los avisos en cuestión, para poder acceder a una serie de espacios, servicios y relaciones, entre otros; porque *v.gr.* si alguien pretende ingresar a una entidad pública donde hay cámaras de videovigilancia instaladas que recopilan datos sensibles y no está de acuerdo con el aviso de privacidad y toma la decisión de no ingresar, entonces esa persona no efectúa el servicio o trámite requerido; por lo cual es frecuente que los ciudadanos sacrifiquen la privacidad e intimidad de estos datos para poder acceder y satisfacer sus requerimientos. En este sentido, Delgado (2019) sintetiza el tratamiento de los datos sensibles y biométricos, así: “con la tecnología que predomina hoy en las calles puede que la legislación actual sea en conjunto, satisfactoria. Pero no está lista para el auge de la identificación facial y la biometría sin comprometer” (p. 61), los derechos a la intimidad, privacidad y de habeas data de los ciudadanos.

Para preservar el orden público, la seguridad ciudadana nacional y local y lograr el ejercicio efectivo de las libertades individuales y de los derechos a la intimidad y a la privacidad, teniendo en cuenta las limitaciones de los avisos de privacidad para la autorización del tratamiento de los datos biométricos recopilados con las cámaras de videovigilancia instaladas tanto en Medellín como en otras ciudades del país y las excepciones planteadas por el legislador al respecto; la Corte Constitucional (Sentencia C-748/11, 2011) ha sido enfática en establecer que los ámbitos exceptuados en la materia, como en este caso el tratamiento de datos biométricos por parte del Responsable del tratamiento (Ejecutivo municipal), sin que medie el respectivo consentimiento, deben ser regulados mediante Leyes Estatutarias especiales y complementarias, acordes con las exigencias del principio de proporcionalidad, el mismo que debe ser vigilado y controlado por un órgano independiente, bien sea común o sectorial y que “deberán (i) perseguir una finalidad constitucional, (ii) prever medios idóneos para lograr tal objetivo, y (iii) establecer una regulación que en aras de

la finalidad perseguida, no sacrifique de manera irrazonable otros derechos constitucionales” (Corte Constitucional. Sentencia C-748/11, 2011, p. 144).

Desde esta perspectiva, se evidencia la vulneración del derecho a la intimidad y de *habeas data* de los habitantes de la ciudad de Medellín con las cámaras de videovigilancia analíticas y de reconocimiento facial, por la falta de las leyes estatutarias referidas en breve, la existencia de algunos cuerpos normativos con las cuales persiguen una finalidad constitucional, como lo es la seguridad ciudadana, pero también se encuentra la ausencia de leyes que no sacrifiquen de manera irrazonable otros derechos constitucionales y que permitan prever los medios idóneos, necesarios y proporcionales para lograr dicha finalidad, lo cual no se presenta con dichas cámaras tal como se referencia en el siguiente apartado.

#### **4.3. Inobservancia de los principios de idoneidad, necesidad y proporcionalidad**

Corolario con los factores referenciados en acápite anteriores que prevalecen la seguridad ciudadana en Medellín y afectan el derecho a la intimidad de los habitantes de la ciudad; se ha hallado que la restricción e, incluso, vulneración de este derecho para garantizar la defensa y seguridad pública municipal con las cámaras de videovigilancia instaladas por la Alcaldía de Medellín, solo es posible cuando el uso de estos dispositivos junto con las actividades esenciales para su implementación están amparadas en la Carta Magna nacional y las leyes, desde el respeto de este y todos los derechos de los ciudadanos y además, según la Corte Constitucional (Sentencia T-407/2012, 2012) dichas acciones deben cumplir con los criterios de necesidad (si es la única forma factible de lograr el fin legítimo buscado), idoneidad (si es factible lograr el objetivo mediante el uso de las videocámaras) y proporcionalidad (si causa más perjuicios que beneficios al afectado o a terceras personas).

En este sentido, la Corte Constitucional (Sentencia T-224/18, 2018) en reiterada jurisprudencia ha proferido que las cámaras de videovigilancia instaladas, en este caso, en la ciudad de Medellín cumplen con el criterio de necesidad, ya que para esta honorable corporación se trata de dispositivos con cobertura extensa y están instaladas

estratégicamente, para lograr un amplio alcance de radio poblacional; por ello considera que estas cámaras de seguridad no pueden ser sustituidas por otros medios menos invasivos y que además, son idóneas para lograr el objetivo de mejorar la seguridad ciudadana en la ciudad, toda vez que, puede identificar a un alto número de personas que según sus datos personales, podrían ser considerados como sospechosos o potenciales autores de conductas punibles e incluso, favorece la reacción temprana y en tiempo real de las autoridades judiciales ante la comisión de delitos en los lugares donde esta instaladas las cámaras de videovigilancia; en términos generales, se busca prevenir y/o disuadir la criminalidad y la represión del delito.

Sin embargo, de acuerdo con los aportes de Osorio y Perozzo (2016), el criterio de idoneidad es limitado, con respecto al objetivo de prevención y abstención en la comisión de delitos, lo que con frecuencia es cumplido por los delincuentes dentro del campo de visualización de las cámaras de videovigilancia públicas; trasladando de esta forma, sus actos delictivos hacia aquellos espacios donde no tienen alcance estos dispositivos, por lo tanto, no solo se presenta la inobservancia de estos objetivos, sino que, además, se produce el traslado de las problemáticas de seguridad ciudadana a otros espacios de la ciudad de Medellín donde no puedan ser identificados con las cámaras.

Por otra parte, con respecto al criterio de proporcionalidad, la Corte Constitucional (Sentencia T-407/2012, 2012) ha reconocido que el uso de cámaras de videovigilancia afecta el goce y ejercicio efectivo del derecho a la intimidad en el espacio público, motivo por el cual se ha hecho indispensable determinar si las mismas son proporcionadas y razonables, es decir, que no haya una alternativa menos lesiva y restrictiva de esta prerrogativa y de las libertades de los ciudadanos. Para llevar a cabo el juicio de proporcionalidad, esta honorable corporación ha señalado la existencia de tres niveles de intensidad en la aplicación del mismo, a saber: test leve, intermedio y estricto; teniendo en cuenta que en el caso objeto de estudio de la presente monografía, le es aplicable este último test, porque entre otros eventos se aplica

cuando la medida –uso de cámaras de videovigilancia públicas–, *prima facie* afecta el goce de un derecho constitucional fundamental (a la intimidad).

En esta misma línea argumentativa, se tiene que uno de los elementos valorados con el test estricto, corresponde con determinar si los beneficios de instalar y usar cámaras de videovigilancia en Medellín para garantizar la seguridad ciudadana en la ciudad son superiores a las restricciones que estas imponen a los principios constitucionales y al derecho a la intimidad afectados con estos dispositivos (Sáenz & Spanger, 2018). Al respecto, es posible prescribir que si bien en materia de seguridad ciudadana, dichos dispositivos –especialmente las cámaras analíticas y de reconocimiento facial– facilitan los procesos de investigación criminal y favorecen la resolución de delitos; también se encuentra que los resultados con estos dispositivos son insuficientes, en comparación con la restricción del derecho a la intimidad; por la recolección indiscriminada de datos personales y el posible tratamiento abusivo que la alcaldía o terceros puedan darle a dicha información.

#### **4.4. Invasión ilegal en el domicilio de los ciudadanos**

Para finalizar el presente capítulo, se tiene que otro de los factores que originan la limitación y vulneración del derecho a la intimidad de los habitantes de la ciudad de Medellín con las cámaras de videovigilancia públicas instaladas por la Alcaldía de Medellín obedece a la invasión en el domicilio de sus administrados, por cuenta de las cámaras móviles que conforman su catálogo de dispositivos tecnológicos para salvaguardar la seguridad ciudadana en este territorio. Esta situación se presenta por la captación de imágenes en el interior del domicilio de los afectados, es decir, una invasión ilegal en su esfera privada o en su núcleo familiar, la cual se deriva de las acciones de vigilancia generalizada efectuadas con las cámaras y con los enfoques selectivos presentados en determinados momentos.

Desde esta perspectiva, es válido clarificar que la invasión al domicilio en sentido amplio, no solo se materializa en la vivienda habitada por los ciudadanos de la ciudad, sino que de acuerdo con (Osorio & Perozzo, 2016), también se puede producir en

algunos espacios externos a la habitación de las personas (*v.gr.* balcones) y según la jurisprudencia de la Corte Constitucional (Sentencia C-204/19, 2019), en otros lugares utilizados transitoriamente por las personas, como un cuarto de hotel.

## 5. Conclusiones

A tenor de la información estudiada en secciones previas, se concluye que, desde el ámbito normativo, doctrinal y jurisprudencial nacional e internacional, se reconoce el derecho a la intimidad como un derecho fundamental inalienable e imprescriptible e inherente a la naturaleza humana de todos los ciudadanos del país; de ahí que no se pueda renunciar al mismo. Como resultado de su conexión con el derecho a la privacidad y de *habeas data*, es una prerrogativa de carácter bidimensional, ya que, por una parte, prohíbe las injerencias arbitrarias de terceros en la vida y los espacios privados de las personas y la divulgación ilegítima de información (dimensión negativa) y, por otra parte, procura proteger la esfera y el espacio internos de las personas, para que, de este modo, puedan tomar decisiones con respecto a su privacidad (dimensión positiva), aquella que se materializa cuando una persona decide exteriorizar su información interna a otros. Desde su perspectiva penal, el derecho a la intimidad está tipificado, a través de diversos delitos informáticos, especialmente, con la interceptación de datos informáticos; mediante los cuales, se espera limitar las injerencias en las bases de datos y en los sistemas informáticos, por parte de terceros no autorizados o que no tengan la custodia de los mismos.

Dentro de los sistemas informáticos, se tienen los sistemas de videovigilancia, los cuales están integrados con cámaras análogas o digitales IP conectadas a un ordenador o dispositivo, donde se reciben señales de video y audio (cuando se requiere) de la información captada en los lugares en los que se encuentran instaladas y donde, además, es controlada por determinadas personas. El catálogo de cámaras de videovigilancia en la ciudad de Medellín, incluye desde cámaras de multisensor (cobertura hasta de 360°) hasta cámaras analíticas y de reconocimiento facial; estas dos últimas, mediante las cuales se recopilan datos sensibles y biométricos y todos estos dispositivos de video en conjunto, conectados y visualizados, a través de un Circuito Cerrado de Televisión (CCTV).

Estas cámaras hacen parte del Subsistema de Videovigilancia y Subsistema de Alarmas Comunitarias y este a su vez, al Sistema Integrado de Emergencias y Seguridad de Medellín (SIES-M), creado con la Política Pública de Seguridad y Convivencia (Acuerdo Municipal 021 de 2015), basado en el Modelo Integral de Gestión Local de la Seguridad y Convivencia y fundamentado en el Desarrollo Humano Integral y la Seguridad Humana, junto con la Seguridad Ciudadana concebida desde una perspectiva multidimensional. En el ámbito nacional y local, las cámaras de videovigilancia y el tratamiento de los datos obtenidos con estas, están regulados principalmente, con la Ley 1581 de 2012, Código de Policía y Convivencia (Ley 1801 de 2016) y Ley Estatutaria 1266 de 2008; las cuales están enfocadas en la protección de los datos personales de los administrados, cuyo tratamiento debe ser consentido por su titular; en regular su uso como un medio para fortalecer las labores de la Policía Nacional y Metropolitana, en la identificación o individualización de los autores o partícipes en la comisión de una conducta punible y también en la clasificación de los datos y los espacios, según su naturaleza y con el alcance del derecho a la intimidad, determinando según los aportes de Galindo y Ramírez (2021), que la privacidad e intimidad de las personas, se reduce entre más abierto al público sean los espacios que transitan.

En definitiva, las cámaras de videovigilancia públicas instaladas por la Alcaldía de Medellín en la ciudad incumplen los criterios de necesidad, idoneidad y proporcionalidad, no solo porque limita y vulnera el derecho a la intimidad por el tratamiento masivo, indiscriminado y generalizado de los datos personales de la población; sino que también se obtienen resultados reducidos en la prevención y represión de los delitos y no son proporcionales y razonables con respecto a la lesión de esta prerrogativa y de las libertades individuales de los ciudadanos. De esta forma, se confirma la prevalencia de la seguridad ciudadana por encima del derecho a la intimidad en este caso, debido a que se trata de un asunto de interés general con un fin legítimo, pero que desprotege este derecho, conforme con las disposiciones legislativas existentes en la materia, en especial con los ámbitos exceptuados y la recolección

discriminada de datos sensibles y con la irrupción en determinados casos del domicilio de algunas personas con las cámaras de video vigilancia móviles.

## Referencias

- Alcaldía de Medellín. (2015a). *Política Pública de Seguridad y Convivencia del Municipio de Medellín. Acuerdo 021*. Medellín: Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). Obtenido de [https://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportalDelCiudadano\\_2/PIandeDesarrollo\\_0\\_1/ProgramasyProyectos/Shared%20Content/Documentos/2015/Politica%20Medellin%20baja%20con%20portada.pdf](https://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportalDelCiudadano_2/PIandeDesarrollo_0_1/ProgramasyProyectos/Shared%20Content/Documentos/2015/Politica%20Medellin%20baja%20con%20portada.pdf)
- Alcaldía de Medellín. (2015b). *SIES-M Sistema Integrado de Emergencias y Seguridad Medellín*. Obtenido de [https://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportalDelCiudadano\\_2/PIandeDesarrollo\\_0\\_1/ProgramasyProyectos/Shared%20Content/Documentos/2015/presentacion%20SIESM.pdf](https://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportalDelCiudadano_2/PIandeDesarrollo_0_1/ProgramasyProyectos/Shared%20Content/Documentos/2015/presentacion%20SIESM.pdf)
- Arboleda, S. (27 de diciembre de 2021). *Este año se realizaron 1.167 capturas gracias al Sistema de video vigilancia de Medellín*. Obtenido de <https://www.medellin.gov.co/irj/portal/medellin?NavigationTarget=contenido/11715-Este-ano-se-realizaron-1167-capturas-gracias-al-Sistema-de-video-vigilancia-de-Medellin>
- Asamblea General de las Naciones Unidas. Resolución 217 (III). (10 de diciembre de 1948). *Declaración Universal de los Derechos Humanos*. Obtenido de undocs.org: [https://www.un.org/es/documents/udhr/UDHR\\_booklet\\_SP\\_web.pdf](https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf)
- Asamblea General de las Naciones Unidas. Resolución 2200 A (XXI). (16 de diciembre de 1966). *Pacto Internacional de Derechos Económicos, Sociales y Culturales*. Obtenido de [www.ohchr.org](http://www.ohchr.org): <https://www.ohchr.org/sp/professionalinterest/pages/cescr.aspx>
- Báez, D. (2019). *Implementación de un sistema de video vigilancia a través de cámaras de seguridad para los laboratorios de la Facultad de Ingeniería Electrónica*. Tunja, Boyacá: [Tesis Presentada Para Obtener El Título De Ingeniero Electrónico]. Universidad Santo Tomás. Facultad de Ingeniería Electrónica. Obtenido de <https://repository.usta.edu.co/bitstream/handle/11634/20953/2019danielbaez.pdf?sequence=4&isAllowed=y>

- Bautista, M. (2015). *El derecho a la intimidad y su disponibilidad pública*. Bogotá D.C.: Universidad Católica de Colombia. Obtenido de [https://repository.ucatolica.edu.co/bitstream/10983/14306/4/07\\_El-derecho-a-la-intimidad-y-su-disponibilidad-p%C3%BAblica.pdf](https://repository.ucatolica.edu.co/bitstream/10983/14306/4/07_El-derecho-a-la-intimidad-y-su-disponibilidad-p%C3%BAblica.pdf)
- Centro de Estudios de Derecho, Justicia y Sociedad [Dejusticia]. (diciembre de 2016). *Acción pública de inconstitucionalidad contra los artículos 32, 95 parcial, 139 parcial, 146 parcial, y 237 de la Ley 1801 de 2016*. Obtenido de [https://www.dejusticia.org/wp-content/uploads/2017/04/fi\\_name\\_recurso\\_897.pdf](https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_897.pdf)
- Congreso de Colombia. Ley 1581. (18 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial No. 48.587*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Congreso de la República de Colombia. Ley 1801. (29 de julio de 2016). Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana. *Diario Oficial No. 49.949*. Obtenido de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1801\\_2016.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1801_2016.html)
- Congreso de la República de Colombia. Ley 906. (1 de septiembre de 2004). Por la cual se expide el Código de Procedimiento Penal. *Diario Oficial No. 45.658*. Obtenido de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_0906\\_2004.html#14](http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html#14)
- Congreso de la República de Colombia. Ley Estatutaria 1266. (31 de diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países (...). *Diario Oficial No. 47.219*. Obtenido de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1266\\_2008.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html)
- Constitución Política de Colombia. (20 de julio de 1991). Constitución Política de la República de Colombia. *Gaceta Constitucional No. 116*. Obtenido de [http://www.secretariasenado.gov.co/senado/basedoc/constitucion\\_politica\\_1991.html#1](http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#1)
- Corte Constitucional. Sentencia C-094/20, Expediente: D-11902 (M.P. Alejandro Linares Cantillo 3 de marzo de 2020). Obtenido de [https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm#\\_ftnref112](https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm#_ftnref112)

- Corte Constitucional. Sentencia C-204/19, Expediente: D-11973 (M.P. Alejandro Linares Cantillo 15 de mayo de 2019). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2019/C-204-19.htm>
- Corte Constitucional. Sentencia C-748/11, Expediente PE-032 (M.P. Jorge Ignacio Pretelt Chaljub 6 de octubre de 2011). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>
- Corte Constitucional. Sentencia C-881/14, Expediente D-10273 (M.P. Jorge Ignacio Pretelt Chaljub 19 de noviembre de 2014). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2014/C-881-14.htm>
- Corte Constitucional. Sentencia T-224/18, Expediente No.: T- 6.438.681 (M.P. Alberto Rojas Ríos 8 de junio de 2018). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2018/T-224-18.htm>
- Corte Constitucional. Sentencia T-364/18, Expediente T-6.488.782 (M.P. Alberto Rojas Ríos 4 de septiembre de 2018). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2018/t-364-18.htm>
- Corte Constitucional. Sentencia T-407/2012, Expediente T-3.348.314 (M.S. Mauricio González Cuervo 31 de mayo de 2012). Obtenido de <https://www.corteconstitucional.gov.co/RELATORIA/2012/T-407-12.htm>
- Corte Constitucional. Sentencia T-414/92, Expediente T-534 (M.P. Ciro Angarita Baron 16 de junio de 1992). Obtenido de [https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm#\\_ftnref16](https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm#_ftnref16)
- Corte Constitucional. Sentencia T-552/97, Expediente T-137.224 (M.P. Vladimiro Naranjo Mesa 30 de octubre de 1997). Obtenido de [https://www.corteconstitucional.gov.co/relatoria/1997/t-552-97.htm#\\_ftnref2](https://www.corteconstitucional.gov.co/relatoria/1997/t-552-97.htm#_ftnref2)
- Corte Constitucional. Sentencia T-574/17, Expediente T-6.142.741 (M.P. Alejandro Linares Cantillo 14 de septiembre de 2017). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2017/T-574-17.htm>
- Corte Constitucional. Sentencia T-787/04, Expediente T-722765 (M.P. Rodrigo Escobar Gil 18 de agosto de 2004). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm>
- Delgado, F. (2019). *Comentarios a los sistemas de video vigilancia en el marco del Régimen de Protección de Datos Personales*. Medellín: [Monografía para optar al

- título de Abogado]. Universidad EAFIT. Escuela de Derecho. Obtenido de [https://repository.eafit.edu.co/bitstream/handle/10784/13794/Federico\\_DelgadoAguilar\\_2019.pdf?sequence=2&isAllowed=y](https://repository.eafit.edu.co/bitstream/handle/10784/13794/Federico_DelgadoAguilar_2019.pdf?sequence=2&isAllowed=y)
- Departamento Nacional de Planeación [DNP]. (14 de junio de 2015). *En 2018 habrá 10.664 videocámaras para fortalecer la seguridad ciudadana en el país*. Obtenido de <https://www.dnp.gov.co/Paginas/En-2018-habr%C3%A1-10-664-videoc%C3%A1maras-para-fortalecer-la-seguridad-ciudadana-en-el-pa%C3%ADs.aspx>
- Fernández -Barbudo, C. (2019). El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista de Estudios Políticos*(185), 139-167. Obtenido de [https://www.researchgate.net/publication/336105882\\_El\\_nuevo\\_concepto\\_de\\_privacidad\\_la\\_transformacion\\_estructural\\_de\\_la\\_visibilidad](https://www.researchgate.net/publication/336105882_El_nuevo_concepto_de_privacidad_la_transformacion_estructural_de_la_visibilidad)
- Galindo, J., & Ramírez, C. (2021). *El derecho a la intimidad como límite al derecho a la prueba en el marco de las nuevas tecnologías*. Medellín: [Monografía]. Universidad EAFIT. Obtenido de [https://repository.eafit.edu.co/bitstream/handle/10784/30697/Carolina\\_RamirezSierra\\_JuanJose\\_GalindoSalazar\\_2021.pdf?sequence=2&isAllowed=y](https://repository.eafit.edu.co/bitstream/handle/10784/30697/Carolina_RamirezSierra_JuanJose_GalindoSalazar_2021.pdf?sequence=2&isAllowed=y)
- García del Valle, J. (2013). *La videovigilancia: tecnologías actuales y aspectos sociopolíticos*. Madrid: [Proyecto Fin de Carrera]. Universidad Politécnica de Madrid. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Obtenido de [https://oa.upm.es/21331/1/PFC\\_JOSE\\_GARCIA\\_DEL\\_VALLE.pdf](https://oa.upm.es/21331/1/PFC_JOSE_GARCIA_DEL_VALLE.pdf)
- Grisales, W., & Bustamante, J. (2020). El derecho fundamental a la intimidad y el Big Data. En J. Sepúlveda, *Apuntes al derecho desde investigación* (págs. 331-345). Medellín: Sello Editorial Universitario Americana. Obtenido de <https://americana.edu.co/medellin/wp-content/uploads/2021/06/Apuntes-al-derecho-desde-investigacion-Libro-completo.pdf#page=331>
- Jasso-López, L. (2020). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en Latinoamérica. *Diké. Revista de investigación en Derecho, Criminología y Consultoría Jurídica*(27), 5-27. Obtenido de <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/914>

- León, J. (28 de enero de 2020). Estado policivo, cámaras y vigilancia masiva. *La Silla Vacía*. Obtenido de <https://www.lasillavacia.com/historias/historias-silla-llena/estado-policivo-camaras-y-vigilancia-masiva/>
- Londoño, I. (2021). *Configuración, usos y relaciones del ensamblado de vigilancia con cámaras en la ciudad de Medellín*. Medellín, Colombia: [Monografía presentada como requisito parcial para optar al título de: Magíster en Estudios de Ciencia, Tecnología, Sociedad e Innovación CTS+i]. Instituto Tecnológico Metropolitano (ITM). Facultad de Artes y Humanidades. Obtenido de [https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5557/lv%C3%A1n%20Santiago\\_%20Londo%C3%B1oOsorio\\_2021.pdf?sequence=1&isAllowed=y](https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5557/lv%C3%A1n%20Santiago_%20Londo%C3%B1oOsorio_2021.pdf?sequence=1&isAllowed=y)
- Megías, J. (2002). Privacidad e internet: intimidad, comunicaciones y datos personales. *Anuario de Derechos Humanos*, 3, 515-560. Obtenido de <https://rodin.uca.es/bitstream/handle/10498/16460/ADH%202002.PDF?sequence=1&isAllowed=y>
- Moreno, M. (2003). La protección del derecho a la intimidad en el Código Penal español. Los delitos de descubrimiento y revelación de secretos. *Revista de Derecho*(6), 65-104. Obtenido de <https://camjol.info/index.php/DERECHO/article/download/1525/1330>
- Nájera, S. (2015). Análisis espacial de la videovigilancia como respuesta táctica a los fenómenos del terrorismo y crimen organizado: Caso práctico de Madrid. *Revista del Instituto Español de Estudios Estratégicos*(5), 1-26. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=5155182>
- Organización de los Estados Americanos [OEA]. (1969). *Convención Americana Sobre Derechos Humanos (Pacto de San José)*. San José, Costa Rica: Departamento de Derecho Internacional OEA. Obtenido de [https://www.oas.org/dil/esp/tratados\\_b-32\\_convencion\\_americana\\_sobre\\_derechos\\_humanos.htm](https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm)
- Osorio, E., & Perozzo, J. (2016). El sistema de videovigilancia policial en Cúcuta y la inviolabilidad del domicilio. *Revista Academia & Derecho*, 7(13), 59-90. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=6713559>
- Presidente de la República de Colombia. Decreto 1074. (26 de mayo de 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio,

- Industria y Turismo. *Diario Oficial No.* Obtenido de [https://www.suin-juriscal.gov.co/viewDocument.asp?id=30019935#ver\\_30058124](https://www.suin-juriscal.gov.co/viewDocument.asp?id=30019935#ver_30058124)
- Real Academia Española [RAE]. (2021). *Definición de privacidad*. Obtenido de <https://dle.rae.es/privacidad>
- Rebollo, L. (2005). *El derecho fundamental a la intimidad*. Dykinson.
- Rivas, J., & Velázquez, C. (2011). *Implementación de sistema de seguridad con videovigilancia y software libre*. México D.F.: [Tesis que para obtener el Título de Ingeniero de Control y Automatización por la Opción de Titulación]. Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica. Obtenido de <https://tesis.ipn.mx/jspui/bitstream/123456789/11622/1/3.pdf>
- Sáenz, P., & Spanger, A. (2018). *Cámaras Indiscretas: Análisis del fallido sistema de videovigilancia inteligente para Transmilenio*. Bogotá, Colombia: Fundación Karisma. Obtenido de <https://web.karisma.org.co/wp-content/uploads/2020/04/C%C3%A1maras-indiscretas.pdf>
- Secretaría de Seguridad y Convivencia. (4 de noviembre de 2021). Estadísticas del boletín del SIESM frente al componente de CCTV. Respuesta a un derecho de petición. *Archivo en PDF*.
- Superintendencia de Industria y Comercio [SIC]. (2016). *Protección de datos personales en Sistemas de Videovigilancia*. Bogotá D.C.: Ministerio de Comercio, Industria y Turismo. Obtenido de [https://www.sic.gov.co/sites/default/files/files/Nuestra\\_Entidad/Guia\\_Vigilancia\\_sept16\\_2016.pdf](https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf)
- Todoelectrónica. (20 de octubre de 2019). *6 Diferencias entre cámaras analógicas y cámaras IP*. Obtenido de <https://www.youtube.com/watch?v=mcEv-vKrlck>
- Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Isegoría. Revista de Filosofía Moral y Política*(57), 533-552. Obtenido de <https://isegoria.revistas.csic.es/index.php/isegoria/article/view/994/990>
- Vítores, S. (27 de 09 de 2018). *Privacidad*. Obtenido de [https://cadenaser.com/programa/2018/09/27/hora\\_25/1538077085\\_587111.html](https://cadenaser.com/programa/2018/09/27/hora_25/1538077085_587111.html)