

**Universidad de Costa Rica
Ciudad Rodrigo Facio Brenes
Facultad de Derecho**



Tesis para optar por el grado de Licenciatura en Derecho.

El uso de los sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la protección de datos personales.

Ivannia Madrigal Chacón
A83605

San José, Costa Rica
Febrero, 2019



28 de febrero de 2019
FD-583-2019

Dr. Alfredo Chirino Sánchez
Decano
Facultad de Derecho

Estimado señor:

Para los efectos reglamentarios correspondientes, le informo que el Trabajo Final de Graduación (categoría Tesis), de la estudiante: Ivannia Madrigal Chacón, carné A83605 denominado: "El uso de los sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la protección de datos personales". fue aprobado por el Comité Asesor, para que sea sometido a su defensa final. Asimismo, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo apruebo en el mismo sentido.

Igualmente, le presento a los (as) miembros (as) del Tribunal Examinador de la presente Tesis, quienes firmaron acuso de la tesis (firma y fecha) de conformidad con el Art. 36 de RTFG que indica: **"EL O LA ESTUDIANTE DEBERÁ ENTREGAR A CADA UNO DE LOS (AS) MIEMBROS (AS) DEL TRIBUNAL UN BORRADOR FINAL DE SU TESIS, CON NO MENOS DE 8 DÍAS HÁBILES DE ANTICIPACIÓN A LA FECHA DE PRESENTACIÓN PÚBLICA"**.

Tribunal Examinador

Informante	Dr. Alfredo Chirino Sánchez
Presidente	Dr. Carlos Estrada Navas
Secretario	Dr. Rafael Segura Bonilla
Miembro	Dr. Ricardo Salas Porras
Miembro	

Por último, le informo que la defensa de la tesis es el **27 de febrero del 2019**, a las 6:00 p.m. en el cuarto piso de la Facultad.

Atentamente,

Ricardo Salas Porras
Director



C. Expediente
C. Archivo



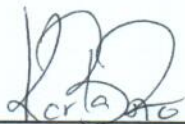
Doctor
Ricardo Salas Porras
Director del Área de Investigación
Universidad de Costa Rica.

15 de febrero de 2019

Por este medio me permito comunicarle que, en mi calidad de directora del Trabajo Final de Graduación de la egresada Ivannia Madrigal Chacón, carné A83605, he leído y revisado la tesis titulada "EL USO DE LOS SISTEMAS DE VIDEOVIGILANCIA COMO MEDIDA DE SEGURIDAD Y SU INCIDENCIA EN LOS DERECHOS DE VIDA PRIVADA, PROPIA IMAGEN Y LA PROTECCION DE DATOS PERSONALES".

A partir de dicha revisión, considero que cumple satisfactoriamente con todos los requisitos de fondo y forma establecidos al efecto por el Área de Investigación para optar por el título de Licenciatura en Derecho. Dicho esto, otorgo mi aprobación del trabajo analizado.

Sin más por el momento, se suscribe.



Dra. Karla Blanco Rojas

San Pedro de Montes de Oca, 18 de febrero de 2019

Señor

Doctor Ricardo Salas Porras

Director del Área de Investigación

Facultad de Derecho

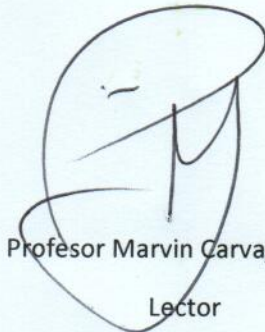
Universidad de Costa Rica

Estimado señor director:

He leído la tesis de la egresada Ivannia Madrigal Chacón, titulada "El uso de los sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de la vida privada, propia imagen y la protección de datos personales", a la cual le doy mi aprobación, pues cumple con todos los requisitos de forma y fondo para ello.

Por estas razones, reitero la aprobación dada al trabajo en cuestión.

Con toda consideración,

A handwritten signature in black ink, consisting of a large, stylized 'M' with a horizontal line through it, enclosed within a large, irregular oval shape.

Profesor Marvin Carvajal Pérez

Lector

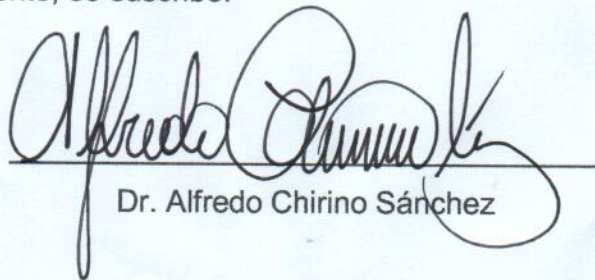
Doctor
Ricardo Salas Porras
Director del Área de Investigación
Universidad de Costa Rica.

15 de febrero de 2019.

Por este medio me permito comunicarle que, en mi calidad de lector del Trabajo Final de Graduación de la egresada Ivannia Madrigal Chacón, carné A83605, he leído y revisado la tesis titulada "EL USO DE LOS SISTEMAS DE VIDEOVIGILANCIA COMO MEDIDA DE SEGURIDAD Y SU INCIDENCIA EN LOS DERECHOS DE VIDA PRIVADA, PROPIA IMAGEN Y LA PROTECCION DE DATOS PERSONALES".

A partir de dicha revisión, considero que esta tesis hace un valioso aporte en materia de videovigilancia pública, se realiza un correcto análisis doctrinal y legal en la investigación, recurriéndose al derecho comparado. Se identifican las condiciones práctico/legales bajo las cuales se deben enmarcar los sistemas de videovigilancia para un correcto uso responsable de esta tecnología. Se concluye la necesidad de integrar el uso de estos sistemas con otras medidas de seguridad, reflexionar sobre el uso desmedido de las cámaras en los espacios públicos y enfocar su funcionamiento a garantizar la protección de datos personales.

Sin más por el momento, se suscribe.



Dr. Alfredo Chirino Sánchez

CARTA DE REVISIÓN DEL FILÓLOGO

San José 13 de junio del 2018.

**SEÑORES
UNIVERSIDAD DE COSTA RICA
FACULTAD DE DERECHO**

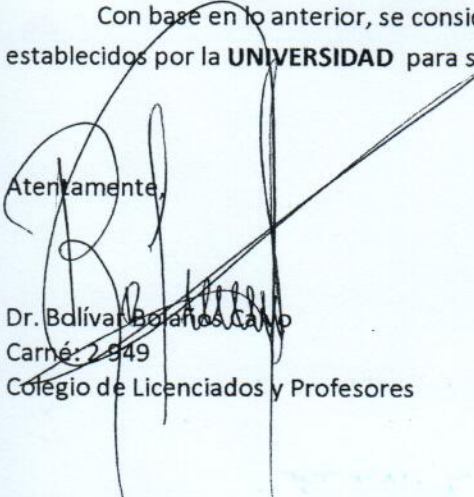
Estimados señores:

Hago constar que he revisado la **TESIS**, de la estudiante **IVANNIA MADRIGAL CHACÓN**, denominado **EL USO DE LOS SISTEMAS DE VIDEOVIGILANCIA COMO MEDIDA DE SEGURIDAD Y SU INCIDENCIA EN LOS DERECHOS DE VIDA PRIVADA, PROPIA IMAGEN Y LA PROTECCIÓN DE DATOS PERSONALES**.

He revisado errores gramaticales, de puntuación, ortográficos y de estilo que se manifiestan en el documento escrito, y verificado que estos fueron corregidos por la autora.

Con base en lo anterior, se considera que dicho trabajo cumple con los requisitos establecidos por la **UNIVERSIDAD** para ser presentado como requerimiento final de graduación.

Atentamente,


Dr. Bdlívar Bolaños Camp
Carné: 2849
Colegio de Licenciados y Profesores

DEDICATORIA

Esta tesis se la dedico a mis padres, quienes han estado siempre a mi lado. Quienes han insistido y presionado para que yo salga adelante en la vida. Gracias porque depositaron su fe y esperanza en mí; me han dado tanto en esta vida que no alcanza el papel para detallar los maravillosos padres que son. Gracias a sus esfuerzos concluyo una etapa más de mi vida. Gracias por haber invertido tanto en mí y por su apoyo en todos estos años. Los amo.

AGRADECIMIENTOS.

Agradecerle a Dios, quien me mantiene con vida, salud y fuerzas para continuar con otras metas futuras. De Él proviene la inspiración para emprender más proyectos y sueños que deseamos cumplir.

A la Universidad de Costa Rica, que se convirtió en un baluarte en mi vida, me albergó en sus aulas y me enseñó la importancia del continuo aprendizaje, nunca se deja de aprender y el nivel de aprendizaje que deseamos depende de nosotros. Gracias a la Universidad por disponer de profesores y personas dispuestas a enseñarnos.

Le agradezco a la profesora Karla Blanco Rojas, por acompañarme en este proyecto que concluye una etapa universitaria, pero que, con él inician otros nuevos proyectos. Gracias por su dedicación y tiempo, y por haber compartido su conocimiento conmigo.

Igualmente, a los profesores Marvin Carvajal y Alfredo Chirino por invertir de su valioso tiempo en este trabajo de investigación y por la vocación que han elegido como profesores universitarios de tan prestigiosa institución.

EPÍGRAFE

“Aquellos que renunciarían a una libertad esencial para comprar un poco de seguridad momentánea, no merecen ni libertad ni seguridad y acabará perdiendo ambas”

Benjamín Franklin

Tabla de contenido

<i>DEDICATORIA</i>	<i>i</i>
<i>AGRADECIMIENTOS</i>	<i>ii</i>
<i>EPÍGRAFE</i>	<i>iii</i>
<i>TABLA DE AVREVIATURAS</i>	<i>vi</i>
<i>RESUMEN</i>	<i>vii</i>
<i>FICHA BIBLIOGRÁFICA</i>	<i>ix</i>
<i>INTRODUCCIÓN</i>	<i>1</i>
<i>CAPÍTULO 1: EL FENOMENO DE LA VIDEOVIGILANCIA</i>	<i>6</i>
Sección primera: Política Criminal y Seguridad	<i>7</i>
1.1 La entrada del neoliberalismo penal.....	<i>10</i>
1.2 La participación ciudadana en materia de seguridad.....	<i>15</i>
1.3 La predominancia de los elementos subjetivos en materia de seguridad.....	<i>18</i>
Sección segunda: La videovigilancia como respuesta rápida dentro de la política “more of the same”	<i>21</i>
Sección tercera: Los antecedentes de los Sistemas de Videovigilancia	<i>28</i>
3.1 El terrorismo en Europa:.....	<i>28</i>
3.2 La inseguridad en América Latina:.....	<i>31</i>
Sección cuarta: Los enfoques de la videovigilancia pública	<i>44</i>
4.1 Por un uso consciente y responsable de la videovigilancia:.....	<i>44</i>
4.2 Por un uso delimitado acorde a la finalidad:.....	<i>48</i>
<i>CAPITULO 2: LA DICOTOMÍA QUE SE DESPLIEGA CON EL USO DE LA VIDEOVIGILANCIA: EL DERECHO A LA SEGURIDAD Y EL DERECHO A LA INTIMIDAD</i>	<i>52</i>
Sección primera: La videovigilancia una herramienta a favor de la Seguridad Pública	<i>54</i>
1.1 La connotación policial de los sistemas de videovigilancia:.....	<i>54</i>
1.2 Funciones de seguridad y orden público.....	<i>57</i>
1.3 Los aportes de los sistemas de videovigilancia en materia de seguridad.....	<i>60</i>

Sección segunda: La incidencia que tienen los Sistemas de Videovigilancia sobre los derechos de intimidad, propia imagen y la protección de datos personales	70
2.1 El derecho a la privacidad.....	70
2.2 Derecho a la propia imagen.....	81
2.3 Derecho a la protección de los datos personales.....	89
2.4 Afectaciones al derecho de protección de datos por malas prácticas en el funcionamiento de los CCTV. .	95
 <i>CAPÍTULO 3: ANÁLISIS NORMATIVO DE LA VIDEOVIGILANCIA EN EUROPA Y COSTA RICA</i>	<i>118</i>
 Sección primera: La videovigilancia en Europa, una respuesta en el Derecho Comparado	119
1.1 Los principios de la videovigilancia.....	119
1.2 Marco Normativo Europeo	127
1.3 Jurisprudencia y Casos en Europa	150
 Sección segunda: Análisis de la videovigilancia en Costa Rica.....	169
2.1 Sobre el Ministerio de Seguridad Pública (MSP)	170
2.2 Sobre la Municipalidad de San José	171
2.3 Sobre la Agencia de Protección de Datos de los Habitantes (Prodhab).....	174
2.4 Decreto 34 104-G-MSP: Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos.....	177
2.5 Sobre Jurisprudencia de la Sala Constitucional en materia de videovigilancia	197
2.6 Propuestas para el mejoramiento de la videovigilancia pública en Costa Rica.	200
 <i>CONCLUSIONES.</i>	<i>211</i>
 <i>BIBLIOGRAFÍA</i>	<i>216</i>

TABLA DE AVREVIATURAS.

CCTV: Circuito Cerrados de Televisión.

PRODHAB: Agencia de Protección de Datos de los Habitantes.

AEPD: Agencia Española de Protección de Datos.

MSP: Ministerio de Seguridad Pública.

OIJ: Organismo de Investigación Judicial.

ICO: Information Commissioner's Office

TEDH: Tribunal Europeo de Derechos Humanos

TJUE: Tribunales de Justicia de la Unión Europea

CEDH: Convenio Europeo de Derechos Humanos

TC: Tribunal Constitucional

RESUMEN

La presente investigación tiene su razón de ser en el reglamento No. 34104-G-MSP y sus reformas posteriores, denominado Reglamento Regulador de la Vigilancia de Calles, Avenidas, Carreteras y Caminos mediante Dispositivos Tecnológicos o Técnicos, emitido por el Ministerio de Seguridad Pública, en conjunto con el proyecto de cámaras de seguridad que opera la Municipalidad de San José en las zonas públicas de nuestra capital.

Ante los problemas de inseguridad que asedia a la población costarricense, las autoridades públicas, principalmente los cuerpos policiales adoptaron los sistemas de videovigilancia como una medida de seguridad, a la que se le atribuyen fines policiales y judiciales, específicamente: la prevención y persecución de la actividad delictiva.

En el año 2008 la municipalidad de San José, inició con la instalación de cámaras en zonas estratégicas de la capital, con la finalidad de fortalecer la seguridad. Iniciaron con sesenta cámaras y al día de hoy el proyecto cuenta con más de doscientas cámaras, la popularidad de estos sistemas se está extendiendo en nuestro territorio. Actualmente, existe un único reglamento que norma el tema de la videovigilancia en espacios públicos. El contenido del reglamento es escueto, deja algunos vacíos legales en materia de derechos protección de datos, y existen contrariedades en relación a lo que establece la norma y lo que se lleva a cabo en la práctica u operación de los sistemas. Además, no se ha analizado la efectividad real de estos sistemas como medios preventivos ante la delincuencia. La deficiente regulación reglamentaria y los errores operativos prácticos que se cometen pueden eventualmente violentar los derechos de vida privada, imagen y protección de datos.

La presente investigación tiene como hipótesis que los sistemas de video vigilancia han surgido como una respuesta apresurada al problema de la inseguridad; no se ha analizado previamente, la efectividad de estos para la prevención y persecución del delito, o bien, determinar bajo qué condiciones resulta más efectivos acordes a su fin. La utilización desmedida y la falta de regulación legal de estos sistemas puede - eventualmente - generar afectaciones a

los derechos individuales de vida privada del ciudadano, he ahí la necesidad de adecuar la videovigilancia a un marco normativo que regule la convivencia de ambos intereses.

El objetivo general es analizar la contraposición de intereses que se despliega a partir del uso de los sistemas de video vigilancia por parte de la Administración Pública en los espacios públicos.

La metodología utilizada se llevará a cabo mediante el método deductivo y de análisis. Se desarrollarán formulaciones generales de la videovigilancia a nivel mundial para concluir en el caso específico de Costa Rica; se estudiarán cada uno de los elementos que comprenden la videovigilancia en espacios públicos; y finalmente se recurrirá al análisis interpretativo del Reglamento que norma la Videovigilancia pública en nuestro país, con la intención de determinar los vacíos legales y las contrariedades operativas/prácticas que suceden actualmente en el funcionamiento de las cámaras de seguridad.

Por último, en cuanto a la conclusión general se tiene la siguiente: la efectividad de los sistemas de vídeo-vigilancia para la prevención y persecución del delito depende de una serie de factores externos, como la presencia policial, la cantidad de las cámaras, la calidad de las imágenes, la accesibilidad del espacio, entre otros. Las autoridades policiales los han implementado como una herramienta tecnológica aislada, y por sí solos, los sistemas de videovigilancia no tienen la capacidad de prevenir el delito, ni de interrumpirlo. Los sistemas de vídeo-vigilancia han demostrado mejores resultados para la identificación de los sospechosos o la aclaración de los hechos.

Las autoridades policiales, bajo el argumento que los sistemas de videovigilancia son una medida de seguridad efectiva, han contribuido a la proliferación desmedida y poco planificada de los mismos en los espacios públicos; sumado a ello, la poca efectividad que tienen respecto a su fin y la carencia de una normativa robusta con garantías que velen por los derechos del ciudadano, los sistemas de videovigilancia se convierten en un mecanismo de control social y espacial por parte de las autoridades policiales.

FICHA BIBLIOGRÁFICA.

Madrigal Chacón, Ivannia. *El uso de los sistemas de Videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la protección de datos personales*. Tesis de Licenciatura en Derecho, Facultad de Derecho. Universidad de Costa Rica. San José, Costa Rica. 2019. ix y 238.

Director (a): Karla Blanco Rojas

Palabras claves: seguridad ciudadana, seguridad pública, orden público, circuitos cerrados de televisión, sistemas de videovigilancia, zonas bajo vigilancia, derecho a la vida privada, derecho a la imagen, derecho a la protección de datos personales, autodeterminación informativa, cuerpos policiales.

INTRODUCCIÓN.

Los sistemas de videovigilancia surgen en el marco de las políticas del derecho penal moderno que promueven nuevos modelos como la prevención situacional y la gestión de riesgos en los espacios públicos. Desde este punto de vista, los sistemas de videovigilancia son una herramienta tecnológica enfocada en la prevención, detección y persecución del delito. Estos sistemas se han popularizado a lo largo y ancho de las grandes y pequeñas ciudades, y su crecimiento ha sido vertiginoso, las calles, avenidas, parques, plazas, centros comerciales/empresariales, estaciones de trenes o buses, aeropuertos y un sinnúmero de lugares públicos y de convivencia, se han colmado de cámaras vigilantes destinadas a proporcionar seguridad a todo aquel que transita por ellos.

En el intento por disminuir o erradicar la delincuencia (“lucha contra la delincuencia”), los Estados han implementado políticas de seguridad más radicales y más represivas, lo que ha ocasionado que los alcances de control y vigilancia por parte de la policía se extendieran, a tal punto, que hemos empezado a ceder parte de nuestra libertad y privacidad, por obtener mayor seguridad. En la mayoría de los casos, el roce de derechos entre seguridad/control y privacidad/libertad surgen por dos motivos principales. Primero, la falta de una legislación que regule la actividad de videovigilancia pública que ocasiona entre otros problemas desorganización en las funciones y competencias institucionales, falta de asesoramiento y participación judicial en estos proyectos, incumplimiento de deberes del responsable del tratamiento y desconocimiento de derechos por parte de los ciudadanos. Segundo, el uso abusivo o desproporcionado de estos sistemas ocasiona afectaciones en la vida privada de los ciudadanos y vulnera, además la autodeterminación informativa y protección de datos personales, principalmente por las capacidades de cotejo, almacenamiento, reproducción y registro de datos.

En nuestro país, hace aproximadamente diez años, la municipalidad de San José inició un proyecto de fortalecimiento de seguridad, instalando cámaras en áreas claves de la capital. El proyecto inició con cuarenta cámaras, a hoy tiene 200 cámaras activas en funcionamiento y la Municipalidad planea incorporar aún más cámaras. La videovigilancia se regula en nuestro país vía reglamento, sin embargo, el documento deja aspectos importantes por fuera que más

adelante se mencionan y que deben reformularse para encaminar esta actividad policial dentro de un marco normativo que garantice los derechos constitucionales de los ciudadanos.

Hipótesis:

En Costa Rica, al igual que muchas ciudades del mundo, la utilización de éstos sistemas se ha expandido rápidamente bajo un fundamento de seguridad pública y ciudadana. La popularidad de éstos sistemas, en la doble función de prevención y persecución del delito, ha provocado la propagación desmedida de su uso. La utilización desmedida y la falta de regulación legal de éstos sistemas puede - eventualmente - generar afectaciones a los derechos individuales de vida privada. La utilización de la video vigilancia debe adecuarse a un marco normativo específico que regule la convivencia de ambos intereses. En nuestro país la normativa reglamentaria que existe es deficiente y se presenta lejana a una realidad que demanda constantes avances tecnológicos.

Objetivos General: Analizar las condiciones legales, prácticas, técnicas y organizativas bajo las cuales los sistemas de videovigilancia inciden sobre los derechos de vida privada, imagen y protección de datos.

Objetivos Específicos:

- a) Determinar los beneficios que aportan los sistemas de video vigilancia en el tema de la seguridad pública y ciudadana en los espacios públicos.
- b) Identificar los derechos constitucionales, concernientes a la vida privada del individuo, que pueden eventualmente verse afectados por la incorporación de sistemas de vigilancia en espacios públicos.
- c) Señalar los requerimientos legales que debe contemplar la Administración Pública para que el uso de los sistemas de video vigilancia este en armonía con ambos intereses, la seguridad pública y la garantía a los derechos individuales de vida privada.
- d) Demostrar que la potestad del Estado de ejercer la video vigilancia, es una facultad que se debe ejercer vía legislativa y no vía reglamentaria.

e) Recurrir a regulaciones prácticas de otros países como insumo para formular una solución al tema de legalidad de los sistemas de video vigilancia en Costa Rica respetando los derechos fundamentales.

Para dar contestación a la problemática de nuestro trabajo: ¿Cuáles son los retos jurídicos que enfrenta Costa Rica en materia de video vigilancia?, se recurrirá en el primer capítulo a contextualizar el fenómeno de la videovigilancia a nivel mundial. Se explica como surge en el contexto de las políticas criminales del derecho penal neoliberal, los antecedentes que los han promovido como medida de prevención situacional y el enfoque que deben tener en el marco de la protección de los datos personales de los ciudadanos.

En el segundo capítulo se analizan las dos perspectivas de la videovigilancia, quienes apoyan y fomentan la utilización de las cámaras como una medida administrativa que tiene aportes considerables en el tema de la seguridad pública y ciudadana; segundo, los detractores de los sistemas de videovigilancia que rechazan la efectividad de las cámaras para prevenir y perseguir el delito, lejos de ser un soporte para los cuerpos policiales, son una herramienta de control social y espacial, que vulneran los derechos a la vida privada, imagen y protección de datos personales.

En el tercer capítulo se analizará la jurisprudencia, normativa y doctrina en general de la Unión Europea, y particularmente el caso de España e Inglaterra, esto con la finalidad de determinar los criterios, principios, aplicaciones prácticas y legales que ellos han implementado para mejorar el funcionamiento de los sistemas de video vigilancia; comparativamente, se analizarán algunas críticas que presenta la videovigilancia en Costa Rica, desde el ámbito legal y práctico, utilizando el derecho comparado se puntualizarán las recomendaciones para que el funcionamiento de las cámaras de seguridad en los espacios públicos mejoren, afines con los derechos civiles del ciudadano.

La metodología utilizada se llevará a cabo mediante un método deductivo y analítico; pues desarrollará formulaciones generales para concluir en el caso específico de Costa Rica. En materia de derecho se tomarán en cuenta los siguientes aspectos: las cámaras de seguridad como

medida administrativa, que forma parte de las potestades de envergadura que mantiene el Estado en temas de seguridad pública y ciudadana, de orden público, bienestar colectivo (tanto personas como bienes materiales); en contraposición, las condiciones en que los sistemas de videovigilancia como medida administrativa lesionan los derechos civiles del ciudadano específicamente el derecho a la privacidad, de propia Imagen y derecho a la protección de los datos personales. El Estado a través de la legislación debe procurar un equilibrio entre ambos intereses. A partir de este método es posible comprender cada uno de los intereses puestos en juego: el interés público y el privado. Este método nos permite comprender los derechos puestos en juego y rescata el papel del Estado como promotor de la seguridad pública.

El derecho comparado es una referencia para el caso de Costa Rica. La doctrina internacional respecto al tema de la video vigilancia, así como jurisprudencia de los Tribunales Europeos de Derechos Humanos, son una guía referencial que enmarca la actividad de videovigilancia pública dentro de un marco garante de libertades civiles, se establecen límites legales y prácticos, se exige la aplicación de ciertos principios generales en la operación de los sistemas de video vigilancia, una referencia útil para el caso de nuestro país.

También se recurrirá al análisis interpretativo del Reglamento que regula la videovigilancia pública en nuestro país. La finalidad del análisis comparativo de Europa, (especialmente el caso español) y el análisis normativo de nuestro país, es identificar los vacíos legales y las contradicciones prácticas operativas de los sistemas de video vigilancia pública, eventualmente, como pueden lesionarse los derechos individuales del ciudadano. Una vez identificados los vacíos o contradicciones de la vigilancia establecer las mejoras que se deben aplicar en nuestro país. Este método se presenta como una corrección o solución del problema que enfrenta nuestro país en materia de video vigilancia, sobretodo la necesidad de someter tales sistemas a un marco jurídico legal.

En nuestro país la incorporación de cámaras con fines públicos y privados es cada vez mayor, es necesario una reforma legal que alinee el funcionamiento de las cámaras, acorde a los principios de la actividad y derechos civiles, se colmen los vacíos e incumplimientos legales que existen, actualmente, y se reorganicen las funciones de cada institución. Además, las

instalaciones de las cámaras deben estar supeditadas a análisis previos que verifiquen la necesidad y viabilidad de las cámaras, así como estudios posteriores, que determinen la efectividad de la cámara para la prevención y persecución del delito.

La presencia de los CCTV en los espacios públicos y los derechos privados del ciudadano pueden convivir en armonía sin conflicto alguno. Para ello es necesario reorientar políticas de seguridad que han incentivado la proliferación de estos sistemas, complementar la legislación con garantías para el ciudadano y delegar a una institución que se encarguen de supervisar el adecuado uso de las cámaras implementando mejoras prácticas en la vídeo vigilancia.

CAPÍTULO 1: EL FENOMENO DE LA VIDEOVIGILANCIA

Este capítulo consta de cuatro secciones. En la primera sección se analizan los sistemas de videovigilancia a partir del contexto político criminal y el papel que desempeñan en las sociedades contemporáneas. Las cámaras de seguridad se posicionan como una herramienta tecnológica moderna de los cuerpos policiales, cuya finalidad principal es la prevención y persecución delictiva. Debido a que los sistemas de videovigilancia responde a un problema relativo a la seguridad, es importante estudiar los argumentos sociopolíticos que le han dado impulso a estos nuevos tipos de vigilancia policial. En la siguiente sección se contextualizan los sistemas de videovigilancia dentro de la política criminal neoliberal y el discurso político de seguridad pública que los promueve como una herramienta efectiva para combatir la delincuencia.

En la tercera sección se exponen las causas o antecedentes que motivaron la utilización de estos sistemas, así como la promoción que se le ha dado a este tipo de proyectos en los últimas dos décadas y que giran en torno a la instalación de cámaras con fines policiales y de seguridad. Finalmente, la cuarta sección sugiere dos enfoques que debe tener los sistemas de videovigilancia, referentes a la seguridad, que en primera instancia es el fin o el objetivo de estos sistemas y segundo que, a pesar de constituirse como una medida de seguridad de los cuerpos policiales, la misma debe estar encaminada al resguardo de los derechos de los ciudadanos, principalmente en la protección de los datos personales.

Sección primera: Política Criminal y Seguridad.

La seguridad es un concepto muy amplio del cual se derivan diferentes subtipos, sin embargo, el desarrollo se limitará a la seguridad pública y ciudadana; derechos que han tomado relevancia en las últimas tres décadas a causa de la problemática de la inseguridad. Aunque existe amplia bibliografía que pretende diferenciar los tipos de seguridad, en la actualidad la seguridad pública, ciudadana, urbana y nacional se utilizan como intercambiables y la seguridad como tal, se ha vinculado o circunscrito a la cuestión de criminalidad, tanto así que la política criminal ha sido sinónimo de la política de seguridad¹. El enfoque del derecho penal moderno, ha provocado cambios en los conceptos de seguridad, en los discursos políticos criminales y en las demandas de una sociedad civil, cada vez más exigente.

La inseguridad es un problema mundial que padecen todos los países, en menor o mayor escala y sus causas se asocian a factores diferentes. Por ejemplo, los problemas de seguridad-inseguridad que sufren los países europeos y Estados Unidos de América, se han vinculado principalmente al terrorismo, mientras que en Latinoamérica la inseguridad se asocia con el aumento de violencia, el crimen organizado, los delitos callejeros y los conflictos que se generan a raíz del narcotráfico.

No es un secreto para nadie que América Latina es una de las regiones más peligrosas y desiguales del mundo; lo confirman una serie de informes institucionales que arrojan datos preocupantes de problemas relacionados a los delitos, la violencia y el crimen organizado². Por ejemplo, un estudio llevado a cabo en la región Latinoamericana por el Banco Interamericano de Desarrollo (en adelante el BID), puso en manifiesto los costos económicos que tiene la violencia sobre los países y la limitante que constituye para el desarrollo del mismo:

“la violencia es en la actualidad –sin duda- la principal limitante para el desarrollo económico de América Latina, a lo cual puede añadirse- sin temor a equivocación- que también es una

¹ (Daroqui 2003, 1)

² (Betancourt y Bielefeldt Astete 2013, 92)

limitante para la democracia, porque corroe y deslegitima a las instituciones democráticas como, por ejemplo, el sistema judicial, la Policía y el Parlamento¹”.

Los datos lanzaron una conclusión: que entre mayor sea la tasa de homicidio, mayores son los coste económicos del país². Esto quiere decir que existe una relación intrínseca entre el debilitamiento de la seguridad y el desarrollo humano y económico de los países; la seguridad constituye uno de los múltiples factores (sociales, políticos y económicos) que intervienen en el desarrollo social de cada país³. Lo cierto es que en materia de seguridad los esfuerzos de la sociedad actual se han centrado en “soluciones a corto plazo” como la prevención delictiva y las políticas criminales/policiales represivas que, al fin y al cabo, no han podido disminuir los índices de criminalidad en la región (ver el informe del Programa de Desarrollo de la ONU con sede en Nueva York y el Informe Regional de Desarrollo Humano 2013-2014).

El reto de la seguridad requiere de propuestas asociadas no solo a la reducción del delito sino a las causas sociales que lo propensa tales como la desigualdad económica, la falta de oportunidades de las clases marginales, la falta de movilidad social, los cambios en la estructura familiar y las deficiencias en el sistema educacional y salud; desafortunadamente los Estados latinoamericanos no han tenido una visión ni voluntad política a largo plazo. Por el contrario, la corrupción, la impunidad y las crisis del sistema penitenciario son un reflejo de la poca capacidad gubernamental en materia de justicia criminal. Innegablemente la inseguridad impacta sobre el desarrollo humano en distintas dimensiones como la persona (calidad de vida), la cohesión social y las instituciones democráticas⁴. Los países con mayores desigualdades socioeconómicas tienden a ser más propensos en la concurrencia de delitos en relación a las

¹ (Carrion 2004, 112)

² Colombia y El Salvador son los países con las tasas de homicidios más altos de la región cuyo costo fue del 24,7% del PIB y 24, 9%, respectivamente. Mientras que Costa Rica y Chile tiene las tasas más bajas de homicidios son los países que más invierten en la seguridad social. Investigaciones del Banco Interamericano de Desarrollo (BID: 1990) señala que Latinoamérica tiene una tasa de homicidios más del doble del promedio mundial; la Organización Paramericana de la Salud (OPS: 1997) indica un crecimiento del 44% en la tasa de homicidios entre 1984 a 1994; (BID: 2001) señala que en América Latina por año hay 140 mil latinos asesinados, 54 familias son robadas por minuto. El Salvador, Guatemala y Colombia son unos de los países que tienen altas tasas de homicidios datos mencionados por (Carrión 2005)

³ (Saiz 2013)

⁴ (Midgley 1995)

sociedades que tienen una mejor distribución de la riqueza y que contribuyen a evitar la violencia¹.

Con el pasar de los años, las estructuras tradicionales que definían la desigualdad e inseguridad social sufrieron una ruptura y en su lugar empezaron a surgir procesos de individualización, fragmentación familiar y social, que afectaron a ciertos sectores que hasta ese momento se encontraban estables y seguras, entonces los problemas sociales que antes afectaban homogéneamente a un determinado sector de la sociedad (estratos bajos), ahora empezaban a afectar a otros sectores sin distinción de clase o status social. A esta “*democratización*” de males o desgracias sociales Ulrich Beck le llamo Sociedad de Riesgo.

Beck explica que la sociedad moderna está expuesta a un peligro inminente, y a un estado de riesgo, que lo define “*como el rasgo que caracteriza un peculiar estado intermedio entre la seguridad y la destrucción*”. Estos riesgos sociales, políticos, económicos, industriales o ambientales, son de índole global por lo que se escapan de las manos de las instituciones de control y protección local de la sociedad; estas amenazas que se generan en la sociedad moderna socavan los fundamentos de las ideas de seguridad de los ciudadanos y desde su perspectiva, el peligro es un actor socialmente construido que afecta la cultura y la política de la sociedad moderna.

El enfoque sociológico y económico que Beck introduce a lo que se le conoce hoy en día como la sociedad de riesgo es aplicable a la materia de justicia criminal. La globalización, los avances tecnológicos y el acceso a las telecomunicaciones potenciaron procesos de conocimiento y riesgo a una velocidad nunca antes vista. Para el tema que nos atañe, los sistemas de videovigilancia son un fenómeno que ha crecido a gran velocidad en la sociedad moderna y se han desempeñado como una herramienta policial en la modelación de riesgos y prevención situacional. Así mismo, la utilización de estos sistemas tecnológicos de vigilancia proyecta otro tipo de riesgos asociados al alcance de sus usos y las posibles afectaciones a los derechos civiles del ciudadano. A continuación, se contextualizan el entorno político criminal en el que surgen los sistemas de videovigilancia con fines públicos.

¹ (CEPAL 2012)

1.1 La entrada del neoliberalismo penal.

El problema de la inseguridad de nuestra región se encuentra ligado a las políticas neoliberales de la década de los noventa que promovieron procesos regresivos y que provocaron fuertes cambios en las *“estructuras económicas, políticas y sociales, que, sumadas a las sucesivas crisis económicas, recayeron en un acentuamiento de los procesos de segmentación y exclusión social, aumento de la pobreza y el desempleo, y un marcado incremento de las tasas de delitos¹”*. Con la entrada del neoliberalismo económico los problemas socioeconómicos de desigualdad social, pobreza, mala distribución de la riqueza, desempleo y exclusión social se agudizaron y fueron vinculados directamente a la delincuencia y criminalidad.

El Estado de Bienestar de los años setenta se replegó por un conjunto de postulados neoliberales centrados en promover la responsabilidad individual y la competitividad de los mercados (distribución de bienes y servicios). El Estado por su parte se abstuvo de intervenir en el ámbito económico lo que generó una desregulación económica y una distribución de la riqueza en pocas manos. Como resultado se acrecentaron la exclusión y la desigualdad social, esta marginación de los sectores más débiles o pobres se asoció a la criminalidad (delitos de pobreza) e incluso se reflejó en el plano urbanístico (zonas peligrosas o conflictivas como precarios). Los efectos del neoliberalismo económico repercutieron sobre el orden jurídico mundial lo que ocasionó una revolución en materia de justicia criminal.

Además de las consecuencias socioeconómicas que generó el modelo neoliberal, el sistema penal de los años setenta se enfrentó a un aumento en las tasas delictivas, a una percepción de fracaso de los programas de rehabilitación, una lentitud y elevado costo de los programas de prevención del delito, lo que motivaba a un cambio en el tratamiento del delito². Por su parte, la globalización y el impacto de la tecnología en la cotidianeidad de la sociedad

¹ (Beltrane 2011, 1-2)

² El Welfare State tenía un enfoque de resocialización del delincuente como medida para prevenir la comisión de futuros delitos. La penalidad neoliberal renuncia a las sanciones del “welfare” o constitucionalismo social principalmente por sus costes en una política social y un supuesto fracaso en la corrección del infractor. En su lugar las políticas “welfaristas” fueron sustituidas por políticas criminales altamente represivas dentro del discurso de la intolerancia.

provocaron un proceso de adaptación a las nuevas circunstancias (Domínguez Figueirido y Rodríguez Basanta 2003). Para esta década el welfare sufrió una ruptura y comenzaron a surgir políticas criminales enfocadas en seleccionar a los potenciales delincuentes para ser sancionados dentro de una sociedad moderna basada en el riesgo.

El neoliberalismo tuvo sus impactos sobre la política y la práctica penal¹, pues con el derecho penal moderno se abogó por la búsqueda de la eficacia al menor costo convirtiendo al derecho penal en la *“prima ratio”*. El enfoque de la penalidad actual se basó en la exclusión social más que en la reintegración con ello emergieron las prácticas de riesgo y *“las preferencias economicistas neoliberales por la prevención -frente a la cura- por la mejora de la eficiencia de costes y por la protección de la ciudadanía^{2”}*.

Los cambios en la política criminal promovieron medidas más represivas como el *“incremento en la producción y configuración de delitos, un endurecimiento progresivo y desproporcionado de las penas (...) medidas penológicas extremadamente severas y lejanas a cualquier idea de rehabilitación y reinserción social, así como un abandono irresponsable de las demás causas sociales que en conjunto configuran la solución o tratamiento del problema criminal^{3”}*. Con la expansión y el endurecimiento del sistema penal, el giro punitivo se centró en el uso creciente y extendido de la prisión, especialmente para los delitos callejeros bajo la premisa de que quitando al delincuente de las calles se neutraliza al individuo para que no continúe cometiendo delitos. También se implementan medidas de seguridad y mayor control por parte de los cuerpos policiales, la protección de ciudadano se presenta como “cliente” de la justicia o “víctimas” del delito y, finalmente la problematización gira entorno a la cuestión del delito y su castigo.

Otras de las influencias del neoliberalismo recayeron sobre la penalidad, principalmente a través de la modelación del riesgo, y en consecuencia se reconfiguran varios aspectos como *“la prevención del delito, la actividad policial, las prácticas de condenar y el contenido de las sanciones”* (O’Malley 2015). Dentro del discurso político, la inseguridad se presenta en un

¹ De Jeremy Bentham, Michel Foucault, Gary Becker, David Garland.

² (O’Malley 2015)

³ (González 2014)

grado de emergencia que requiere necesariamente, la intervención del Estado y la inversión de recursos destinados a prevenir y reprimir el delito.

Bajo la tesis neoliberal y con diferentes perspectivas algunos autores sostienen la capacidad causal de este modelo económico sobre la materia penal. Por ejemplo, Reichman (1986) introdujo la lógica del seguro al control del delito en varios postulados: primero, la gestión de categorías de comportamientos que se refiere a los factores y grupos de riesgo según el comportamiento delictivo, alegando que existen causas biográficas y sociales que motivan la conducta delictiva; segundo, la discriminación selectiva de los agresores; tercero, el control de las contingencias relacionadas a las víctimas, que consiste en minimizar las probabilidades de pérdidas ocasionadas por el delito, sea cambiando el comportamiento o el entorno físico¹. Bernard E. Harcourt (2007) propuso las políticas criminales actuariales que se caracterizan por *“haber renunciado a identificar las causas psicosociales de la delincuencia, a actuar sobre las mismas y rehabilitar al delincuente, orientándose hacia el mero control²”*. David Garland (2005) propuso la utilización de nuevos dispositivos de control del delito y la justicia penal y *“el papel de instituciones que se hacen cargo de un nuevo espacio de control: es el caso de la prevención y otro más amplio, la seguridad³”*.

Bajo esta línea de ideas, las funciones estatales sufren una transformación fundamentalmente en los cambios del diseño, promoción y planificación de las políticas públicas, es decir, en las políticas de control del delito.

“Debemos pensar el concepto de prevención como elemento que funciona e influye en la producción social del delito. La prevención supone el encauzamiento de conductas (posiblemente) delictivas para el control social del delito y busca la no ocurrencia de estos últimos. De este modo, el modelo basado en la prevención actuará y desplegará determinadas estrategias que tendrán su eje en el tratamiento de ciertos tipos de delitos como hurtos, delitos contra la propiedad, violencia callejera, entre otros; es decir, los delitos que -actualmente- son considerados como la nueva delincuencia y causa principal de la inseguridad social” (Beltrane 2011, 2).

¹ (Reichman 1986)

² (Domínguez Figueirido y Rodríguez Basanta 2003, 3)

³ (Jiménez n.d., 2)

Con las nuevas estrategias de control y gestión de los espacios públicos, el riesgo y la peligrosidad se trasladaron a determinadas zonas y grupos específicos, por habitar en ellos potenciales ofensores, prácticamente una propuesta que instauró la “governabilidad de la nueva cuestión social” trayendo consigo un proceso de exclusión y desafiliación, como lo llamó Castel¹. La idea de la prevención se enfocó en ejercer control sobre aquellas personas o lugares que son potencial o posiblemente “peligrosos”²; el control por parte de las autoridades de seguridad es disuadir las conductas delictivas. La “Nueva Prevención”, como le llama Beltrane, plantea nuevas técnicas de intervención que se propone la no comisión de los delitos, es decir, *“apuntan al encauzamiento de conductas (posiblemente) delictivas para el control social del delito”* (Beltrane 2011, 5).

Las políticas criminales neoliberales de los Estados se enfocaron en revitalizar las medidas de seguridad y control en nuestra sociedad, bajo el argumento justificativo de brindarle protección a la ciudadanía en general, de los delincuentes considerados “peligrosos”³. El problema “seguridad-inseguridad” se plantea en términos de defensa social.

“Esta defensa social asume principalmente dos carriles: por un lado aumento y consolidación del sistema penal conforme a su capacidad represiva, y por otro incorporación de estrategias vinculadas a la prevención del delito, ya no en cuanto a la reacción penal posterior a la infracción (prevención especial y prevención general) sino en formas de la prevención anteriores a la infracción, por lo tanto no penales” (Daroqui 2003, 2).

En palabras de Rangugni *“se asiste una exacerbación de la violencia del sistema penal que, con nuevos fundamentos de intervención, redefine los nuevos “blancos” de represión*

¹ (Castel 1997)

² En palabras de Hener y Niszt el “encasillamiento” ya no se genera sobre individuos asilados sino de sectores enteros de población. Estos son enunciados por los medios de comunicación como “potenciales delincuentes” y acusados de poner en riesgo al resto de la sociedad. Se consolida, de esta manera, la imagen de una nueva delincuencia provocada y caracterizada mayormente por jóvenes de barrios marginales. Estos son enunciados como grupos de riesgo, suponiendo “la construcción de sujetos portadores de esta definición y que, una vez identificados, constituyen una amenaza para otros segmentos de la población”.

³ (Sernaqué y Alfonso, Control social, neoliberalismo y derecho penal 2002)

penal, complementados por una nueva gestión preventiva del delito¹". El nuevo modelo propició una reforma del gobierno para lograr una mejor eficacia, frente a las grandes amenazas que sufre la sociedad y el Estado, como el terrorismo, el crimen organizado, el narcotráfico, etc. Entre los cambios se pueden mencionar la creación de leyes que tipifican nuevas conductas criminales e imponen sanciones más severas a los delincuentes; así mismo, la implementación de medidas destinadas a fortalecer las instituciones y actividades públicas encargadas de combatir la actividad delictiva, como por ejemplo: la inversión de recursos en infraestructura y equipamiento de los cuerpos policiales; la utilización de tecnología para prevenir, perseguir, localizar y desarticular al crimen organizado, el narcotráfico, entre otros. Este Estado fuerte *"supone el cambio cualitativo en el concepto de la justicia y en el recorte de los derechos fundamentales e individuales, privilegiando la defensa del Estado como guardián de la seguridad ciudadana, en detrimento de los individuos. O sea, consolidando la ley y el orden²"*.

En la defensa de la seguridad ciudadana y la seguridad del Estado, se adoptaron medidas de control que, de una u otra manera, afectan al día de hoy, las libertades ciudadanas ¿En qué sentido? Primeramente, con los avances tecnológicos, las medidas tienden a ser más incisivas; segundo, que el control social y espacial que ejerce el Estado es sobre una expectativa de delito, un control justificado en una posibilidad.

En Estados Unidos de América y algunos países de Europa, el control por parte del Estado surgió a causa de los atentados terroristas, y como respuesta ante las amenazas de la seguridad nacional: *"Si bien el 11 de setiembre de 2001 constituye- y constituirá- una fecha clave en lo que se refiere, entre otras cosas, la redefinición de los conflictos intersubjetivos, es claro que uno de los impactos más importantes fue el maximizar la figura del Estado/Leviatán como centro neurálgico del poder, aumentando sus capacidades de perseguir, reprimir y, eventualmente, punir ideologías, personalidades, razas, aludiendo a un claro derecho penal de autor. De esta forma el derecho penal se transforma en la prima ratio, olvidando el carácter subsidiario y de última ratio que le asignan los postulados garantistas³"*.

¹ (Rangugni 2009)

² (Sernaqué y Alfonso, El neoliberalismo y el derecho penal en las sociedades democráticas 1997)

³ (Riquert 2010, 159)

En América Latina, el control por parte de las autoridades estatales surgió debido al aumento de la delincuencia, la violencia y las exigencias de una sociedad poco tolerante, esto *“entrañó una respuesta del Estado que, a través de la aplicación de ciertas políticas de seguridad, propició una sobrevulneración de los derechos de los sectores perjudicados y vulnerables de nuestra sociedad”* (Beltrane 2011, 2).

Teniendo como justificación los antecedentes antes mencionados, los gobiernos optaron por cambiar las políticas de seguridad, cuya tendencia fue aumentar el intervencionismo estatal punitivo: *“El delito y el problema de la inseguridad que a éste se suele asociar, se han posicionado en las últimas décadas como una cuestión estratégica fundamental para las gestiones de gobierno. Como consecuencia, las políticas de seguridad se han centrado en una intensificación de los mecanismos de control social dirigidos a la prevención del delito y una mayor intervención del Estado en los espacios públicos¹”*.

Los modelos de tratamiento del delito reactivo –punitivo dejan de postularse y en su lugar se articuló el nuevo modelo preventivo del delito, cuyo planteamiento se cimenta en la utilización de recursos extrapenales con dos tipos de estrategias de intervención: *“a) la estrategia situacional, la cual “está basada en intervenciones específicas que se dirigen sobre todo a las víctimas potenciales, a la seguridad de los edificios y al ambiente; b) la estrategia social o comunitaria que trata, en lugar de esto, de modificar con programas generales las condiciones de vida en ambientes determinados, por ejemplo un barrio, de manera que se aumenten las oportunidades de comportamientos conformes a la ley y se disminuyan los comportamientos ilegales”* (Beltrane 2011, 5).

1.2 La participación ciudadana en materia de seguridad.

Este panorama de seguridad-inseguridad se convierte en un problema de todos, tanto para el Estado como para los ciudadanos, tomando relevancia el concepto de seguridad y participación ciudadana. A diferencia de la seguridad ciudadana, la seguridad pública es una

¹ (Lío, Cámaras de seguridad y prevención del delito. La utilización de la videovigilancia en la ciudad de Buenos Aires 2015)

función reservada estrictamente al Estado que le es concedida por la Constitución Política; a través de una estructura y organización. El Estado ostenta la participación y el poder para mantener el orden público nacional y en consecuencia tiene un enfoque represivo en la comisión de los delitos¹.

Uno de los elementos importantes de la seguridad ciudadana, es que la comunidad o vecindario además de convertirse en el objeto de las intervenciones también es actor. En el plano de la prevención del delito, los ciudadanos participan para reconstruir el control social del territorio donde habitan, sin embargo, Pavarini advierte que en esa defensa comunitaria se puede caer en conductas socialmente represivas, como el aislamiento del enemigo, marginación y exclusión social de ciertas minorías en determinados espacios o la privatización de los espacios públicos (Massimo Pavarini le llama la criminología del otro).

Para el autor la inseguridad se convierte en una limitante para el ciudadano en el sentido de que éste cambia su estilo de vida, los ciudadanos (víctimas) modifican sus comportamientos diarios y su libertad personal es socavada ante esta problemática². Para Pavarini los gobiernos locales del bien público seguridad, deben implementar medidas administrativas de tipo reactivo o proactivo que estén enfocadas en incidir en los niveles de riesgo o las condiciones que le preceden, evitando que dicha intervención pase al plano represivo estatal³.

¹ La seguridad pública es la garantía que debe brindar el Estado para el libre ejercicio de los derechos de todos los ciudadanos. El Estado a través su organización gubernamental y subsistemas policial, judicial y administrativo provee la seguridad pública, que se refiere precisamente a la protección del ciudadano.

(Sozzo 2009)²

³ Desde el punto de vista personal, la seguridad pública constituye una imposición para el Estado y un derecho para todos los ciudadanos. Sin embargo, considero que el derecho a la seguridad ciudadana y el derecho comunitario son atribuciones parcialmente disfrutadas por la ciudadanía, en el sentido, de que su ejercicio pleno no está al alcance de todas las comunidades. El ejercicio de este derecho esta relegado a factores socioeconómicos y urbanísticos de las distintas clases sociales. Por ejemplo, las comunidades o vecindarios de clase media alta, cuentan con condiciones favorables para organizarse (empresa de seguridad privada, alarmas o uso de tecnología) y pueden llevar a cabo su participación dentro de la sociedad en políticas preventivas contra la delincuencia. Mientras que los ciudadanos que viven en sectores marginados o conflictivos están se les imposibilita el ejercicio pleno de este derecho y se les tacha de potenciales delincuentes (zonas rodeadas de bunkers para consumo y venta de droga, asaltos, guerra entre pandillas relacionadas al narcotráfico, etc).

“La seguridad ciudadana no es sinónimo de seguridad pública, aunque en la práctica se le confunda conscientemente, al extremo de buscar neoenemigos (pandillas, narcotráfico, tratas), construir lógicas de combate (estigmas, guerras, ausencia del derecho del ofensor) y producir un discurso ambivalente ante la población... Mientras la seguridad pública busca la defensa del orden público estatal frente a un enemigo interno (amenaza) y tiene un marco institucional nacional con características represivas (policía, justicia y cárcel), la seguridad ciudadana se refiere a la necesidad de mantener y potenciar las relaciones interpersonales en el marco de la ley y la cultura, expresadas en el respeto al derecho ajeno bajo la norma, para lo cual tiene presencia un conjunto de instituciones públicas (municipio, justicia, cárcel) y sociales (universidades, medios de comunicación, defensores de derecho humanos). Allí radica la condición ciudadana de la seguridad: los derechos y los deberes individuales y colectivos de la población en el marco de un Estado que debe garantizarlos”¹.

Ante la problemática de seguridad, se convoca al ciudadano a participar como agente activo de la seguridad y su participación en el orden público lo faculta a eliminar las amenazas de violencia contra la población, facilitando la convivencia segura. El ciudadano se convierte en protector de la organización social a la que pertenece, respetuoso del “derecho ajeno”. El derecho ajeno es un reconocimiento que se le hace a la otra persona de sus derechos y libertad personal, lo que busca es dar seguridad a todos los ciudadanos en el ejercicio (público o privado) de sus derechos y deberes² (Carrión 2005, 32).

Un ejemplo de la participación ciudadana son las comunidades organizadas con comités de vigilancia, contrataciones de servicios de seguridad privada, seguridad electrónica, entre otros. Aunque la seguridad ciudadana permite la participación del ciudadano, la gestión y provisión de la seguridad recae predominantemente en el poder del sector público. La seguridad ciudadana envuelve en el plano político-social la seguridad de todos, y trasciende como concepto jurídico como un derecho cuyo eje central es la ciudadanía y una obligación estatal garantizarla³.

¹ (Carrión, Hacia una nueva comprensión de la violencia y la seguridad 2011)

² La seguridad pública tiene una connotación estado-céntrica y represiva, porque ante la comisión de un delito lo que busca es la restauración del daño causado y el castigo al culpable.

³ (Serbín, Sojo y Salomón 2001)

1.3 La predominancia de los elementos subjetivos en materia de seguridad.

A raíz de la nueva participación ciudadana, la dimensión subjetiva de la seguridad adquiere mayor relevancia¹. Los indicativos objetivos o delincuencia real que predominan con mayor fuerza dejan su popularidad y en la década de los ochenta se incorporan la opinión-percepción ciudadana como un indicativo más de medición del problema de la seguridad y se empieza a abordar los análisis de victimización y percepción ciudadana a través del uso de encuestas de opinión general con el objetivo de medir la extensión de la delincuencia².

“Las encuestas de victimización confieren centralidad a la víctima porque se basan precisamente en la información que ésta proporciona. Basándose en una muestra representativa de la población, informan del porcentaje de personas que dicen haber sido víctimas de algún hecho que consideran delictivo. Esto supone que son los propios entrevistados los que deciden cuánta delincuencia hay, al margen de lo que pueden constatar las estadísticas policiales y/o judiciales” (Murriá y González, La seguridad ciudadana: instrumentos de análisis 2010, 7).

Se sabe que la seguridad ciudadana en un reflejo, en parte, de las condiciones socioeconómicas de un país; el desempleo, la pobreza y la falta de recursos sociales, económicos y culturales son algunos aspectos que inciden en el nivel de seguridad del país, e influyen en la percepción ciudadana. La inseguridad se compone del riesgo percibido: *“la inseguridad (o riesgo percibido) es el resultado de una percepción o valoración del peligro de ser víctima de un delito. Es la probabilidad subjetiva de victimización³”*. Además de estar relacionada con las condiciones de vida que rodean al sujeto, es consecuencia de la percepción objetiva o del riesgo real, es decir, de la victimización real o la probabilidad de ser víctima de la delincuencia. La percepción ciudadana se ha convertido es un factor indicativo de la inseguridad e incluso se ha posición como prioridad en relación a otro tipo de problemas sociales que sufre nuestra sociedad como el desempleo, la pobreza o la corrupción.

¹ (Murriá y González, La seguridad ciudadana: instrumentos de análisis 2010, 1)

² Las encuestas de victimización ofrecen datos de cantidad de delitos que han sufrido, descripción de los episodios delictivos y las características de las víctimas.

³ (Thomé 2004, 280)

“Para el año de 1995 la percepción ciudadana era de un 5%, creciendo constantemente hasta un 27% en el año 2010, desde el 2008 en la región es considerado el principal problema por superar, y en 2010 en 12 de los 18 países encuestados, los ciudadanos lo señalaron como tal. Ante la problemática de inseguridad nace un temor entre los ciudadanos de sentirse inseguro y atemorizados de ser víctimas de la delincuencia. En el caso de América Latina la percepción de inseguridad de los ciudadanos oscila entre el 30% al 43%, lo que resulta bastante alta en comparación con otras regiones” (Arias, Rosada Granados y Sain 2012, 12)

Desde el punto de vista subjetivo, los resultados de estudio relevan que la inseguridad se ha convertido en un grave problema social en aumento, especialmente para la región latinoamericana, convirtiéndose en una de las prioridades de los gobernantes.

Aunque la percepción subjetiva se cualifica y cuantifica en estadísticas, el malestar del ciudadano o la “sensación de inseguridad” no corresponden necesariamente *“con el riesgo real de victimización al que se encuentra expuesto, sino que a menudo responde a un miedo difuso que depende de múltiples factores que forman un esquema explicativo complejo (sociales, económicos, territoriales, individuales, etc)”* (Murriá y González, La seguridad ciudadana: instrumentos de análisis 2010, 1).

Los medios de masa por su parte dan una amplia cobertura a los sucesos delictivos: asaltos, secuestros, robos, homicidios, tráfico y venta de drogas, violencia callejera, actos de vandalismo, entre otros; transmitiendo una percepción de peligrosidad al ciudadano, quien vive atemorizado por la inseguridad que lo rodea. Al dimensionar la realidad con violencia mediática fomentan el “miedo del otro”, y en muchas ocasiones son los responsables de regular la repartición de papeles de la víctima y del agresor, y de provocar la “demarcación social” de ciertos individuos (Daroqui 2003, 3). Finalmente, el ciudadano es el receptor de todos los discursos (cero tolerancias, mano dura, más cárcel, aumento de la violencia e inseguridad, etc.) e interioriza estas opciones como “verdaderas soluciones” al problema de la inseguridad.

Con la nueva concepción del delito y el nuevo modelo de prevención, el sistema penal visualizó nuevos objetos de intervención social, principalmente enfocado en aquellas conductas

que perjudican el orden social como las “incivildades”¹ o “ilegalismos” de aquellos grupos de riesgo que ponen en peligro la calidad de vida del resto de ciudadanos. Además, con la participación ciudadana se convoca al ciudadano, a gestionar la seguridad de los barrios y las comunidades de actos delictivos y de aquellos individuos o grupos que pueden, eventualmente, poner en “riesgo” a la ciudadanía (Daroqui 2003).

En este nuevo tratamiento del delito orientado a la prevención, otros tipos de conductas (incivildades) se consideraron transgresoras del orden público o la “calidad de vida” de los ciudadanos como los ruidos molestos, los jóvenes tomando alcohol en la vía pública, la venta de drogas en las calles, etc., todas ellas aumentan la “sensación de inseguridad” de los ciudadanos (Beltrane 2011, 8).

De la misma manera que la criminalidad se ligó a las clases marginales, la inseguridad se asoció al espacio geográfico. Las llamadas “zonas calientes” o “zonas rojas”, se conceptuaron como lugares de riesgo o peligrosos, donde es común la delincuencia y habitan en ellos, delincuentes o potenciales ofensores². El delito empieza a ser entendido exclusivamente en relación a la criminalidad de la calle y las políticas de seguridad se orientaron a objetivos de control y gestión del conflicto social. “El concepto de control aquí es clave, pues es el eje que atraviesa las nuevas prácticas de prevención del delito que buscan no una homogeneización de las conductas y supresión de las desviaciones, sino una nueva gestión de los riesgos y conflictos sociales”³.

¹ (Baratta 1996)

² Para Gabriel Kessler (2007) los grupos sociales poderosos empezaron a ejercer presión exigiendo mayor seguridad y presencia policial en los barrios mejor posicionados, esto fomentó un desplazamiento de la delincuencia y procesos de estigmatización, desigual social, exclusión y fragmentación social.

³ (Antillano 2007)

Sección segunda: La videovigilancia como respuesta rápida dentro de la política “more of the same”

En los últimos veinte, la lucha contra la delincuencia se ha tornado en un tema de interés para todos los que la sufrimos, que de una u otra manera contextualizamos como un problema de nunca acabar, y que ha criterio de los ciudadanos va de mal en peor. La respuesta estatal ante el fenómeno delincriminal ha sido neutralizar a toda costa la peligrosidad emergente de los focos criminógenos. Las políticas de “mano dura” y “cero tolerancias” han incidido en el tratamiento del delito, el cual se ha centrado en medidas rápidas como el encarcelamiento y medidas orientadas a aumentar el intervencionismo estatal bajo el argumento de salvaguardar el orden público. De la mano de la importación de modelos ideológicos que proponen la implementación de programas públicos destinados a proveer seguridad surge la instauración de una era tecnológica destinada a concretar tales ideas¹.

Las cámaras de seguridad en espacios públicos, forman parte de los cambios en las políticas neoliberales de seguridad y criminalidad que tomaron los Gobiernos, medidas tendientes a la prevención y persecución penal, el control policial de los espacios y las personas, y la participación ciudadana en temas relacionados a la seguridad².

Las presiones sociales ante la crisis de la seguridad pública (aumento en la inseguridad, violencia y después de los atentados terroristas) y el incremento del mercado de la seguridad, proliferaron el uso de los sistemas de videovigilancia en las últimas dos décadas, incorporándose principalmente en los espacios públicos de las ciudades así como en los espacios privados³. Principalmente los Gobiernos promovieron la masificación de estos sistemas en los programas públicos presentando los CCTV como una solución a corto plazo, de resultado insustancial pero inmediato.

¹ (Zolezzi y Valenzuela Herrera 2017)

² Para Ramírez Zolezzi y Valenzuela Herrera la videovigilancia como práctica gubernamental está íntimamente ligada con cambios en la estructura política y social, los cuales ocurren de forma más o menos pronunciada y favorecen la adopción de ciertos programas públicos sobre otros.

³ (Sánchez 2010)

La respuesta estatal se concentró principalmente en la prevención del delito y el modelo se centró en tres aspectos generales: “1. *Focalizar la atención en las faltas y contravenciones que afectan la calidad de vida (incivildades); 2. Trabajar en las comunidades –no con ellas– para la reducción de estas faltas; 3. Evaluar los riesgos y, sobretudo, las poblaciones que constituyen un riesgo para la seguridad – que en la práctica son los sectores marginados, de determinado origen y color*”¹.

Este nuevo enfoque del delito basado en la prevención se torna más represivo porque se empieza a ejercer un control de los espacios y las personas, basados en la peligrosidad y potencialidad del riesgo². Es decir que, sin cometer ninguna acción delictiva, se comienza a vigilar ciertos grupos de personas que por sus condiciones físicas o socioeconómicas son consideradas potenciales delincuentes o de riesgo.

En la prevención del delito resaltan dos nuevos modelos aplicables a la incorporación de los CCTV, el modelo de enfoque situacional y el de seguridad ciudadana. El primero de ellos defiende la intervención dirigida a “*neutralizar aquellas situaciones de riesgo que ofrecen un mayor atractivo al infractor, de manera que, teniendo en cuenta las hipotéticas ventajas de cometer el delito y las dificultades que encuentra para su comisión, el sujeto considere que no es razonable o utilitario intentarlo*”³.

Bajo esta nueva modalidad los sistemas de videovigilancia surgen como una medida de seguridad orientada al control de los espacios (geo-prevención). Los cuerpos policiales las incorporan con dos finalidades específicas: la prevención y la persecución de la actividad delictiva. Debido a su capacidad de reproducir y grabar hechos, se sostiene que con la presencia de las cámaras el delincuente desistirá de cometerlos y, en consecuencia, los niveles de delincuencia disminuirán. Desde esta perspectiva los cuerpos de seguridad pueden “ventanear”

¹ (Pueblos 2018, 2-3)

² En palabras de Carles Soto Urpina, la prevención ambiental busca cambiar las características específicas del entorno que pueden causar los hechos delictivos. Incluye la prevención situacional y las iniciativas de planificación cuyo objetivo es reducir la delincuencia mediante el diseño y/o modificar el entorno físico para reducir las oportunidades que produzca el delito. La prevención social del delito se dirige a tratar las causas sociales y económicas que subyacen la delincuencia, así como la motivación.

³ (Urpina 2015, 31)

por medio del ojo electrónico al delincuente callejero, el que comete incivismo, al transgresor de las leyes de tránsito, al carterista, en fin, la delincuencia *in fraganti*.

El modelo de seguridad ciudadana se “*caracteriza por la titularidad privada de su gestión y con una intolerable dejación de funciones de los poderes públicos*” (Urpina 2015). La distorsión en la percepción de inseguridad (incertidumbre y pánico) y la desconfianza ante la gestión policial motivó a los ciudadanos a proteger sus intereses particulares y exigir a las autoridades estatales el despliegue de medidas que garanticen su seguridad. De esta manera, la ciudadanía también se sumó a la instalación de cámaras con fines privados en sus casas, barrios organizados, condominios, centros comerciales, ciudades corporativas, entre otros. Una de las críticas que señala Soto Urpina es que la crisis de la seguridad pública fue sustituida por la seguridad privada, esta seguridad no tiene por objeto estar al servicio del ciudadano sino al servicio del contratante, es decir, de quién lo puede pagar. Esto quiere decir, que las personas menos pudientes quedan por fuera de su protección.

Los Gobiernos han insistido en promover políticas criminales enfocadas en neutralizar la delincuencia y la violencia, medidas instantáneas de corto plazo que no solucionan el problema del delito. El tratamiento del delito lo componen una serie de factores complejos que responden a las profundas deficiencias de la estructura social (distribución de la riqueza, aumento de la pobreza, desempleo, etc.) y se materializa en desigualdades económicas e inequidades sociales y espaciales (Zolezzi y Valenzuela Herrera 2017), a sabiendas de la complejidad que conlleva soluciones efectivas al delito, las autoridades sostienen que la ciudadanía no puede esperar los efectos de las medidas a largo plazo, y que es indispensable enfrentar los constantes ataque de la delincuencia. “*El discurso es uniforme en este sentido: la delincuencia y la violencia responden a causas profundas que no pueden ser enfrentadas de forma instantánea pero la ciudadanía merece protección inmediata. En dicho contexto, los organismos públicos implementan medidas de corto aliento y de notoria publicidad. La visibilidad de la medida se torna más relevante que la eficacia de ella, así las autoridades proyectan una permanente preocupación por la criminalidad e inseguridad pública¹*”

¹ (Calzado, Fernández y Lío 2012)

Este rol protagónico del delito dentro del discurso político, es lo que Simón ha denominado “gobernar a través del delito”, el autor sostiene que el conjunto de discursos, acciones y políticas no están destinadas a controlar el fenómeno delictual sino a gobernar el delito¹, lo que implica que la centralidad política que ocupa el fenómeno no tiene correlato en las acciones desplegadas por el Estado. *“El denominado gobierno a través del delito es un fenómeno complejo que se caracteriza por tres cuestiones. En primer término, el delito ocupa regularmente una posición estratégica en el debate político. Luego, las acciones políticas se legitiman recurrentemente como intervenciones “contra el delito”. y en tercer lugar, el discurso de la seguridad ciudadana toma relevancia al interior de diversas instituciones políticas y sociales. Es en este sentido que la criminalidad e inseguridad pública proporcionan nuevas alternativas de gobernanza asociadas al discurso de la seguridad ciudadana”* (Zolezzi y Valenzuela Herrera 2017, 54-55)

Los sistemas de videovigilancia ubicados en espacios públicos encuadran dentro de este conjunto de políticas promovidas por los Gobiernos y presentados como instrumentos eficaces y efectivos en la reducción, prevención y persecución del delito. Las instituciones gubernamentales que ejercen labores de vigilancia, control y cuidado, afirman que los CCTV son una herramienta capaz de proveer seguridad pública en distintos aspectos: disminuyen la inseguridad subjetiva, aumentan la inteligencia policial, facilitan la persecución penal y permiten la reacción temprana ante emergencias de diversa naturaleza².

Quienes promueven el uso de estos sistemas utilizan un discurso retórico de eficacia, afirmando los beneficios de estos sistemas para combatir la delincuencia, *per se* a no contar con estudios exploratorios que corroboren los efectos de los CCTV sobre la criminalidad y la sensación de inseguridad de los ciudadanos. Para Vozmediano, Vergara y San Juan es preocupante que los programas estatales destinados a controlar los fenómenos de la delincuencia y la sensación de inseguridad no estén enfocados en alterar las condiciones que los promueven,

¹ (Simón 2011)

² (Carrión Mena 2008)

y en cambio los esfuerzos públicos se centren en medidas de dudosa eficacia y elevada notoriedad¹.

Pese a la falta de claridad en los objetivos de estos sistemas, la falta de idoneidad y la incertidumbre que los envuelve por la falta de pruebas y estudios que demuestren sus efectos o beneficios, la ciudadanía se mantiene inerte y la medida pareciera auto legitimarse con su mera aplicación². *“Las alternativas de gobernanza que proporciona los riesgos, la criminalidad y la inseguridad pública se asocian al relato de la seguridad ciudadana. En dicho contexto las medidas de dudosa eficacia como la vigilancia se aceptan pacíficamente por la ciudadanía, como si fueran medidas concretas para controlar la actividad delictual”* (Zolezzi y Valenzuela Herrera 2017, 57)

La videovigilancia ha tenido un apoyo considerable por parte de las municipalidades, los organismos de seguridad estatales, organizaciones dedicadas a la seguridad ciudadana, las empresas de seguridad privada e incluso los mismos ciudadanos, lo cierto es que se debe analizar acertadamente esta práctica, vislumbrando los efectos que tienen sobre los objetivos que declaran quienes promueven su uso mediante nuevas perspectivas de investigación. Gemma Galdon haciendo referencias al Reino Unido señala que: *“tras años de seguir a rajatabla las doctrinas de ventanas rotas y de monitorizar y reglamentar los comportamientos en el espacio público, tanto el incivismo como la sensación de inseguridad no ha ni siquiera disminuido (...) la mayor parte de las sanciones no llegan a cobrarse y los comportamientos que se pretenden censurar persisten (o empeoran, según algunas voces). Desde el punto de vista de la eficiencia y eficacia de las políticas públicas, es evidente que algo está fallando. Sin embargo, a día de hoy la única propuesta en firme que ha salido del consistorio de la ciudad condal es la petición de instalar más cámaras de videovigilancia en el barrio del Raval, con el fin de atajar la inseguridad, la prostitución y los comportamientos incívicos³”*

Para los gobiernos ha sido irrelevante averiguar los efectos de las cámaras en la disminución de la criminalidad, pero si le han dado importancia suficiente a la visibilidad y

¹ (Sáenz, Vergara Iraeta y San Juan Guillén 2010)

² (Santiago 2010)

³ (Clavell 2009)

publicidad dentro de la “lucha contra la delincuencia” de tal manera que han apaciguado las presiones ciudadanas en este aspecto. En este marco, los sistemas de videovigilancia ya no tendrían por objeto controlar el fenómeno del delito y la inseguridad pública, sino que dentro del modelo neoliberal la violencia, el delito y los riesgos se posicionan como núcleo de la actividad política.

La publicidad que se le da a este tipo de proyectos tiene más transcendencia en el ámbito político que en de la eficacia. El problema de la delincuencia y la inseguridad se ha convertido en un tema relevante a la hora de las elecciones para obtener votos y los representantes políticos ofrecen este tipo de medidas como soluciones al problema sin considerar la idoneidad de la medida en el tema de seguridad.

Sería gratificante ver la acreditación de este discurso en el plano real. Comprendería que las instituciones que emprenden estos proyectos tengan el interés de verificar si efectivamente contribuyen en disminuir el índice de criminalidad o la percepción de inseguridad, mediante estudios que cuantifiquen y cualifiquen el fenómeno delictivo en las áreas bajo vigilancia; también se debe darle continuidad y seguimiento a las condiciones técnicas, organizativas o ambientales bajo las cuales resulta más efectivo el funcionamiento de estos sistemas y determinar la relación costo/beneficio en la adquisición de estos sistemas, debido a que se pueden invertir millones de recursos públicos en una medida poco eficaz para combatir la delincuencia.

No se trata de instalar cámaras por doquier argumentando lo útiles y efectivas que son para contrarrestar la delincuencia, sino de demostrar la idoneidad de la medida para el fin que persiguen o por las que fueron creadas; de no ser así, los sistemas de videovigilancia se convierten en un instrumento de control social y espacial, como se verá más adelante.

La situación de la inseguridad pareciera que no llega a su fin, y que las soluciones que han propuesto las autoridades públicas y políticas han sido poco exitosas. Ante los reiterados fracasos de la seguridad pública, vale la pena reflexionar acerca del enfoque de la política criminal de los últimos treinta años y los motivos por los cuales ha tenido poca efectividad ante

la perpetua situación de inseguridad, que al parecer se ha vuelto insostenible para las autoridades y la ciudadanía en general. Insistir en medidas de corto alcance para combatir la inseguridad ha sido una mala decisión y más de lo mismo. Se debe repensar una política criminal más acertada y enfocada en mejorar las condiciones sociales, económicas y culturales asociadas al delito.

Sección tercera: Los antecedentes de los Sistemas de Videovigilancia.

El desarrollo de los sistemas de videovigilancia ha sido un proceso motivado por muchos factores, sin embargo podría decirse que la causa principal en la que se fundamenta el uso de los sistemas de videovigilancia es la seguridad de los espacios públicos¹. Las cámaras se presentan en el escenario de la seguridad, como un medio preventivo ante la delincuencia, cuyo propósito es disuadir las conductas delictivas, pues se afirma que el delincuente por temor a ser grabado, dejar rastro del delito o incluso ser identificado desiste de cometerlo.

3.1 El terrorismo en Europa:

En Europa y Estados Unidos los atentados terroristas de los últimos 16 años han sido el principal antecedente de la incorporación de los sistemas de video vigilancia en espacios públicos. En estos países, la defensa por la seguridad nacional recobró fuerza y surgió la necesidad de ejercer mayor control espacial y social, sobre aquellos individuos que representaban un peligro para el país², de ahí la iniciativa de invertir millones del presupuesto en crear redes tecnológicas que permitan controlar los espacios públicos³.

“Los acontecimientos terroristas ocurridos en 2001 en Estados Unidos, así como los atentados de marzo del 2004 y junio del 2005 ocurridos correspondientemente en Madrid y Londres, han justificado la utilización de estos sistemas surgiendo como una posible respuesta tecnológica frente a la demanda de seguridad. Desde entonces, la utilización de la tecnología no ha dejado de crecer y expandirse en los demás países europeos” (Calfa, Sebastian y Bourgeois 2010, 13).

En el caso específico de los Estados Unidos e Inglaterra las cámaras de videovigilancia han demostrado ser útiles instrumentos en materia de persecución del delito e identificación de personas involucradas en actos terroristas, *per se* a que los sistemas no previenen la eventualidad de estos sucesos. En el 2005. fue posible la identificación de 4 sujetos que participaron en el atentado terrorista de Londres, gracias a una de las setenta y seis cámaras instaladas en la

¹ (Calfa, Sebastian y Bourgeois 2010)

² El control social se enfoca en ciertos grupos minoritarios como los extranjeros, por ejemplo, los musulmanes en EEUU.

³ (Botello 2016, 194)

estación de King's Cross. Posteriormente en diciembre del 2010, un grupo de protestantes invadieron y tomaron posesión temporal de la sede del Partido Conservador, por medio de las cámaras de videovigilancia fue posible identificar y detener a ciento ochenta personas que participaron en la protesta¹.

Otro evento terrorista donde las cámaras de seguridad mostraron su importancia y eficacia fue la maratón de Boston ocurrida en Estados Unidos el 15 de abril de 2013 en el que logró identificarse a los hermanos Tsarnaev. Las cámaras de seguridad ubicadas en la calle Boylston situaron a ambos sospechosos en el lugar del atentado, además la notable nitidez de las imágenes obtenidas gracias a las cámaras de seguridad y su posterior difusión facilitaron la captura de ambos terroristas².

El caso más reciente fue el ocurrido el 14 de julio de 2016 en Niza, Francia, un camión atropelló a gran velocidad (noventa kilómetros por hora aproximadamente) y a lo largo de dos kilómetros en el Paseo de los Ingleses, a los grupos de turistas y ciudadanos que se encontraban en el boulevard. Resultaron ochenta y cuatro fallecidos y un centenar de heridos. El suceso se declaró como un atentado terrorista, pues el atacante era un francés de origen tunecino y *“la fecha elegida para el ataque era muy significativa: la fiesta nacional es una demostración de unidad en torno a las fuerzas armadas, implicadas en los frentes de Oriente Próximo y África para combatir a los yihadistas³”*.

Las imágenes obtenidas a través de las cámaras de seguridad desmintieron la versión del gobierno el cual afirmaba que se habían tomado fuertes medidas de seguridad, sin embargo, las cámaras captaron que solo había un vehículo de la policía municipal, bloqueando el lugar por donde pasó el camión. Para las autoridades de Niza las grabaciones obtenidas podrían ser una prueba determinante de lo sucedido en la noche del 14 de julio ante *“las declaraciones vertidas por parte del gobierno, quien aseguró que la policía nacional se encontraba fuertemente armada en el lugar por donde entró el camión⁴”*.

¹ (Coyle 2011)

² (Infobae 2013)

³ (Yáñez y Teruel 2016)

⁴ (Puchol 2016)

Los valores probatorios de los registros obtenidos por las videocámaras han demostrado ser de gran utilidad, especialmente en el momento de dilucidar los hechos y la identificación de los involucrados ante actos delictivos y terroristas. Sin embargo, la función preventiva ha sido la más cuestionada, pues los resultados obtenidos por medio estudios e investigaciones realizados principalmente en Europa, señalan la poca efectividad que tienen los CCTV en la reducción del delito¹.

Si bien es cierto, los gobiernos han incentivado el uso de los CCTV en los espacios públicos como una medida de seguridad, es claro que la existencia de los mismos no evita la comisión de delitos, sobre todo, sí se utilizan de manera aislada. Las autoridades deben plantear la necesidad de combinar de manera integral, los aportes tecnológicos modernos (como lo son los CCTV), con otros mecanismos de vigilancia más tradicionales, tales como la vigilancia física, mayor coordinación y cooperación interinstitucional (policía municipal, centro de comando, policía de tránsito, etc.), programas comunitarios de cuidado enfocados en la seguridad ciudadana, entre otros.

Las pruebas o imágenes digitales que se obtienen a través de las cámaras de seguridad, son una muestra o argumento que alimenta con mayor fuerza la credencial de estos sistemas de vigilancia y promueven la aspiración al perfeccionamiento de los mismos. Por ejemplo, los nuevos softwares en materia de videovigilancia están programados para detectar “comportamientos anormales o inhabituales”; por medio de un análisis estadístico el programa tiene la capacidad de detectar si una persona merodea, o “salta los molinetes del subterráneo o si alguna persona deja un paquete y se aleja”, a esto se le conoce como Analítica de Comportamiento en Video. La Analítica de Comportamientos aprovecha la investigación sobre los procesos de aprendizaje y la memoria del cerebro humano y aplica estos procesos para el análisis de los datos visuales. El resultado es una nueva tecnología probada para identificar de forma autónoma comportamientos anormales dentro del campo de visión de una cámara de

¹ Para el caso de Inglaterra véase (Welsh y Farrington 2002) (Gill y Spriggs 2002). Para el caso de España véase (Cerezo Domínguez y Díez Ripollés 2009)

vigilancia en tiempo real, permite al personal de seguridad monitorear más vídeo de forma exponencial de una manera más eficaz.

3.2 La inseguridad en América Latina:

En cuanto a la seguridad, el discurso cambia en las regiones, en el caso de Latinoamérica los sistemas de videovigilancia se presentan como instrumentos que fortalecen la seguridad pública. A diferencia de Europa o Estados Unidos, la región Latinoamericana contiene con enemigos muy diferentes al terrorismo, por eso los argumentos del discurso cambian en nuestra región.

A. Inseguridad relacionada al delito callejero.

Los conflictos se relacionan con el aumento de la violencia, el crimen organizado, los homicidios, el narcotráfico, la delincuencia callejera y en menor escala, sicariatos, homicidios, robos y hurtos. Así lo confirma el Programa de las Naciones Unidas para el Desarrollo, en su Informe Regional de Desarrollo Humano 2013-2014¹ (en adelante PNUD), en el que se indica los déficits que tienen los Estados latinoamericanos en materia de justicia y seguridad, especialmente con la violencia, el crimen y la inseguridad. El informe indica que el *“delito callejero es la amenaza que más afecta, de forma insistente y cotidiana, al ciudadano promedio, a través del principal delito que se asocia: el robo”* (PNUD 2013, 76). Según el informe, el panorama general de la región presenta un crecimiento en las tasas de robo, con excepción de Costa Rica, Guatemala, El Salvador y Venezuela. Las estadísticas también confirman un crecimiento en el uso de la violencia al cometerlo, pues suelen involucrar el uso de armas de fuego o arma blanca (PNUD 2013, 57).

Señala que *“en la última década la región ha sufrido una epidemia de violencia, acompañada por el crecimiento y difusión de los delitos, así como el aumento del temor entre los ciudadanos”* (PNUD 2013, v). Las tasas de homicidios en nuestro continente duplican el promedio mundial, incluso algunos países lo quintuplican. Un informe de la Secretaría General

¹ (PNUD 2013)

Organización de los Estados Americanos manifestó que: *“Algunos de nuestros países en América Latina y el Caribe ostentan las tasas más altas de homicidios del mundo. No obstante que en la región sólo habita un 8% de la población mundial, se materializa el 42% de todos los homicidios por arma de fuego y el 66% de todos los secuestros del planeta”*¹.

Por ejemplo, en la región latinoamericana y el Caribe, la tasa de homicidios creció un 11 por ciento durante el período 2000 a 2010, los robos se triplicaron en los últimos veinticinco años, las víctimas diarias en delitos de violencia sexual son aproximadamente cuatrocientos sesenta y el aumento en los delitos patrimoniales, producen un deterioro de la seguridad pública y dispara la percepción de inseguridad en la ciudadanía.

La necesidad de garantizar la seguridad de los habitantes y las demandas de la sociedad en ese sentido han incentivado la instalación de los sistemas de videovigilancia con la finalidad de reprimir hechos delictivos, tanto en ámbitos públicos como privados. La utilización de los sistemas de videovigilancia ha estado vinculada al enfrentamiento de los problemas de inseguridad pública, considerados instrumentos para reforzar la “batalla contra el crimen” y garantizar la seguridad de los espacios públicos.

Los sistemas de videovigilancia se presentan como herramientas que favorecen la captura visual de los delitos callejeros, tales como los robos, hurtos, la violencia o agresiones, infracciones administrativas (el uso en el tránsito vehicular); en un menor nivel de incidencia los homicidios, la delincuencia organizada y el abuso policial.

B. La inseguridad relacionada a la corrupción o ineficiencia estatal.

Además de la inseguridad relacionada a los delitos callejeros (la pobreza, el desempleo, la desigualdad económica y la falta de oportunidades son factores que desmejoran la seguridad pública y ciudadana), la inseguridad en la región latinoamericana se extiende hasta los altos poderes del Estado.

¹ (SGOEA 2008)

En algunos países, los casos de corrupción y la comisión de delitos de cuello blanco han generado la pérdida de confianza en los poderes públicos, principalmente en el poder judicial. La confianza en el sistema judicial se refleja en los índices de impunidad, la transparencia de los funcionarios públicos (intolerancia a la corrupción), la eficiente resolución de las sentencias y la estabilidad de los centros carcelarios. En muchos de los países latinoamericanos estos parámetros se han debilitado provocando un contexto social distorsionado por el temor y la desconfianza de la ciudadanía, donde la justicia por mano propia es común en el día a día: *“En la última década el Poder Judicial ha sufrido un descenso en las mediciones sobre confianza ciudadana y no escapa a los cuestionamientos que se hacen al sistema político, en este caso sobre su capacidad para brindar una justicia pronta, cumplida e igual para todos. Aunque esta erosión la padece también la mayoría de las instituciones públicas, impacta de manera particular por ser el Poder Judicial uno de los cimientos del Estado democrático de derecho¹”*.

Además, se incentivan las políticas criminales de “mano dura” y cero tolerancia contra el delincuente, lo que ocasiona la promoción de las penas carcelarias y la secuela de las crisis carcelarias, que lejos de solucionar el problema lo empeora (PNUD 2013, 5).

Aunado a las deficiencias en los sistemas de administración de justicia, la gran mayoría de países latinoamericanos carecen de controles policiales suficientes para disminuir los índices de criminalidad. En muchos de los países de Latinoamérica las instituciones públicas sobresalen por problemas de corrupción, falta de recursos tecnológicos, carentes de personal capacitado o con bajos niveles de profesionalización, y capacidades de investigación muy limitadas convirtiendo las funciones policiales poco eficaces y eficientes².

C. El auge de proyectos de videovigilancia policial en América Latina:

Desde la década de los noventa Inglaterra (1993), Chile (1993), España (1999) y un poco más tardíos en la década siguiente México (2008), Colombia, Argentina, Paraguay, Ecuador, adoptaron la utilización de las cámaras de vigilancia con el objetivo de fortalecer la seguridad pública interna. Para los cuerpos policiales las cámaras de seguridad son una medida

¹ (Nación 2015, 35)

² (Arias, Rosada Granados y Saín 2012, 7)

de prevención situacional, un sistema eficiente, con capacidades de disuasión delictiva que ponen en riesgo al delincuente, pues al sentirse vigilado, el delincuente cambiará su comportamiento y no delinquirá. Incluso la ciudadanía, ha dado el apoyo a estas iniciativas, pues en apariencia aumenta la seguridad subjetiva. Un estudio llevado a cabo en la ciudad de Málaga España, mostraba que el 85,5 por ciento de los encuestados opinaron que las cámaras servían para controlar la delincuencia y sólo un 14,5 por ciento opinó lo contrario. También se le consultó a los comerciantes de las zonas bajo vigilancia, si creían que con la presencia de las cámaras se había reducido la delincuencia, el 49,1 por ciento contestó afirmativamente¹. La ciudadanía apoya considerablemente los sistemas de videovigilancia, porque a su criterio, la presencia de las cámaras en espacios públicos los hace sentir más seguros y las consideran una herramienta útil de prevención delictiva.

En nuestra región a pesar de que no existe suficiente evidencia científica sobre la relación entre la delincuencia y el uso de estos dispositivos, los Gobiernos han invertido grandes sumas de dinero en adquirir y expandir su infraestructura tecnológica, especialmente con los CCTV, que al parecer se han convertido en la herramienta preferida de los gobiernos².

“Según Norris, la difusión de estos sistemas es una tendencia que se ha manifestado globalmente, cuyo crecimiento fue verificado en cuatro etapas: una difusión inicial en el sector privado; la introducción de la video-vigilancia en el transporte y la infraestructura pública; una utilización limitada en espacios públicos, que funcionó como el puntapié inicial para la migración a su uso gubernamental en la prevención del delito; y un último momento en el que el monitoreo tiende a la ubicuidad, con sistemas a gran escala que cubren ciudades enteras y que integran cámaras de seguridad del sector público y privado”³

Según el reporte del IMS Research llevado a cabo en el 2014, actualmente América Latina se ha convertido en uno de los nichos de crecimiento más importantes de la industria de estos dispositivos electrónicos a escala global.

¹ (Díez Ripollés y Cerezo Domínguez 2010, 4)

² (Crespo 2010)

³ (Norris, McCahill y Wood 2004) mencionado por (Lío, Ciudades, cámaras de seguridad y video-vigilancia: estado del arte y perspectiva de investigación 2015, 275)

“El mercado de la videovigilancia en América Latina mantuvo una tasa de crecimiento del 40,5% desde el 2008 hasta el 2013 y, según las previsiones hechas en dicho reporte, se espera que esa tasa se mantenga cuando menos hasta el 2019. De hecho, se considera que para ese año la venta de dispositivos de videovigilancia llegará a los 200 millones de dólares. El crecimiento del mercado de la videovigilancia en América Latina se encuentra por encima de otras regiones del mundo. Brasil, Argentina, Colombia y México, encabezan los mercados con mayor crecimiento” (Botello 2016, 195).

En los últimos veinte años, el uso de la videovigilancia ha tomado primordial importancia en la planificación urbana, proponiendo nuevas formas de desarrollo urbano. Ciudades como Lima, Santiago de Chile, Quito, México, Bogotá y Buenos Aires son algunos ejemplos regionales que han asegurado la vigilancia de los espacios públicos¹.

En la década de los noventa, en la ciudad de Santiago se instaló el primer sistema de videocámaras con fines de seguridad en espacios públicos. Para el año 2006 modernizaron el sistema antiguo de vigilancia, e instalaron cámaras digitales que permitían la captación de imágenes y sonidos, la interconexión con bases de datos, el almacenamiento y cotejo de información².

En el año 2002, el Municipio del Distrito Metropolitano de Quito impulsó una iniciativa que contaba con la instalación de ocho cámaras en la zona del Centro Histórico. Seis años después, existían ciento treinta y seis cámaras de seguridad que cubrían dos sitios turísticos de la ciudad el Centro Histórico y la Mariscal. El proyecto de vigilancia se expandirá con doscientos cincuenta cámaras en seis provincias fronterizas del país, al norte con Colombia y al sur con Perú, principalmente con el objetivo de debilitar las actividades de narcotráfico, contrabando de combustible y tráfico ilegal de armas.

México desde el año 2009 inició con el “Programa Ciudad Segura”, un proyecto de seguridad pública orientado a ampliar la cobertura de las cámaras de seguridad en los espacios públicos de diversas delegaciones³. En el 2003, el municipio de Puebla inició un Programa

¹ (Durán Segura 2012, 123)

² (Palacios Huerta 2007, 20)

³ (Seguridad 2010, 4)

llamado Centinela, que constaba de la instalación de cámaras cuyo objetivo primordial era la prevención delictiva. Con los vídeos obtenidos lograron descifrar el *modus operandi* de la delincuencia local, el cómo están operando estas personas, y persuadir y perseguir el delito en caso de que se cometa. Para el año 2015 se instalaron aproximadamente quinientas setenta y seis videocámaras y se espera para el 2016 se instalen cuatrocientos más para el corredor turístico y gastronómico de la ciudad¹. Querétaro, por su parte, contaba con trecientas cincuenta y ocho cámaras de vigilancia². Se suman a la lista el Municipio de Tlaxcala con cuarenta cámaras de vigilancia para el año 2013³. Ese mismo año el Municipio de Cuernavaca instaló sesenta y siete cámaras⁴. Cada una cuenta con su propio Observatorio Ciudadano (centro o mando de control).

En Argentina el caso más paradigmático es del Municipio de Tigre a partir del cual se desarrolló el resto de la infraestructura de videovigilancia en Argentina. Según una investigación realizada por la Revista Innovación⁵ sobre los planes de seguridad urbana llevados a cabo a lo largo del país, el año 2011 culminó la adquisición de estos sistemas, pues hubo un aumento en la necesidad de contratación de nuevos dispositivos por parte de los gobiernos provinciales y de los municipios. *“Entre 1995 y 2002 las estadísticas recopiladas por la Dirección Nacional de Política Criminal denotaron un incremento del 88% en los delitos denunciados en agencias policiales. Luego de 2002, los niveles comenzaron a descender, la inseguridad paso a ocupar el primer puesto entre los problemas nacionales superando al desempleo”* (Lio 2015, 34)

En Colombia el alcalde de Cali, Rodrigo Guerrero inició un proyecto de seguridad que consistía en la consecución de quinientas cuarenta y un nuevas cámaras de seguridad, con la finalidad de combatir los robos, la microextorsión y microtráfico de drogas⁶. En enero del 2015, ya se había instalado doscientas cámaras de las previstas. Según las cifras dadas por el Ministerio y la policía local, los índices de la delincuencia en comparación entre los años 2013 y 2014 habían disminuido; en 2014 se registraron mil quinientos treinta homicidios en Cali,

¹ (E-Consulta 2015)

² (Rodríguez 2015)

³ (Ayuntamiento de Tlaxcala 2015)

⁴ (Buscará Ayuntamiento de Cuernavaca instalar 50 cámaras de vigilancia más en el municipio 2015)

⁵ (Greenberg 2010)

⁶ (Gobierno anuncia la instalación de más de 500 cámaras en Cali para combatir inseguridad 2015)

cuatrocientos cuarenta y dos casos menos que en el 2013; se reportaron ocho mil setecientos sesenta hurtos a personas, quinientos treinta y seis casos menos y setecientos cuarenta y ocho hurtos a residencias, doscientos cuarenta y cuatro casos menor. Luis Alfredo Gómez, secretario del Gobierno de Cali, atribuye los buenos resultados gracias a las políticas de seguridad dentro de la que se encuentran las cámaras de vigilancia¹.

La mayoría de estos proyectos responden a la idealización de mantener ciudades seguras y ambientes sanos, adecuados y óptimos para el desarrollo humano. Las autoridades estatales, principalmente los municipios, se han encargado de promover el uso de los CCTV, revitalizando sus localidades. Por eso han promovido la recuperación y el repoblamiento de sus localidades según sea su valor arquitectónico, social, comercial, económico, turístico, o bien, cultural. Comúnmente estos centros (Centros Históricos, cívicos o simbólicos: museos, edificaciones coloniales, patrimonio cultural, etc.) son considerados espacios públicos de placer y disfrute, además cuentan con un atractivo turístico-comercial, que atrae a una clase social consumidora quienes aportan ingresos y divisas al país (Durán Segura 2012)

Las autoridades públicas en el afán de aprovechar el atractivo de estos lugares, han fomentado las corrientes higienistas de los espacios públicos, preservando una imagen ciudadana atractiva. Un ejemplo de lo anterior, es la Plaza Mayor de Madrid, un centro turístico que alberga entre diez mil y doce mil personas por día. La iniciativa de introducir CCTV fue impulsada primordialmente por los comerciantes de la zona y el Ayuntamiento de Madrid, con el objetivo de mejorar la seguridad del lugar para los turistas. La introducción de las 14 cámaras fijas y doce móviles, son una estrategia de prevención situacional².

Quienes exigen la recuperación de los lugares públicos argumentan una invasión de la delincuencia, el vandalismo y el desorden. Por medio de las cámaras de seguridad las autoridades locales lograron someter a ciertas minorías urbanas que deseaban fiscalizar y deportar, tales como los delincuentes callejeros, drogadictos e indigentes. Por ejemplo, en Valencia España, la Asociación de Comerciantes del Centro Histórico de Valencia, solicitaron al

¹ (Cali fue la campeona en reducción de delitos de alto impacto en Colombia 2015)

² (A. Betancourt 2008, 3)

Ayuntamiento la instalación de videocámaras en las zonas turísticas para reforzar la seguridad de los turistas y del lugar. Además, eliminar la presencia de vendedores ilegales (quienes venden productos falsificados), actividades como la prostitución y la reducción de los actos vandálicos que destruyen los bienes, tales como el esparcimiento de ácido, pintura y grafitis sobre los establecimientos del centro.

En nuestro país, a este proceso se le conoce como “gentrificación”, que se refiere al *“aburguesamiento, elitización o aristocratización de los espacios urbanos”* (Durán Segura 2012, 123), en la que pretende dar una imagen ciudadana limpia, expulsando a los vendedores ambulantes, indigentes o drogadictos de determinadas áreas urbanas desarrolladas con algún fin comercial, domiciliario o turístico.

En la actualidad, son muchos los países que se suman a la adquisición de los sistemas de videovigilancia en espacios públicos. En el caso de nuestro país ya son dos los municipios que promueven la utilización de las cámaras de videovigilancia: la Municipalidad de San José y la de Cartago. La iniciativa lanzada por ambos municipios, está dirigida a disminuir la delincuencia local, además cuenta con el apoyo de convenios suscritos con el Ministerio de Seguridad, cuerpos policiales, comerciantes y un porcentaje de la ciudadanía. Los proyectos cuentan aproximadamente con ciento setenta cámaras en el casco josefino, y treinta y dos cámaras de seguridad en el Municipio cartaginés ubicadas en puntos estratégicos¹. Ambos planes contemplan aumentar la cantidad de cámaras de vigilancia con la finalidad de cubrir puntos riesgosos en ambas localidades. En el caso específico de nuestro país, la utilización de estos sistemas va en aumento y es necesario encaminar las iniciativas dentro del marco de legalidad.

Los antecedentes terroristas, el aumento de la inseguridad y la violencia son las principales causas que han motivado el uso de los CCTV en los espacios públicos. Las autoridades en el afán de recuperar la seguridad de los espacios públicos han promovido la instalación de las cámaras de seguridad a lo largo y ancho de sus ciudades, como un instrumento tecnológico dirigido a reforzar la seguridad nacional, pública y ciudadana.

¹Para la provincia de San José véase (Arguedas 2016) Para Cartago véase (Ugarte 2016)

Existen otros factores sociales y tecnológicos que promovieron el desarrollo avanzado de estos sistemas. El contexto social bajo el que se desarrollan los CCTV involucra una serie de factores como el crecimiento de las áreas urbanas, la dispersión poblacional hacia ciertas ciudades (concentración poblacional en centros urbanos) y la sociedad de consumo de la década anterior, convirtieron a la videovigilancia en una herramienta útil para monitorear hurtos, robos, eventos masivos (principalmente en aquellas manifestaciones en las que había un grado de violencia), hospitales, escuelas, transporte públicos, etc.¹

En la década de los ochentas, la videovigilancia se utilizaba principalmente en el ámbito privado, los bancos y comercios lo utilizaban para disuadir la delincuencia; en centros de trabajo y empresas se utilizaban para mejorar la calidad del servicio, vigilar la producción de los trabajadores y bajar los costos de producción por pérdidas internas y externas de los productos o materia prima. Posteriormente, las cámaras de vigilancia fueron implementadas en el transporte público urbano para controlar el tráfico vehicular, por motivos de eficiencia en el servicio, el control de multitudes y la reducción de los hechos vandálicos (Carrión Mena 2008, 1).

D. El desarrollo de nuevas tecnologías asociadas al uso de los CCTV:

Otro factor que permitió el avance significativo de los CCTV fue la expansión de la Tecnología de Información y las Comunicaciones (TIC). Los CCTV sobresalen dentro de este proceso de modernización de los Estados. Desde los años noventa, el uso de estos sistemas ha ido en franco crecimiento convirtiéndose en una de las herramientas tecnológicas más populares del siglo. Sin embargo, los usos de las cámaras se remontan a la década de los sesentas en Estados Unidos e Inglaterra, cuyo fin era la vigilancia de bancos, tiendas y el tráfico vehicular. El desarrollo tecnológico de la videovigilancia, introdujo paulatinamente otros programas destinados a integrar, perfeccionar o renovar los instrumentos de control social y espacial, como la tecnología del reconocimiento facial (Caballero Julián, et al. 2017) y las bases de datos policiales (Carli 2008, 5).

¹ (Carli 2008)

La tecnología del reconocimiento facial es de vital importancia, porque que este tipo de tecnología permite identificar a una persona a través del método comparativo. El reconocimiento facial es *“una aplicación computadorizada para identificar o verificar automáticamente una persona a partir de la imagen digital o de un cuadro de una fuente de video, traduce los rasgos faciales a simples fórmulas matemáticas que pueden ser comparadas con bancos de datos”* (Carli 2008, 5).

La aplicación realiza un análisis algorítmico de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una fuente de vídeo, y se comparan con una base de datos¹. Inicialmente en 1988 Kirby y Sirovich² utilizaron una técnica estándar del álgebra lineal y descubrieron que se requerían al menos cien valores para cifrar acertadamente la imagen de una cara convenientemente alineada y normalizada. En 1991, Turk y Pentland³ logran efectuar el reconocimiento facial en tiempo real fidedigno mediante la técnica Eigenfaces. Con esta técnica se quitaba la información no útil del rostro y se revelaba la más efectiva estructura de baja dimensión de los patrones faciales. Con ello, es posible descomponer de manera más precisa la estructura facial en componentes ortogonales conocidos como Eigenfaces (Caballero Julián et al. 2017, 69). Posteriormente, los usos del reconocimiento facial se expandieron a lo largo de otros países y actualmente es utilizado en aeropuertos, lugares turísticos escuelas, estaciones de buses y trenes, entre otros⁴ (Carli, 2008), y se utiliza para combatir el fraude de pasaportes e identificaciones y la identificación de niños extraviados.

Otro ejemplo que surge a raíz de la expansión de los CCTV son las bases de datos policiales computarizadas. Las bases de datos policiales son un conjunto de información relacionada que se encuentra agrupada o estructurada; la información recopilada se centra principalmente en la actividad criminal internacional o nacional. Estas bases de datos permiten el almacenamiento y la accesibilidad rápida de la información, así como el cotejo (comparación)

¹ (Caballero Julián, y otros 2017)

² (Sirovich y Kirby 1987)

³ (Turk y Pentland 1991).

⁴ En EEUU en la Estatua de la Libertad y en la Isla Ellis, también en la Escuela de Educación Media Royal Palm en Phoenix, Arizona destinado al rastreo de niños perdidos y registro de agresores sexuales. En Australia en el aeropuerto Internacional de Sídney se escanea los rostros de los miembros de la tripulación y confirma las imágenes con las de los pasaportes.

de información con la base de datos. La INTERPOL cuenta con la base de datos policiales más grande del mundo. La amplia gama de esta entidad contiene millones de registros sobre huellas dactilares, perfiles de ADN, vehículos robados, armas de fuego, documentos de viaje robados y perdidos, entre otras cosas¹.

Los avances tecnológicos de los sistemas de información y telecomunicación, de la nueva era globalizada permiten una mayor gestión de datos entre los países y las organizaciones encargadas de la seguridad internacional. Parte de la estrategia y usos de los equipos electrónicos como los CCTV, utilizados por las instituciones estatales es el control de las poblaciones, especialmente de aquellos grupos criminales y terroristas². En este sentido, el trinomio tecnológico de los CCTV, reconocimiento facial y bases datos ofrecen algunas ventajas para los cuerpos policiales como: el trasiego y la accesibilidad de la información, el cotejo de la misma en tiempo real y la localización geográfica de personas buscadas por las autoridades policiales nacionales o internacionales. Los países que cuentan con antecedentes o amenazas de terrorismo, han incorporado esta tecnología argumentando la defensa del Estado, y físicamente se ha aprovechado para el control espacial de determinados lugares e implícitamente el control poblacional de algunas minorías consideradas peligrosas o sospechosas.

En los países donde la amenaza más fuerte es la inseguridad, los CCTV se han utilizado como un instrumento de prevención situacional en dos aspectos: sea “impidiendo el acceso del potencial delincuente al lugar de posible comisión del delito o reduciendo las ocasiones en que sea factible cometer un delito sin ser descubierto”. Y segundo, para garantizar la efectividad de las funciones policiales, *“facilitando una rápida intervención preventiva y perfeccionando la tasa de esclarecimientos de los delitos ya cometidos”* (Cerezo Domínguez y Díez Ripollés 2009, 175)

En la actualidad, los sistemas de videovigilancia forman parte de la vida cotidiana en sociedad, esto hace que la vigilancia se encuentre estrictamente ligada a nuestra adaptación al

¹ (INTERPOL 2017)

² En el 2015, se creó la base de datos analítica de la INTERPOL, con más de 16 mil sospechosos de ser combatientes terroristas extranjeros y recibieron información nominal de 51 países.

orden y control social actual¹. En la sociedad moderna, esta práctica tecnológica facilita la vigilancia y el control a un menor esfuerzo, lo que permite un aprovechamiento del tiempo propio de la lógica capitalista. Por su capacidad de registro las autoridades públicas y los particulares consideran que la presencia de las cámaras incidirá sobre la conducta del delincuente, evitando la comisión de actos violentos o delictivos (Foucault le denominó normalización del individuo). Michel Foucault basado en el modelo del panóptico de Jeremy Bentham, habla de las sociedades de seguridad y control. En su libro *Vigilar y Castigar* publicado en 2002, plantea que en las sociedades contemporáneas *“la administración de los riesgos aparecen como un nuevo y poderoso mecanismo de control vinculado al poder, ese poder se ejerce positivamente sobre la vida e implica controles precisos y regulaciones generales”*². Lo que en su momento el autor planteó como un simple diseño arquitectónico para una cárcel, hoy en día tiene una aplicación más sutil apoyada en la tecnología como instrumento de control, disciplina y dominación del comportamiento humano³.

La aceptación social de estos sistemas es una muestra de lo presente que están en la vida cotidiana de los ciudadanos. La presencia de las cámaras en zonas públicas aumenta la sensación de seguridad de los ciudadanos en un gran porcentaje. Investigaciones llevadas a cabo en diversos países, analizan la aceptación pública de los CCTV por parte de los *ciudadanos* *“según datos del 2009, del 68,7% de la población española que apoya la videovigilancia un 66,4% de los encuestados lo hace porque las cámaras les dan seguridad, 18% porque considera que permiten la identificación de delincuentes y el 15,2% porque cree que es una forma de prevención de la delincuencia”* (Clavell 2009, 92)

¹ Para Coleman y Sim (2000) la instalación de las cámaras tiene una connotación higienista urbana (campañas de limpieza) enfocada en atraer el turismo. Para Lyon (2007) estos sistemas se justifican en la necesidad de construir ciudades seguras. Norris (2003) indica que hay una panoptización del espacio urbano que incide en dos transformaciones: primero como mecanismo de control social (gestión de la sospecha, ponderación de la peligrosidad, etc.) y la segunda relacionada a la capacidad de almacenamiento de información por medio de las cámaras.

² (Foucault 1977-1978) mencionado por (Lío, Cámaras de seguridad y prevención del delito. La utilización de la videovigilancia en la ciudad de Buenos Aires 2015, 278) También se puede hacer referencia a las novelas distópicas de George Orwell, que hablaba del omnipresente “Gran Hermano” que vigilaba las actividades de los pobladores del territorio de Oceanía, un imaginario que representaba la vigilancia en las sociedades contemporáneas.

³ (Valencia Grajales and Marín Galeano 2017, 512)

La videovigilancia no debe entenderse como un concepto aislado y estático, sino susceptible al continuo cambio en la innovación de nuevas técnicas, procedimientos, usos y manejos. Paralelo a los CCTV, se crearon nuevas tecnologías enlazados a la vigilancia, como los sistemas de reconocimiento facial, bases de datos computarizados para el rastreo de personas, grabación de sonidos y voces por medio de micrófonos, identificación automática de matrícula, y un sinnúmero más de programas y usos que permiten alertar la comisión de un delito y la identificación de las personas u objetos.

Aunque las autoridades promueven el uso de estos sistemas, es importante considerar los resultados de la evidencia científica. Aunque en la región latinoamericana no se han llevado a cabo muchas investigaciones, en el ámbito anglosajón existe múltiples evaluaciones de los sistemas de videovigilancia y las contribuciones en la reducción de la delincuencia. Los resultados son mixtos y divergentes, sin embargo, se señalan efectos positivos en la disminución de la delincuencia en ciertas categorías de delitos; las investigaciones ponen en manifiesto la aplicación de otras medidas securitarias para el mejor aprovechamiento de las cámaras de seguridad en espacios públicos¹.

¹ Algunos resultados positivos de la videovigilancia en complemento con otras medidas de seguridad son: el impacto de las cámaras es mejor cuando existen carteles informativos (que pueden generar un efecto disuasorio) y en espacios de acceso limitado (Díez Ripollés y Cerezo Domínguez, 2009); la presencia de las cámaras disminuye en un 4 por ciento los delitos (Welsh y Farrington, 2002); las cámaras influyen sobre ciertas categorías de delitos, no sobre todos los delitos, las cámaras tienen un impacto positivo sobre los delitos contra la propiedad, pero no tiene efecto sobre los delitos violentos y delincuencia sobre las personas (Hier 2010).

Sección cuarta: Los enfoques de la videovigilancia pública.

El proceso de incorporación de las cámaras de seguridad en la mayoría de los casos, ha sido precipitada y de rápida ejecución¹, En las grandes ciudades se pasó de cientos a miles de cámaras en poco tiempo. La tesis de que las cámaras de seguridad son útiles en la reducción de la delincuencia, tomó fuerza en los gobiernos y en los particulares, provocando la propagación de estos sistemas en aeropuertos, estaciones de buses o trenes, parques, centros comerciales, parques, condominios, residenciales, entre otros. Aunque el fenómeno de la videovigilancia surgió con rapidez, la creación normativa referente a la videovigilancia no se dio con la misma velocidad ya que estos sistemas empezaron a operar sin un marco jurídico que lo respaldara.

Lo primero y lo más importante es orientar la tecnología a un uso consciente y responsable por parte de las autoridades estatales, teniendo pleno conocimiento de las afectaciones que pueden incidir sobre las libertades de los ciudadanos, esto se logra por medio de políticas y prácticas que mitiguen los efectos nocivos de la tecnología. Lo segundo, es orientar y delimitar el uso de los sistemas de videovigilancia a fines de prevención y persecución delictiva. Uno de los errores que se ha cometido es la utilización de estos sistemas para fines administrativos y de orden público.

4.1 Por un uso consciente y responsable de la videovigilancia:

Los usos de la tecnología se han globalizado, y lo que hace unas décadas atrás pensábamos que era una utopía, hoy en día es una realidad. La interconectividad que existe en el plano global ha generado una especie de codependencia de la sociedad con la tecnología (proceso que surge gracias al internet) a tal punto que la ausencia de ella dificulta nuestra cotidianeidad².

¹ (La videovigilancia fracasa en Londres 2007)

² La sociedad de consumo incorporó de una manera desmedida y abusiva los usos de la tecnología (teléfonos y pantallas inteligentes, sistemas de seguridad integrados con cámaras, alarmas y sensores, aplicación de gps, etc.)

La tecnología permite ejercer casi de manera anónima, invisible y automática el poder y la vigilancia¹, los ciudadanos por su parte pasan inadvertidos con las nuevas fuerzas de control. Uno de los peligros que generan las nuevas tecnologías es la discreción con que llevan a cabo sus funciones, casi imperceptible para los ciudadanos. Los CCTV forman parte de esta gama tecnológica que se ha expandido y se incorpora a las funciones estatales de cuidado y vigilancia, enfatizada principalmente en la prevención y persecución delictiva.

De la mano de las nuevas técnicas de vigilancia surge otra gama de aplicaciones o programas que intensifican los alcances y proporcionalidad de la tecnología ya existente, ya no se trata de una simple observación a través de cámaras sino la incorporación de programas enlazados al funcionamiento de los CCTV, que ponen en riesgo la privacidad y los datos de los ciudadanos. Por ejemplo: los Análisis de Contenido de Vídeo (o VCA son sus siglas en inglés) depuran y facilitan el proceso de vigilancia. El VCA es esencialmente el análisis automático de imágenes obtenidas por CCTV, utilizando algoritmos avanzados para crear información útil sobre el contenido. El alcance de la analítica busca identificar cambios o movimientos en una escena en particular, se utiliza para detectar intrusos, paquetes abandonados, vehículos mal estacionados o conteo de personas (Insecurity s.f.).

La alta definición (HD por sus siglas en inglés) es otra aplicación que se ha unido al funcionamiento de las cámaras. La alta calidad de las imágenes, permiten de manera fácil la identificación de las personas que transitan en las zonas vigiladas. La imagen constituye un dato personal de la persona que la hace identificable. Indistintamente si el objetivo es un sospechoso o un ciudadano común, dicha capacidad pone en riesgo la imagen propia de todos los ciudadanos.

La creación de las bases de datos, es otra herramienta accesoria que ha crecido paulatinamente al lado de los CCTV. Lo importante de resaltar con ellas, es que facilitan el análisis y cotejo de la información con las imágenes que son obtenidas a través de las cámaras. La información obtenida a través de las bases de datos o CCTV, puede ser procesada por

¹ (Bernal Martín 2015)

programas de reconocimiento facial, análisis de comportamiento monitoreo o rastreo de personas enlazados a los CCTV, permitiendo la identificación o ubicación de la persona.

Con estos tres ejemplos, basta decir que la tecnología se innova con el pasar del tiempo, y bajo el argumento de eficiencia tecnológica mejora su alcance y capacidad. Estamos hablando de sistemas que tienen una amplia capacidad de registro, almacenamiento y procesamiento de información o bien de rastreo, ubicación y seguimiento de personas u objetos, estas características potencian el tratamiento de datos personales no consentidos violentando derechos como la privacidad y la autodeterminación informativa.

En la obra De Orwell al cibercontrol se advierte sobre los riesgos que puede generar el uso inadecuado o irresponsable de la tecnología y redes sociales. El autor invita al lector a reflexionar sobre las “redes de vigilancia mundial” y su compatibilidad con los principios de una sociedad democrática. Por ejemplo, el trinomio tecnológico de CCTV, bases de datos y reconocimiento facial, permiten en un pequeño lapso de tiempo identificar y ubicar a una persona. Para el autor, estas estrategias de hipervigilancia y mecanismo de control transgreden la autonomía y libertad de los ciudadanos, quienes viven vigilados por el gran ojo electrónico con el pretexto de garantizarle su propia seguridad.

Con la certeza de que las nuevas tecnologías apuntan a ser más eficientes, automatizadas y analíticas, los países pioneros empiezan a reflexionar en la necesidad de contrarrestar los efectos y alcances que tiene la tecnología sobre la vida de los ciudadanos, pues en la medida que mejora la calidad de estos sistemas en más riesgo se expone la privacidad y los datos personales del ciudadano¹. Surge la necesidad de establecer por medio de leyes, reglamentos o códigos de conductas, las pautas básicas de funcionamiento de estos sistemas.

Los encargados de estos sistemas readecuaron los lineamientos sobre los que se venía trabajando, lo que implicó un giro no solo operativo, sino también legal, pues se incorporaron principios tendientes a proteger la privacidad y los datos de los ciudadanos. La Unión Europea ha sido un claro ejemplo de ello, como región han hecho innumerables esfuerzos por adoptar

¹ (Insecurity s.f.)

políticas acordes a la protección de datos personales y privacidad en el funcionamiento de los CCTV, por medio de la Oficina de Protección de Datos se ha procurado homogenizar la normativa de los diferentes países relativa a los CCTV por medio de directrices que protegen los derechos de los ciudadanos¹.

Además de regular normativamente la videovigilancia se incluye un modelo llamado *privacy by design*². Esta política surge como una defensa o respuesta ante el vertiginoso desarrollo tecnológico que innova constantemente y obliga a los Estados a estar en una continua reformulación normativa. La privacidad por diseño es un política que se ha incorporado en las normas o directrices (en la Directiva 95/46/CE) que regulan los sistemas de videovigilancia, y está dirigida a las organizaciones, públicas o privadas, que tratan datos personales, sea como responsable o encargados del tratamiento: *“La aplicación del modelo de privacidad por diseño trata de asegurar, desde la fase inicial de desarrollo de un sistema de información o planteamiento de un modelo de negocio y durante todo el ciclo de vida, la protección de datos personales a través de la aplicación de los principio y deberes exigibles³”*.

El objetivo de estas políticas o modelos es minimizar el tratamiento de datos personales que surgen con la implementación de mejores tecnologías, y a la vez, garantizar los principios y deberes de la protección de datos personales de los responsables y encargados del tratamiento de datos personales. Los principios que se abogan son la licitud, el consentimiento, la información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; de la misma manera se le imponen deberes de seguridad y confidencialidad a los responsables o encargados del tratamiento de datos: *“El modelo de privacidad por diseño es una aproximación holística, ya que considera tanto el cumplimiento normativo como la adecuación de las prácticas de la organización, a la protección de datos personales, de manera que implica que el sujeto obligado deba adoptar medidas atendiendo a todos los aspectos que se plantean y que van*

¹ (EDPS, Follow-up Report to the 2010 EDPS Video-surveillance Guidelines 2010)

² Fue creada por la Dra. Ann Cavoukian y se adoptó en la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. La privacidad por diseño tiene por objeto servir como aproximación de manera que los nuevos modelos o prácticas de negocio, las especificaciones tecnológicas y las infraestructuras físicas incluyan principio de privacidad de manera que respeten el derecho fundamental a la protección de datos personales.

³ (Prosoft 2013, 47)

desde la designación de una persona o departamento de datos personales durante todo el tratamiento y hasta la supresión segura de los datos personales” (Prosoft 2013)

La privacidad por diseño significa la protección de datos a través del diseño de tecnología¹. Es una idea que impulsa la Unión Europea en la que se promueve las políticas de protección de datos en la ingeniería de software y la utilización de la tecnología, incluyendo a los sistemas de videovigilancia²; lo que propone es incorporar desde la etapa inicial del diseño medidas técnicas de precaución que permitan una mayor protección de los datos personales y la privacidad de las personas filmadas. Este método toma en cuenta los valores morales subyacentes a la protección de datos personales, las decisiones que se toman en la etapa de concepción deben justificarse sobre la base de consideraciones morales claras y convincentes³. Este tipo de modelo es un buen ejemplo que demuestra como las nuevas tecnologías pueden ser creadas y construidas en el resguardo de la vida intimidad de las personas.

Es evidente que la amplia gama tecnológica que se desarrolla alrededor de los CCTV, expone la información personal de los ciudadanos. La finalidad de incorporar modelos como el de privacidad por diseño es garantizar que el tratamiento de los datos sea legítimo, controlado e informado a fin de garantizar la privacidad y el derecho de autodeterminación informativa de las personas. De la misma manera, se obliga al responsable o encargado del tratamiento de datos a adoptar medidas técnicas y organizativas que cumplan con la normatividad de este derecho.

4.2 Por un uso delimitado acorde a la finalidad:

En el contexto de las políticas neoliberales, los sistemas de videovigilancia se presentan como una herramienta útil enfocada en mejorar la seguridad mediante la prevención, reducción, detección y represión del delito, bajo este argumento las cámaras empiezan a ocupar los espacios públicos y como consecuencia, las autoridades policiales ejercen un mayor control sobre la población y el espacio.

¹ (GDPR s.f.)

² (Secretaría General s.f.)

³ (Van den Hoven 2010)

“Los fines que persigue la videovigilancia no son exclusivos de la era de la vigilancia electrónica, dado que la actitud vigilante del Estado no es una función moderna o novedosa, sino que una constante histórica, común a todos los modelos de Estado (Estado Policía, Estado Liberal o Estado Social) y de Administración Pública¹”.

El enfoque debe limitarse en un sentido estricto precisamente por las características particulares de estos sistemas. La vigilancia que proponen las videocámaras dista de ser limitada, es una vigilancia con alta capacidad de registro y almacenamiento, automatizada, generalizada e indiscriminada (pues vigila al delincuente y al que no lo es). Por estas y otras razones, es importante establecer límites al uso de estos sistemas. Los límites son establecidos en la norma legal, la cual debe garantizar los principios y deberes *supra* mencionados.

Extender los usos de una herramienta tan vasta como los CCTV es desvirtuar el propósito intrínseco para el cual fueron creados, la actividad de la vigilancia policial debe girar en torno a los actos delictivos sea con la detección del delito, o con la persecución, una vez cometidos. Utilizar las cámaras por motivos de orden público en lato sensu, es convertir los sistemas de videovigilancia en un instrumento represivo de control policial.

Ahora, las videocámaras son utilizadas para captar infracciones administrativas referentes al orden público. Por ejemplo, en Reino Unido y en Europa, los CCTV están siendo cada vez más utilizados en la aplicación de la ley y el orden, para todo, desde la observación del tráfico (y la emisión automática de boletos) hasta la observación de zonas o vecindarios con un alto índice de delincuencia. Este uso de la tecnología de CCTV ha preocupado a ciertos sectores de la sociedad que denuncian afectaciones a la privacidad, particularmente, porque se han convertido en una parte rutinaria de los procedimientos policiales².

Con esto se intensifican y revolucionan las funciones policiales de cuidado, vigilancia y control sobre las personas y los espacios. Los ciudadanos son vigilados constantemente en zonas

¹ (Rivera Ortega 2002, 25)

² (Rouse 2012)

públicas y privadas, situación que lejos de resguardar la privacidad del ciudadano, maximiza el tratamiento de sus datos personales.

En el contexto de la actividad de delictiva, a las cámaras de seguridad, se le atribuyen dos funciones, la función disuasiva y la forense¹. La función disuasiva está relacionada con la prevención del delito y responde a la lógica de que el delincuente al sentirse vigilado desistirá de cualquier conducta delictiva. Se supone que, en los espacios públicos controlados por cámaras, el delincuente hace una valoración de los riesgos previo a la comisión del delito, principalmente por la evidencia que queda registrada en las cámaras. Bajo este argumento, se cree que en las zonas vigiladas hay una reducción de la delincuencia.

Una de las críticas que han surgido en este aspecto es que, si bien es cierto, las cámaras de seguridad tienen la capacidad de registrar hechos delictivos y aportar evidencia sobre el mismo, éstas no tienen la capacidad de evitarlos o interrumpirlos (como lo podría hacer un policía) por lo que el elemento disuasivo de las cámaras disminuye. Esta imposibilidad de las cámaras de prevenir la comisión de delitos por sí solas, hacen que la efectividad preventiva dependa de otros factores como la asistencia y el rápido despliegue de la acción policial. Otros estudios (que se mencionan más adelante) demuestran resultados poco significativos de las cámaras en la prevención del delito y surten un efecto disuasivo únicamente sobre ciertas categorías de delitos.

Las cámaras como herramienta forense permiten la recolección de evidencia una vez ocurrido el hecho delictivo. Al documentar la información de los hechos, es posible obtener información valiosa sobre los involucrados y de cómo ocurrieron los hechos (por ejemplo, la vestimenta del sospechoso, el tipo de vehículo que andaba, la hora exacta en que ocurrieron los hechos, que dirección tomaron, etc.). Esta función toma más efectividad, debido a la integración de los CCTV con dispositivos de monitoreo, rastreo, reconocimiento facial y/o algoritmos de análisis de comportamientos o reconocimiento de objetos, que facilitan la detección, casi inmediata, del delito. Los operadores de las cámaras de seguridad, procesan gran cantidad de imágenes diariamente, por lo que este tipo de software depuran o facilitan el proceso de

¹ (Facilitiesnet s.f.)

vigilancia. Cuando es posible obtener registros de las cámaras se aporta evidencia del delito y en algunos casos permite la identificación de los sospechosos.

Es innegable que el avance tecnológico paralelo a los CCTV, el uso excesivo o desmedido de estos sistemas son factores que transgreden los derechos de vida privada, imagen y protección de datos de los ciudadanos. Debe existir una consciencia de los encargados y responsables del tratamiento de datos personales, de la necesidad de establecer parámetros técnicos, operativos y legales en el desarrollo de proyectos o negocios como los CCTV, que garanticen el derecho fundamental a la protección de datos personales y le generen confianza al propio ciudadano, por ejemplo la eliminación o reducción de sus datos (minimización del tratamiento), evitar los tratamientos innecesarios o no deseados, o bien aumentar el control de la información propia.

A continuación, se exponen las dos aristas que se desprenden con el uso de los CCTV, quienes la apoyan y consideran que es una herramienta para la prevención, reducción y persecución de delito, y los detractores, quienes consideran a los CCTV una herramienta tecnológica policial que afecta los derechos de privacidad, imagen y protección de datos personales del ciudadano.

CAPITULO 2: LA DICOTOMÍA QUE SE DESPLIEGA CON EL USO DE LA VIDEOVIGILANCIA: EL DERECHO A LA SEGURIDAD Y EL DERECHO A LA INTIMIDAD

El desarrollo del presente capítulo expone dos posiciones que surgen a raíz del uso de los sistemas de videovigilancia: quienes justifican y apoyan su uso fundamentados en la necesidad de prevenir y detectar el crimen porque los consideran una medida de seguridad que fortalece las funciones policiales en los espacios públicos en la reducción, prevención y persecución del delito. Y segundo, quienes alertan sobre las amenazas que representan estas tecnologías sobre los derechos de privacidad, imagen y datos del ciudadano, principalmente porque facilitan el almacenamiento, recolección y procesamiento de datos por parte de las autoridades estatales, convirtiéndolo en un peligroso instrumento tecnológico de control social y espacial.

Las afectaciones que tienen los sistemas de vigilancia, ubicados en áreas públicas, sobre los derechos concernientes a la privacidad del individuo pueden derivarse del uso excesivo de estos sistemas por parte de las autoridades policiales, quienes, en la lucha por mejorar la seguridad de los espacios, utilizan las cámaras para ejercer mayor control social y espacial¹. A pesar de que la ciudadanía apoya considerablemente la utilización de la videovigilancia, la propagación desmedida de estos sistemas puede afectar los derechos propios del individuo, ya que al hablar de videovigilancia es inevitable no ligarla con la esfera de privacidad de las personas².

Desde el punto de vista constitucional se confrontan el derecho a la seguridad y a la privacidad, el debate se centrará en la coexistencia de ambos derechos, es decir, un balance entre las demandas de seguridad y las luchas que protegen la privacidad, en palabras de Edwards *“las víctimas potenciales prefieren sacrificar un grado de privacidad personal por un grado de*

¹ Como se mencionó en el capítulo anterior, la sociedad moderna ha incorporado la tecnología en las funciones policiales bajo modelos de riesgos y prevención situacional, estrategias criminales que tienden a ser represivas y punitivas.

² (Proyect 2014)

protección personal” y a la inversa, “los riesgos se desplazan del ámbito de la integridad individual a los derechos individuales¹”.

. La videovigilancia es una actividad administrativa llevada a cabo por los cuerpos policiales que procura el mejoramiento de la seguridad, *per se*, dicha actividad no puede ser arbitraria, sino que debe ser encuadrada en un marco legal proporcionado con garantías para el ciudadano y facultades de actuación para la Administración Pública. A partir de la ley, se establecen los límites y alcances del avance tecnológico aplicado a la seguridad, siempre en resguardo del derecho a la privacidad de los ciudadanos.

Un matiz muy importante a considerar en esta discusión o confrontación de derechos que surge a partir de los CCTV es en plano normativo en dos sentidos. La primera que se caracteriza por la productividad normativa de la videovigilancia y posteriormente su implementación se hace efectiva. O bien la segunda, que predomina en la mayoría de países, que es cuando la creación normativa surge posterior a la emergencia de estos sistemas; a falta de regulación normativa (o normativa existente con lagunas legislativas) los usos de los sistemas de videovigilancia se presentan como una amenaza que potencia la vulneración de derechos². La finalidad del análisis contrapuesto pretende determinar el grado de incidencia que tienen las cámaras sobre los derechos de vida privada, imagen y protección de datos personales, y accesoriamente se desarrolla los aportes que ofrece la videovigilancia en el tema de prevención y persecución del delito, tomando como base la efectividad de los mismos para dicho fin. A continuación, el desarrollo del segundo capítulo.

¹ (Edwards 2005)

² (Lío y Urtasun 2016)

Sección primera: La videovigilancia una herramienta a favor de la Seguridad Pública

En la presente sección, nos limitaremos a hablar de la videovigilancia pública, entendida como la vigilancia que llevan a cabo las autoridades públicas, principalmente los cuerpos policiales, que consiste en la vigilancia por medio de videocámaras ubicadas en espacios públicos, las cuales están enlazadas entre sí y las imágenes son monitoreadas desde un centro de comando operativo, cuya finalidad gira entorno a la detección, prevención y persecución de la actividad delictiva.

1.1 La connotación policial de los sistemas de videovigilancia:

Palacios identifica una serie de elementos que deben cumplir o tener los sistemas de videovigilancia empleada por los cuerpos policiales. El primero de ellos es el elemento objetivo, que es el medio o instrumento mediante el cual se realiza la actividad de vigilar. Propiamente las cámaras pueden ser fijas o móviles, con capacidad de grabar imágenes y/o sonidos. En la actualidad, se utilizan cámaras digitales con infrarrojo (graban en la noche), con sensores de movimiento e incluso ligadas a programas o softwares y bases de datos.

El elemento orgánico se refiere a la institución u órgano estatal que utiliza y controla estos sistemas, que en la mayoría de las veces son las fuerzas policiales o municipales, o bien policía de investigaciones. El elemento teleológico consiste en el fin que pretende alcanzar la videovigilancia, que es garantizar el orden y la seguridad pública. El elemento espacial se refiere al lugar donde se lleva a la cabo las grabaciones, puede ser un lugar público, tales como calles, plazas, parques o bien privado, como edificios estatales, centros comerciales o residenciales. Por último, el elemento garantista que indica que toda intervención del Estado debe hacerse en apego a los derechos constitucionales de los ciudadanos (Palacios Huerta 2007, 22-23).

En relación a éste último, el uso de los CCTV, considerada una política pública de seguridad debe garantizar el cumplimiento de las libertades civiles de los ciudadanos. Si bien es cierto, es responsabilidad del Estado instaurar políticas de seguridad idóneas a la necesidad, las

mismas deben ser acordes al respeto de los derechos civiles. Esto quiere decir que, la videovigilancia como medida administrativa no puede ir en detrimento de los derechos de privacidad, imagen y protección de datos personales de los administrados.

El avance tecnológico y el proceso de globalización evolucionaron drásticamente las estrategias y técnicas de seguridad de las fuerzas policiales; la tecnología les permite a los cuerpos policiales extender y reforzar las funciones de cuidado, vigilancia y control. Además, con la presencia de las cámaras los cuerpos policiales mejoran sus tiempos de respuesta y aseguran la captura de imágenes de posibles delincuentes o infractores. La utilización de las cámaras de seguridad ha ofrecido aportes considerables principalmente en la persecución del delito, pues facilita la identificación de los sospechosos a través de las imágenes guardadas¹ y la aclaración de los hechos ocurridos. Otro aporte importante atribuido a las cámaras ha sido el rastreo de objetos y personas (sospechosos buscados por las autoridades policiales o víctimas de secuestros), gracias al enlace de los CCTV con bases de datos computarizadas y algoritmos de reconocimiento facial². Sin embargo, la versatilidad de la tecnología también le ha permitido a la delincuencia, mejorar su capacidad de organización, y en muchos casos, aumentar el nivel de violencia utilizada para la comisión de los delitos³

Los sistemas de videovigilancia como instrumento para instaurar el orden *“se justifican en el discurso de la seguridad bajo los argumentos de la eficacia tecnológica en la reducción de riesgo y la administración del espacio público”*⁴. Las ciudades han evaluado los sistemas de videovigilancia en espacios públicos, como un instrumento que pudiera mejorar la seguridad de sus ciudadanos, apostando a los potenciales beneficios que ofrece esta tecnología. Como medida administrativa, los sistemas de videovigilancia deben cumplir con los siguientes requerimientos: *“el juicio de idoneidad (si tal medida es susceptible de conseguir el objetivo propuesto), juicio de necesidad (si esa medida es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia) y el juicio de*

¹ La identificación del sospechoso depende de factores como que ande el rostro descubierto y la buena calidad de los datos o imágenes.

² (Sorpreniente reconocimiento facial identifica a criminal durante un concierto en China 2018)

³ (Dammer 2008, 11)

⁴ (Espinola Frausto 2013, 5)

proporcionalidad en sentido estricto (si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto)¹”.

En otras palabras, los sistemas de videovigilancia deben ser una estrategia policial idónea para reducir, prevenir o perseguir la actividad delictiva; debe surgir ante una necesidad, que en este caso sería una problemática de inseguridad y prevención situacional, sin ser proporcional al fin que persigue, lo que implica que debe estar enfocada en la delincuencia sin afectar los intereses generales del resto de la ciudadanía.

Las autoridades públicas encargadas del manejo y operación de los sistemas de video vigilancia deben analizar la relación costo / beneficio de las cámaras para determinar si el alto costo de la inversión de los sistemas de video vigilancia, responden favorablemente o solucionan en cierta medida el problema de la delincuencia. Se sabe que las adquisiciones de las cámaras de seguridad implican un gasto económico alto en la compra, mantenimiento y capacitación del personal, así como la constante innovación del equipo tecnológico.

Por ejemplo, en España, Reino Unido y Estados Unidos, se han llevado a cabo investigaciones sistemáticas (que más adelante se desarrollan) que evalúan el antes y el después de las cámaras en determinados lugares, con fin de establecer los efectos de las cámaras sobre el delincuente². Determinar el grado de efectividad de las cámaras sobre la delincuencia es importante porque se comprueba que el medio empleado, en este caso las cámaras, aportan un beneficio al problema de inseguridad.

¹ (Legálitas 2014)

² La finalidad de las investigaciones, en su mayoría, es cuantificar la comisión de delitos en espacios públicos sin cámaras, y otro análisis con la presencia de las cámaras. Esto con la finalidad de determinar el efecto disuasorio de las cámaras sobre las conductas delictivas, así como los aportes para la resolución del caso en la identificación de los sospechosos.

1.2 Funciones de seguridad y orden público.

En sentido amplio, las cámaras de seguridad son utilizadas en dos direcciones. La primera relacionada al delito, principalmente en prevención, reducción y persecución del delito; y la segunda para el mantenimiento del orden público. Con los postulados del derecho penal moderno la prevención, la reducción del riesgo y la administración del espacio tomaron relevancia. Los sistemas de videovigilancia son producto de esa nueva propuesta, una propuesta que incluye, mayor intervencionismo estatal centrado en la conservación del orden de los espacios públicos, vigilancia y exclusión de los potenciales delincuentes o zonas consideradas peligrosas, participación ciudadana en el resguardo de la seguridad, disuasión de comportamientos delictivos, entre otros. *“La videovigilancia en los espacios públicos es clave en el programa de seguridad comunitaria de Glasgow, cuyo objetivo es contribuir a la reducción de la delincuencia, la reducción del miedo a la delincuencia y el abordaje de temas comunitarios más amplios, como el vandalismo, los grafitis, los carteles y los incendios provocados”* (Galdon Clavell 2015).

En la parte preventiva, las videocámaras de seguridad les permiten a los cuerpos policiales monitorear simultáneamente muchos lugares, personas y actividades. Estos dispositivos les permiten a las autoridades policiales extender la capacidad de “ver” (visual), incrementando el margen de certidumbre sobre determinados espacios públicos, lo que permite anticipar los actos violentos o delictivos en contra de los ciudadanos.

Otra función preventiva que se atribuye a las cámaras de seguridad es la disuasión de comportamientos criminales y sucesos delictivos, pues se cree que, con la vigilancia permanente en los espacios públicos, es menos probable este tipo de conductas. Los CCTV como medida administrativa además de tener una connotación policial, tienen una finalidad de orden público, debido a que el mantenimiento del orden está generalmente a cargo de los cuerpos policiales, y su función tradicional es constatar que las conductas se adecuen a las normas establecidas¹. Para quienes apoyan esta tesis, los sistemas de videovigilancia inciden intrínsecamente en los

¹ (Vida Fernández 2013, 1) La actividad administrativa de orden público incide “sobre la libertad de los ciudadanos a través de medidas de prohibición, limitación, imposición y coacción”

comportamientos de las personas, pues el individuo al “sentirse bajo vigilancia”, no actuará con la misma libertad y espontaneidad como en el caso de que no lo estuviera, bajo este supuesto la persona pensará dos veces realizar un acción o acto delictivo. *“Los CCTV proporcionan una amenaza disuasiva que se extiende a los potenciales agresores haciéndoles creer que alguien los observa y tomará acción ante su mal comportamiento, o bien, que serán identificados y arrestados después basados en las grabaciones del CCTV¹”*.

Quienes apoyan el efecto disuasivo de las cámaras de seguridad sobre las conductas delictivas afirman que estos sistemas ofrecen buenos resultados en la reducción, prevención y persecución de la delincuencia y mejoran la administración del espacio, pues ayudan a mantener el orden público y velan por la seguridad de los ciudadanos en las zonas públicas.

Los promotores de la videovigilancia preventiva insisten que la presencia de las cámaras mejora la convivencia ciudadana, la seguridad de la comunidad y la calidad de vida de los ciudadanos² (vecinos de la zona, comerciantes y los transeúntes). Debido a su carácter disuasorio, se reduce y se previenen los problemas de convivencia (vandalismo, alteración del orden, peleas, disturbios, etc.) y los relacionados con la comisión de delitos y/o faltas. Además se asegura la utilización pacífica de las vías y espacios públicos y el cuidado de las cosas públicas frente a las perturbaciones de las actividades individuales³ (daños a la propiedad del Estado o particulares).

En relación a la persecución del delito, los sistemas de videovigilancia aportan información valiosa para la investigación policial, como medios de pruebas digitales, permiten dilucidar la comisión de los hechos delictivos, o bien en ocasiones, permiten la identificación de las personas involucradas. Con la evidencia recolectada por las cámaras de seguridad es posible ver los niveles de violencia y agresión del delincuente, así como la hostilidad mostrada por quienes perpetraron el del delito.

¹ (Clarke y Eck 2003, 120)

² (Calvo 2009)

³ (Jurídica 2014)

En cualquiera de las dos funciones de los CCTV, la participación activa de los cuerpos policiales es un requisito indispensable para obtener buenos resultados en la reducción, prevención o persecución del delito, pues los sistemas de videovigilancia son una herramienta tecnológica que deben desarrollarse dentro de una política de seguridad integral. *“La videovigilancia no puede operar como un elemento aislado, porque su virtud y funcionalidad dependerá de la infraestructura, la lógica y la integración a los sistemas correspondientes de prevención, respuesta e inteligencia; caso contrario su eficiencia será baja e incluso, nula”* (Carrión Mena 2008, 1).

La policía vendría a ser el ente encargado de asegurar el cumplimiento y sometimiento de todos los individuos a la ley para que la convivencia dentro de los espacios públicos pueda llevarse a cabo, permitiendo el desarrollo social y humano de cada individuo. Si bien es cierto, el Estado con sus potestades administrativas puede utilizar las cámaras de videovigilancia con fines preventivos de orden y seguridad pública, es necesario que tales sistemas cuenten con requerimientos mínimos que se ajusten a los estándares exigidos en la normas de protección de datos personales, de tal manera que la utilización de estos sistemas no resulten intrusivos en la intimidad o privacidad de los ciudadanos, y que, por el contrario, garanticen el ejercicio genuino de los mismos.

Los Estados tienen la obligación de proporcionar la seguridad a sus habitantes y mantener el orden dentro de la sociedad, pues sin ambos sería imposible la convivencia humana. En un Estado democrático, los ciudadanos otorgan estas potestades al Estado, para que las proporcione y las garantice. Bajo esta línea de ideas las instituciones estatales que promueven los sistemas de videovigilancia, deben sustentar la necesidad de su implementación y verificar que su uso aporta soluciones al problema de la inseguridad.

La delincuencia es un hecho social inherente a toda sociedad, y existen diferentes instrumentos que permiten cuantificarla, describirla y analizarla. Las estadísticas judiciales y policiales que se obtienen de los delitos denunciados, enjuiciados y los sentenciados reflejan, en parte, las condiciones de inseguridad del país y suministran datos reales y verídicos de la cotidianeidad del delito y su incidencia (Murriá y González 2010, 3).

También se utilizan otro tipo de estadísticas como las encuestas de victimización e inculpaación, sin embargo, son encuestas con una dimensión subjetiva, basadas en la opinión del ciudadano sobre temas de seguridad. Este tipo de datos maximizan las dimensiones del problema, pues están basadas en opiniones, sentimientos de inseguridad y vivencias subjetivas de la población respecto a la seguridad; datos basados en la percepción ciudadana pueden variar sustancialmente los registros criminales. Sumando a ello, los medios de comunicación tienen gran influencia en la percepción ciudadana pues la información seleccionada o las noticias transmitidas se enfocan en sucesos delictivos (homicidios, robos, asaltos, etc., agudizando el sentimiento de inseguridad en la ciudadanía.

Con el pasar del tiempo, el debate de la seguridad ha sufrido una metamorfosis donde el concepto de seguridad pública se cambió por el de la seguridad ciudadana, argumentando que ésta última implica la convivencia constitucional. Por un lado, la seguridad pública sufrió un debilitamiento ante la inoperancia de los gobiernos, de que por sí solos, lograrán reducir la inseguridad; y, por otro lado, el discurso de la seguridad orientado hacia el ciudadano tomó fuerza principalmente por la posibilidad de inclusión social del ciudadano, en participar en el campo de la seguridad. Los sistemas de videovigilancia son una estrategia que nacen y forman parte de los cambios sufridos en las políticas de seguridad. En este contexto, surgen como una herramienta policial consignada a establecer el orden, el control y la seguridad de los espacios públicos, tanto en la administración del espacio como en la reducción de los riesgos y la prevención delictiva.

A continuación, se hace mención de algunas investigaciones que demostraron los aportes beneficios de los sistemas de videovigilancia en el mejoramiento de la seguridad.

1.3 Los aportes de los sistemas de videovigilancia en materia de seguridad.

La gran mayoría de las autoridades estatales que promueven los sistemas de videovigilancia señalan que el propósito principal de estos sistemas es fortalecer la seguridad de los espacios públicos. En el año 2003, referente a los sistemas de videovigilancia en Londres, el Secretario de Interior Michael Howard aseguró que: *“Las cámaras de circuito cerrado de*

televisión atrapan a criminales. Ven los delitos, identifican a los delincuentes y contribuyen a la captura de los culpables. La difusión de esta tecnología significa que más centros urbanos, recintos comerciales, espacios de negocios y zonas de aparcamiento se convertirán en zonas donde los delincuentes no osarán entrar (...) la videovigilancia es un maravilloso complemento tecnológico al trabajo policial (...) un policía de Liverpool afirmaba que su sistema de veinte cámaras era como tener veinte agentes más de servicio 24 horas al día, tomando notas de forma constante”¹.

Otras investigaciones han hecho énfasis en la efectividad de estos sistemas, la incidencia que han tenido en los índices de criminalidad y, en general, los aspectos positivos que despliegan estos sistemas. Los resultados de los sistemas de videovigilancia señalados por los diferentes ciudades y países varían según la sociedad en la que se desarrollan. A continuación, se mencionan algunos resultados positivos de los CCTV en el tema de la seguridad.

Los reconocidos investigadores de la criminología española Cerezo y Díez Ripollés, realizaron un estudio en abril del 2007 donde se evaluó la eficacia de cuarenta y un cámaras de videovigilancia colocadas en el Centro histórico de Málaga, con énfasis al desplazamiento del delito. La metodología de la investigación fue cuantitativa y cualitativa, para ello se tomaron datos delictivos procedentes de registros oficiales, encuestas de victimización y entrevistas a comerciantes e incluso a los operadores del sistema de videovigilancia. La investigación analiza dos períodos, antes y después de la instalación de las cámaras. La investigación analizó seis mil doscientos cuarenta y cinco delitos, en los que se distribuyeron geográficamente las infracciones en dos áreas: área de tratamiento (calles con cámaras y calles cercanas a las cámaras) y un área de control (calles con características similares a las calles con cámaras y calles con características similares a las calles cerca de cámaras).

De la investigación se derivan los siguientes resultados: *“con la instalación de las cámaras se observa una disminución del delito de 1,9% en las 10 calles con cámaras. También parece que la estadística general sobre los delitos en la ciudad de Málaga es de disminución entre las dos épocas de estudio, ya que en las calles cercanas a las cámaras ha habido una disminución de la delincuencia del 1,4%. La tasa de victimización general comparando los dos*

¹ (C. Norris 2003)

períodos de estudio se ha visto reducida. Se ha producido un ligero descenso del índice de victimización entre los años 2006 y 2008: de una tasa de 20,2% de malagueños que aseguran haber sufrido un delito durante los últimos 12 meses (2006) se reduce a una tasa de victimización de 19,4% que afirmaron lo mismo en la segunda encuesta realizada en marzo del 2008. Los autores concluyen que la existencia de las cámaras en algunas calles del centro histórico ofrece a los comerciantes una mayor tranquilidad; se aprecia una opinión favorable hacia la instalación de las cámaras por parte de los vecinos y, particularmente, de los comerciantes de la zona videovigilada. Se confirmó un descenso poco significativo principalmente en delitos contra la propiedad, según las tasas policiales y las encuestas de victimización, pero también un efecto de desplazamiento de la delincuencia, comprobaron que había un ligero decremento del índice de victimización entre los años 2006 y 2008 (Díez Ripollés y Cerezo Domínguez 2010)”¹.

Otro efecto positivo que tienen las cámaras de videovigilancia es influencia sobre la delincuencia premeditada. La existencia de vigilancia en ciertos lugares fue un factor para que determinados delincuentes no perpetuaran la comisión del delito, puesto que le tomaban interés al hecho de ser grabados; es decir que existe una conexión entre la vigilancia y la elección racional que influye en el comportamiento del delincuente y disuade su propósito de delinquir.

Los investigadores Brandon C. Welsh y David P. Farrington² realizaron un estudio en el año 2002, en el cual evaluaron la evidencia sobre la eficacia de los CCTV en la prevención de la delincuencia en Estados Unidos y Reino Unido. La investigación tiene dos objetivos principales: informar los resultados de una revisión sistemática (la incorporación de técnicas de meta análisis) de la evidencia de la investigación disponible sobre los efectos de circuito cerrado de televisión sobre la delincuencia, e informar la política pública y la práctica de la prevención del delito mediante el uso de intervenciones de CCTV. Las 22 evaluaciones se llevaron a cabo en tres escenarios principales: en el centro de la ciudad o vecindarios públicos, transporte público y aparcamientos. De los resultados obtenidos se concluyó lo siguiente: de las 22 evaluaciones incluidas, la mitad (11) encontraron un efecto deseable sobre el crimen y en cinco se encontró un

¹ (Urpina 2013, 19)

² (Welsh y Farrington 2002) y (Gill y Spriggs 2005)

efecto indeseable sobre el crimen¹. En cinco evaluaciones se encontró un efecto nulo sobre el delito (es decir, una clara evidencia de ningún efecto), mientras que el restante fue clasificado como la búsqueda de un efecto incierto sobre el delito (es decir, la evidencia de un efecto claro).

Los resultados del meta análisis proporcionan una imagen más clara de la eficacia de los CCTV y la prevención del delito. El estudio mostró que, de las dieciocho evaluaciones, la mitad (nueve) mostró pruebas de un efecto deseable de CCTV con el crimen. Por el contrario, los otros nueve estudios no mostraron evidencia de ningún efecto deseable del CCTV con el crimen. Los cinco estudios norteamericanos estaban en este grupo y los otros cuatro del Reino Unido no proporcionaron los datos necesarios para ser incluidos en el meta análisis. Se concluyó que los CCTV tuvieron un efecto significativo sobre la delincuencia deseable, sin embargo, la reducción general de la delincuencia en un lugar pequeño fue apenas de un cuatro por ciento (Cerezo Domínguez y Díez Ripollés 2009, 17).

El meta-análisis también examinó el efecto de los CCTV sobre los tipos de delitos más frecuentemente medidos. Se encontró que el circuito cerrado de televisión no tuvo ningún efecto sobre los crímenes violentos (de cinco estudios), pero tuvo un efecto deseable significativo sobre los crímenes de robo y hurto de vehículos (de ocho estudios).

En cuanto a la prevención del delito en las tres zonas de estudio, estos fueron los resultados. En el centro de la ciudad y los vecindarios, las pruebas mostraron que los CCTV llevaron a una reducción insignificante del delito del dos por ciento en las zonas experimentales en comparación con las áreas de control. En el Reino Unido, los CCTV tuvieron un efecto pequeño pero significativo sobre la delincuencia. De las cinco evaluaciones tres fueron deseables y dos no deseable. De las cuatro evaluaciones realizadas en América del Norte, ninguna tuvo efecto sobre la delincuencia.

Las cuatro evaluaciones de los CCTV en los sistemas de transporte públicos presentan pruebas contradictorias de la eficacia: dos encontraron un efecto deseable, uno no encontró ningún efecto, y uno encontró un efecto indeseable sobre el crimen. Para los dos estudios efectivos, el uso de otras intervenciones hace que sea difícil decir con certeza que los CCTV produjeron las reducciones observadas del crimen. El tamaño del efecto combinado de los cuatro

¹ (Macarena y Prosser L. 2009)

estudios era deseable (una reducción del seis por ciento en áreas experimentales en comparación con las áreas de control), pero no significativa.

En aparcamientos, había indicios de que CCTV condujo a una reducción estadísticamente significativa en el delito de alrededor del cuarenta y un por ciento en áreas experimentales en comparación con las áreas de control. Sin embargo, en estos estudios había otras medidas que estaban en funcionamiento al mismo tiempo que los CCTV. *“Según la revisión sistemática que realizaron Welsh y Farrington se concluyó que la videovigilancia produce un efecto significativo, aunque limitado, en la prevención del delito. Los CCTV resultan más eficaces en los estacionamientos en el Reino Unido, concretamente en la prevención del robo en y de vehículos (investigación del 2007)”*¹ (Lío 2015, 284-285).

Medina concuerda con los investigadores, pues afirma que *“los únicos estudios que demuestran un impacto positivo es cuando se trata de cámaras de vigilancia en sitios concretos como aparcamientos o determinados establecimientos comerciales, donde sí ha servido para reducir hurtos”*². La autora también señala el efecto positivo que han tenido los CCTV en la reducción de accidentes de tráfico en carreteras.

Distintas investigaciones sugieren que la efectividad de la videovigilancia depende de una serie de factores, que en conjunto complementan el mejoramiento de la seguridad (Galdon-Clavell 2015, 86). El primero de ellos señala que entre mayor cobertura espacial haya, mejores resultados se obtendrán con los CCTV dentro de las áreas controladas, por ejemplo en estacionamientos o edificios; además para que estos sistema se consideren óptimos requieren de una cobertura amplia, y la cobertura depende no solo de la cantidad de cámaras instaladas, sino también de otros factores como la organización en la sala de mando, la buena comunicación con los cuerpos policiales, el despliegue y la efectividad policial, etc³. Otra investigación realizada por Martín Gill y Ángela Spriggs en el año 2005, de igual forma señalan que la videovigilancia tiene mejores resultados en espacios restringidos y con un acceso controlado (Gill y Spriggs 2005).

¹ (Varona Martínez 2012, 39)

² (País 2011)

³ (Welsh y Farrington 2008)

Las mejoras en la iluminación de las calles son otro factor complementario de los CCTV pues redujeron significativamente los hechos delictivos; las mejoras del alumbrado público ocasionaron un aumento de orgullo de la comunidad, además de la inversión que se le inyecte a la zona, así como la recuperación de zonas comerciales que antes estaban desoladas y que eran peligrosas; pero también se logró comprobar que la efectividad de estos sistemas incrementa con la colaboración de los cuerpos policiales¹.

El incremento del patrullaje continuo de determinadas zonas por parte de los cuerpos policiales funciona dentro de la prevención situacional. La efectividad de la vigilancia formal se focaliza en los llamados “lugares calientes” o “zonas rojas”. El patrullaje aleatorio específicamente es estos lugares ha tenido un impacto sobre la comisión de delitos, así como los arrestos y la solución de problemas en estas zonas. Los autores Braga y Andrew concluyen en su estudio que la policía *“puede maximizar la reducción del desorden y delincuencia en puntos calientes al hacer patrullajes focalizados, aleatorios e intermitentes, con una permanencia de entre 10 y 15 minutos en el lugar, haciendo así máximo la disuasión y minimizando el tiempo innecesario gastado en estos lugares”*².

Un estudio desarrollado en Estados Unidos por el experto Joel Caplan³ introduce el Modelo de Terreno de Riesgo (RTM, por sus siglas en inglés: Risk Terrain Modeling) que básicamente lo que propone es la realización de un estudio previo a la instalación de las cámaras para valorar el impacto de los riesgos contextuales de un determinado lugar. Caplan *“centrándose en las agresiones y los delitos contra la propiedad, concluye que las cámaras poseen un efecto preventivo menor en zonas con valores altos de concentración de riesgos, de forma que la falta de eficacia de las cámaras no es totalmente atribuible a las mismas”*⁴. Se consideran otras alternativas accesorias como mejoras en la iluminación, en el diseño arquitectónico, estrategias de reducción de la delincuencia como presencia policial centrada en espacios concretos, que en conjunto con las cámaras *“proporciona una perspectiva multidimensional que puede incrementar la capacidad disuasoria de las cámaras en la prevención de la delincuencia”*.

¹ (Farrington y Welsh 2007)

² (Braga y Andrew 2012) mencionado por (Mertz 2013)

³ (Caplan y Kennedy 2009) mencionado por (Varona Martínez 2012, 42)

⁴ (Emirhan 2012) mencionado por (Varona Martínez 2012, 42)

Las investigaciones realizadas por la Organización Nacro, encontraron un vínculo causal entre el uso de CCTV y la reducción de crímenes, específicamente en los delitos asociados a la propiedad (hurtos y robos en estacionamientos) y en las infracciones de estacionamiento de vehículos¹. En el caso de Londres los CCTV han influido específicamente en tres tipos de delitos: homicidios, asaltos y delitos contra la propiedad. Según las estadísticas de la capital entre 2000 y 2010 los homicidios pasaron de ciento noventa a ciento trece por año, lo que representa una reducción del cuarenta por ciento, los asaltos pasaron de 77.083 a 43.571 por años, un cuarenta y tres por ciento menos, en cuanto a los delitos contra la propiedad pasaron de 115.027 a 33.480, lo que implica un setenta y un por ciento menos².

Otro aporte de los CCTV, ha sido su efectividad para la resolución de crímenes, específicamente para identificar a los presuntos imputados; esto se evidencia en distintos países. Por ejemplo, Barcelona, España “las cámaras permitieron a las autoridades encontrar a un hombre español que atacó agresivamente a un hombre latinoamericano en el metro”³. En los atentados suicidas del 7 de junio del 2005 en Londres, se realizó una investigación exhaustiva de todas las grabaciones de personas y lugares mínimamente relacionadas al ataque. *“Una de las 76 cámaras instaladas en la estación de King’s Cross dio la clave; uno de los policías del equipo de rastreo advirtió de 4 hombres que caminaban de dos en dos por el pasillo de un supermercado. Se realizó la comparación de rostros con las fotografías de los carnets de conducir y fue suficiente para identificarlos”⁴*.

En Bolivia, en la ciudad de El Alto, se detectan en promedio veinticinco delitos diarios. Los CCTV detectaron en el 2013, entre marzo y noviembre tres mil trescientos cuarenta y cinco delitos en los que participaron siete mil setecientos veintinueve individuos que incurrieron en algún tipo de ilícito. En el año 2014, entre enero y febrero las cámaras filmaron mil doscientos delitos. Al ser una “zona roja” de peligro los delitos más recurrentes son la venta y consumo de drogas, las riñas, asaltos y robos. El ente policial de la zona señala que por medio de los CCTV

¹ (NACRO 2002) mencionado por (Carli 2008)

² (Inglaterra , el país que combate el crimen sin armas 2012)

³ (Cambon 2007)

⁴ (Coyle 2011)

se ha logrado identificar a los involucrados así como el *modus operandi* de los ladrones e incluso asesinos¹.

En Colombia se data de tres casos importantes en los que la información aportada por medio de la videovigilancia fue esencial para dilucidar a los culpables de los delitos. El primero en mayo de 2012, un menor de edad puso una bomba tipo lapa en el vehículo del exministro Fernando Londoño. Las cámaras capturaron al sospechoso en el sector donde ocurrió el atentado. En julio de 2011 se logró la identificación de 6 taxistas que participaron en el asesinato del agente de la DEA James “Terry” Watson, al norte de Bogotá. Y, por último, el caso de Jonathan Vega quien atacó con ácido a Natalia de Ponce de León en marzo del 2012. Todos estos casos se lograron resolver gracias a la información recabada de los sistemas de videovigilancia².

Otro aspecto importante que señala Don Bawin respecto al uso de los sistemas de videovigilancia y la sustitución del recurso humano, es que, a diferencia del personal de seguridad, “las cámaras no están sujetas a fatiga o pérdida de concentración y, por lo tanto, proporcionan un esfuerzo ininterrumpido y consistente. Entonces, la carga financiera de comprar e instalar el sistema es contrarrestada por su efectividad a largo plazo, en contraste con la contratación de oficiales de policía adicionales que pueden ser menos costosos. Además, los sistemas de CCTV son también una herramienta clave para ayudar a las fuerzas policiales a resolver crímenes”³.

Para otros autores la videovigilancia constituye un complemento útil para el trabajo policial. Heidi Mork Lomell “*sugiere que los sistemas de CCTV no son un reemplazo de la fuerza policial, pero sí mejora su trabajo. En este caso, estos sistemas son más efectivos cuando son utilizados en conjunto con otras medidas de reducción del crimen como el patrullaje policial*”⁴. Para Valverde “*es indudable que desde el punto de vista de la seguridad ciudadana y de la prevención de delitos por medio de la videovigilancia, estos sistemas pueden ser un medio*

¹ (Entrevista a Rodrigo Guaraya 2014)

² (16 meses, cámaras de seguridad llevaron a 8 mil capturas 2014)

³ (Bawin 2007) mencionado por (Carli 2008, 10)

⁴ (Mork Lomell 2004) mencionado por (Carli 2008)

eficaz, igual que puede serlo posteriormente como prueba material de la comisión y de la autoría de un hecho delictivo cometido en esos espacios públicos¹”.

De los estudios investigativos que se han realizado en la materia se desprenden diferentes conclusiones, algunas indican los beneficios que se obtienen con los sistemas de videovigilancia en el tema de la seguridad, y otros efectos negativos que se desprenden a partir de ella.

La vigilancia de los espacios públicos por medio de cámaras de seguridad, es una actividad que debe estar conferida por un marco legal, a partir del cual se cumpla con el principio de legalidad y se faculte a la Administración Pública las potestades para emplear las cámaras con fines policiales y delictivos. Por involucrar derechos con rango constitucional (privacidad y seguridad), la norma que regule la actividad de vigilancia pública debería regirse por el principio de reserva de ley. Esto implicaría deberes y prohibiciones para los responsables del tratamiento de datos, así como la posibilidad de ejercer los derechos de autodeterminación por parte de los ciudadanos. La legislación además de incorporar principios rectores en la actividad de la videovigilancia, vendría a establecer límites a las prácticas abusivas como la falta de información o consentimiento en el tratamiento de datos por parte de las autoridades públicas. El ejercicio de las buenas prácticas como la *privacy by design*, permiten la convivencia de ambos derechos: a la seguridad y a la privacidad.

Los límites de la videovigilancia pública estarían definidos por ley. El principio de legalidad le otorga las facultades a la Administración de utilizar los sistemas de videovigilancia para prevenir y perseguir los delitos, así como ejercer mayor control y seguridad en los espacios y las personas, sin embargo, esta actuación debe estar pautada por prácticas que protejan al ciudadano frente a las potestades de imperio del Estado, ofreciendo la posibilidad al ciudadano de ejercer los derechos relativos a la protección de datos personales y autodeterminación informativa, como defensa ante los posibles abusos o arbitrariedades por parte de las autoridades estatales. Queda claro que los programas de videovigilancia forman parte de las políticas de prevención con un enfoque integral y transversal a fin de generar mayor seguridad en la ciudadanía, u cuyo fin debe girar en torno a los ciudadanos y estar al servicio de los mismos.

¹ (Valverde Espinoza 2013)

En la próxima sección se desarrolla la otra perspectiva que surge con la utilización de las cámaras de videovigilancia. Desde este punto de vista, los sistemas de videovigilancia ubicados en espacios públicos son una medida de seguridad invasiva que incide sobre los derechos de privacidad, imagen y protección de datos personales, sea por motivos relacionados a prácticas abusivas y/o desproporcionadas en el uso de las cámaras, falta de normativa que regule la actividad y la existencia de evaluaciones que descartan la eficacia de las cámaras en la prevención, reducción o persecución de la delincuencia. Para los detractores de estos sistemas, el uso policial de las cámaras maximiza de manera injustificada el control represivo del Estado sobre los espacios y las personas.

Sección segunda: La incidencia que tienen los Sistemas de Videovigilancia sobre los derechos de intimidad, propia imagen y la protección de datos personales

La discusión que gira entorno a los sistemas de videovigilancia plantea una restricción a los derechos de vida privada, principalmente porque la videovigilancia involucra la captación y/o grabación de información personal en forma de imágenes. Es decir, las personas son representadas a través de imágenes y con ello es posible su identificación. Esta situación no solo vulnera el anonimato de las personas cuando transitan en lugares públicos, sino que propicia una invasión a la intimidad de estos individuos. La necesidad de regular la aplicación y tratamiento de los CCTV se hace aún mayor, pues el indebido uso de ellos afecta los derechos a la intimidad, propia imagen y la protección de los datos personales.

A continuación, se expondrá la incidencia que tienen los CCTV sobre los derechos individuales concernientes a la vida privada de la persona, especialmente cuando estos se desarrollan como una medida de seguridad aislada a la protección y respeto de las libertades individuales. Los derechos que se verán a continuación, son derechos denominados doctrinalmente derechos de la personalidad, se caracterizan porque *“suponen la atribución de un poder a su titular para que lo ejerza y lo defienda, quedando así, la protección y la tutela jurídica del interés protegido a disposición del sujeto¹”*.

2.1 El derecho a la privacidad.

La transformación social que surge a partir del vertiginoso desarrollo tecnológico y la Era de información, lanza una advertencia y a la vez un reto que obliga a repensar los alcances y usos de la tecnología en la cotidianeidad de nuestra sociedad. Con la incorporación de la tecnología, la interconexión de la información está cada vez más a la mano de las empresas públicas o privadas que se dedican a recolectar y utilizar nuestra información con fines muy variados. Las cámaras de seguridad son un ejemplo de ello, la sociedad panóptica se ha hecho una realidad y está presente en la vida de los ciudadanos, quienes se han “acostumbrado” a

¹ (De Lamo Merlini s.f., 14)

convivir y transitar con la presencia de las cámaras. La gran parte de los ciudadanos se han adaptado muy bien a esta “convivencia tecnológica”, sin dudar de los riesgos o alcances que tiene la misma sobre la vida personal de cada uno. *“Si partimos de que en sí misma la tecnología de la información es peligrosa, que es esencialmente el lado opuesto de la intimidad de la persona, y que por encima de los usos positivos que se le puedan extraer ya representa una amenaza, -al igual que lo entendemos sin dificultad para el caso de las armas de guerra en relación con la vida-, no escatimaríamos en desplegar esfuerzos para proteger a las personas del manejo de sus datos, entenderíamos que no se trata de un problema individual o sectorial, sino social, y que las soluciones deben pasar desde la educación y la prevención hasta el castigo¹”.*

Lo que queremos decir es que el uso de la tecnología potencia el manejo y el tratamiento de datos personales, lo que conlleva un peligro para la esfera privada de los individuos, y por ello es necesario, que los responsables del tratamiento de datos, así como los ciudadanos tenga interés en construir políticas que resguarden la privacidad y los datos personales de los posibles afectados. Ahora bien, esta reflexión orientada a analizar y delimitar los desarrollos perniciosos de la tecnología moderna y proteger la privacidad de los ciudadanos, ha progresado sobre todo en los países europeos, poniendo sobre la mesa debates en torno a esta problemática. Por el contrario, Cassese señala que en América Latina los problemas de privacidad que surgen con el desarrollo de la tecnología le han tomado poca importancia, propiciando el desarrollo tecnológico y haciéndolo deseable, en consecuencia, los intentos por propugnar restricciones a los usos de la tecnología han sido escasos².

La privacidad es un derecho fundamental que es inherente a la persona humana y se encuentra ligada al desarrollo y gesta de su propia personalidad e identidad, es de vital importancia que “cada quien cuente con un área que se encuentre libre de la intromisión de extraños que comprenda ciertos aspectos de su vida individual como familiar³”.

¹ (Camacho 2004, 145)

² (Cassese 1991) mencionado por (Camacho 2004, 146)

³ (De Dienheim Barriguete 2001)

El respeto a la vida privada de las personas, está consagrado en los tratados internacionales y las normas constitucionales, sea en mención del derecho a la intimidad o el derecho a la privacidad. En sus diferentes acepciones, la protección legal enmarca la privacidad, la inviolabilidad del domicilio, la correspondencia, las comunicaciones privadas, la propia imagen, el honor, la privacidad informática, el derecho a no ser molestado, entre otros. En relación a este derecho fundamental existen un sin fin de normas internacionales y nacionales que lo tutelan.

Para Morales Godo, el derecho a la intimidad se divide en tres puntos importantes, primero, la tranquilidad que se refiere al “derecho de ser dejado solo y tranquilo” o “ser dejado en paz¹”. El control de la información que se refiere a la autodeterminación informativa; esta tiene dos aspectos: “la posibilidad de mantener ocultos algunos aspectos de la vida íntima”, y segundo “la posibilidad de controlar el manejo y circulación de la información, cuando ha sido confiada a un tercero” y finalmente la autonomía que consiste en la capacidad de elección, de libertad en la toma de decisiones, sin que otros puedan interferir, manipular o chantajear. “*Está referida a la libertad del ser humano para la toma de decisiones respecto a su vida sin interferencias directas, indirectas o sublimadas*”².

En la sociedad moderna que vivimos, el contacto directo y diario que tenemos con la tecnología hace que nuestra privacidad corra peligro sobretodo porque existe una tendencia a expandir sus usos y mejorar la calidad y eficiencia de la misma. El uso e incidencia de la tecnología sobre la privacidad de las personas es un fenómeno que afecta a millones de individuos a la vez pues la recopilación de datos personales es una cuestión que sucede a diario; los dispositivos tecnológicos se perfeccionan en sus diseños para tener mayor capacidad y alcance, todo esto influye sobre los comportamientos de los ciudadanos³.

¹ Fue utilizado por primera vez en la jurisprudencia norteamericana del caso “Olmstead vs. United States” en la década de los 20 por el juez Cooley. “Es el derecho que tiene toda persona a disponer de momentos de soledad, recogimiento y quietud que le permiten replegarse sobre sí mismo. El derecho a llevar una vida en el anonimato, libre de la malsana curiosidad de los demás”

² (Morales Godo 2007, 68)

³ (Pouillet, Pérez Asinari y Palazzi 2009, 89) mencionado por (Rodríguez Steller 2016, 26)

Las cámaras de videovigilancia colocadas en lugares públicos presentan un conflicto, pues permiten la grabación y la captación de conductas que, aunque se realizan en lugares públicos se presumen un anonimato social¹. La captación, el almacenamiento y la posterior difusión de éstas y otras imágenes viola el derecho a la privacidad pues la captación de las imágenes corresponde al ámbito de autonomía de una persona y puede transformarse en una violación al derecho a la privacidad.

En este sentido, el derecho a la privacidad no es exclusivo del ámbito familiar o doméstico. Este derecho acompaña al individuo, solo que en diferentes niveles. Por ejemplo, no se tiene la misma privacidad en la calle que en la sala o comedor de la casa. Cuando nos trasladamos de un lugar a otro, o transitamos en los espacios públicos no pensamos que estamos siendo observados por un tercero o creemos tener cierto grado de privacidad y anonimato cuando realizamos nuestras actividades en la vía pública². La Comisión Europea para la Democracia señala que en el caso de la videovigilancia en el “espacio público los individuos esperan un menor nivel de privacidad, aunque no esperarían ser privados de sus derechos y libertades en sus propias esferas privadas e imagen”³. Al ser considerada la esfera privada como inviolable, no debe ser sujeto de intrusión sin haber una causa que la justifique.

Si bien es cierto los sistemas de videovigilancia son utilizados como una medida de seguridad en los espacios públicos, su propia naturaleza socava este derecho por distintas razones. Además de perder el anonimato dentro de los espacios públicos como se mencionó anteriormente, los individuos quedan expuestos o visibles ante el ojo atento del Estado (Goold 2010, 29). La vigilancia constante y generalizada que se realiza por parte del Estado representa una intrusión a la privacidad de los ciudadanos, que, en ocasiones, no saben tan siquiera que están siendo observados. La gran mayoría de estos proyectos carecen del principio de información, sobre todo, cuando los espacios públicos son amplios y la visibilidad e información de las cámaras se minimiza (por ejemplo, los parques o plazas).

¹ (Caso Peck contra Reino Unido 2003)

² (Goold 2010, 28)

³ (Commission) 2007) mencionado por (Carli 2008, 4)

La capacidad que tienen los CCTV permite que la vigilancia sea continua y generalizada. La continuidad se refiere al tiempo, es decir, vigilancia ininterrumpida por 24 horas al día y 7 días a la semana, y la segunda hace referencia a la indiscriminación de las personas, es decir, toda persona que transite por estos espacios será sometida a vigilancia, sin importar que su comportamiento o actitudes sean normales, sospechosas o bien delictivas. *“Las autoridades utilizan también los mecanismos de las tecnologías de la información y la comunicación para vigilar y controlar a los ciudadanos, en una red que no diferencia entre personas respetuosas de la ley y aquellos sospechosos de cometer un delito¹”*

Los CCTV a diferencia de la vigilancia física (presencia policial), permiten monitorear a mayor escala las actividades que se realizan dentro de estos espacios. Pueden detectar el movimiento, además pueden complementarse con programas capaces de analizar conductas irregulares y bases de datos para identificar personas, están en una posición beneficiosa (ubicadas en domos o estructuras altas), permiten almacenar la información, lo que implica que la información pasada es fácil de acceder.

Por el contrario, la vigilancia física carece de estos elementos. Es una vigilancia limitada a las capacidades humanas, lo que implica horas de descanso para el vigilante, limitaciones visuales propias del ojo humano, la información es susceptible a la percepción e interpretación humana, por lo que puede resultar contradictoria (diferentes versiones de los testigos, relatos alterados, o mentiras, etc.). *“El primer tipo de innovación es cuantitativo: el alcance de estos ojos electrónicos es mucho más penetrante y omnipresente. El segundo tipo es cualitativo: la tecnología del reconocimiento facial y la digitalización de la información, conectada a una base de datos central, ofrecen la perspectiva de un desplazamiento: desde los propósitos defensivos o de seguridad pasiva, en los que se ha empleado básicamente hasta ahora esta tecnología, hasta una nueva era de identificación activa y de localización de individuos²”*.

No hay duda de que los sistemas de videovigilancia han invadido cada vez más el espacio público. A medida que se intensifica el uso de ellos, más se propensa el derecho a la privacidad en diversos aspectos que se explican a continuación.

¹ (Carvajal Pérez y Chirino Sánchez 2003, 4)

² (Whitaker 1999, 103)

Cualquier persona que transite por las áreas bajo vigilancia queda sometida a la misma, esté o no apercebido del funcionamiento de las cámaras. Los CCTV recopilan la información de manera generalizada, grabando las actividades y comportamientos de los ciudadanos, aun cuando estos no son delictivos ni sospechosos, sino consideradas normales. Si bien es cierto, la información de los datos personales queda grabada y almacenada únicamente bajo fines de una eventual persecución del delito, se genera una incertidumbre que pone en tela de duda en mano de quién están nuestros datos personales, quien tiene acceso a ellos o si serán utilizados correctamente.

Al respecto, explica Choclán Montalvo: *“Desde luego que lo que, en modo alguno, estaría legitimado es una disposición continuada de cámaras de vídeo para filmar la generalidad de los actos que todas las personas que transiten por la zona puedan desarrollar un determinado espacio público sin que concurran indicios fundados de que se va a cometer un delito -funciones de prevención- o de que se esté cometiendo -funciones de represión y defensa del orden-, pues, un sistema de vigilancia indiscriminada de las actividades de los ciudadanos en general por parte de la autoridad pública, constituiría una injerencia prohibida en el ámbito de la intimidad que comprende las manifestaciones públicas de la vida privada¹”*.

Los CCTV permiten almacenar y recopilar información sobre la vida privada de las personas. Por ejemplo, con un sistema integrado de cámaras es posible seguir a una persona, la información recopilada puede detectar el momento, el lugar y hasta la compañía de una persona (con quién estaba la persona, los lugares que visitó, las actividades que realizó, cuál fue su ruta o lugares visitados, entre otros)². En este sentido, la información es almacenada sin el consentimiento pleno de la persona, poniendo en riesgo datos de su vida privada, los cuales pueden, eventualmente, ser publicados, hackeados o utilizados con propósitos no policiales. Sin embargo, el tema de la protección de datos se analizará con detalle más adelante.

La instalación de las cámaras de seguridad en los espacios públicos, limitan el derecho de libertad de vida privada de cada persona. El derecho a la libertad es un concepto sumamente amplio. Para efectos de este trabajo es necesario conceptualizar el ejercicio de ese derecho como

¹ (Choclán Montalvo 1995) mencionado por (Cornelis 2015, 17)

² (De Arriba Coro 2018)

la libre decisión y disposición que tiene el individuo de determinarse a hacer o no hacer algo, o de disponer o no de su imagen o vida privada. La libertad de decidir si se quiere o no ser grabado, de que sus datos sean almacenados en una base de datos o bien sometidos a análisis comparativos, es un derecho limitado. Con la videovigilancia masiva e indiscriminada, los ciudadanos que transitan por los espacios vigilados no tienen la alternativa o determinación de escoger ser o no vigilados, y, consecuentemente, decidir el almacenamiento de sus datos personales.

En cuanto a la privacidad de los datos recopilados, los encargados o responsables del tratamiento de datos tienen la obligación de guardar secreto y confidencialidad de la información, también deben resguardar los datos con mecanismos que eviten su divulgación o fuga, finalmente, sólo pueden utilizar la información para los fines por los cuales se recopilan. Como señala Vincenzo Ricciuto *“de la privacidad, entendida como el rechazo a dar conocer a terceros aspectos de la propia persona, se ha llegado a hablar de un derecho a que los aspectos de la propia persona conocidos por terceros no sean utilizados con finalidades de discriminación y, en consecuencia, de un derecho a que las informaciones personales pasen de ser secretas a ser controlables¹”*.

Con los CCTV, la información personal pasa a ser controlada por las autoridades públicas, con el almacenamiento, la circulación, el cotejo y el eventual uso que se le vaya a dar a la información personal del ciudadano bajo vigilancia, perdiéndose de esta manera el secreto de la información personal. Una de las críticas que han surgido alrededor de los sistemas de videovigilancia es en relación al carácter disuasorio que le asocian los cuerpos policiales, en relación a las conductas delictivas en los espacios públicos. Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos, señala que: *“ser observado cambia el modo de comportarse. Por cierto, cuando somos observados muchos de nosotros censuramos lo que decimos o lo que hacemos y ciertamente tal es el efecto de una vigilancia continua y generalizada. Saber que cada movimiento y que cada gesto está controlado por una cámara*

¹ (Ricciuto 2001, 43)

puede tener impacto psicológico y cambiar nuestro comportamiento, lo cual constituye una intrusión en nuestra privacidad¹”.

La función preventiva de los sistemas de videovigilancia se fundamenta en esa característica o efecto disuasivo. Desde el punto de vista práctico, los CCTV son una herramienta tecnológica que le facilita a las autoridades policiales la vigilancia de los espacios públicos, tendientes a prevenir, detectar, desmotivar o evitar la comisión de un delito. Se parte de la premisa, que el delincuente se abstendrá de delinquir dentro de un espacio vigilado por las autoridades policiales y en caso de que lo haga, corre un riesgo mayor de ser detectado e identificado por medio de la prueba digital; en consecuencia, se producirá -casi de manera automática- una reducción de los delitos en los espacios públicos vigilados.

Aunque en el discurso de la seguridad, las cámaras tienen un enfoque en la disuasión de conductas delictivas, la realidad es que las cámaras no distinguen entre el delincuente y el que no lo es. Esto quiere decir que también se vigila al ciudadano común: al anciano, al adulto, a los niños, a la madre y su bebé, a todos; lo que conlleva implicaciones a la privacidad del ciudadano, según lo mencionado: *“las expectativas que genera la videovigilancia, es razonable esperar que algunas personas sientan una aguda pérdida de privacidad y modifiquen su forma de actuar, no porque no crean que estén haciendo algo mal, sino porque no desean llamar la atención de la policía o correr el riesgo de que sus acciones sean malinterpretadas”* (Goold 2010, 30)

Para Koskela, desde el punto de vista sociológico, la vigilancia en los espacios públicos tiene como objetivo “normalizar” el espacio urbano. Ello multiplica el efecto de las normas sociales que contribuyen en el control de la conducta y representa “una visión ordenada y controlada” del espacio público (...) la vigilancia rutinaria del espacio urbano tiene por objeto garantizar la exclusión de la delincuencia o desviación². Las personas que saben que están siendo observadas por las autoridades policiales, actuarán de manera normal procurando pasar inadvertidas ante las cámaras, mantendrán el orden establecido y se abstendrán de cometer cualquier comportamiento desviado o delictivo.

¹ (Buttarelli 2010)

² (Koskela 2003)

Koskela menciona dos efectos que se generan a partir de la videovigilancia: el primero es en relación al espacio físico, al cual le llama “*espacio de coerción*”. La autora manifiesta que, ante la existencia de los CCTV en las ciudades, los ciudadanos mantienen el orden público establecido dentro de los espacios, quienes actúan de manera civilizada y se abstienen de cometer cualquier acto delictivo o desviado; segundo, que la videovigilancia tiene la capacidad de producir un evento emocional sobre la persona vigilada. Para ella, las videocámaras influyen sobre el comportamiento de las personas, positiva o negativamente ya que pueden generar una sensación de seguridad, así como una señal de peligro, a esto le llama “*espacio emocional*”.

Bajo esta línea de ideas, algunos detractores de los sistemas de videovigilancia argumentan que la vigilancia de las ciudades modernas muestra un interesante paralelismo con el modelo del panóptico de vigilancia diseñado por Jeremy Bentham. El “Panóptico electrónico”, como le dicen algunos autores, hace referencia al uso de las nuevas tecnologías de información y comunicación para la vigilancia de las ciudades y poblaciones; el panóptico electrónico se presenta como un discurso o modelo de “*carácter político y sistema social, en una red de vigilancia que combina todo tipo de información: imagen, sonido, datos, huellas digitales, correo electrónico, movimiento, teléfono, ficha genética y patrones de comportamientos*”¹. Esta gama de información le permite a los Estados perfeccionar el control sobre los espacios y las personas.

La vigilancia por medios de cámaras de seguridad es más prolongada, más intensa e íntimamente vinculada al poder del Estado. El objetivo de las videocámaras de los cuerpos policiales es prevenir los comportamientos delictivos y aspira influir sobre aquella población que considera causante de la inseguridad y la violencia, haciéndoles saber que su actuar está siendo observado y evidenciado. Sin embargo, consideramos que el ejercicio de ese control debe enfocarse directamente en el espacio físico y no sobre las personas, pues se convierte en un mecanismo de control social, afectando los derechos de privacidad, imagen y datos personales del resto de ciudadanos.

¹ George Orwell (1984) mencionado por (Godina Herrera 2006)

Uno de los problemas que se generan con el desarrollo de la tecnología en el campo de la videovigilancia, es que se perfila un control social mucho más especializado y técnico, con la capacidad de seleccionar y expandir el escrutinio de poblaciones, grupos y personas. La propuesta de espacios públicos limpios y seguros que pretende obtenerse con los sistemas de videovigilancia, provoca, consecuentemente, una segregación urbana y social. Los CCTV se convierten entonces, en un instrumento tecnológico que reproduce e institucionaliza ciertas lógicas de exclusión social¹. Uno de los retos que enfrentan los operadores de los CCTV es la visualización de gran cantidad de imágenes transmitidas por las cámaras a los monitores, que en la mayoría de las veces no queda más que orientar la mirada sobre aquellos comportamientos o formas de vestir de las personas consideradas “sospechosas” o “extrañas” (por ejemplo, una persona que use un turbante, o algún indigente). De este modo, quienes operan estos sistemas ponen en juego, prejuicios y tipificaciones, orientando su mirada a ciertas personas en particular².

A raíz de la observación tecnológica se genera otra dificultad, que es la construcción de perfiles basados en estereotipos sociales. Con los sistemas de videovigilancia, únicamente se aprecian ciertas representaciones o facetas de la persona, por ejemplo, qué lugares visita o si tiene propensiones al consumo, entre otros. Según Ricciuto, con el tratamiento de los datos personales: *“la persona es distribuida así en las redes, en los bancos de datos inmateriales; no coincide ya con ella misma, porque padece el injerto continuo de mecanismos que alteran su fisonomía y provocan la crisis de la pretensión de autodeterminación (...) la elaboración de perfiles y la reconstrucción de personalidades individuales, efectuadas con medios automatizados y utilizadas para anticiparse a decisiones que impliquen una valoración del comportamiento humano, presenta una lesividad potencial que trasciende la esfera de la tutela de la privacidad y de la identidad personal del interesado para colocarse, seguramente, en una dimensión súper o meta individual. Se ha destacado que tales técnicas podrían alimentar el conformismo, el determinismo, contribuir a ejercitar el control, estigmatizar perfiles “abstractos”, tipo “buen trabajador”, “buen ciudadano”, “persona realmente necesitada de*

¹ (Norris, Moran y Armstrong 1998) mencionado por (Arteaga Botello 2010, 268)

² (C. Norris 2003)

asistencia”, que podrían luego provocar tratos discriminatorios a sujetos que no se correspondan con tales “modelos ideales” (Ricciuto 2001, 45-46).

Lo que sucede con los CCTV es que se pierde el concepto de identidad personal, considerada esta como la representación integral del sujeto. Los operadores de los sistemas de videovigilancia deben analizar gran cantidad de imágenes dentro de los espacios públicos. En este proceso de observación y análisis conductuales influyen, de manera consciente e/o inconsciente, una serie de factores subjetivos, tales como prejuicios o estereotipos sociales.

Por último, otra crítica que han recibido los sistemas de videovigilancia es en relación al ingreso controlado de ciertas minorías a determinados espacios. Los operadores de los centros de mando en conjunto con las fuerzas policiales pueden, a través de la videovigilancia, controlar el ambiente de un determinado lugar, por ejemplo: *“prohibiciones de acceso de colectivos desviados o marginados a ciertos lugares públicos; la exclusión de determinadas actividades en lugares públicos en los que se quiere preservar una imagen atractiva en algún sentido, con prohibiciones de práctica de mendicidad o vagancia, de oferta de servicios, venta callejera o distribución de publicidad a transeúntes, de acampada, bebida de alcohol, descanso o aglomeración, incluso de realización de protestas políticas; y la vigilancia intensiva de actividades o movimientos llevados a cabo en ciertos ámbitos públicos, sean edificios o instalaciones de acceso público, establecimientos comerciales, lugares residenciales, o lugares de tránsito ciudadano” (Cerezo Domínguez y Díez Ripollés 2009, 173).*

Bajo este supuesto, el derecho a la libertad de estas minorías segregadas se ve limitado o desmejorado por un asunto asociado a la seguridad y orden público “disfrazados”. Una de las características del orden público es utilizar métodos de intervención en la esfera de libertad de los particulares con la finalidad de tutelar una seguridad concebida en un sentido muy amplio y vinculada a la seguridad del Estado. En el caso de la videovigilancia, los motivos pueden fundamentarse en problemas de seguridad, percepción ciudadana de la actividad delictiva, o bien, por motivos de eficiencia en las funciones administrativas. La observación espacial que se logra a través de las cámaras le permite a la Administración ejercer un control sobre

determinados espacios, y de manera indirecta sobre sus habitantes, limitando en cierto grado las libertades individuales de los administrados.

En su doble función, la videovigilancia responde a la seguridad pública enfocada en la prevención, reducción y persecución de la delincuencia; y el orden público dirigido al control social, principalmente la sumisión de aquellas conductas desviadas. Es importante aclarar que, para efectos de este enunciado, el control social o espacial que ejercen los sistemas de videovigilancia esta específicamente dirigido a aquellos comportamientos ilícitos o actividades delictivas dentro de los espacios públicos.

El control que ejerce el Estado sobre los espacios y sobre la ciudadanía en general, debe ejercerse únicamente con el fin de garantizar la seguridad pública y el orden público. Las cámaras de videovigilancia, no pueden convertirse en una medida abusiva, que lejos de proteger al ciudadano se convierte en un instrumento en contra de la privacidad y libertad de tránsito. Es necesario que el funcionamiento de estos sistemas se encuentre en armonía con el derecho a la protección de datos personales.

2.2 Derecho a la propia imagen

El derecho a la imagen forma parte de los derechos de la personalidad y se entiende como el “...*derecho a reproducir o representar la figura corpórea de determinada persona, en forma reconocible, con entera independencia del objeto material en que se contiene*”¹. Concepto dentro del cual quedan comprendidas las grabaciones de imágenes obtenidos mediante sistemas de videovigilancia. Este derecho es autónomo, de la personalidad, porque “*contribuye a definir la personalidad haciendo a las persona única, diferente y diferenciable de otras personas*”² y es necesario para el libre desarrollo de la misma.

¹ (Munar Bernart 1995)

² (López Ávila 2014)

El derecho a la imagen involucra la capacidad comunicativa que integra la dignidad personal propia del ser humano y permite la individualidad de la persona¹. El bien jurídico protegido consiste en “*la manifestación, la representación y no la imagen humana en sí misma considerada*”².

Estrada señala que el derecho a la imagen es la “*facultad que el Ordenamiento Jurídico concede a la persona para decidir cuándo, por quién y de qué forma pueden ser captados, reproducidos o publicados sus rasgos fisionómicos reconocibles*”³. La jurisprudencia española, le otorga la facultad de derecho fundamental, que consiste en “*impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad – informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde*”⁴.

Parte de la doctrina ha concebido el derecho a la imagen como un derecho fundamental implícito al derecho a la vida privada, pues consideran a la imagen el aspecto externo más característico y definitorio de la persona. La imagen se convierte en el dato personal más cercano a la identificación de la persona y se vulnera cuando es posible hacer la identificación e individualización del sujeto. En el caso de nuestro país, este derecho se encuentra intrínsecamente consagrado con el artículo que protege el derecho a la vida privada. En Costa Rica, todavía no existe una regulación legal específica del derecho de imagen como tal, sino que la protección de éste derecho se encuentra enmarcado dentro del numeral 24 de la Constitución Política, al señalar que “*Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones (...)*”. La jurisprudencia nacional ha indicado que la imagen forma parte del derecho a la intimidad y que dentro de este artículo se protege la publicación de imágenes sin el consentimiento del titular.

¹ (Azurmendi Adarraga 1997, 22)

² (Vercellone 1959, 10-11) *apud* GITRAMA, “Imagen (derecho a la propia)”, *Nueva Enciclopedia*. cit., p. 304 mencionado por (Rodrigues da Cunha e Cruz 2009)

³ (Estrada 1990, 348)

⁴ (Sentencia 81/2001 2001)

El voto 4819-96 de la Sala Constitucional señala que: *“la libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno, y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas o grabaciones de las conversaciones privadas y en la difusión o divulgación posterior de lo captado y obtenido sin el consentimiento de la persona afectada¹”*.

Por otro lado, están quienes sostienen que, aunque el derecho a la propia imagen tiene vinculaciones con la privacidad en un sentido amplio, debe considerarse como un derecho autónomo. Esta doctrina la siguen países como Alemania, Austria, Finlandia, Portugal, Suecia y España consagran en sus Constituciones de manera expresa este derecho². El Tribunal Constitucional español ha señalado el reconocimiento y protección individual de este derecho con independencia del derecho al honor, la intimidad o la privacidad, pudiendo en ocasiones vulnerarse solo uno de ellos. Para Lara Gamboa, el derecho a la imagen goza de autonomía:

“La imagen no es un bien jurídico del honor ni del secreto personal, ya que la reproducción arbitraria de una figura humana puede no lesionar el honor ni la intimidad de la persona, pero sí podría estar vulnerando el derecho a la imagen” Continúa diciendo *“...que dentro de los derechos de la personalidad se encuentra el derecho a reproducir o representar la figura corpórea de determinada persona, en forma reconocible, con entera independencia del objeto material en que se contiene. Basándome en esta definición podría decirse que el derecho de la imagen no es el derecho a la intimidad, ya que no se trata de que exista espacio reservado alguno, nadi vulnera el derecho a la imagen por conocer aspectos íntimos del sujeto; sin embargo, sí se vulnera el derecho a la intimidad por el conocimiento de aspectos reservados a la intimidad, mientras que se vulnera el derecho a la imagen simplemente por la reproducción de una imagen reconocible sin el consentimiento del titular³”*.

¹ (Voto 1996)

² Por ejemplo, en España el artículo 18.1 de la Constitución española, *“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen...”*. La doctrina española señala que el derecho a la propia imagen es un derecho autónomo, cuya protección no interfiere por medio de la defensa de otros, como el honor, la intimidad o la privacidad.

³ (Lara Gamboa 2004, 190)

En cuanto a la delimitación de este derecho, la tutela de la imagen engloba los atributos más característicos y propios de la persona, a partir de la cual se proyecta socialmente el individuo. Al ser la imagen la representación gráfica de la figura humana (mediante un procedimiento mecánico o técnico de reproducción), estos atributos físicos deben ser visibles y reconocibles, es decir, que la persona pueda ser identificada e individualizada por su aspecto físico. No se trata de la figura humana corpórea como tal, para que este derecho se vulnere requiere necesariamente de la identificación del individuo.

“El derecho fundamental a la propia imagen garantiza un ámbito de libertad respecto de sus atributos más característicos y propios de la persona, que la identifican en cuanto tal, como es la imagen física visible. Asimismo, protege el poder de decisión sobre los fines a los que haya de aplicarse las manifestaciones de la persona a través de la imagen y un ámbito de libre determinación sobre la materia (Alegre Martínez 1997)¹”.

Este derecho tiene dos acepciones, la positiva que es la facultad exclusiva que tiene la persona de permitir o autorizar la difusión o publicación de su propia imagen (es consciente de que su imagen será utilizada para los fines que a bien lo tenga), y la acepción negativa, que es el derecho de evitar su publicación o uso².

Este derecho exige el pleno consentimiento de la persona en dos etapas, el previo que sería el consentimiento informado para la obtención de la imagen o fotografía y, el posterior para su eventual uso o difusión pública. *“El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo; frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana. Con la protección constitucional de la imagen se preserva no solo el poder de decisión sobre los fines a los que hayan de aplicarse las*

¹ (Nogueira Alcalá 2007, 261)

² La LO 1/1982 y la STC 14/2003 del 28 de enero señalan el ámbito o concepto positivo del derecho a la imagen: “establece que el derecho a la propia imagen atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puedan tener difusión pública. La misma sentencia indica la manifestación negativa o prohibitiva de este derecho: se impide la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad perseguida.

manifestaciones de la persona por medio de su imagen, sino también una esfera personal y, en este sentido, privada, de libre determinación y, en suma, se preserva el valor fundamental de la dignidad humana¹”.

El derecho a la propia imagen está profundamente condicionado por la actividad del sujeto cuando se trata de personas con una actividad o cargo público, profesión de notoriedad o proyección pública. La Resolución 1.165 de 1998 de la Asamblea parlamentaria del Consejo de Europa define en forma general persona pública a *“toda aquella que desempeña un papel en la vida pública bien político, económico, artístico, social, deportivo u otro”*.

En cada caso, es importante analizar la licitud de la conducta y el lugar donde se han llevado a cabo las conductas. Debe tomarse en cuenta si la persona se encuentra en el desempeño de sus funciones públicas o si, por el contrario, la actividad realizada pertenece al ámbito personal y privado. Las imágenes captadas en la realización de un acto público, lugar abierto al público, y con un interés general, corresponden al ámbito público de la persona. El interés público es para averiguar si una información merece o no la protección legal, se refiere, a algo que *“es importante o relevante para la formación de la opinión pública o que afecta al conjunto de los ciudadanos o a la vida económica o política del país²”*. En cuanto las personas públicas están más propensas a las publicaciones o interferencias de su vida privada; eso no significa que la ley desampare los derechos concernientes a la vida privada, ya que al igual que todos tienen la protección legal de su esfera personal y privada³.

En la LO 1/1982 de Protección Civil del Honor, a la Intimidación Personal y Familiar y a la Propia Imagen, no se considerarán intromisiones en la vida privada de la persona, las imágenes obtenidas en lugares públicos a personas de notoriedad o proyección pública⁴. La excepción del consentimiento o autorización para la captación o difusión de imágenes lo constituyen las

¹ (Arzo Santisteban 2002, 147)

² (Fayós Gardó 2014)

³En el (Asunto Von Hannover c. Alemania 2004) el TEDH manifestó que las personas públicas no pueden invocar una afectación a la vida privada a menos que se encuentre en un lugar aislado y fuera de la vista de la gente.

⁴ (la LO 1/1982 de Protección Civil del derecho al Honor 1982) Véase también el artículo 18.1, Constitución Española

personas con la condición de notoriedad, siempre y cuando se cumplan los requisitos antes mencionados. Quedan excluidas todas aquellas actividades que se lleven a cabo dentro de la vida privada de la persona pública.

El consentimiento de la persona engloba la captación, el almacenamiento, la reproducción y la difusión de la imagen. Aun cuando la imagen se obtenga en lugares públicos no autoriza por sí sola su reproducción, y la simple reproducción de la imagen reconocible sin el consentimiento del titular trasgrede el derecho a la propia imagen. Indistintamente de que existan o no motivaciones de índole económica para la captación o reproducción de la imagen, la persona debe dar su consentimiento¹. Por medio de la imagen es posible la identificación de la persona pues los rasgos físicos externos permiten la individualización de la persona; además como elemento integrante del bien “imagen” se encuentra la voz y el nombre de la persona. En efecto, dentro del marco de la videovigilancia, las voces captadas por las cámaras (o micrófonos) son consideradas un dato de carácter personal atribuible a la persona física incluso si no están asociadas a los datos de identidad de la persona.

La imagen, la voz y la figura son atributos de la persona que permiten la identificación del individuo y los hacen reconocibles ante los demás. Aunque esos atributos son característicos, propios e inmediatos del derecho a la imagen, en la mayoría de los casos carecen de un reconocimiento legal expreso como derechos fundamentales.

El debate que gira en torno al derecho a la imagen y los sistemas de videovigilancia se centra en el equilibrio que debe existir entre el avance tecnológico aplicado a la seguridad y la vulneración que puede sufrir este derecho cuando la vigilancia se convierte en un método abusivo contra los datos personales de las personas.

Los CCTV son instrumentos tecnológicos que permiten la recopilación de datos personales. Principalmente, la imagen es importante recalcar que la imagen será considerada un dato personal cuando permita la identificación de la persona. La que la identificación sea posible se requieren de dos elementos: una base de datos y el dato personal suministrado. Actualmente

¹ (Pace 1988)

existen bases de datos que almacenan datos biométricos como las huellas digitales, el iris del ojo o la voz, una vez procesados, permiten identificar a una persona. Cuando una imagen es sometida a una base de datos para su comparación es posible vincular con toda certeza la identificación de esa persona, incluso es posible determinar el lugar, el momento y las circunstancias donde fue captada su imagen.

Relacionado con el tratamiento de imágenes, surgen varias críticas importantes. La primera, en cuanto al consentimiento del titular al momento de obtener la imagen. En la mayoría de los casos, los ciudadanos carecen de información en relación con el uso e instalación de los CCTV dentro de los espacios públicos. Generalmente, estas iniciativas propuestas por los gobiernos locales, carecen del respaldo legal en cuanto al tratamiento de datos personales; inician con el funcionamiento de las cámaras de vigilancia sin contar con normas que garanticen el uso correcto de esos sistemas acorde con la protección de los derechos individuales de los ciudadanos.

La segunda de ellas tiene que ver con el almacenamiento y cotejo de la imagen. Miles de cámaras distribuidas a lo largo y ancho de las ciudades vigilan a los transeúntes, graban el tránsito y los movimientos de las personas que entran por estos amplios espacios públicos vigilados: calles, parques, estaciones, terminales, subterráneos, aeropuertos, estacionamientos de vehículos, aceras, edificios gubernamentales y privados. Los alcances de estos nuevos sistemas nos permiten no solo documentar hechos, sino también capturar imágenes, ubicar cronológicamente objetos y personas (seguimiento de personas). También las imágenes obtenidas desde las cámaras de videovigilancia son sometidas a programas de reconocimiento facial y análisis conductuales. Los CCTV tiene la capacidad de captar y almacenar las imágenes de forma continua e ininterrumpida, lo que ocasiona una recolección de datos abusiva por parte de los poderes públicos. Esta recolección de datos que se realiza, no se enfoca únicamente en la prevención o persecución de la actividad delictiva como manifiestan, pues el monitoreo de los espacios públicos involucra a todo aquel individuo que transite por ellos, incluso de aquellas personas que no tiene relación con el delito o intención de delinquir. Si bien es cierto, los CCTV como medida de seguridad deben responder al interés público y procurar el resguardo de los ciudadanos, no pueden convertir en un mecanismo de control social, donde se transgredan los derechos individuales de los ciudadanos.

Por último, dentro del contexto judicial la imagen ha tomado relevancia y fuerza como medio de prueba dentro del proceso. Los jueces y autoridades judiciales, le han atribuido a la imagen, un alto grado objetividad y credibilidad, pues hace una representación visual de los hechos. Sin embargo, no debe descartarse la posibilidad de que la misma sea objeto de manipulación. *“En el caso de la imagen, se da más por su capacidad para instalarse como verdad en el escenario social que como prueba sobre lo distinto y, por lo tanto, peligroso. El problema de la objetividad de la imagen está siempre presente y, aunque la representación visual ha sido objeto de manipulación sea solo por la elección del punto de vista, o bien por la disposición que, actualmente, existe de gran cantidad de recursos digitales que permiten editar, trucar o recomponer el registro visual, la credibilidad le sigue siendo consustancial”* (Espínola Frausto 2013, 5)

La utilización de la imagen debe necesariamente responder al interés público, sea para la prevención o persecución del delito. En este caso, las barreras legales que revisten este derecho deben rendirse ante el interés público. *“Calificado así resulta claro de que el primer elemento a salvaguardar sería el interés del sujeto en evitar la difusión incondicionada de su aspecto físico, que constituye el primer elemento configurador de su intimidad y de su esfera personal, en cuanto instrumento básico de identificación y protección exterior y factor imprescindible para su propio reconocimiento como individuo. En este contexto, la captación y difusión de la imagen del sujeto solo será admisible cuando la propia – y previa – conducta de aquel o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que pueda colisionar con aquel¹”*.

No cabe duda de que la videovigilancia puede afectar los derechos concernientes a la vida privada de las personas. Convenimos con Luis Cordero en que la videovigilancia es una condición de riesgo que afecta los derechos del ciudadano, pues le permite al Estado observar a sus ciudadanos sin que estos sepan, además de que queda registro de las imágenes las cuáles

¹ (Sentencia 1987)

podrían ser sometidas a un proceso de almacenamiento, clasificación o tratamiento sin conocimiento ni consentimiento de los ciudadanos¹.

2.3 Derecho a la protección de los datos personales

Las nuevas tecnologías de información y la sociedad computadorizada en la que vivimos inmersos permiten que la recolección, el procesamiento y la transmisión de datos personales, sea cada vez mayor y de manera más eficiente. Bajo esta premisa, es necesario dotar de protección la vida privada de las personas, concediendo derechos a los individuos e imponiendo deberes a quién controla y accede a los datos.

La protección de los datos personales es un derecho de la personalidad porque preserva ocultar información relativa a la vida privada de los individuos garantizando el desarrollo individual y el libre ejercicio de sus derechos; es un derecho inherente a la persona que le permite desenvolver su personalidad y su “*vulneración priva a la persona del disfrute y goce de los más significativos derechos y libertades*”². Se alberga dentro de la rama del Derecho Informático y su reconocimiento se encuentra fuertemente ligado al desarrollo social, y a los cambios progresivos de una sociedad cada vez más tecnológica. En la actualidad los nuevos avances tecnológicos exigen respuestas jurídicas concretas, acordes a los cambios sociales que van surgiendo. La protección de datos además de proteger la esfera privada de las personas, regula los procedimientos para la tutela de nuevos derechos e involucra la configuración de autoridades específicas de control³.

Es una garantía que tiene la persona de controlar su propia información (datos personales) frente al tratamiento automatizado o manual de sus datos, los cuales pueden estar albergados en sistemas de cómputo o en algún otro soporte que permita su utilización, sea para el almacenamiento, organización y/o acceso. “*Entendemos por protección de datos personales el estatuto jurídico destinado a definir las condiciones sobre las cuales terceros podrán hacer uso de datos que conciernen a una persona. Ello principalmente, porque un mal uso de dichos datos*

¹ (Cordero 2009)

² (Herrán Ortiz 2003, 16)

³ (Rodríguez Ruíz 1997, 18)

puede afectar su entorno personal, social o profesional desde las esferas más públicas de su persona hasta los límites de su intimidad (...) la protección de datos no persigue abstraer del conocimiento público la información de una persona, sino dotarla de los medios necesarios para controlar quién, cómo, dónde y con qué motivo conoce cualquier información acerca de su persona, sea está calificable como íntima o no, pública o secreta¹”.

Es importante diferenciar dos términos, los datos personales y el tratamiento de los mismos. La Directiva 95/46/CE del Parlamento Europeo y el Consejo en el artículo 2, conceptúa los datos personales y dice que es *“toda la información sobre una persona física identificada o identificable; una persona se considerará identificable cuando su identidad pueda determinarse directa o indirectamente, sea mediante un número de identificación o por elementos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social²”*.

Existen diferentes tipos de categoría de datos, por ejemplo, los de identificación (nombre, domicilio, estado civil, etc.), patrimoniales, ideológicos, entre otros. Un dato personal es cualquier información concerniente a la persona física, a partir de la cual pueda identificarse a esta misma.

En Europa, nació la discusión si la identificabilidad de una persona incluye conocer sólo el nombre, o si bien abarca datos que, sin identificar en sentido estricto a una persona, se puede individualizar. La Agencia Española de Protección de Datos defiende la amplitud del concepto de dato personal cubriendo aquellas circunstancias en las que se desconoce el nombre del sujeto, pero se tiene un perfil completo de él, como las cookies y las direcciones IP (Grupo de Trabajo del Artículo 29)³.

Por otro lado, el tratamiento de datos personales es el proceso que recibe la información desde “la obtención, uso (acción de acceso, manejo, aprovechamiento, transferencia o

¹ (Garriga Domínguez 2016)

² (Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos 1995)

³ (Palacios González 2012, 63)

disposición de datos personales), divulgación o almacenamiento de datos personales, por cualquier medio”¹. Nuestra legislación define el tratamiento como:

“cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros”².

El derecho a la protección de datos establece límites y condiciones para el responsable o encargado de los datos, quien hace uso de los mismos, garantizando que la recolección y uso sean acordes al fin. Debe entenderse que la protección al tratamiento de los datos personales no solo es frente a los poderes públicos sino también frente a la actuación de los particulares.

La discusión en cuanto a la categorización de los datos personales se centra, además de la forma del procesamiento de los datos (manual y electrónico), en los caracteres que permiten definir cuando un dato es sensible o no³. Los datos sensibles se refiere a “cuestiones privadas cuyo conocimiento general puede ser generador de perjuicios” para el interesado y que pueden eventualmente afectar la privacidad del individuo o incidir en conductas discriminatorias⁴.

De acuerdo con el Reglamento General de Protección de Datos (en adelante RGPD) de la Unión Europea, los datos sensibles hacen referencia a cualquier dato que revele *“el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos con el objetivo de identificar de manera exclusiva a un individuo y los datos relativos a la salud o la vida sexual y/o la orientación sexual”⁵*, básicamente son

¹ Artículo 3 (Ley Federal de Protección de Datos Personales en Posesión de los Particulares 2010)

² Artículo 3 (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Ley No. 8968 2011)

³ Simitis y otros, BDSG, párrafo 1, No. m 119 mencionado por (Carvajal Pérez y Chirino Sánchez 2003, 19)

⁴ (Peña Ortiz y Achío Gutiérrez 2011, 67)

⁵ (Criteo 2018)

aquellas rasgos físicos o morales de las personas o hechos o circunstancias de su vida privada o intimidad¹.

Existen otros tipos de categorización de datos basados en la graduación de la protección. Gils Carbó señala tres categorías: los datos de libre circulación (los de identificación); los datos de circulación restringida, que son susceptible de tratamiento mientras haya una causa de justificación legítima, pero tienen cierto grado de limitaciones y los de recolección prohibida, que no permiten el tratamiento por afectar la intimidad personal o familiar (datos sensibles)²

La legislación costarricense reconoce además de los datos sensibles, los datos personales de acceso irrestricto y de acceso restringido. El primero se refiere a *“los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual fueron recabados”* (Art. 3 inciso c de la Ley No. 8968) , y el segundo son, los datos que *“aun formando parte de registro de acceso público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública”*³.

Referente al tratamiento de datos, la Directiva Europea establece de manera puntual protecciones especiales a los datos sensibles, como la necesidad de obtener el consentimiento explícito del interesado para el tratamiento de sus datos; otra exigencia es el interés legítimo de los responsables del tratamiento de datos, específicamente con la aplicación del principio de limitación de objetivos que establece que los datos deben tratarse con un objetivo específico, y no puede utilizarse o transferirse para fines incompatibles al mismo (Quirós Camacho 2004). Con esto se establecieron límites a la práctica administrativa de compartir datos entre países, incluso se creó una prohibición para instituciones pertenecientes a la Unión Europea de enviar datos personales a países que no cumplan con el estándar de protección similar al europeo o estén fuera del ámbito de vigencia de la reglamentación (Carvajal Pérez y Chirino Sánchez 2003, 12).

¹ (Moya Jiménez 2010, 28)

² (Gils Garbó 2001) mencionado por (Puccinelli 2004, 165-169)

³ Artículo 3 de la (Ley de Protección de la Persona frente al Tratamiento de sus datos personales. Ley No. 8968 2011)

También el artículo 7 de la misma norma, señala que ninguna persona está obligada a suministrar datos sensibles, salvo cuando la información sea necesaria y en beneficio de la misma persona, por motivos de asistencia médica o cuando la información recopilada sea necesaria para la afiliación de un grupo político, religioso o sindical y dichos datos no sean comunicados a terceros sin el consentimiento de la persona¹.

Con las nuevas tecnologías de información las fronteras de la vida privada se dilataron, facilitando el manejo, la accesibilidad y la circulación de las informaciones personales. Ante la invasión tecnológica, dentro de los espacios públicos el aspecto de la libre elección individual se ha acentuado, y las autoridades públicas han tenido que construir un conjunto de reglas sobre la circulación de las informaciones personales.

En este proceso nace el derecho a la autodeterminación informativa considerado como el derecho a mantener el control sobre las propias informaciones (Llácer Matacás 2001, 43). La autodeterminación informativa, es un derecho amplio que no se puede enmarcar en conceptos tradicionales del derecho. Por el contrario, es un derecho que surge y obedece a los cambios sociales; la amplitud de este bien jurídico puede afectar el núcleo de los derechos fundamentales del individuo. En consecuencia, es un bien jurídico que apareja la evolución de la sociedad con las necesidades del ser humano. *“Los vertiginosos cambios ocurridos por el avance en el manejo de la información, imponen la necesidad de proteger al ser humano de ese manejo, no con una simple indemnización o reparo, sino fundamentalmente impidiendo que trasciendan datos y uso de los mismos contra su voluntad”* (Quirós Camacho 2004, 155)

Para Chirino la autodeterminación informativa es un derecho protector y facilitador, que consiste en *“la potestad que tiene toda persona de controlar el flujo de informaciones que conciernen a sí misma”*; es la soberanía que tiene toda persona sobre su propia información personal acerca de quién, cuándo, dónde y bajo qué circunstancias terceras personas tomaron contacto con ellas (informaciones personales)². Esto no quiere decir, que la autodeterminación

¹Artículo 9 de la (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Ley No. 8968 2011)

² (Chirino Sánchez s.f.)

informativa le confiere a la persona, un poder absoluto sobre sus datos¹, sino más bien el derecho que tiene el ciudadano de estar informado acerca del procesamiento de sus datos y los fines para los que son utilizados, y en caso de que esto le genere un perjuicio, poder ejercer los derechos de defensa que la ley reconoce (acceso, corrección o eliminación de sus datos). *“No se trata de un derecho del ciudadano a poseer los datos, ni tampoco de exigirlos como si se tratara de un ejercicio derivado del derecho a la propiedad. Se trata más bien de instrumentar una verdadera garantía procedimental para que realce un derecho sustantivo que a su vez intenta proteger el derecho del ciudadano a saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales”* (Carvajal Pérez y Chirino Sánchez 2003, 26)

Esta potestad de controlar y manejar la información personal propia funciona como una defensa ante las intromisiones del Estado o de terceros, pero no implica que el ciudadano tenga un poder absoluto de sus datos. Este derecho le permite a la persona ejercer el control sobre la información personal que le atañe, independientemente si esta almacenada en registros públicos o privados de medios informáticos. El contenido de este derecho está integrado por diferentes facultades que se le reconocen para controlar el uso de información personal, desde el tratamiento, la conservación hasta obtener el fin y la transmisión de los datos (Peña Ortiz y Achío Gutiérrez 2011, 34).

En el caso de una afectación del derecho a la autodeterminación informativa, el hábeas data es la acción constitucional procesal que corresponde interponer, que faculta al afectado o interesado a acceder al registro de datos para conocer qué información existe sobre su persona, y en todo caso, solicitar la corrección de esa información si le causara algún perjuicio.

La autodeterminación informativa se conceptúa como una extensión del derecho a la intimidad, y no puede desvincularse el uno del otro. Para José Cuervo el *“derecho a la autodeterminación informativa es un derecho que se construye a partir de la noción de intimidad (privacy, riservatezza o vie privée) y se encamina fundamentalmente, a dotar a las*

¹ (Chirino 1997, 44)

personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales¹”.

A diferencia de otros países, el derecho a la autodeterminación informativa no se encuentra expresamente regulado en la Constitución Política de nuestro país, sin embargo, la jurisprudencia constitucional le ha dado el reconocimiento autónomo a este derecho; incluso la Sala amplió la protección estatal señalando la necesidad de controlar y regular el uso de los datos de las personas, sean íntimos o no². Los sistemas de videovigilancia forman parte de la amplia gama tecnológica de información, que influye sobre los datos personales del ciudadano, pues su funcionamiento le permite a las autoridades estatales obtener datos personales de los ciudadanos, principalmente la imagen, aunque no se descarta la posibilidad de obtener mayor información del ciudadano.

Finalmente consideramos que la imagen de una persona constituye un dato personal sensible que revela rasgos físicos externos que facilitan la identificación, en efecto les resulta aplicable el régimen de protección de datos personales previstas por ley. Por medio de los sistemas de videovigilancia, es posible recolectar información personal de los ciudadanos, desde la imagen hasta las actividades que realiza, los lugares que transita, las personas que la acompañan, entre otros.

2.4 Afectaciones al derecho de protección de datos por malas prácticas en el funcionamiento de los CCTV.

La protección de datos y la autodeterminación informativa son derechos que pueden restringirse o afectarse con el funcionamiento de los CCTV. Para el caso de la región latinoamericana, las afectaciones de ambos derechos se atribuyen por diferentes motivos: algunas de índole legal, como el incumplimiento de principios rectores de la videovigilancia y protección de datos, o la falta de normativa integral e institucional que establezca parámetros legales y prácticos a los sistemas de videovigilancia, acorde a políticas que garanticen la

¹ (Cuervo 1998-2009) mencionado por (Peña Ortiz y Achío Gutiérrez 2011, 23)

² (Sentencia 1999)

privacidad y la protección de datos de los ciudadanos; otras afectaciones están relacionados propiamente a los alcances y capacidades tecnológicas de estos sistemas.

A. Falta de consentimiento y deber de informar:

El primer requisito que podríamos mencionar es el consentimiento y el deber de informar. Uno de los requisitos práctico-legales que omiten las autoridades policiales en los espacios públicos vigilados es la instalación de rótulos informativos que exponen la presencia de las cámaras. En la legislación europea el consentimiento se establece como un requisito indispensable para el tratamiento de datos, pues a falta de recopilación de los datos es considerada ilícita¹. El ciudadano tiene el derecho de saber que transita por un área bajo vigilancia y que sus datos están siendo reproducidos o recopilados por un tercero.

La discusión que gira entorno a las cámaras de seguridad es si basta sólo con informar la presencia de las cámaras o si es necesario pedir el consentimiento. En mi criterio considero que es poco probable obtener el consentimiento libre, específico, informado e inequívoco de cada una de las personas que transita por un determinado lugar; sin embargo, el deber de informar la presencia de las cámaras en los lugares que están siendo vigilados es indispensable² porque le permite al ciudadano ejercer libremente su derecho a la autodeterminación informativa.

La rotulación informativa visible y legible, constituye un requisito de licitud para la recopilación de los datos, pues con ella se garantiza la libre voluntad del ciudadano de transitar por un área de tratamiento de datos. Por el contrario, cuando las cámaras funcionan sin la debida rotulación, los encargados de las videocámaras, además de incumplir con una obligación, violan el derecho a la autodeterminación informativa, pues el ciudadano no está consintiendo el tratamiento de su imagen, ni para su reproducción y mucho menos recopilación.

¹ (Reglamento relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, del Parlamento y Consejo Europeo, UE 2016/679 2016)

² Considerando 11 del (Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos de Costa Rica 2007). Ver Artículo 3 de (Instrucción 1/2006 de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras 2006)

La Ley Orgánica 15/1999, de Protección de Datos en España enfatiza el deber de información sobre la captación y/o grabación de imágenes, así como del responsable de la videovigilancia y de donde pueden ejercitarse los derechos relativos a la protección de datos. La normativa costarricense en el Reglamento regulador de la vigilancia pública señala que el Ministerio de Seguridad Pública es el responsable de colocar letreros de aviso que le permita al ciudadano saber cuál es el área que está siendo vigilada.

La falta de información acerca del funcionamiento de las cámaras trasgrede el principio de transparencia por parte del encargado del tratamiento. Sobre éste principio se asienta la base para que el titular pueda controlar la información que le concierne; es que se le provea de un sólido derecho a ser informado. La transparencia le permite al titular ejercer el *“derecho a la información y el libre acceso como garantías vinculadas al respeto a la verdad que forjan el camino hacia una democracia realmente participativa”* (Moya Jiménez, 2010)

A pesar de que existen normas que establecen el deber de informar las áreas bajo vigilancia, en la práctica, muchas de las cámaras funcionan de manera oculta o “clandestina”, el ciudadano desconoce dónde están ubicadas, quién es el responsable, cuál es la finalidad de información recopilada y a quién debe acudir en caso de que su libertad, privacidad o datos personales sufran un menoscabo.

B. Desproporcionalidad y desviación del fin:

Otra manera en que los CCTV afectan la autodeterminación informativa y los datos de los ciudadanos, está ligada al fin y a la proporcionalidad de su uso. En el tratamiento de datos, existe la obligación de especificar el fin para los cuales se registrará la información, los contenidos y la caducidad de los datos contenidos. Las autoridades deben informar la finalidad específica del tratamiento, desde la recolección, el almacenamiento, la circulación y/o supresión de los mismos por medio de mecanismo que garanticen su posterior consulta¹. Los encargados del tratamiento tienen la responsabilidad de darle el uso o finalidad apropiada para el cual fueron

¹ Artículo 22 de la (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal 1999)

recopilados los datos. Puede ser que los datos fueran obtenidos directamente del titular, por un tercero o a raíz de otros sistemas de tratamiento de información, de cualquier forma, requieren del consentimiento de la persona. También es indispensable el requisito objetivo de que los datos suministrados sean ciertos, precisos, íntegros y obtenidos de acuerdo a la ley y conforme a las finalidades establecidas. De la misma manera, se establece como límite la proporcionalidad en el uso de las informaciones y que el método sea proporcional al fin que se busca.

Aunque las cámaras de seguridad están dirigidas a detectar la actividad delictiva de los espacios públicos, en la práctica la vigilancia policial se aplica a todas las personas que transiten por un determinado espacio, indistintamente si la persona tiene comportamientos normales o delictivos. Surge una especie de daño colateral, donde las cámaras con el objetivo de detectar y prevenir los actos delictivos, arrastra el registro y reproducción de acciones y comportamientos que no merecen ser vigilados y que pertenecen a la esfera de privacidad de las personas como, por ejemplo, una madre amamantando a su bebé en un lugar de tránsito público.

La vigilancia por medio de cámaras se caracteriza por ser más invasiva, generalizada, indiscriminada y desenfocada, evidentemente esto lesiona la esfera de privacidad de los ciudadanos quienes son vigilados en una sociedad que previene aparentes riesgos. Parafraseado sería algo como: “por su seguridad lo estaremos vigilando” o “para evitar que le pase algún daño, usted será vigilado”. Expuesto así, los sistemas de videovigilancia pueden convertirse en un mecanismo de estigmatización y control social, e indudablemente la operatividad de estos sistemas concede un poder a quien los controla. Muchas personas pueden considerar que no tiene nada que temer o esconder, y quizás no hayan analizado los alcances que pueden tener los CCTV sobre sus vidas privadas. Sin embargo, la importancia en el fondo depende de quién observa, la razón por la que está observando y la manera en que perciben nuestras acciones¹.

En este mismo orden de ideas, otro error que cometen las autoridades policiales con las cámaras es la utilización de la evidencia para fines no delictivos y relacionados al orden público, como para la imposición de infracciones administrativas que finalmente no constituyen un delito

¹ (Proyect 2014)

y que maximizan las funciones represivas del Estado como, por ejemplo, la detección de ventas ambulantes, ingesta de licor en vía pública, etc.

Recordemos que el fundamento que media en los sistemas de videovigilancia pública es el interés público por parte de las fuerzas o cuerpos de seguridad, este interés público es la seguridad de los ciudadanos y el orden público, evitando o suprimiendo las acciones o los hechos que perturben la seguridad¹. Por sí solo, el mantenimiento del orden público incide en la libertad y en los derechos fundamentales de los ciudadanos; sin embargo, la crítica se centra en que los sistemas de videovigilancia son una herramienta que se caracteriza por ser invasiva (que evoluciona rápidamente con el pasar del tiempo) y que en la mayoría de los casos se propaga desmedidamente y desprovisto de garantías que protejan al ciudadano.

Cabe destacar que las autoridades policiales deben intervenir con pleno cumplimiento de la ley, y no se puede reprimir arbitrariamente todo tipo de conductas con el pretexto de garantizar el orden público o la eficacia de la acción policial, lo que se procura es evitar “una intervención expansiva sobre los ciudadano para salvaguardarles de peligros indefinidos”², sobre todo cuando los sistemas de videovigilancia se caracterizan por ser un mecanismo intrusivo y hasta desproporcional para usos distintos a los delictivos.

Indudablemente los derechos de participación del ciudadano se reducen a una actitud pasiva ante la vigilancia de la policía administrativa del Estado, una vigilancia que le toma más importancia a la persecución del delito que a la seguridad de los ciudadanos, y lejos de garantizar la privacidad de los ciudadanos se caracteriza en ser más represiva con ellos.

¹ El artículo 6 del (Reglamento General de Protección de datos 2016/679 del Parlamento y Consejo Europeo 2016) señala que el tratamiento de datos personales es lícito bajo seis supuestos: bajo el consentimiento inequívoco del individuo, interés vital del individuo, interés público, necesidad contractual, en cumplimiento de obligaciones legales y por el interés legítimo del responsable del tratamiento de datos, (consultado el 24 de octubre de 2018)

² (De la Serna Bilbao 2016, 138)

C. Conservación de las imágenes:

Otro requisito indispensable para evitar afectaciones al derecho de protección de datos, es la temporalidad de los registros o información. La información obtenida por medio de las cámaras debe ser temporal, implica que la conservación de los datos se limitará al necesario para alcanzar la finalidad para la cual se han recolectado; y material, que exige que los datos recaudados sean solo los necesarios para cumplir con las finalidades perseguidas, lo que implica que los datos deben ser adecuados, pertinentes y acordes¹.

La conservación de las imágenes debe ser proporcional y cumplir con un plazo determinado de tiempo. En materia de imágenes, la Ley Orgánica 15/1999 de España, señala que las imágenes deben conservarse el tiempo imprescindible para su fin, que la Instrucción fija un máximo de un mes, pasado este periodo la información debe ser eliminada de la fuente principal, para que el dato ya no pueda ser recuperado².

La proporcionalidad en materia de datos es comprobar si el tratamiento es necesario para alcanzar un determinado interés legítimo y si las medidas adoptadas son las adecuadas para asegurar que la intromisión en los derechos a la vida privada y al secreto es mínima. En términos generales lo que se pretende es aplicar medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales³, lo que implica necesariamente que los datos objeto de tratamiento deben ser adecuados, pertinentes y limitados en relación con los fines para los que son tratados.

Otra parte donde se proyecta este principio es a través de la cantidad de cámaras que se instalan, así como el tipo de cámaras, porque no es lo mismo la captación de imágenes por

¹ (Concepto No. 13-102526 emitido por la Oficina Asesora de la Superintendencia de Industria y Comercio 2013)

² Artículo 15 y 16 (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal 1999)

³ (Biberley 2018)

medio de una cámara fija que la que se realiza mediante las denominadas “domo”, que permiten grabaciones de 360 grados, o las cámaras móviles¹.

A propósito de la temporalidad de la información, cabe mencionar el derecho al olvido se define como el *“principio a tenor del cual ciertas informaciones deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refiere, para evitar que el individuo quede prisionero de su pasado”*².

El derecho al olvido es la potestad que tiene el titular de los datos de solicitar al encargado (quien los tenga en su poder), la eliminación del registro de datos sea por haberse cumplido el tiempo de vigencia, por haberse ejecutado la finalidad para la cual fueron brindados o porque la información personal no es verídica y no tiene por qué estar al alcance de otras personas. En este sentido el titular de los datos, puede ejercer un derecho de defensa en caso de abuso por parte de funcionarios de instituciones públicas, administrativas o privadas. *“El derecho al olvido es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado, en los sistemas de indexación de los buscadores de internet”*³.

D. Incumplimiento del deber seguridad y confidencialidad del responsable de los datos:

Otra posible afectación a la protección de datos personales se puede derivar del incumplimiento a los deberes de seguridad y confidencialidad por parte del responsable de los datos. Las cámaras de seguridad están conectadas a internet y utilizan conexiones de redes WiFi o Bluetooth que les permite enviar imágenes a los ordenadores a los que están comunicados y que reciben las imágenes para ser guardadas o tratadas⁴.

¹ (Guía sobre el uso de videocámaras para seguridad y otras finalidades Agencia Española de Protección de Datos)

² (Gozaini 2011, 186)

³ (De Terwangne 2012, 53)

⁴ (De la Calle 2016)

Eventualmente, el tránsito de datos podría ser hackeados desde las propias cámaras o bien desde los ordenadores por personas no autorizadas. La alternativa de poder manipular las cámaras a distancia es un arma de doble filo, pues así como le permite al propietario legítimo manejar las cámaras y las imágenes, incluso desde su propio móvil, de la misma manera personas no autorizadas pueden intentar hacerlo¹ El deber a *“la seguridad y la transparencia son requisitos fundamentales, la primera en cuanto debe garantizar el carácter secreto de la información obtenida, estableciéndose la necesidad de regular el derecho de acceso de los datos. Mientras la transparencia es básica para controlar los procesamientos de datos personales”* (Peña Ortiz y Achío Gutiérrez 2011, 32).

El deber de confidencialidad garantiza que la información sea accesible únicamente a personal autorizado y que se empleen las herramientas y las políticas de seguridad necesarias para alcanzar el fin. *“Los responsables de la operación de videocámaras y otros equipos, deberán adoptar las medidas necesarias que garanticen la seguridad y confidencialidad de las imágenes, sonidos y datos por ellas obtenidos, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Cualquier persona que, en razón del ejercicio de sus funciones o de un modo accidental, tenga acceso a las imágenes, sonidos y datos que regula la presente ley, deberá observar absoluta reserva y confidencialidad”*².

Además de ser deberes, el secreto y la confidencialidad son una garantía para la protección de datos, porque permiten que los datos personales sean conocidos por el afectado y por aquellos usuarios autorizados y competentes para usar, consultar, modificar o incluir los datos en los sistemas de información. La imposición de estos principios pretende garantizar que las imágenes guardadas no sean accesibles a personas no autorizadas y minimizar los riesgos de una posibles divulgación, sustracción o manipulación indebida de la información.

Otras afectaciones al derecho a la protección de datos surgen a partir de la evolución de estos sistemas, principalmente por su capacidad para recopilar información fotográfica y sonora en determinados lugares y personas, y también por la amplia capacidad de almacenamiento y

¹ (Cid 2016)

² (Acerca de la videovigilancia 2010)

posibilidades de compilación e interconexión de bases de datos que ofrecen los nuevos programas.

Aunque en la región latinoamericana, los sistemas de videovigilancia se han expandido vertiginosamente, el tipo de tecnología que se obtiene en los países subdesarrollados es más limitada en capacidad y calidad en comparación con el desarrollo tecnológico del primer mundo. Pero es cuestión de tiempo para que los costos de estos dispositivos sean accesibles económicamente para nuestros gobiernos y sean implementados en las urbes latinoamericanas.

E. Obtención de datos sensibles (la imagen):

Actualmente se comercializan cámaras con alta definición de imágenes y que permiten obtener información sensible de las personas, como *“los escáneres de identificación personal por método biométrico, la fotografía y grabación digital infrarroja, el zoom de alta definición, la grabación por voz y las cámaras aéreas desplegadas en drones y globos aerostáticos”* (Zolezzi y Valenzuela Herrera 2017, 23).

Los sistemas de videovigilancia permiten la recopilación de imágenes, un dato sensible que revela características físicas de la persona, a partir de la cual es posible la identificación de la persona. Los centros operativos reciben la reproducción de las imágenes de forma permanente y algunas son almacenadas temporalmente, esto permite que la información registrada digitalmente sea muy variada. Según sea la cantidad de cámaras en los espacios públicos, es posible obtener horarios, trayectos, rutinas, acciones e interacciones en el espacio público, hábitos, lugares frecuentados, así como participaciones en actividades culturales o políticas (Zolezzi y Valenzuela Herrera 2017).

Para Ramírez Zolezzi y Valenzuela Herrera las cámaras de vigilancia son una práctica expropiatoria de derechos fundamentales porque registra, o puede registrar, información sensible del titular sin su consentimiento, que a su vez lesiona y limita la vigencia de la intimidad personal como garantía para la interacción y exposición en el espacio público debido a las intervenciones estatales de las autoridades públicas.

F. Construcción de perfiles del titular de los datos:

Con las nuevas tecnologías, el uso de instrumentos informáticos permite una mejor organización de los datos personales, creando perfiles más completos de los titulares. El tratamiento de datos se caracteriza por la existencia de un soporte físico en el que se registran los datos, estos registros o bases de datos permiten obtener información muy variada y específica del titular: *“el primer presupuesto necesario en el tratamiento de datos personales será un soporte físico materializado en la forma de un fichero, registro o banco de datos, conceptualizándose como el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquier sea la forma o modalidad de sus creaciones y organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos”* (Peña Ortiz y Achío Gutiérrez 2011, 30).

Los archivos o registros son el resultado visible del proceso del tratamiento, desde la recolección hasta la comunicación de los datos. Uno de los peligros que conlleva la recopilación de registros es la posibilidad de construir perfiles de personalidad, preferencias o tendencias a partir del procesamiento de datos personales; datos que podrían considerarse insignificantes, pero que tienen la capacidad de contribuir en la realización de medios de control social a través de la comparación, reunificación y redefinición de los datos haciendo nugatoria la realización del modelo democrático (Quirós Camacho 2004). Eventualmente estos sistemas podrían ser utilizados para estigmatizar y controlar ciertas minorías sociales, y creando “categorías” de ciudadanos según sus antecedentes, conductas o hábitos.

Las agencias de protección de datos, son las responsables del manejo o manipulación de las bases de datos; ahí mismo los ciudadanos hacen valer sus derechos de acceso a la información, rectificación, oposición o supresión de los mismos. En el caso de nuestro país, se creó la Agencia de Protección de Datos de los Habitantes (en adelante Prodhab) y es la encargada de velar por el cumplimiento de la normativa relacionada a este derecho y la de resolver las quejas planteadas por los ciudadanos.

El personal de las Agencias de Protección de Datos o los responsables de manejar las bases de datos tienen la obligación y/o el deber de confidencialidad. Este deber es una especie de secreto profesional que implica que la información debe ser únicamente utilizada para los fines públicos que la ley establece y el acceso a la misma se realiza en el ejercicio de sus facultades dadas por ley. Nuestra ley establece una sanción para quien incumpla con el deber de confidencialidad¹.

En nuestro país, la legislación concerniente a la protección de datos y la videovigilancia se regula de manera aislada, pues no existe una conexión normativa entre ambas. En nuestro país se creó el Reglamento No. 34104 –G-MSP, que regula la videovigilancia de los espacios públicos. El documento instaura una serie de principios técnicos y organizativos en el tema de la vigilancia y parte con el respeto al derecho a la intimidad; también existe la Ley No. 8968 y el Reglamento 37554-JP referentes a la protección de la persona frente al tratamiento de sus datos, que a su vez ofrece definiciones, delega competencias institucionales, otorga obligaciones a los responsables del tratamiento y derechos/garantías para los ciudadanos.

Sin embargo, en materia de videovigilancia falta por unir y complementar ambas normas; por ejemplo, con una participación institucional en conjunto de la Prodhav / Cuerpos policiales y ciudadanos. En materia de videovigilancia es importante la participación consultiva o reguladora de la institución encargada de la protección de datos, de esa manera es posible corroborar las buenas prácticas de esta actividad, el cumplimiento técnico y organizativo de los CCTV, se controlan posibles abusos de autoridad y se le ofrecen alternativas al ciudadano para ejercer sus quejas o denuncias acerca del funcionamiento de las cámaras.

La videovigilancia en espacios públicos así como la protección a los datos y el respeto a las libertades individuales, es una actividad que le concierne a las autoridades estatales. Una adecuada protección legal de la privacidad es crucial en el desarrollo de sistemas tecnológicos

¹ Artículo 11 del (Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos de Costa Rica 2007). Artículo 10 de la (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal 1999). Artículo 21 de la (Ley Federal de Protección de Datos Personales en Posesión de los Particulares 2010).

como los sistemas de videovigilancia. Recordemos que la privacidad forma parte de nuestra identidad, y el hecho de sentirnos constantemente bajo observación, juzgados por quienes operan estos sistemas, además de la posibilidad que tienen de controlar nuestra información, afecta en menor o mayor grado el pleno ejercicio de nuestra libertad e identidad como ciudadanos dentro de una sociedad democrática de derecho.

En efecto es de vital importancia que “...los responsables de la gestión y la operación de estos sistemas de vigilancia sean plenamente conscientes del peligro que representa la vigilancia del espacio público y que hagan todos los esfuerzos necesarios para garantizar que la videovigilancia no constituya una amenaza para los derechos fundamentales” (Goold 2010, 27).

No se trata de “satanizar” el uso de estos sistemas, se trata de que la infraestructura disponible en el espacio público reconozca la existencia del derecho a la intimidad y que lo que está plasmado en una norma sea realizable en la práctica, sin abusos ni omisiones. Cómo se ha venido exponiendo los CCTV, forman parte de una gama tecnológica que conforme avanza, restringe o limita el derecho a la privacidad de los ciudadanos en los espacios públicos y privados. Esto conlleva, necesariamente, una evolución normativa que brinde protección al ciudadano e imponga límites a las medidas (o mecanismos) tecnológicas que proponen los gobiernos en el desempeño de sus funciones públicas.

Los retos que plantean las nuevas tecnologías en el plano legal deben enfocarse en que su utilización garantice el respeto de los derechos y garantías constitucionales de los ciudadanos¹. Si bien es cierto, las Constituciones son la norma suprema, tampoco pueden convertirse en un impedimento omisivo para resolver los conflictos que surgen a raíz del uso de las nuevas tecnologías de información, cuando por el contrario puede ser un instrumento legal comprometido a brindar garantías y protección a quien así lo requiera (la parte débil)².

Además de las valoraciones normativas-técnicas y la inclusión de políticas acordes con el derecho a la privacidad, cabe mencionar que los gobiernos deben considerar en un futuro, los

¹ (Barbone 2005, 48)

² JNCom. No. 18, Secr. No. 36, 23-10-2001, “G., D. E. c/C. SA s/Diligencia preliminar”, www.eldial.com.ar

resultados del funcionamiento de estos sistemas en el tema de la seguridad, principalmente en la reducción, prevención y persecución del delito. De esta manera se evalúan los beneficios u aportes de las cámaras ante el problema de inseguridad, y se reconsidera la continuidad de los mismos o la implementación de otras medidas de seguridad que lo complementen.

Como se mencionó a lo largo del capítulo, un elevado grado de inseguridad impide el desarrollo de la sociedad como grupo, pero también afecta el libre ejercicio de las libertades del individuo, quien por temor o miedo evita la realización de actividades habituales. La seguridad tiene por objetivo garantizar las libertades del hombre y dentro del orden democrático, la seguridad se vuelve una necesidad para la sociedad y una obligación para el Estado, quien debe implementar todos sus recursos y aplicar toda su fuerza a quienes perturben la paz u obstaculicen la convivencia ciudadana de los individuos que desean vivir con tranquilidad y libertad.

A continuación, se mencionan algunos estudios e investigaciones llevadas a cabo en otros países que afirman la poca efectividad de estos sistemas para prevenir la actividad delictiva.

G. Problemas de efectividad que presentan los sistemas de videovigilancia en los espacios públicos.

En principio, los sistemas de videovigilancia como medida de seguridad están dirigidos a la prevención, la reducción y persecución de la actividad delictiva; consecuentemente, la información recopilada por medio de ellos debe ser exclusivamente para tales fines. Sin embargo, como se detallará más adelante, los sistemas de videovigilancia han sido fuertemente criticados por la poca efectividad que han demostrado en la prevención y reducción del delito, aunque sí han tenido considerables mejorías en la persecución del delito, como medio de prueba digital.

Actualmente, Reino Unido es considerado el “padre de la videovigilancia”, debido a que desde los años ochenta el gobierno de este país se ocupó de instalar progresivamente cámaras en

lugares públicos a una tasa de quinientas por semana¹; Reino Unido actualmente es el país europeo que se encuentra en la vanguardia del uso de tecnología por motivos de seguridad. Desde hace veinticinco años, Inglaterra ha promovido el desarrollo exponencial de estas tecnologías, y hoy es el líder mundial en uso de la videovigilancia. Al ser Inglaterra el país más incisivo con los CCTV y con mayor cobertura tecnológica de vigilancia, las polémicas en este país han sido mayores, sin embargo, las opiniones han estado divididas. Resaltamos algunos de los aspectos negativos de la videovigilancia en este país:

Para el 2007, el partido Liberal demócrata del Reino Unido, realizó un estudio llamado “The Inquirer”. Los datos demuestran la poca efectividad que han tenido las cámaras de vigilancia en la resolución de los crímenes. Para ese entonces, el ochenta por ciento de los crímenes cometidos en las calles no habían sido resueltos, a pesar de las diez mil cámaras de seguridad instaladas en las calles londinenses. Una de las conclusiones a las que arribaron fue que la cantidad de millones invertidos en estos sistemas de seguridad había sido un gasto exagerado e inútil en la lucha contra la delincuencia. Además, que la cantidad de cámaras de vigilancia instaladas en los barrios, no estaba directamente relacionada con los casos resueltos por la policía de la zona.

Datos suministrados por la Policía Metropolitana de Londres en el año 2008 pusieron en manifiesto la poca efectividad de las cámaras de vigilancia para la resolución de delitos. De acuerdo a esos datos tan solo se descubrieron mil delitos gracias a las cámaras de seguridad. Por cada mil cámaras de seguridad que hay en la ciudad, tan solo se consigue resolver un delito al año. Interesante resultados que ponen en duda las justificaciones policiales para el funcionamiento de estos sistemas². Para este mismo año, solo se detectaron cinco delitos en la vía pública gracias a los sistemas de videovigilancia³. Mick Neville, Inspector Jefe de la Policía de Londres manifestó que durante un mes las cámaras solo sirvieron para encarcelar a ocho de doscientos sesenta y nueve sospechosos de robo en todo Londres⁴.

¹ (Töpfer 2010, 74)

² (I. Sáenz de Ugarte 2009)

³ (Lobohem 2010) mencionado por (Lozano Jiménez 2012, 416)

⁴ (La videovigilancia contra el crimen en Londres fracasa 2009)

Un informe interno de Scotland Yard publicado en el diario The Independent en el 2009, reveló que en el año anterior solo se había resuelto un delito por cada mil cámaras de videovigilancia. En el 2008, los casi cuatro millones de cámaras (incluyendo las del sector privado empresarial) de videovigilancia únicamente sirvieron para descubrir a los autores de unos mil delitos. En los delitos de robo, solo un tres por ciento de los robos que se cometieron en las calles se esclarecieron gracias a los sistemas de videovigilancia.

Posteriormente en el 2014, las tres agencias de inteligencia británicas hicieron una investigación sobre los sistemas de videovigilancia. Durante un año se dedicaron a analizar los procedimientos, el alcance y las implicaciones de estos sistemas sobre la ciudadanía inglesa. Una de las conclusiones señaló que *“es evidente que el marco legal que autoriza la interceptación de comunicaciones no es claro, no ha seguido el ritmo de los avances de la tecnología de las telecomunicaciones, y no sirve ni al gobierno ni al público general de manera satisfactoria. Se requiere un nuevo marco legal más amplio y claro”*. También el Comisionado de las Cámaras de Vigilancia en Reino Unido indicó que *“el público general no se da cuenta del alcance de la monitorización en Reino Unido y carece de la comprensión suficiente para consentir lo que está sucediendo”*¹.

Los opositores de los CCTV, manifiestan que el Gobierno inglés ha invertido millones de libras en la financiación de estos proyectos y los resultados han sido pocos significativos en el tema de la detección, reducción y prevención del delito. Aunado a ello, el crecimiento exponencial de estos sistemas de videovigilancia y el uso desmedido de los mismos lesionan los derechos de privacidad de los ciudadanos ingleses. Se estima que en la ciudad de Londres hay un dispositivo de CCTV por cada 14 personas aproximadamente. Esto convierte a la ciudad *“en un espacio de observación total, ningún rincón queda a la sombra de su visualización, cada paso o movimiento en las calles o vía pública, queda grabado y registrado en las bases de datos de la policía, con el único fin de mantener bajo seguridad a sus ciudadanos y asegurarse un ambiente de máxima seguridad en el país”* (Lozano Jiménez 2012, 416). Para David Davis, exministro de Interior, los *“CCTV produce un gasto inmenso y una eficacia mínima. Supone una clara intrusión en la privacidad, sin embargo, no facilita una mejora de la seguridad”*².

¹ (De Arriba Coro 2018)

² (I. Sáenz de Ugarte 2099)

Newburn y Hayman señalaron que la expansión de los CCTV en Inglaterra constituye una forma de presión del gobierno nacional contra el aumento de las tasas de criminalidad¹, así como los antecedentes de ataques y amenazas terroristas y la constante demanda de los ciudadanos en el tema de seguridad.

En Inglaterra, la política criminal de persecución del delito se ha hecho un tanto represiva, pues las autoridades judiciales implementaron penas más severas, tomaron medidas de restricción de movimientos para jóvenes que no habían delinquido, pero que pertenecía a bandas implicadas en crímenes². Además, la demanda creciente de seguridad, convirtieron a los CCTV en una forma de vigilancia excesiva y violatoria del derecho a la intimidad. El Observatorio de CCTV Camera Watch de Inglaterra, estima que hasta un noventa por ciento de las cámaras del país operan ilegalmente y transgreden el código de información y los límites de privacidad (Betancourt 2008)

Otra de las críticas que surgen a raíz de los CCTV, es la falta de integración institucional entre las entidades que intervienen (operadores de CCTV y policía metropolitana), lo que provoca una ineficiencia del sistema. Por ejemplo, el Estudio de Investigación de la Home Office del Reino Unido señalan que *“la videovigilancia del crimen es positiva, pero se desvanece con el tiempo, principalmente porque muchas veces la calidad del vídeo es baja y existe un retraso en tiempo de despliegue y la acción policial³”*.

Una conclusión que se deriva de lo anterior es que la disminución de la inseguridad no puede atribuirse únicamente a un sistema integrado de videovigilancia. Una de las principales críticas que rodean a la videovigilancia es que no solucionan los problemas de raíz o las causas del crimen, que principalmente están ligadas a las estructuras sociales (pobreza, desempleo, desigualdad económica, etc.). Sino que forman parte de las transformaciones político criminales que abogan por la prevención frente a cura, con su enfoque meramente represivo se consideran un “arreglo rápido” ante el eventual delito. Las cámaras no pueden asumirse como una solución mágica a un problema que es multifactorial.

¹ (Newburn y Hayman 2002, 198)

² (Inglaterra, el país que combate el crimen sin armas 2012)

³ (Gill y Spriggs 2005) mencionado por (Carli 2008, 11)

Los sistemas de videovigilancia se implementaron en Europa y EEUU por las consecuencias del terrorismo y en la región latinoamericana por el aumento de la inseguridad y la violencia, bajo una política criminal de cero tolerancia, un discurso de seguridad ciudadana y teorías de la prevención situacional; es innegable que la inseguridad pública como tal, es un problema social que requiere de un tratamiento más profundo, que involucra aspectos sociales, económicos y políticos criminales¹.

Para que los CCTV funcionen de una manera efectiva, requiere del respaldo y la capacidad institucional, para dar respuesta a las condiciones que influyen en la ocurrencia de los delitos². Paralelo a la instalación de los CCTV, la implementación de otras medidas de seguridad en conjunto con estos sistemas que han demostrado mejoras en la seguridad de ciertos lugares, como la iluminación de las calles, más presencia policial, participación de ciudadanía en programas de seguridad comunitaria, etc.

El peso de la inseguridad no puede recaer únicamente en un recurso tecnológico, que por sí solo no tiene la capacidad de prevenir o reducir los delitos, sino que requiere de otros factores para potenciar su efectividad.

Las autoridades de Londres han optado por otras estrategias, como la no portación de armas de fuego por parte de la policía urbana londinense, puesto que han comprobado que con ello se aumenta la violencia y las muertes; también aumentaron los controles presenciales en la calle logrando disminuir la portación de armas blancas; aumentaron la iluminación pública de ciertas aéreas que se consideraban peligrosas, y por medio de la participación integral de la comunidad y la creación de programas sociales³ ayudaron al mejoramiento de la seguridad (Inglaterra, el país que combate el crimen sin armas 2012)

¹ La inseguridad está asociada al aumento de la pobreza, la desigualdad social y económica, el desempleo, la deserción estudiantil, poca asistencia de programas sociales, la falta de oportunidades de reinserción de la población presidiaria, falta de oferta de bienes y servicios públicos por parte del Estado, sólo por mencionar algunos ejemplos.

² Por ejemplo, a nivel local se debe integrar el patrullaje policial con estos sistemas tecnológicos e incluir al desarrollo urbano a zonas que han estado al margen de la presencia estatal.

³ El Programa Justicia de las Comunidades, consistía en la resocialización de los jóvenes excluidos, con dificultades y problemas de conducta, la ayuda era dada en conjunto por las comunidades y las autoridades de control social.

En un documento elaborado en su mayoría por oficiales de policía, llamado The National CCTV Strategy de 2007, afirmaron que la disminución en la tasa de criminalidad no se encuentra estrictamente vinculada a la presencia de las cámaras en determinadas zonas (no es un indicador válido que refleje el éxito de los CCTV), y que era pertinente “*prestar atención a otros indicadores como el número de veces que ha servido como prueba durante un juicio o el tiempo que se ha ganado durante el procedimiento judicial*” (Coyle 2011).

Otros problemas adicionales que pueden presentar las cámaras de seguridad son los relacionados al área técnica u organizativa: “*área de cobertura limitada, mala calidad de diseño y de la cinta, uso inapropiado, falta de mantenimiento, entrenamiento y de disponibilidad de manuales/lineamientos*”, entre otros (Carli 2008, 11). Los sistemas de videovigilancia pueden presentar problemas en relación a la conexión, la falta de integración del sistema, la calidad de las imágenes y dificultades al momento de recuperar material filmado con tecnología digital, así lo ha señalado la Asociación de Jefes de Policía después de los atentados terroristas del 2005 en Londres. Es importante que los sistemas de grabación que se utilicen dentro de este contexto, cuente con una calidad mínima requerida (calidad y nitidez de la imagen) que permita la identificación de la persona o personas que cometen hechos delictivos, así como la detección de los hechos. Además, la ubicación de las cámaras de seguridad debe ser en puntos estratégicos, como accesos, puertas de entrada y/ o salida (Gill y Spriggs 2005)¹.

Idealmente la función punitiva de las cámaras es facilitar la identificación de los sospechosos de un delito, sea por el rostro o rasgos físicos, la vestimenta o la placa del vehículo si es que tienen. Si los CCTV reproducen imágenes de mala calidad o están ubicadas en lugares poco estratégicos, los mismos serían ineficientes en este aspecto. De la misma manera, para el supuesto de detectar delitos (delitos de flagrancia) mientras estos transcurren se requieren de otros elementos como tener una buena infraestructura de cámaras, la respuesta y el rápido despliegue policial. Sin embargo, debido a la gran cantidad de imágenes que llegan a los centros de comandos, es difícil procesar tanta información y detectar la comisión de un delito.

La industria de la videovigilancia está avanzando rápidamente en el mejoramiento de la imagen, se empezó con las cámaras análogas a cámaras digitales, ahora conectadas en red IP que

¹ Mencionado por (Lío 2015)

reproducen imágenes de alta definición debido a su resolución en megapíxeles¹. Estos avances prometen dar un giro a la calidad de la imagen dándole un papel importante, incluso con la creación de una nueva generación de cámaras en camino: las cámaras ultra HD 4k.²

Bajo esta línea de ideas, en España específicamente en Málaga los CCTV, han permitido la resolución de crímenes. Un estudio empírico realizado en el 2007 por Cerezo y Díez Ripollés, analizó la eficacia de los CCTV en la prevención de la delincuencia en el centro histórico de esta ciudad; en esta ocasión se concluyó una disminución poco significativa en los delitos contra la propiedad y un efecto de desplazamiento de la criminalidad a aquellas zonas no monitoreadas (Cerezo Domínguez y Díez Ripollés 2009). Otro resultado que se evidenció fue que los sistemas de videovigilancia no tienen el mismo impacto sobre la delincuencia impulsiva y violenta que sobre la delincuencia premeditada, provocando una disminución sobre esta última³.

Sobre la efectividad de la videovigilancia en Reino Unido y España, Medina Ariza afirma que: *“ninguna de las evaluaciones realizadas ha logrado documentar un impacto sensible en los niveles de delincuencia, si hablamos de videovigilancia en la calle... los únicos estudios que demuestran un impacto positivo es cuando se trata de cámaras de vigilancia en sitios concretos como aparcamientos o determinados establecimientos comerciales, donde sí ha servido para reducir hurtos. También, han tenido efecto muy positivo en la reducción de accidentes de tráfico en carreteras. Pero a nivel general no ha tenido un impacto en la prevención de la delincuencia común en las ciudades y eso pese a su muy elevado costo económico⁴”*.

Otra crítica que se ha hecho acerca de los CCTV, es la utilización de técnicas de segregación social a *“grupos vulnerables y/o minorías étnicas, como, por, a jóvenes negros (Hirsch, Wakefield y Garland, 2004; Armitage 2002), o personas de origen musulmán, quienes después de la tragedia del 11 de setiembre en Estados Unidos se han convertido en objeto de la*

¹ (Ortiz 2016)

² La tecnología Ultra HD 4K, es la abreviatura de 4.000 píxeles y se refiere a una nueva resolución de imagen que algunos catalogan de hiperrealidad por su realismo, incluso superior a las imágenes 3D.

³ (Miller 2007)

⁴ Entrevista en El País, 23.06.11, pp.30-31, mencionado por (Varona Martínez 2012, 39)

*videovigilancia*¹”, provocando que los Estados anhelan tener mayor control sobre sus habitantes. Para Artega, los sistemas de videovigilancia son “*dispositivos utilizados para ponderar la peligrosidad de las personas, sin embargo, en estos sistemas no existe una comunicación entre quien conduce la vigilancia (operador de mando) y el aparente sospechoso (vigilado)*”, por lo que el operador pondrá en juego prejuicios y tipificaciones, según su parecer o criterio subjetivo.

Los operadores al enfrentarse a un enorme número de imágenes, empiezan a “...orientar la mirada sobre el comportamiento o forma de vestir de las personas consideradas “sospechosas” o extrañas”. *En este sentido, “...las tecnologías de la vigilancia juegan un importante papel en la reproducción e institucionalización de ciertas lógicas de exclusión social”* (Norris, Moran y Armstrong 1998, 267-268). Los programas de Identificación, Detección Visual y análisis de comportamientos, tiene como propósito seleccionar cuidadosamente las imágenes de posibles sospechosos; estas imágenes son almacenadas en una base de datos donde la información puede ser accesada por los cuerpos policiales, y pueden ser utilizadas contra los criminales en caso de delito. El problema que surge es la subjetividad de la selección en el seguimiento a determinado individuo. El operador del sistema, basado en sus experiencias y conocimientos seguirá a cualquier persona que a su parecer sea sospechosa. “*Esas imágenes quedan almacenadas, y a no ser que haya una evidencia de crimen, permanecerán estancadas en los servidores de la policía por si acaso. Una forma de prevención un tanto intrusiva*²”.

La comisión y posterior descubrimiento de un delito cometido por una persona con rasgos físicos distintivos hace que todos los demás individuos pertenecientes al grupo sean considerados como posibles autores de la misma clase de delitos. Por ejemplo, en Reino Unido la comunidad de “*pakistaníes se les asocia con el terrorismo a raíz de los atentados terroristas en Londres en julio de 2005*”, no sólo en Londres sino en otros países como Estados Unidos, los musulmanes son sobrevigilados, y sufren de arrestos y acosos policiales³. Según el informe lo mismo sucede a lo largo de Europa: “*en Grecia, los albanes y búlgaros son comúnmente los sospechosos, y son considerados como los responsables de la mayoría de los delitos de robo, robo a mano armada y asesinato; en Italia y Europa oriental, los gitanos han sido etiquetados*

¹ (Löfberg 2008, 5)

² (La videovigilancia contra el crimen en Londres fracasa 2009)

³ (Sagant y Shaw 2010, 51)

como criminales e indeseables y sufren por la persecución y la falta de protección. En Francia y España, los norteafricanos son penalizados de manera similar”.

Los sistemas de videovigilancia se presentan como instrumentos tecnológicos en favor de la seguridad, a pesar de que la actividad como tal –vigilar-, incrementa las lógicas de exclusión social de las minorías. Varona concluye que: *“no puede negarse que disponer de espacios públicos abiertos y seguros es una de las condiciones que debería cumplir cualquier sociedad democrática –sobre todo porque los espacios públicos inseguros expulsan siempre a los más débiles- Pero esa demanda no puede convertirse en excusa para llevar adelante políticas que no resuelven problemas, que no tienen en cuenta la relación costo - beneficio y que no son evaluadas de forma regular para que la ciudadanía pueda determinar si mantenerlas tiene sentido”* (Varona Martínez 2012, 41-42).

La autora menciona dos investigaciones empíricas que se llevaron a cabo en diferentes lugares de Europa, y que arrojan conclusiones muy similares en cuanto a la poca efectividad de los CCTV en la reducción y prevención de la delincuencia.

Dos estudios realizados por el profesor Francisco Klauser del Instituto de Geografía de la Universidad de Neuchâtel en Suiza y publicados en la revista internacional *Information Polity*¹, se analizaron los efectos de la videovigilancia en doce países, en opinión del profesor *“la instalación de las cámaras se banaliza en detrimento de la reflexión sobre su utilidad. Si bien las cámaras permiten esclarecer algunos delitos, el efecto preventivo no dura en el tiempo. En la delincuencia en que funciona la elección racional, ponderando costes y beneficios, se produce un desplazamiento hacia zonas no cubiertas por las cámaras (...) Si bien se advierte una reducción inicial de las tasas delictivas y del sentimiento de inseguridad, esa reducción desaparece relativamente rápido (...) No se trata de demonizar las cámaras o de ver intereses puramente económicos, sino de realizar una reflexión más serena sobre su uso, en un momento de restricciones presupuestarias, donde la población valora más la presencia policial”* (Varona Martínez 2012, 48)

¹ El primero apareció en 2011 (vol. 16, n. 4) y el segundo en 2012 (vol. 17, n. 1).

La otra investigación que menciona la autora, es la del profesor Nils Zurawski y el Instituto de investigación social criminológica de la Universidad de Hamburgo (2003-2006), llamado “Ciudad, espacio, vigilancia”. En el estudio se documentó: *“las cámaras no reducen necesariamente la percepción individual de inseguridad, sino que puede producirse el efecto contrario, haciendo que las personas piensen sobre la inseguridad de un sitio, cuestión que antes quizá no se hubieran planteado. Esto puede ayudar, de alguna manera, a la estigmatización de ese lugar como peligroso (...) En todo caso, dada la importancia de la percepción del espacio sobre el sentimiento de inseguridad, se distinguen dentro de las percepciones y experiencias de la población las de los residentes, los turistas, las mujeres, los ancianos, los jóvenes y las minorías étnicas (...) el apoyo a la instalación y funcionamiento de las cámaras depende del contexto espacial y situacional, lo cual tiende a minusvalorarse en las encuestas. Sin embargo, las cámaras sí pueden tener efectos negativos respecto de las percepciones de los espacios en general en dos sentidos: a) reforzando o amplificando las percepciones de inseguridad (efecto amplificador); b) marcando los espacios como inseguros al existir cámaras y, por tanto, percibiéndose finalmente como tales (efecto marcador)”* (Varona Martínez 2012, 49-50)

La efectividad de los CCTV, dependerá una serie de factores que lo integran y complementan. Es necesario que los Gobiernos, previo a invertir millones de dinero en la instalación de estos equipos, evalúen la eficacia, eficiencia de estos sistemas a corto y largo plazo. También, deben considerar los motivos y las interacciones que pueden contribuir al éxito o el fracaso de la videovigilancia.

Es innegable que los sistemas de videovigilancia en espacios públicos producen una injerencia en la vida privada de los ciudadanos. Es necesario que su incorporación práctica y legal como política pública de seguridad responda a los fines establecidos: prevención, persecución y reducción de la delincuencia. En Latinoamérica los sistemas de videovigilancia se han ido incorporando poco a poco en las ciudades para combatir el problema de la inseguridad. Aunque el crecimiento de estos sistemas se ha materializado en la práctica, a nivel doctrinal y jurisprudencia el desarrollo de la materia ha sido escaso. Es cierto que en muchos países latinoamericanos existe legislación acerca del uso de los sistemas de videovigilancia y la protección de datos personales, sin embargo, la legislación es dispersa y regula de manera

aislada la actividad de la videovigilancia pública, carente de una infraestructura institucional que se encargue de velar por el buen funcionamiento de los mismos.

A diferencia de nuestra región, en Europa la videovigilancia se encuentra en una etapa más avanzada de reflexión; las políticas se han reorientado a incluir las garantías civiles y la participación del ciudadano dentro de esta actividad. Por eso resulta importante analizar la experiencia de algunos países europeos que han estado en la vanguardia de la videovigilancia y en general de la comunidad europea, que ha hecho grandes esfuerzos por consolidar la videovigilancia con los principios de una sociedad democrática.

CAPÍTULO 3: ANÁLISIS NORMATIVO DE LA VIDEOVIGILANCIA EN EUROPA Y COSTA RICA

A raíz de la proliferación de los sistemas de videovigilancia ha surgido una serie de preocupaciones relacionadas con la vulneración de la privacidad y la obtención de datos personales que se obtienen por medio de estos. Ante estas preocupaciones, las autoridades y operadores de estos sistemas han procurado hacer de la videovigilancia una actividad que respete los derechos de los ciudadanos, evitando que se conviertan en sistemas de control social y represores de las libertades civiles.

Este capítulo pretende analizar el tratamiento jurídico de la videovigilancia en los distintos países, así como los principios generales que rigen esta actividad pública y su adecuación a la protección de datos personales.

En la primera sección se analizará la videovigilancia en Europa, pues ahí yacen los países pioneros en el tema de la videovigilancia. En Europa, se encuentra dos vertientes, los países que aplican disposiciones generales sobre la materia por medio de dictámenes, directrices o códigos de conducta; y los países que han abordado la videovigilancia con legislación específica para el tratamiento de datos. Específicamente, se analizará el caso de Inglaterra y España. El primero de ellos, porque cuenta con una de las redes de CCTV más amplia del mundo, y a pesar de ello, cuenta con pocas normas o recursos legales que respalden el funcionamiento de estos sistemas con apego a las garantías de los derechos de vida privada y protección de datos personales; y el contrario, España que se ha esmerado en la creación de leyes e instituciones que respaldan el funcionamiento adecuado de estos sistemas. Se analizará también jurisprudencia internacional, relacionada con el funcionamiento de estos sistemas y la incidencia que tienen sobre la vida privada de las personas.

En la segunda sección se analiza el caso específico de Costa Rica, las circunstancias jurídicas, prácticas, técnicas y organizativas en las que se desarrolla la videovigilancia en nuestro país. Se analizará si, en realidad, existe una adecuación de la videovigilancia a los principios de protección de datos personales, y si el funcionamiento de estos sistemas se adecua a las reglas de la buena práctica, tal y como lo establece la legislación.

Sección primera: La videovigilancia en Europa, una respuesta en el Derecho Comparado

1.1 Los principios de la videovigilancia.

De manera genérica e introductoria se mencionan los principios más importantes aplicables a la práctica gubernamental de la videovigilancia en espacios públicos. Algunos de los principios de protección de datos y derecho administrativo son aplicables en la videovigilancia, otros han ido surgiendo por medio de la creación de normas específicas en videovigilancia o bien, se han establecido por criterios o recomendaciones de instituciones internacionales encargadas en la materia. La incorporación de estos principios legales en la práctica de vigilancia asegura que sus usos y enfoques sean permeados por las garantías constitucionales.

El primero de ellos es el *principio de legalidad*. Este principio establece la necesidad de un marco legal de orden interno que permita la actuación policial por parte de las autoridades estatales para la utilización de videocámaras en lugares públicos. Como parte de una sociedad democrática moderna, los cuerpos policiales pueden utilizar medios tecnológicos, eficaces y productivos, que permitan mejorar las funciones de prevención de la delincuencia, control social, seguridad pública y protección de los ciudadanos y bienes.

Además, constituye un factor de legitimidad de las grabaciones obtenidas y que sin perjuicio de la facultad jurisdiccional pueden ser tomadas como medios o fuentes de prueba, para su correspondiente apreciación y valoración dentro de un proceso judicial. En este sentido, Pérez Cruz manifiesta que el funcionamiento de estos sistemas debe cumplir necesariamente con este requisito, pues la falta de soporte legal en la recolección de la prueba y la utilización de la misma dentro de un proceso devendría una violación a esfera privada del individuo¹.

¹ (Pérez Cruz 1997) mencionado por (Cornelis Ramírez 2015)

Desde luego, es importante que el marco interno legal de estos sistemas de videovigilancia garanticen el libre ejercicio de los derechos fundamentales, creando un equilibrio entre el interés público (seguridad) y las libertades individuales de cada persona, evitando transgresiones o menoscabos individuales. El grado de intromisión de las cámaras no puede resultar de la sensibilidad individual o criterio subjetivo de las partes implicadas, sino que debe proceder de criterios o límites generales otorgados por la legislación al respecto.

Este principio se establece expresamente en el artículo 8.2 del Convenio Europeo de Derechos Humanos: “*toda injerencia de la autoridad pública en el derecho a la intimidad e integridad física debe estar prevista en la Ley*”¹. La legalidad y los límites de la actuación administrativa están previstos en la ley. Jurisprudencialmente se examina este requisito bajo cuatro aspectos, “1) Que la norma jurídica prevea expresamente la actuación impugnada; 2) Si la disposición es accesible al ciudadano; 3) Si está expuesta con la precisión suficiente que permita prever las consecuencias de su acto; y 4) Que exista un medio eficaz contra la interferencia arbitraria de la autoridad pública en el derecho reconocido en el Convenio”².

El segundo criterio es el *principio de proporcionalidad* que se refiere a si la medida optada es proporcional al fin legítimo perseguido (Morenilla 2002). En sentido estricto, de este principio se derivan tres subprincipios. El primero, es el *principio de necesidad* indica que la iniciativa propuesta debe considerarse realmente necesaria para lograr el objetivo propuesto. El Estado debe evidenciar la concreta necesidad del medio empleado, para responder a una identificada exigencia social (Palacios Huerta 2007).

En el caso de los sistemas de videovigilancia, el motivo que justifica su uso se relaciona con los índices de criminalidad, la problemática de inseguridad y la reacción de temor que afecta la calidad de vida de los ciudadanos. El propósito buscado debe referirse exclusivamente a aspectos relacionados con la seguridad, específicamente en la reducción,

¹ (Convenio para la protección de los Derechos Humanos y de las libertades Fundamentales del Tribunal Europeo de Derechos Humanos 2010)

² (Sentencias Huvig y Kruslin 1990) (Sentencia Sunday Times 1979) (Sentencia Malone 1984) mencionado por (Morenilla 2002)

prevención y persecución del delito¹. En este sentido, la medida justifica el fin que el legislador busca alcanzar, afectando en la forma menos gravosa los derechos protegidos, en este caso correspondientes a la esfera privada de los ciudadanos, “es el equilibrio que debe existir entre el medio empleado –la videovigilancia- y el fin perseguido – mayor seguridad” (Parrilli 2012). En una sociedad democrática, el criterio de necesidad quiere decir que los límites sean necesarios para conseguir un fin legítimo. Si existe una “necesaria presión social” en relación con los fines alegados en una sociedad caracterizada por “el pluralismo, tolerancia y amplitud de miras”².

El *principio de idoneidad* declara que la medida es apta para conseguir el objetivo propuesto, debe ponderarse si las cámaras ubicadas en espacios públicos son un medio idóneo para disminuir, prevenir o perseguir la actividad criminal. La jurisprudencia europea ha indicado que “...solo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, siempre de conformidad con su Ley reguladora”³. Y finalmente la intervención mínima que de interpretarse como una ponderación entre la finalidad de la medida y las eventuales lesiones a derechos civiles, como la imagen o la privacidad. A grosso modo: “*el principio de proporcionalidad en sentido amplio implica que únicamente será constitucionalmente admisible aquella limitación o intervención en los derechos y libertades fundamentales que es adecuada y necesaria para obtener la finalidad perseguida por el legislador, que deberá, en todo caso, estar constitucionalidad justificada, y siempre y cuando tal injerencia se encuentren en una razonable relación con la finalidad perseguida*”⁴.

Como se ha expuesto a lo largo del trabajo, los sistemas de videovigilancia son una herramienta tecnológica cuyas características y capacidades son de amplio alcance, motivo por el cual se necesita establecer límites o pautas técnico legales en su funcionamiento de tal manera que se garantice el respeto a los derechos de los ciudadanos. La videovigilancia es una

¹ (Arzoz Santisteban 2010)

² (Sentencia Observer y Guardián contra Reino Unido 1991) (Sentencia Handyside contra Reino Unido 1976)

³ (Berning Prieto 2008)

⁴ Cfr. (De Hoyos Sancho 1997) mencionado por (Pérez Cruz 1997)

práctica gubernamental que realiza el intervencionismo estatal en los espacios públicos y se convierten en una medida de seguridad administrativa orientada a ejercer mayor control sobre los espacios y las personas.

Por eso es necesario constatar que las cámaras de seguridad cumplan con estos tres requisitos: *“que sea medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad) y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad, en sentido stricto)”¹*.

Las videocámaras deben ser instrumentos útiles para la prevenir y perseguir el delito (efectivos en la investigación y resolución del delito), considerarse indispensables en el mejoramiento de la seguridad, y por último, su funcionamiento debe ser lo menos intrusivo en la vida privada de los ciudadanos, minimizando el tratamiento de los datos personales.

El *principio de eficacia* considera si la medida optada es verdaderamente esencial y reflexiona sobre qué tan eficaz es la misma, lo apropiado es hacer una demostración sustentada en presupuestos válidos, como investigaciones empíricas o análisis comparativos de resultados. Para Varona Martínez responder a la cuestión de la eficacia de la videovigilancia *“implica resaltar el interés social, criminológico y policial sobre esta realidad en sus diferentes modalidades de uso y en su impacto en las distintas escalas individuales, relacionales y sociales”* (Varona Martínez 2012, 5).

Es importante resolver interrogantes como ¿si la utilización de sistemas cada vez más intrusivos en nuestra intimidad resuelven o no el problema de la seguridad? ¿Realmente los índices de delincuencia disminuyen a razón de estos mecanismos o realmente a los delincuentes no les importa la existencia ellos? ¿Cuántos procesos penales logra una

¹ (Sentencia 66/1995 1995) (Sentencia 55/1996 1996) (Sentencia del 207/1996 1996) mencionado por (Pérez Cruz 1997, 406)

condenatoria satisfactoria o al menos se resuelven a partir de la incorporación de la prueba visual obtenida por las cámaras de videovigilancia? En definitiva, la utilización de videovigilancia impone la obligación de resolver varias interrogantes. En países como España e Inglaterra se han realizado investigaciones donde se cuantifica la eficacia de estos sistemas, por ejemplo, si en determinada área vigilada las tasas de criminalidad han bajado, en qué tipo de delitos influye la presencia de estos dispositivos, cuantos delitos se han logrado resolver por medio de las imágenes obtenidas de los CCTV, entre otros.

Aunque las investigaciones desarrolladas en el capítulo anterior demuestran resultados variantes y dispersos de la efectividad de los CCTV, lo cierto es que los resultados más significativos se mostraron mayoritariamente en el plano represivo, especialmente para la identificación de personas dentro de una investigación policial o en un proceso penal. Ahora, no se está descartando o invalidando la efectividad de estos sistemas para la prevención de los delitos, lo que sí resulta curioso, es la interrogante que se plantea, si su justificación es preventiva ¿por qué tienen mayor éxito en el plano represivo? En este sentido valdría la pena valorar la proporcionalidad de su funcionamiento.

Como indica Chirino Sánchez en relación a las nuevas tecnologías *“estas poderosas herramientas de observación, de constatación de hechos, de elaboración de perfiles, de anotación y comparación de costumbres y desviaciones, de seguimiento de tendencias y de movimientos” pueden no ser equilibradas dentro del Estado de Derecho y la protección de la dignidad humana ya no constituye un “límite fáctico y real para la construcción de un derecho procesal penal”¹*.

En el plano procesal, los derechos fundamentales sufren una reducción por la implementación de las nuevas tecnologías en la persecución del delito. Las nuevas tecnologías buscan ser más eficientes para contrarrestar la delincuencia y averiguar la verdad real a como de lugar, incluso si implica vulnerar derechos constitucionales (Chirino Sánchez, Protección de datos y moderno proceso penal. Aspectos constitucionales y legales 1999).

¹ (Chirino Sánchez, Protección de datos y moderno proceso penal. Aspectos constitucionales y legales 1999)

Los esfuerzos de las corrientes populistas de “cero tolerancias” y “lucha contra la delincuencia” se han enfocado en instaurar medidas represivas destinadas a repeler con gran fuerza la delincuencia. Por ejemplo, se incrementa el número de cuerpos policiales o se les dota de más armas y equipo tecnológico¹. Si los esfuerzos en materia de seguridad han tenido un enfoque más represivo invirtiendo recursos para ello, pues lo lógico es que los resultados se reflejen en ese plano (Gómez Calderón 2013)²

La desproporcionalidad de la medida por motivos de abusos, usos excesivos o incumplimiento de la normativa por parte de las autoridades estatales, podrían incidir sobre los derechos del ciudadano, principalmente sobre el derecho a la autodeterminación informativa; los Estados en la búsqueda de la seguridad pueden perder el enfoque aplicando medidas excesivas que constriñen el principio de proporcionalidad y que facilitan la recopilación, procesamiento, almacenamiento y transmisión de datos personales de los ciudadanos, sin estar apercibidos de ello. *“El equilibrio de derechos entre los intereses de la colectividad y los del ciudadano, no es cosa fácil de alcanzar cuando hay un acuerdo de que el derecho a la autodeterminación informativa debe ceder, cuando haya un sobrepeso en interés de la seguridad. No obstante, las limitaciones que este derecho sufra han de contar, con un suficiente basamento legal y en la ley que así lo acuerde se establezcan las ponderaciones derivadas del principio de proporcionalidad que resulten necesarias³”*.

Bajo este supuesto, la efectividad de los CCTV podría debatirse o discutirse pues su efectividad no estaría supeditada al funcionamiento correcto del sistema como tal, sino a la desproporcionalidad del mismo. A pesar de que estos sistemas en algunos países han colaborado con la disminución de los índices de criminalidad, han sido insuficientes para disminuir considerablemente la comisión de delitos en general. En este sentido, es importante analizar si la eficacia de las cámaras en la reducción criminal justifica la inversión millonaria

¹ En Estado Unidos Rudolph Giuliani, alcalde de New York y William Bratton, ex jefe de la policía de ese estado desataron una guerra represiva expansiva contra marginados de la sociedad, los resultados una política criminal basada en aspectos discriminatorios como la raza, clase social, etc.

² Uno de los enunciados de los CCTV es que entre mayor sea la cobertura de las cámaras mayor es la efectividad del sistema (Welsh y Farrington 2002).

³ (Chirino Sánchez 2008) mencionado por (Gómez Calderón 2013)

de estos dispositivos. La videovigilancia ofrece un aporte significativo en determinados delitos, en los cuales, suponiendo que los equipos no fallen, es posible la identificación de los implicados y el contexto de los hechos¹.

El *principio de eficiencia*, para que los sistemas de videovigilancia cumplan con el objetivo requerido es necesario el cumplimiento de diversos factores: que la información de su operación sea confiable y transparente, mejorar la comunicación entre la persona operativo de la videovigilancia y los cuerpos policiales, la realización de estudios que demuestren la eficiencia operativa y práctica de estos sistemas, como lo pueden ser la proporcionalidad de cámaras por personas, la capacitación de los operadores en el tema de la videovigilancia y estudios de comportamientos criminal, etc.

El *principio del riesgo* señala que “...la utilización de este medio exige un riesgo razonable para la seguridad ciudadana (videocámaras fijas) o un determinado peligro (videocámaras móviles)” (Berning Prieto, 2008). Bajo la misma idea de la intervención mínima, se escoge de entre todas las alternativas, la menos invasiva a la privacidad del individuo. Se refiere a ciertas prohibiciones en el uso de las cámaras en ciertos lugares y bajo ciertas condiciones ².

El *principio de deber de información* tiene mucha importancia en la práctica, ya que, a partir de él, se abre o no un “portillo” para alegar inconstitucionalidades acerca de estos sistemas. Hace referencia a que la empresa encargada de los sistemas de videovigilancia tiene la obligación de informar a los usuarios - en este caso los ciudadanos-, de las áreas específicas que están siendo vigiladas, es decir el individuo debe estar notificado si su imagen está siendo captada o grabada, esto con la finalidad de que el ciudadano proteja su intimidad y evite expresiones o conductas que puedan exponer aspectos personales.

¹ (Santillán 2007)

² Prohibiciones de las videocámaras para tomar imágenes o sonidos del interior de las viviendas, los vestíbulos, salvo previo consentimiento del titular o previa autorización judicial, ni en los lugares permitidos por ley si se afecta de forma grave y directa a la intimidad de las personas, ni conversaciones de índole privada. Se establece la destrucción inmediata de las imágenes y sonidos obtenidos accidentalmente de este tipo de casos por la persona responsable de su custodia.

Este deber se materializa por medio de rotulación visible en los lugares o zonas públicas que están bajo vigilancia además, debe tener información básica del responsable o encargado de la vigilancia para que el ciudadano pueda ejercer los derechos de acceso y cancelación de las grabaciones, ya que es un elemento esencial para garantizar el derecho a la protección de los datos personales y permite, en su caso, ejercer otros derechos¹.

El *principio de seguridad y deber de secreto*, establece que el responsable de la utilización o tratamiento de éstos sistemas de vigilancia debe establecer pautas procedimentales que garanticen que la información contenida en las imágenes va a ser accesible únicamente para aquellas personas o entidades autorizadas².

Los sistemas de videovigilancia que carezcan de los principios antes mencionados, pueden, eventualmente, declararse inconstitucionales y violatorios de los derechos fundamentales de los individuos, si no se regulan adecuadamente y en pleno cumplimiento de estos. Es necesario enmarcar la videovigilancia dentro del principio de legalidad, dando legitimidad a la Administración. Contar con un marco normativo, garantiza la regulación de los intereses contrapuestos que surgen con la videovigilancia: la seguridad pública y la limitación a las libertades individuales de los administrados.

El *principio de calidad de los datos* indica ciertas características que deben tener los registros: primero, los datos deben ser adecuados al fin, pertinentes, no excesivos, exactos, completos, veraces y claros. También se exige que el tratamiento sea lícito y legítimo, destinados a fines, específicos y su conservación estará limitado a un periodo temporal³. Este principio se reconoce en la Directiva 95/46/CE y en otras normas legislativas, establece que los datos sean actuales y serán eliminados eventualmente, cuando hayan dejado de ser

¹ (Millán Gómez s.f.)

² Artículo 9 de la (Instrucción 1/2006 de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras 2006)

³ (Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos 1995)

necesarios; en caso de no ser veraces o estar incompletos, el encargado de la base de datos, deberá modificarlos o eliminarlos, o bien cuando ya no cumplan con la finalidad propuesta¹.

En la etapa de recolección de los datos se exige el consentimiento informado del titular; como regla general, la captación de imágenes obtenidas en espacios públicos tienen como finalidad la seguridad pública y sólo se obtendrán imágenes cuando resulte imprescindible para dicho fin o resulte imposible evitarlo por la ubicación de las cámaras². El objetivo principal de este enunciado es limitar el registro de los datos a criterios de veracidad y necesidad, en caso de que estos presupuestos cambien o dejen de existir, así lo hará el registro de los mismos.

1.2 Marco Normativo Europeo

A continuación, se mencionan algunos cuerpos normativos que regulan el tema de la protección de datos específicamente en la utilización de los sistemas de videovigilancia en la Comunidad Europea.

El **Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales**, adoptado por el Consejo Europeo el 4 noviembre de 1950, en su artículo 8 promulga el derecho que tiene toda persona del respeto a la vida privada y familiar, del domicilio y de la correspondencia. Sin embargo, establece varios supuestos bajo los cuales las autoridades públicas pueden interferir en la privacidad de las personas: “seguridad nacional, seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”.

De la misma manera se garantiza el mismo derecho en el artículo 7 de la **Carta de Derechos Fundamentales de la Unión europea**; en el artículo 8 se reconoce el derecho a la

¹Artículo 5 b del (Parlamento y del Consejo Europeo 2016)

² (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

protección de los datos personales, estableciendo que el tratamiento debe ser legal, con fines determinado y con el consentimiento del titular o en virtud de otro fundamento legal previsto por ley. Además, se garantizan los derechos de acceso y rectificación al titular de los registros, siguiendo las reglas de control por parte de la autoridad competente. Por otro lado, el Consejo Europeo plantea los procedimientos para utilizar la tecnología de los CCTV acertadamente con la finalidad de proteger la información.

El **Convenio No. 108/1981** del 28 de enero de 1981, emitido por el Consejo de Europa sobre la protección de las personas respecto del tratamiento automatizado de datos de carácter personal, en los que se incluye los sistemas de videovigilancia. *“Las actividades de videovigilancia entran dentro de su ámbito, en la medida en que implican el tratamiento de este tipo de datos, según lo define la Convención n° 108, y el Comité de Consulta¹”*.

Este convenio fue ratificado por 40 países de Europa y se convirtió en el primer instrumento internacional base en establecer normas mínimas en la protección de los datos personales. Este instrumento reúne una serie de principios que rigen la grabación, recopilación, registro, comunicación y tratamiento de datos de carácter personal automatizados que surgen con las nuevas tecnologías de la información. Parte de su contenido limita el tratamiento de datos a determinados fines, a plazos estrictamente necesarios para la conservación de las imágenes, al uso adecuado, y no excesivo de estos sistemas, así como la pertinencia y la obligación de actualizar los datos. Su aplicación rige tanto para el sector público y privado.

Algo importante es la categorización de dato personal que el Comité consultivo le otorgó a las voces y las imágenes, siempre y cuando la información facilite la identificación de la persona, directa o indirectamente², excluye el tratamiento de los datos sensibles y garantiza el derecho que tienen las personas de conocer el registro de la información personal y exigir las rectificaciones que correspondan.

¹ (Lim 2010, 90)

² (Grupo del artículo 29 2002, 5)

La **Directiva 95/46/CE**, relativa a la protección de personas físicas respecto del tratamiento de los datos de carácter personal y a la libre circulación creada el 24 de octubre de 1995 por el Parlamento Europeo y el Consejo Europeo. Recientemente se derogó esta Directiva por el Reglamento General de Protección de Datos (en adelante RGPD) que más adelante se menciona. En su momento, la Directiva se utilizó como base de las legislaciones nacionales referentes a la tutela de los datos, con ella establecieron principios de tutela y obligaron a sus miembros al cumplimiento de los objetivos marcados en sus disposiciones¹. La Directiva propuso la libre circulación transfronteriza de los datos personales entre los Estados miembros, eliminando los obstáculos o trabas en este aspecto, por eso, la importancia de homogeneizar la legislación interna de cada país (ver artículo 1, inciso 2).

La particularidad de esta Directiva es que limita el tratamiento de datos personales a un fin muy particular, el derecho comunitario (ver artículo 3, inciso 2). En relación a la libertad de circulación de datos, ésta tiene dos aristas. Desde el punto de vista del ciudadano, solo puede estar sujeta a restricciones necesarias y proporcionales a la consecución de fines específicos. *“Los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como el seguimiento de su conducta a causa de la utilización desproporcionada de la vigilancia por videocámara por parte de varias entidades en diversos lugares públicos o abiertos al público²”*.

En relación a esta Directiva, en el 2004, las autoridades europeas, específicamente el Grupo del Artículo 29, emitió una resolución que interpretaba las disposiciones contenidas en la Directiva. En ella se menciona la necesidad que tienen las instituciones estatales respectivas de controlar la proliferación de estos sistemas e insta a los Estados miembros a hacer una evaluación general de la videovigilancia para evitar la proliferación desmedida de estos sistemas y evitar la restricción injustificada de derechos fundamentales (Gude Fernández 2014, 86).

¹ (Reglamento relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, del Parlamento y Consejo Europeo, UE 2016/679 2016)

² (Grupo del artículo 29 2002, 6)

También se instó a utilizar otros métodos de vigilancia como la estática convencional que documenta acontecimientos específicos y sus autores; diferente a las nuevas tendencias del desarrollo informático del reconocimiento fisionómico y los programas de análisis conductual, los cuales analizan a la persona como tal, programas que, probablemente, acarrearán riesgos de discriminación y abusos a la esfera privada.

La Directiva en el artículo 6 reconoce el principio de calidad de los datos, faculta al ciudadano a ejercer acciones a su favor como solicitar la rectificación de sus datos, en caso de que éstos no sean reales o verídicos al momento de ser consultados. O bien solicitar cancelación de ellos, en caso de que ya se cumpliera con el propósito por el cual fueron creados¹.

Es una solicitud que hace el titular de la imagen al ente responsable del fichero, para que rectifiquen o borren las imágenes que le ocasionen un perjuicio o se trate de una infracción a las disposiciones de ley. Al ser la imagen un dato personal sobre el que se solicita la rectificación, el afectado no podrá indicar que el dato es erróneo, dado que nuestra imagen es la que es. Sin embargo, la legislación da la posibilidad, al ciudadano de que sus grabaciones sean borradas del fichero cuando se hayan obtenido sin su consentimiento o estas les afecte.

En el artículo siguiente la Directiva se refiere a otros principios relativos a la legitimación del tratamiento de datos mediante videovigilancia, tales como el “*consentimiento inequívoco, la necesidad de obligaciones contractuales, de cumplimiento de una obligación jurídica, de protección del interés vital del interesado, el cumplimiento de una misión de interés público o inherente al ejercicio del poder político, equilibrio de intereses, etc.*”².

¹ Artículo 7 (MSP 2007) y artículo 16 (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal 1999)

² Artículo 7 de la (Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos 1995)

En el artículo 8 mencionan las categorías especiales de los datos entre los que se encuentran los datos sensibles y establece la prohibición del tratamiento de los mismos. Finalmente, en el artículo 33 se reconoce la imagen y el sonido como datos de carácter específico y sensible a partir del cual surge un compromiso para presentar propuestas más acordes o en función de los avances tecnológicos de la información.

La **Resolución N° 1 604** adoptada por el Consejo de Europa el 25 de enero de 2008, pide a los Estados miembros la aplicación conjunta de los “*principios directivos para la protección de las personas respecto de la recopilación y el tratamiento de datos por medios de la videovigilancia*”. Esta resolución es una norma más específica para las operaciones de videovigilancia, que procura homogenizar las leyes nacionales en materia de videovigilancia.

“El Consejo ha afirmado, insistiendo singularmente en las siguientes condiciones: una utilización pertinente, adecuada, y no excesiva respecto de la finalidad que se persigue; evitar que los datos recopilados sean indexados, comparados y conservados sin necesidad; no efectuar una videovigilancia si el tratamiento de los mismos puede producir una discriminación contra algunos individuos o grupos de individuos, por razón de su opinión política, de sus convicciones religiosas, de su vida sexual, de sus características raciales o étnicas; informar claramente y de forma adecuada a las personas, indicando la finalidad del sistema y la identidad de los responsables; garantizar el ejercicio del derecho de consultar sus imágenes y grabaciones y, por último, proteger la seguridad e integridad de todos los afectados por medio de toda medida técnica y organizativa necesaria” (Lim 2010, 92).

Una de las recomendaciones dadas por el Consejo de Europa a sus miembros es prever dentro de sus legislaciones ciertas disposiciones técnicas destinadas a limitar la instalación de estos sistemas, por ejemplo: excluir las zonas privadas del ámbito de aplicación de los CCTV; codificar criptográficamente los vídeos para darle más seguridad a la información; crear mecanismos jurídicos donde el ciudadano pueda acudir en caso de prácticas abusivas de estos sistemas en cuanto a la privacidad e imagen; se exige la señalización uniforme de estos equipos en las zonas físicas donde se encuentran, y por último, se insta a continuar con una

actitud de reflexión sobre la proliferación de estos sistemas a la vista de los progresos técnicos constantes que surgen.

La norma más reciente en materia de protección de datos entró vigor el 25 de mayo de 2016 el **Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento y el Consejo Europeo**. Este reglamento sustituye la Directiva 95/46 que, debido a los cambios del internet, de las nuevas tecnologías y “el big data” se había quedado atrás. Este reglamento garantiza el tratamiento y circulación de datos por parte de empresas privadas y autoridades públicas. Su objetivo es restituirle a los ciudadanos el control sobre sus datos personales, garantizando estándares de protección adaptados al entorno digital en toda la Unión Europea¹. Dentro de las novedades se puede mencionar el derecho al olvido, que es la solicitud del interesado en suprimir los datos cuando ya no son necesarios, el titular decide retirar el consentimiento, o bien, si se han utilizado de forma ilícita.

Se establece que el consentimiento debe ser claro y afirmativo, expreso y no tácito, libre e inequívoco, informado e individual. Esto implica que los responsables del tratamiento de datos deben explicarle al ciudadano, para qué se va a utilizar, por cuanto tiempo y quien será el responsable del tratamiento por el tiempo por el que se van a utilizar. Si se utilizan los datos para diversos fines se deberá pedir el consentimiento separado de ellos². Un cambio que se incluyó fue la portabilidad o el derecho a trasladar los datos a otro proveedor de servicios, esto le permite al titular de los datos pedir, recibir y transferir directamente sus datos automatizados de una entidad a otra. Otra novedad es que se le informa al titular cuando sus datos han sido pirateados, se le exige al responsable de los datos a utilizar un lenguaje claro y comprensible sobre las cláusulas de privacidad y por último, se imponen multas económicas a las empresas responsables del tratamiento en caso de infracción.

En el reglamento se introduce la figura de un Comité Europeo de Protección de Datos, el cual velará para que el reglamento se aplique correctamente y de manera coherente en toda la Unión Europea, las decisiones que tomen son de carácter vinculante. El reglamento abre la

¹ (Reformas de la protección de datos -Nuevas reglas adaptadas a la era digital 2016)

² (Mariño 2018)

posibilidad de intercambio de datos transfronterizos dentro de Unión Europea para cuestiones judiciales y policiales y definen estándares mínimos para el tratamiento de datos en cada país: *“la intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales, sea como víctimas, acusados o testigos, mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas¹”*.

En la aplicación del derecho comunitario (*sui generis*), la Unión Europea ha implementado los códigos de conducta como un método para dirigir un sector o actividad de manera uniforme². Los grupos de legislaciones nacionales plantea una dificultad para la regulación comunitaria. Europa ha hecho grandes esfuerzos por consolidar el uso de los sistemas de videovigilancia y las libertades individuales de los ciudadanos. La creación de éstos convenios asegura la unificación y homogeneidad del tratamiento de datos y el uso de estos sistemas de vigilancia y se garantiza la aplicación adecuada de los principios y disposiciones técnicas/legales en el funcionamiento de los mismos. A continuación, se analizará el contenido de las legislaciones nacionales en materia de vigilancia de dos países, España e Inglaterra.

A. Normas de videovigilancia en España.

España es uno de los países que mayor importancia le ha dado al uso de los sistemas de videovigilancia. Los esfuerzos se han enfocado en regular la actividad de la videovigilancia pública de manera integral y completa. Desde la creación de normas específicas en esta materia, tanto en el sector público como privado, la creación y el fortalecimiento institucional de una Agencia de Protección de Datos para el ciudadano, la creación de herramientas procesales en caso de que algún derecho sea vulnerado, hasta la realización de investigaciones científicas y empíricas que miden la efectividad de los CCTV en la prevención y reducción de la delincuencia. A continuación, el desarrollo de la videovigilancia en el caso español.

¹ (Reformas de la protección de datos -Nuevas reglas adaptadas a la era digital 2016)

² Un ejemplo es el Código de Conducta Europeo de la FEDMA (Federation of European Direct and Interactive Marketing) destinado a la utilización de datos personales en la comercialización directa

A nivel normativo en España puede mencionarse la **Ley Orgánica de Protección de Datos de Carácter Personal** (LOPD 15/1999, de 13 de diciembre), el **Reglamento de Desarrollo de la Ley Orgánica** (RDLOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre), la **Ley Orgánica 5/1992** de 29 de octubre, sobre la Regulación del Tratamiento Automatizado de los Datos de Carácter (acerca del tratamiento automatizado de imágenes y sonidos) establecen los principios rectores y las garantías para el tratamiento de datos personales.

La **Ley Orgánica 4/1997**, de 4 de agosto, regula el uso de videovigilancia en espacios públicos por parte de los cuerpos policiales, y el reglamento que desarrolla su ejecución, es el RD 596/1999, de 16 de abril. El objetivo o fin público de esta norma en la prevención o persecución delictiva, utilizando las imágenes en el plano procesal exclusivamente hay aparente delito.

Esto quiere decir que se excluyen de esta ley, los sistemas de videovigilancia que no cumplan con esta finalidad policial. El funcionamiento de las cámaras de videovigilancia deberán responder a la “prevención de actos delictivos, faltas e infracciones relacionadas con la seguridad pública, la protección de las personas, la conservación y custodia de bienes que se encuentren en situación de peligro especialmente en lugares abiertos al público, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos”¹

La instalación de las cámaras fijas o móviles debe pasar por un proceso de valoración para su posterior aprobación. Primero, se valora qué tan necesaria es la instalación de la cámara en el lugar, y segundo, si dicha instalación supone un incumplimiento de los criterios contenidos en el artículo 4 (se mencionan más adelante). Si la instalación de la cámara es aprobada, debe emitirse una resolución donde se motiva y se indica cuál será el objeto de observación de la cámara. La resolución deberá contener:

1. Identificadas las vías públicas o tramos susceptibles de ser captados por las cámaras.

¹ Artículo 1 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

2. Indicar las medidas técnicas u organizativas que garanticen la conservación, accesibilidad, resguardo e integridad de los registros obtenidos.

3. Deberá indicar quien es el órgano responsable de resolver las solicitudes de acceso y cancelación.

Los criterios de autorización se encuentra contenidos en el artículo 4 de la ley: *“Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos, salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la acusación de daños a las personas y bienes”*.

Las Fuerzas y Cuerpos de Seguridad del Estado son los responsables de utilizar las videocámaras para la captación, reproducción, tratamiento y uso de imágenes y sonidos obtenidos. Los operadores de los centros de comando o *“cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas”*¹.

Los sistemas de videovigilancia pueden estar compuestos por cámaras fijas, móviles, y cualquier otro medio análogo que permita la grabación, ubicados en vías o lugares públicos. Se incluyen, además, aquellas cámaras que, aunque no pertenecen a los cuerpos policiales, ejercen un control y dirección efectiva del proceso completo de captación, grabación, reproducción y custodia de imágenes.

Del artículo 6 establece varios principios, entre ellos el de proporcionalidad, idoneidad e intervención mínima (una cámara es admisible cuando no exista un medio menos invasivo y exista un riesgo razonable para la seguridad ciudadana)² y el deber de información sobre la captación y/o grabación de las imágenes.

¹ Artículo 8 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

² Artículo 6 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

El deber de informar más que un principio es una obligación que tienen los administradores de estos sistemas; sin embargo, es uno de los puntos donde más se incumple; es un elemento esencial del derecho a la protección de datos y su cumplimiento resulta obligatorio. La importancia que reviste este principio es darle a conocer al ciudadano que está transitando por un área bajo vigilancia, que está siendo observado y que sus datos están siendo recopilados (pueden ser cámaras que solo reproducen, o bien, que graban). Si el ciudadano es debidamente informado, podrá decidir si transita o no por esa zona, o tendrá la posibilidad de adecuar su comportamiento a las normas establecidas, sin llamar la atención de las autoridades. Por otro lado, las autoridades argumentan que la rotulación de las zonas vigiladas es una clase de aviso para el delincuente, y que bajo ciertos supuestos es mejor omitir el carácter informativo de las cámaras (por ejemplo, cuando existe una denuncia de crimen organizado o venta de droga en una zona determinada).

Existe una discusión en relación con el deber de informar. La discusión versa sobre si existe la obligación de declarar la utilización de sistemas de videocámaras que no graban imágenes, y si estas generaran un fichero que deba inscribirse. La Agencia de Protección de Datos Española (en adelante la AEPD) ha manifestado que ante la existencia de una videocámara con independencia de que grabe o no, por el solo hecho de que recoge imágenes, debe cumplirse con el deber de informar, pues la simple reproducción de imágenes supone un tratamiento de datos personales¹.

El deber de informar se logra por medio de la instalación de distintivos informativos dentro de las zonas que están bajo vigilancia, específicamente en cada uno de los accesos de las zonas, sean exteriores o interiores. Este deber de información se materializa con los carteles informativos, o bien, con los ficheros. El artículo 3 de la Instrucción 1/2006, señala que los carteles informativos deben ser acordes con el espacio en que se vayan a ubicar las cámaras, además el rótulo debe colocarse en un lugar lo suficientemente visible.

¹ Informe jurídico de videovigilancia obtenido en el sitio web oficial de la Agencia Española de Protección de Datos.

Cuando exista algún tipo de grabación, deben de colocarse los ficheros. El fichero es “un conjunto organizado de datos de carácter personal, que permite el acceso a los datos bajo una serie de criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso”. Nos referimos a cuando las imágenes o vídeos son almacenadas en un soporte informático, que puede ser consultado, revelando datos del día, hora de grabación, cruce de imágenes, el lugar físico registrado, entre otros.

Todos los ficheros deben inscribirse. Los ficheros de titularidad pública deben publicarse su creación mediante en el diario oficial correspondiente y, después se procede a la inscripción. Los ficheros privados deben notificarse a la AEPD previo a la inscripción de los mismos en el Registro General. En el supuesto de los equipos que no graban, sino que solo reproducen o emiten imágenes en tiempo real, no es necesario la colocación del fichero, pero sí es necesario el cartel informativo de que el área cuenta con cámaras de seguridad.

Los ficheros deben contener la siguiente información: la finalidad recogida, indicar quienes son los destinatarios de la información obtenida, cual es el procedimiento de recogida, los usos previstos, donde se ejercen los derechos referentes a los datos personales, la identidad y dirección del responsable del tratamiento, o del representante¹. La ley prohíbe la instalación de cámaras en ciertas zonas como los interiores de viviendas cercanas, vestíbulos, baños o vestuarios o espacios físicos ajenos al específicamente protegido por la instalación.

En el caso de la comisión de un delito, los cuerpos de seguridad, deberán de oficio, aportar la evidencia del delito (copia o soporte de la grabación) y la denuncia al juez en el plazo establecido por ley. Si se tratara de una infracción administrativa se despachará al órgano competente para que inicie el procedimiento sancionador².

Para la conservación de las imágenes se establece el plazo de un mes. Se hace la salvedad, en los casos de infracciones penales o administrativas graves relacionados a la seguridad pública, donde exista un proceso penal o administrativo, con una investigación

¹ Artículo 20 de la (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal 1999)

² Artículo 7 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

policial, un proceso judicial o administrativo abierto. Se prohíbe la transferencia o copia de imágenes y sonidos a terceros¹. En cuanto a las grabaciones obtenidas por estos sistemas, los ciudadanos podrán ejercer sus derechos de acceso, rectificación y cancelación de las mismas (artículo 9). Finalmente, la ley menciona las infracciones y sanciones en caso de que se incurra en una violación en materia de tratamiento de datos personales y los recursos previstos por ley contra las resoluciones dictadas por la instancia correspondiente.

El Reglamento de ejecución de la presente ley es el **Real Decreto 596/1999, de 16 de abril, por el cual se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997**. Este reglamento es un marco jurídico que contempla tres aspectos importantes: determina el régimen de autorización para la instalación de las cámaras (fijas y móviles, la regulación es diferente en ambos casos), describe los principios de su utilización, y por último establece las garantías concretas contra las grabaciones obtenidas. La finalidad del decreto es establecer pautas respetuosas con los derechos de los ciudadanos en la utilización de las cámaras².

A partir del capítulo II, se establecen los procedimientos que deben seguirse para la autorización y utilización de las cámaras fijas y las móviles. El reglamento también contempla la renovación y el registro de las autorizaciones para las instalaciones de las cámaras. A partir del Capítulo III, se define la denominación, naturaleza, composición, funcionamiento y competencia de las Comisiones de Garantía de la videovigilancia. En los últimos capítulos se resalta la importancia del derecho de información al público por medio de las placas informativas, las cuales deben cumplir con una serie de requisitos previstos por ley; señala los plazos y procedimientos para la destrucción y conservación de las grabaciones y finalmente indica los derechos que pueden ejercer los ciudadanos en caso de inconformidades con imágenes obtenidas por estos sistemas.

¹ Artículo 8 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

² (Preámbulo del Real Decreto 596/1999 por el que se aprueba el Reglamento de Desarrollo y Ejecución de la Ley Orgánica 4/1997 1999)

La videovigilancia con fines de seguridad privada se consagra en la **Ley de Seguridad Privada número 23/1992 del 30 de julio** y la **Instrucción 1/2006, del 8 de noviembre**. Esta normativa se aplica a ciertas empresas que ofrecen sus servicios en el ámbito privado, en razón de sus condiciones y cualificación. La Instrucción 1/2006 regula el uso de cámaras con fines y entornos privados.

El propósito de esta ley es regular la captación de imágenes con fines distintos a los policiales, como por ejemplo garantizar la seguridad de edificios, vigilancia y protección de bienes, establecimientos, espectáculos, entre otros; empresas dedicadas a la instalación y mantenimiento técnico de cámaras, dispositivos y sistemas de seguridad y alarmas, sistemas de videovigilancia con y sin acceso a las imágenes, empresas de seguridad que trabajan en conjunto con las Fuerzas de Policía y la videovigilancia laboral.

Las empresas de seguridad que realicen ese tipo de operaciones deberán formalizar su obligación por medio de un contrato que les legitime para el tratamiento de datos. En caso de que la empresa privada capte y/o registre imágenes con fines de seguridad privada, utilice videocámaras o pueda acceder a las imágenes por medio de su personal, es indispensable que el contrato cumpla con las pautas legales en materia de tratamiento de datos y además se reúnan los requisitos legales que habiliten la prestación del servicio. Si la empresa de seguridad tiene prohibido acceder a las imágenes deberá estipularse expresamente en el contrato en conjunto con las obligaciones de confidencialidad y secreto de los datos para el personal que presta el servicio.

En ambos casos la empresa privada y su personal deben cumplir con el deber de secreto, confidencialidad y sigilo en relación con las imágenes. Cuando se detecte o grabe un delito o infracción administrativa el responsable deberá poner en conocimiento a una autoridad competente y pondrá a disposición de la autoridad las imágenes correspondientes.

En España puede hacerse referencia a dos instituciones encargadas de la protección de datos personales con énfasis en los sistemas de videovigilancia. La primera es la **Agencia Española de Protección de Datos**, que “es la encargada de velar por el cumplimiento de la

legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos”¹.

Atiende peticiones y reclamos de personas afectadas, le comunica a los ciudadanos de los derechos que le asisten por medio de campañas de difusión y se asegura de la publicidad de los ficheros de datos de carácter personal. Para los encargados o responsables de los datos “emite autorizaciones previstas en la ley, solicita medidas de corrección, ordena el cese en el tratamiento y la cancelación de los datos en casos de ilegalidad, ejerce la potestad sancionadora en los términos previstos en la Ley Orgánica de Protección de Datos, recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones, autoriza las transferencias internaciones de datos y participa en la elaboración de normas y recomendaciones”².

La resolución del 18 de marzo de 2010, emitida por AEPD se crea la **Sede Electrónica de la Agencia**. Con fundamento en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se *“regula la creación de la sede electrónica como aquella dirección electrónica disponible para los ciudadanos por medio de las redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias”*³. Con ella se materializa el derecho que tienen los ciudadanos de acceder a los datos personales obtenidos por medios electrónicos dirigidos o manejados por la Administración Pública. De esta manera, se les permite a los ciudadanos formular quejas o sugerencias, sea de manera presencial, vía telefónica o electrónica.

La segunda institución son las **Comisiones de Garantía de la Videovigilancia**, estas comisiones son órganos colegiados y tienen autonomía territorial. Son las encargadas de autorizar la instalación de las cámaras. Realizan dos tipos de informes, uno previo para

¹ Artículo 35.1 de la LOPD y artículo 1 del Estatuto de la AEPD mencionado por (Arenas Ramiro 2006)

² Información obtenida del sitio web oficial de la Agencia Española de Protección de Datos (consultada el 19 de febrero del 2018)

³ (Preámbulo de la Resolución de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos. 2010)

autorizar la instalación de cámaras fijas, y uno a posteriori, para las cámaras móviles. Tiene atribuciones consultivas y los informes emitidos tienen carácter vinculante (el informe puede ser negativo o condicionante), entre otras funciones: debe ser informada cada 15 días de la utilización que se le haga a la videocámara, resguarda el soporte físico de las grabaciones de ser necesario, ordena la destrucción de las grabaciones cuando se constate inobservancia de los criterios legales y, formula las recomendaciones que considere oportunas.

Una de las características que tiene la videovigilancia (tanto pública como privada) en España es que su contenido ha sido normado con el rango de ley. Está claro que, a falta de una adecuada regulación los sistemas de videovigilancia pueden afectar directa o indirectamente la privacidad y datos del ciudadano. Enmarcar la videovigilancia con el principio de reserva de ley garantiza el equilibrio entre los dos intereses contrapuestos: la seguridad pública/ciudadana y los derechos concernientes a la vida privada.

La reserva de ley garantiza que una determinada materia sea regulada por ley, y no vía reglamento (Poder Ejecutivo), pues se considera al legislador el cuerpo más representativo de la sociedad, y el más apropiado para regular los derechos, en virtud del principio democrático y del Estado de Derecho, excluyendo así a la Administración como regulador primario de los derechos fundamentales¹. La regulación de los derechos fundamentales está entregada en el orden constitucional exclusivamente al legislador por medio de la garantía normativa de la reserva de ley.

B. Normas de videovigilancia en Reino Unido.

Inglaterra se caracteriza por ser el país con mayor número de cámaras de vigilancia y por tener una de las redes de CCTV más grande del mundo. A pesar de que el gobierno inglés ha invertido millones en su red tecnológica los resultados en la prevención, reducción y persecución del delito han sido poco significativos. A diferencia de Latinoamérica, Inglaterra y España, han realizado estudios investigativos en relación a la efectividad de estos sistemas en el área de la prevención y persecución del delito. Las estadísticas en Londres señalan que

¹ (Nogueira Alcalá 2005)

existe una cámara por cada catorce personas, a pesar de la intensa utilización de las videocámaras solo el tres por ciento de los robos que se cometen en las calles se resuelven con la ayuda de estos sistemas. *“Es importante mencionar que en la actualidad es probable que el número de videocámaras en la Gran Bretaña se aproxime a los 4,2 millones, una por cada 14 personas y que, por tanto, un mismo individuo puede ser grabado por más de 300 cámaras al día. Se calcula que durante los últimos diez años se han invertido unos 500 millones de libras esterlinas del erario público en la infraestructura de cámaras de CCTV, aunque un estudio del Ministerio del Interior llegó a la conclusión de que los programas de uso de CCTV que se han evaluado han tenido un resultado general limitado respecto los niveles de delincuencia¹”*.

Una de las principales críticas hechas a este país, es que el Gobierno ha hecho una gran inversión en la compra e instalación de estos sistemas, transformándolo en un gran gigante tecnológico encargado de vigilar excesiva y abusivamente de los ciudadanos ingleses, y que además han tenido malos resultados en la prevención y persecución del delito. *Per se* a la proliferación de estos sistemas, existe poca legislación encargada de garantizar el derecho de vida privada y protección de datos personales.

El argumento principal que ha incentivado el crecimiento desmedido de estos sistemas es la lucha contra el terrorismo. El gobierno inglés en el afán de querer mitigar los posibles ataques terroristas, ha incurrido en prácticas y políticas inquisitivas sobre sus propios ciudadanos. *“La combinación de cámaras de CCTV, biometría, banco de datos y otras tecnologías forman parte de una red mucho más amplia de sistemas inteligentes interconectados que permiten seguir el mínimo comportamiento de millones de personas en el tiempo y en el espacio, señala el informe. Esa obsesión de las autoridades por saber lo que hace cada ciudadano en todo momento se ha visto espoleada por la llamada lucha contra el terrorismo²”*.

¹ (Téllez Valdés 2016)

² (Los británicos, los ciudadanos más vigilados 2006)

Cada una de las áreas administrativas de Londres (en total son treinta y tres) cuenta con su propio sistema de videovigilancia. Existen además, algunos proyectos de CCTV que son utilizados propiamente por las autoridades públicas en espacios públicos¹. En Inglaterra las cámaras están posicionadas por doquier: en las carreteras y autopistas, estaciones de buses, trenes, aeropuertos, hospitales, escuelas, bancos, museos, centros comerciales, centros deportivos, entre otros. Los sistemas de video-vigilancia son operados por varias instituciones entre ellas la policía, los servicios de seguridad, las agencias gubernamentales e instituciones privadas (Téllez Valdés 2016, 773). Uno de los problemas que se genera al tener múltiples operadores de estos sistemas, es la accesibilidad y trasiego de información de los datos personales de los ciudadanos.

El gobierno inglés, lejos de resguardar la privacidad y los datos de los ciudadanos, ha sido permisivo y poco riguroso en el control de la información. Puede mencionarse el incidente ocurrido con el Consejo de Distrito de Brentwood, el cual entregó a la cadena televisiva BBC material obtenido por medio de los CCTV, donde se apreciaba que un hombre intentaba suicidarse (Carli, Valoración del CCTV como una herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes 2008, 14). El gobierno inglés fue demandado y condenado a pagar los daños y perjuicios ocasionados al ciudadano por la divulgación de las imágenes. Después de estos hechos se obligó al gobierno inglés a crear lineamientos más estrictos y firmes para la entrega de imágenes a terceros.

Las políticas y recursos del Gobierno inglés han estado dirigidas al mejoramiento de la seguridad nacional (atentados terroristas), pública y ciudadana. Sin embargo, ha antepuesto este derecho por encima de otros, y en ese proceso, ha perdido de vista el interés individual, el que concierne al ciudadano. El Gobierno inglés desmedidamente ha utilizado estos sistemas pretendiendo una seguridad que al día de hoy han logrado cambiar minúsculamente, y a ese costo han acordonado las libertades civiles del ciudadano. La normativa inglesa en materia de protección de datos personales y videovigilancia no es muy extensa en comparación con la de otros países de derecho continental como España o Francia, y algunas normativas han recibido fuertes críticas por ser extremas dentro de una democracia.

¹ (Bayes 2010)

El **Decreto de Protección de Datos de 1998**, es la nueva ley que vino a derogar la Ley anterior de 1984 y en transposición de la Directiva 95/46/ce del Parlamento Europeo y del Consejo. El objetivo de esta norma es garantizar el equilibrio entre los derechos de las personas físicas de quienes tienen razones legítimas para usar la información personal. Tiene *“mayor relevancia en la materia y establece los fundamentos jurídicos para manejar información en el Reino Unido, ya que proporciona los instrumentos para que los ciudadanos se sientan más arropados en cuanto a datos personales se refiere”*¹.

En el año 2000 se crea el primer **Código de Prácticas sobre Sistemas de Videovigilancia del Espacio Público** con matices de la Data Protection Act de 1998. En el año 2009, introdujeron dos reformas, primero, la obligación de señalar con detalle el controlador de los datos en los sistemas de videovigilancia pública y segundo, incluir la finalidad de la vigilancia.

La Oficina del Comisionado de Información (Information Commissioner’s Office) es la institución encargada de velar por la protección de datos en el país y se creó mediante el Data Protection Act de 1998. En Reino Unido la normativa de protección de datos, se rigen por dos tipos de códigos de buenas conductas, los primeros emitidos por la Oficina del Comisionado de Información en aplicación de la Ley de Protección de Datos 1998, y los segundos con origen en asociaciones de comercio, los cuales necesitan la consideración y opinión del Comisionado².

El Código de Buenas Prácticas para Sistemas de Circuito Cerrado de Televisión forma parte de los primeros, y está únicamente destinado a los responsables que operan un CCTV u otros aparatos análogos que reproducen o graban imágenes de personas. El Comisionado de Información es el encargado de la formulación y emisión de estos códigos (CANIETI s.f., 173).

¹ (Toledo Báez 2010)

² (CANIETI s.f., 172)

En Código contiene recomendaciones sobre el uso del equipo, la apropiada administración del sistema, selección y colocación de las cámaras y búsqueda y uso de imágenes guardadas. El código permite la publicación o revelación de imágenes a terceras por motivos de persecución del crimen (Carli, Valoración del CCTV como una herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes 2008, 14). Los ciudadanos pueden solicitar un duplicado de las imágenes guardadas en las que aparezca, excepto cuando se trate de salvaguardar la seguridad nacional o exista un supuesto de detección o investigación criminal. Algunos de los lineamientos que pueden encontrarse en este decreto son la manera que deben procesar, obtener, guardar y compartir los datos.

El **Decreto de la Industria de la Seguridad Privada**, es una normativa que regula las empresas que brindan el servicio de seguridad privada, y las obliga a obtener una licencia para el desempeño de esta actividad. Un ejemplo de ello, es la seguridad privada que se brinda a los centros comerciales que incluye patrullajes de agentes de seguridad privados y cámaras de seguridad. Generalmente, la policía local les entrega un protocolo de seguridad asistida y manejo de datos personales. Otro ejemplo muy similar y común son los eventos deportivos o culturales como conciertos musicales (Bayes 2010, 193).

La **Sección 163 de la Ley de Justicia Criminal y Orden Público de 1994** que regula los poderes de las autoridades locales en materia de videovigilancia. El **párrafo b) del artículo 57 de la Ordenanza sobre Telecomunicaciones**, en relación a la vigilancia intrusiva por medio de CCTV, establece el delito para aquella persona que utilice sin autorización del Gobernador, salvo cuando exista un proceso judicial en curso¹.

La **Ley de Regulación de los Poderes de Investigación o RIPA**, es una ley sumamente reciente. Aunque no regula la actividad de la videovigilancia de manera específica, si incluye nuevos mecanismos de control e investigación policial por medio de la videovigilancia. Además, el contenido y trasfondo de la Ley RIPA enmarca peligrosamente el tratamiento de datos personales.

¹ (Examen de los Informes presentados por los Estados Partes de conformidad con el artículo 40 del Pacto 2006)

Esta Ley creada por el Parlamento inglés, regula los poderes de los organismos públicos para llevar a cabo la vigilancia e investigación, y que abarca la interceptación de las comunicaciones electrónicas de la persona. La ley se conoce popularmente como “Snoopers Charter” (Carta de los Fisgonas), fue propuesta en el año 2012 por David Cameron del Partido Conservador, y fue hasta el año 2016 que se convirtió en ley tras el consentimiento real. A pesar de que la ley recibió mucha oposición y fuertes críticas de parte de la ONU y Amnistía Internacional por considerarse una ley de vigilancia intrusiva y violatoria al derecho de privacidad, la ley se aprobó bajo el discurso de lucha en contra del terrorismo, el crimen organizado y la pedofilia online.

La normativa lo que requiere es que las compañías de comunicación de telefonía e internet almacenen los datos (hora y destinatarios de la conversación; el historial de internet y de las apps del teléfono móvil) de los usuarios durante 12 meses, y se le otorgan poderes a la policía, los servicios de seguridad y las agencias oficiales de datos para *hackear* los ordenadores y teléfonos, con la finalidad recolectar masivamente los datos¹. Entre la información que pretenden acceder pueden mencionarse datos personales, páginas web visitadas, medios y redes sociales, aplicaciones, entre otras. *“La ley busca unificar todos los mecanismos de vigilancia y obtención de datos de que disponen las fuerzas de seguridad y agencias de inteligencia británicas. El punto más polémico del borrador es que obliga a las operadoras a almacenar una especie de historial de navegación de todos sus clientes (da igual si se navega desde PC o dispositivos móviles) durante todo un año”²*.

Para lo anterior lo único que se necesita es la orden de autorización de un juez que permita acceder al historial comunicativo del ciudadano, sin embargo, en casos de extrema urgencia no se necesita este requisito³. Además la normativa permite que las agencias de inteligencia y cuerpos de seguridad, accedan a información como *“reservas de viajes, transacciones de bancos o historiales médicos”⁴*.

¹ (Se aprueba la Ley de Poderes de Investigación en Reino Unido 2016)

² (Zahumenszky 2015)

³ (C. Rodríguez 2016)

⁴ (Maza 2015)

La ley determina 5 tipos de vigilancia: la interceptación de comunicaciones (teléfonos, correos electrónicos, etc), la vigilancia intrusiva (vigilancia encubierta en locales, residencias o vehículos privados), la vigilancia dirigida que es una vigilancia encubierta, pero en un lugar público donde se monitorea secretamente movimientos y acciones de objetivos específicos, mediante escuchas o filmaciones. Se trata de investigaciones u operaciones específicas dirigidas a obtener información personal o familiar sobre una persona; las fuentes encubiertas de inteligencia humana que se refiere a agentes o informantes, que bajo la dirección de una autoridad pública, establecen una relación con algún sospechoso para obtener información y comunicarla a las agencias de seguridad o similares y finalmente los datos de comunicaciones (como registros de llamadas telefónicas, correos electrónicos o visitas a sitios web, en este caso, no se releva el contenido, pero si se obtiene datos como fecha, hora, tiempos de duración, destinatario, lugar y momento donde se llevó a cabo la comunicación, entre otros)¹.

Quienes se oponen a esta normativa, y están en defensa de las libertades civiles de los ciudadanos ingleses, sugieren que el almacenamiento de datos procede únicamente en aquellos casos donde exista evidencia suficiente de que la seguridad nacional se encuentra amenazada o ante la eventualidad de la comisión de un delito grave, y debe estar dirigida a personas en particular, y no a clases de ciudadanos en masas².

Aunque la Ley RIPA no se refiere específicamente a los sistemas de videovigilancia, es un claro ejemplo de lo indagador que pueden ser las autoridades policiales o administrativas, y lo expuesto que se encuentran los datos de los ciudadanos ingleses. Un caso extremo de videovigilancia por parte de las autoridades inglesas ocurrió en Peterborough: *“el gobierno implementó un aparato aéreo no tripulado que puede vigilar cualquier terreno y puede despegar verticalmente desde una superficie sólida. Puede viajar aproximadamente entre 30 y 40 millas por hora. La tecnología de CCTV se ha convertido en una importante herramienta de seguridad para unos cuantos países y trata asuntos de protección y seguridad versus derechos individuales”* (Carli 2008).

¹ (Regulation of Investigatory Powers Act 2000 2000)

² (Lorenzetti 2014)

Se puede observar como la videovigilancia ejercida por las autoridades inglesas se torna arbitraria y contraria a las buenas prácticas que rigen la actividad. El principio de proporcionalidad para el caso inglés es ilusorio en la práctica y en la legislación ligeramente mencionado. A continuación, algunos problemas que se derivan de la legislación y del ejercicio de esta actividad en el Reino Unido.

En el Reino Unido, la colocación de las cámaras se ha hecho de manera repentina y con poca planificación. En un principio, no se tomó en consideración el impacto potencial que podían tener estos sistemas sobre el desplazamiento de la delincuencia, la efectividad en la reducción o prevención del delito y las repercusiones sobre los derechos de los ciudadanos (vida privada). En algunos casos, las cámaras tuvieron que quitarse, trasladarse e incluso redistribuirse por zona. *“Se sostiene con mayor determinación que el uso y la colocación de las cámaras se ha hecho un poco al azar (...) Estos problemas son ahora tratados de manera más estructurada gracias al desarrollo de una estrategia nacional para la videovigilancia, con los consejos del Ministerio del Interior. Manifiestamente, esta actividad llega después de que la utilización de esta tecnología haya sido bien establecida”* (Bayes 2010, 194)

La poca o mala planificación en la instalación de estos sistemas y la gran cantidad de cámaras existentes a lo largo y ancho del país, dificultan que la operación de estos sistemas se concentre en una sola institución u organismo. Desde que se inició con los CCTV en 1985 estos sistemas han sido operados por las autoridades locales, es decir, que no están bajo el control directo de las autoridades policiales, aunque sí tienen acceso a las imágenes.

“Siempre se previó que la policía tuviera acceso a las cámaras, ya fuera por medio de los policías en las salas de control o por las imágenes retransmitidas en directo en las salas de control de la policía, donde también se encuentra el personal capacitado para controlar las cámaras, para vigilar los incidentes específicos (...) Ahora hay un cierto número de salas de control de videovigilancia que están situadas en las salas de control de la policía, y aunque los operadores de la videovigilancia son personal que depende de las autoridades locales, los policías tienen acceso constante a las imágenes en directo” (Bayes 2010, 195).

A pesar de que las cámaras no pertenecen directamente a los cuerpos policiales, el Gobierno inglés manifiesta que existe cooperación, rápida respuesta y relaciones eficaces entre la policía y las autoridades locales, lo que contribuye a borrar cualquier tipo de distinción entre ambos en el manejo de la videovigilancia.

Uno de los problemas que se genera a raíz de los múltiples operadores de estos sistemas es la vulneración en el tratamiento de los datos personales; esto quiere decir, que las imágenes (datos personales) de los ciudadanos están en manos de varias instituciones (públicas, privadas, policiales, locales no policiales). Se debe recordar que los CCTV cumplen una función muy específica, que es la prevención, reducción y persecución del delito, por lo que sus fines son meramente policiales y de investigación judicial. Por este motivo, son los cuerpos de seguridad o fuerzas policiales los responsables de manejar y operar estos sistemas.

Otro aspecto importante de mencionar, es que, en Reino Unido, no existe una normativa legal específica para la videovigilancia. La legislación en esta materia se encuentra respaldada por la Ley de Derechos Humanos, la Ley de Protección de Datos y el Código de conducta que enmarca los aspectos relacionados con la videovigilancia. Actualmente, los artículos referentes a la videovigilancia se encuentran dispersas en varios cuerpos legales. *“Hay que señalar que no existe ninguna cláusula legal específica para la videovigilancia en el Reino Unido. No obstante, la legislación, incluida la Ley de Protección de Datos, se aplica a todos y no se limita a los organismos públicos. Además, como ya hemos señalado, la estrategia nacional para la videovigilancia prevé el desarrollo de un código de conducta que cubra todos los aspectos relacionados con la videovigilancia”* (Bayes 2010, 196).

Otro problema que se suscita con los CCTV, es la poca información que tienen los ciudadanos acerca de la presencia específica de estos aparatos. Aunque la ley exige que las cámaras estén anunciadas con un cartel que contenga la información del operador del sistema, el principio de información es escasamente cumplido. Los carteles informativos les permiten a los ciudadanos contactar a los operadores, sin embargo, dichas señalizaciones son casi ignoradas (Bayes 2010, 196).

La videovigilancia también tiene aspectos positivos que son importantes de mencionar. Dentro de las políticas de este país, los CCTV forman parte de una iniciativa cuyo enfoque nacional es el mantenimiento del orden y la seguridad de los barrios, donde los ciudadanos se convierten en auténticos militantes de estos proyectos locales. La seguridad ciudadana parte del principio de que los ciudadanos son agentes activos de la seguridad: se debe promover, incentivar y prevenir, así como beneficiarios de la misma. A pesar de que los CCTV tiene más de 25 años de estar funcionando en este país, las autoridades inglesas y los mismos ciudadanos han llegado a la reflexión de que la instalación y uso de los mismos deben hacerse de manera prudente y analítica. Debe estudiarse la relación costo / beneficio, tomando en cuenta la efectividad de los mismos y las condiciones que favorecen el funcionamiento adecuado de esta tecnología.

La videovigilancia ha demostrado ser una herramienta útil e irrefutable para la identificación de conductas y de personas. Estudios han demostrado *“que la existencia de pruebas obtenidas gracias a la videovigilancia facilita el que la gente se declare culpable en un alto porcentaje, lo que evita el que se haga un juicio y además permite economizar gastos. De hecho, se ha demostrado que en los casos en los que se utilizan imágenes de videovigilancia se dictan sentencias más severas”* (Bayes 2010, 199)

A continuación, se analizará la jurisprudencia nacional de algunos países europeos, así como internacional referente al manejo y uso de los CCTV y su incidencia en los derechos de vida privada, propia imagen y datos personales.

1.3 Jurisprudencia y Casos en Europa

La materia que nos atañe tiene mayor desarrollo jurisprudencial en el derecho comunitario de la Unión Europea. En materia de videovigilancia pública, ellos han consolidado legislación, doctrina y jurisprudencia. A continuación, se analizará algunos criterios emitidos por los Tribunales europeos y también se analizarán varios casos discutidos por los tribunales nacionales de diferentes países, que fueron elevados a instancias superiores

como el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) y los Tribunales de Justicia de la Unión Europea (en adelante, TJUE), entre otros.

Los aspectos importantes de la jurisprudencia tienen que ver con la injerencia que tienen los sistemas de videovigilancia sobre la vida privada y la imagen, violaciones en la recolección de los datos personales (imágenes y voz), interpretación normativa de la materia de CCTV y el tratamiento de datos personales por medio de CCTV. En lo referente a las nuevas tecnologías de información y su influencia sobre el derecho a la vida privada y la propia imagen, los tribunales han determinado la importancia de extender el alcance de ambos derechos. A partir del desarrollo de las nuevas tecnologías, surge la libertad informática como un derecho que complementa y envuelve el derecho a la vida privada y propia imagen¹.

Las nuevas tecnologías no solo interfieren en la privacidad de las personas, sino que algunas de ellas se convierten en herramientas masivas de recopilación de datos personales. A raíz de ello, surgen nuevos problemas y la necesidad de establecer normas y principios que rijan el funcionamiento adecuado de las mismas. Los sistemas de videovigilancia o CCTV forman parte de este grupo².

El TEDH ha señalado que las obligaciones de los Estados incluyen deberes de abstención y obligaciones positivas que giren en torno a un sistema efectivo que permita la seguridad de la vida privada de los individuos y sus familias, dentro de una sociedad tecnológica. Dentro de los estándares del derecho internacional relacionado a las intromisiones en la esfera de privacidad de las personas, se han establecido algunos criterios generales que deben seguir los Estados en el ejercicio de su función pública, para que dichas medidas no resulten abusivas o atenten contra los derechos del ciudadano.

En relación al contenido de una medida intrusiva que afecte la vida privada de una persona, lo primero que han establecido los Tribunales Europeos es que toda injerencia a la vida privada de una persona debe estar autorizada por ley, conforme con el principio de

¹ (Sentencia 292/2000 2000)

² (Caso Hannover 2004)

legalidad. Además, las leyes nacionales de cada Estado deben ser congruentes con los principios resguardados en la legislación comunitaria de Europa. El Convenio Europeo de Derechos Humanos, (en adelante, CEDH), constituye el instrumento legal que conjuga de manera general los derechos fundamentales, bajo el cual queda comprometido cada Estado miembro por cumplir y respetar.

Para que una ley nacional satisfaga los estándares de la CEDH debe ser lo suficientemente accesible para los ciudadanos (as); regular las hipótesis de interferencia con suficiente precisión *“de modo de permitir a los ciudadanos regular su propia conducta”* e incorporar medidas efectivas de resguardo que protejan a las personas frente a intromisiones arbitrarias, tales como limitaciones temporales, evitar la apropiación de la información por terceros, etc.¹. Segundo, las medidas que afecten la privacidad del ciudadano también deben perseguir un fin legítimo: *“típicamente, serán aceptable solo aquellas intromisiones que puedan justificarse como necesarias en una sociedad democrática-² y respetar los demás criterios que cada disposición contemple como fines aptos para la regulación de los derechos”*. Le corresponde a los Estados demostrar que la medida es estrictamente necesaria para poder satisfacer tal fin³.

En tercer lugar, *“...se deben especificar con detalle las circunstancias en que podrán autorizarse injerencias en la vida privada de las personas”⁴*. Esto quiere decir, que la interpretación de las mismas debe hacerse en sentido estricto, evitando regulaciones vagas, amplias, inexactas y que no estén sujetas a controles posteriores. Por último, incorporó *la autodeterminación informativa*, que es la posibilidad que tiene el ciudadano de *“acceder, revisar y demandar la actualización, rectificación o eliminación de datos personales, sea que estos estén contenidos en bancos de datos públicos o privados”*.

Ahora bien, el artículo 8.2 CEDH establece las condiciones específicas bajo las cuales puede habilitarse la intervención de la autoridad, las cuales son: *“la seguridad nacional y*

¹ (Portales 2017)

² (Alston y Goodman 2013, 160) mencionado en el (Portales 2017, 395)

³ Schutter, International Human Rights Law, p. 313 mencionado en el (Portales 2017, 395)

⁴ (Humanos s.f.)

pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral y la protección de los derechos de terceros”. Aunque estos objetivos son amplios, han sido acompañados “de una práctica decisional del Tribunal que ha conferido amplio margen a los Estados a la hora de definir esos intereses. Sin embargo, él mismo suele enfatizar el deber cuidado de los Estados en el ejercicio de poderes tan intrusivos¹”.

En el plano constitucional, los derechos de vida privada y seguridad, son garantías que se amparan en la norma suprema nacional (evidentemente, porque el reconocimiento de ellos data de tiempo atrás y, además, son derechos fundamentales), sin embargo, otros derechos como la autodeterminación informativa, el hábeas data, la protección de datos personales e incluso el derecho a la propia imagen (en algunas constituciones), no se encuentran protegidos expresamente en la Constitución, sino que su protección se encuentra en la ley, ya sea porque su interpretación deriva de otro derecho fundamental, o bien, porque son derechos que surgen a partir de los cambios tecnológicos.

Los sistemas de videovigilancia como medida de seguridad utilizados por los cuerpos policiales deben estar orientados a garantizar el respeto de los derechos civiles del ciudadano. *“El legislador ha de ponderar, pues, los valores constitucionales en juego, de modo que la protección de los medios de actuación de las Fuerzas de Policía no puede suponer un sacrificio de bienes y derechos constitucionales y del propio respeto del Estado de Derecho, ni una limitación efectiva de la posibilidad de verificar judicialmente los abusos o extralimitaciones, por excepcionales que puedan ser, en que eventualmente incurran los miembros de las Fuerzas de Policía en el ejercicio de sus funciones”².*

Se encuentra frente a dos supuestos: primero, la garantía del derecho a la seguridad que le corresponden a las fuerzas policiales y, segundo, las garantías legislativas que deben existir para el ciudadano, en caso de que la función administrativa resulte abusiva a los derechos y libertades civiles. Aplicado a los CCTV, si bien es cierto, son utilizados como

¹ (Mowbray 2007, 591) en (Portales 2017, 400)

² (Sentencia 55/1990 FJ. 5 1990) mencionado por (Arzoz 2002)

medida de seguridad pública y ciudadana, la misma legislación debe dotar de herramientas necesarias al ciudadano, en caso de que estos sistemas violenten su derecho a la vida privada, imagen o protección de datos personales (se refiere a los derechos de acceso de información, oposición, cancelación, rectificación, entre otros).

La Ley Orgánica española reconoce los derechos de acceso, rectificación o cancelación que pueden ejercer los ciudadanos frente a sus datos personales, el artículo 9, inciso 2, de la Ley Orgánica 4/1997, a su vez, señala cuatro excepciones donde la administración puede impedirle al ciudadano el ejercicio de estos derechos: “la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones”.

En este aspecto, el Tribunal Constitucional (en adelante TC) español manifestó que denegarle a un ciudadano el ejercicio de estos derechos atenta contra su derecho de defensa y, además, consideró que estas cuatro excepciones al ser tan extensivas y genéricas dan mucho campo a la discrecionalidad administrativa. La sentencia 292/2000 del Tribunal Constitucional desarrolla cada una de ellas:

- ***“...peligros que pudieran derivarse para la defensa del Estado”***: para el TC esta limitación es bastante indeterminada e incongruente con la finalidad de las cámaras, que según la Ley Orgánica 4/1997 deben perseguir un fin muy específico que es la prevención delictiva, faltas e infracciones administrativas relacionadas a la seguridad ciudadana. El término defensa del Estado es muy ambiguo y amplio.

- ***“la seguridad pública”***: la seguridad pública es el fin legitimador de la videovigilancia, pero la ley debe determinar con precisión los postulados materiales de la limitación del derecho fundamental, pues no se determinan con certeza y previsibilidad los casos específicos en que se aplica esa restricción.

- ***“la protección de los derechos y libertades de terceros”***: esto permitiría al responsable de los datos negarle la propia información al interesado y negar los derechos de defensa que lo protegen. Negarle el acceso, rectificación o cancelación de los datos al interesado *“conllevar abandonar a la decisión administrativa la fijación de un límite al derecho fundamental a la protección de datos de carácter personal sin ni siquiera establecer*

*cuáles puedan ser esos intereses ni las circunstancias en las que quepa hacerlos valer para restringir de esa forma este derechos fundamental*¹. El ejercicio de estos derechos forma parte del contenido esencial del derecho fundamental a la protección de datos.

- “...**las necesidades de las investigaciones**”: el Tribunal Constitucional señaló que sancionar infracciones o faltas administrativas es insuficiente como límite para el acceso a los archivos o registros administrativos. Negarle al interesado el acceso a sus datos personales produce una grave indefensión carente de todo fundamento constitucional². El TC señaló que los cuerpos de seguridad no pueden oponerse al acceso, la rectificación o la cancelación de los datos, tratándose de una investigación administrativa. Referente a la “...protección de los derechos y libertades de terceros” el tribunal considera que es imposible establecer una limitación legal tan genérica. Aunque en el caso de España la legislación reconoce el ejercicio de los derechos civiles de los ciudadanos frente a la recopilación de sus datos personales, a la misma vez lo deniega bajo algunos supuestos que los tribunales españoles consideraron ambiguos y poco certeros (Portales 2017, 395).

El TEDH ha sido muy enfático que las medidas administrativas o policiales que llevan a cabo los Estados en el ejercicio de sus poderes deben ser claras y detalladas de tal modo que no sean arbitrarias³, y sean lo menos intrusivas en la vida privada de los ciudadanos. Dichas interferencias deben tener objetivos definidos⁴; las medidas deben ser necesarias y proporcionales, de tal manera que el Estado disponga de garantías suficientes y efectivas contra los eventuales abusos que puedan cometerse, por ejemplo, evaluar la naturaleza de las medidas, la duración, las bases y condiciones para poder ordenarlas, la autoridad competente, entre otros (Asunto Weber and Saravia contra Alemania 2006).

Aunque los Estados gozan de un amplio margen de apreciación en el criterio de necesidad, el TEDH ha indicado “que la medida será necesaria mientras logre demostrarse que ella, interpretada de manera restringida, responde a un interés social acuciante y es

¹ STC 292/2000 refiriéndose al artículo 24.2 de LOPD, España.

² (Arzoz 2002)

³ (Asunto Weber and Saravia contra Alemania 2006)

⁴ Artículo 8.2 de la CEDH.

proporcionada”¹. El Tribunal Europeo de Justicia, recientemente, sentenció: *“que los sistemas de recopilación masiva o indiscriminada de datos afectan decisivamente la proporcionalidad de las interferencias, en la medida que es tal la cantidad de información a la que se tiene acceso, que permite trazar conclusiones bastante precisas relativas a los hábitos, movimientos, lugares de visita y de permanencia de las personas. Sin duda -prosiguió el TEJ- existe la posibilidad de configurar perfiles sobre las personas construidos a partir de información especialmente sensible”*².

Es imperante que los sistemas de videovigilancia cumplan con los criterios de proporcionalidad, necesidad y fin, evitando que su uso sea con fines de control social; como instrumento de vigilancia masiva, el uso de las cámaras de seguridad deben *“someterse a las condiciones antes identificadas: legalidad, persecución de un fin legítimo, racionalidad medio-fin, necesidad, excepcionalidad, carácter taxativo y estricto de las autorizaciones”*³.

La jurisprudencia del TEDH, como se verá más adelante, permite bajo ciertos supuestos muy específicos y según cada caso, el uso de cámaras ocultas, grabaciones sin el consentimiento del titular de los datos, además se pronuncia sobre la capacidad de registro (almacenamiento) de estos sistemas, la permanencia o temporalidad de su uso en un espacio determinado o generalizado y otra serie de condiciones que matizan en el uso de estos sistemas. Para el caso de la videovigilancia secreta de las comunicaciones el TEDH ha resaltado la importancia de incluir medidas lícitas, adecuadas y suficientes para evitar violaciones a derechos fundamentales⁴.

¹ (Asunto Sommer contra Alemania 2017) mencionado en (Portales 2017)

² (Tele 2, Sverige AB contra Post-och Telestyrelsen y Secretaría del Departamento de Estado contra Watson, Brice and Lewis 2016) mencionado (Portales 2017)

³ (Lanza 2017)

⁴ (Sentencia Klass y otros 1978, 23,50) (Sentencia Malone 1984, 37, 81) (Sentencias Huvig y Kruslin 1990, 24,34,35,56) mencionado por (Arzoz 2002, 166)

Casos elevados a Tribunales Internacionales.

Los casos que se mencionan a continuación versan sobre el uso de los sistemas de videovigilancia en espacios públicos y privados, con fines públicos o particulares. Los aportes son diferentes en cada caso, unos relacionados con la incidencia que tienen sobre la esfera privada del ciudadano, sobre el derecho a la imagen, y otros aspectos como la captación espacial de las cámaras, la posibilidad de obtener datos personales por medio de estos sistemas y su aporte como medio de prueba ante delitos, así como la legalidad o ilegalidad de su obtención y la aplicación del principio de proporcionalidad en su uso y el deber de información, videovigilancia en el trabajo, entre otros.

El asunto *Peck contra Reino Unido*¹, sentó el precedente para determinar cuándo un sistema de videovigilancia transgrede el derecho a la propia imagen y el derecho de protección de datos. En Inglaterra, un ciudadano llamado Dennis Peck fue captado por las cámaras de seguridad mientras caminaba con un cuchillo en la mano por media vía pública, al parecer con intenciones suicidas. Las autoridades policiales intervinieron evitando una tragedia mayor. Dado el éxito que provocó la instalación y uso de las cámaras, un par de meses después, las autoridades realizaron un informe de prensa promoviendo la eficacia de estos sistemas y utilizaron el incidente de Peck. Se publicaron dos fotografías del acontecimiento del señor Peck y omitieron cubrirle el rostro. Las imágenes del intento suicida fueron transmitidas por televisión y difundidas en medios impresos, a pesar de que permitían identificar perfectamente el señor Peck.

El TEDH analizó la necesidad de la difusión de las imágenes y consideró que no hubo un equilibrio entre el interés público y el privado, pues no era necesario la revelación de los datos personales del señor Peck para demostrar la efectividad de las cámaras. Se analizaron diversos factores como la naturaleza y relevancia de los intereses en juego y la gravedad de la intromisión. Para el caso en específico se consideró que el interés público del Estado es perseguir y prevenir los delitos, al ser esa la función principal de los sistemas de videovigilancia, la publicidad debe girar en torno a la efectividad de los mismos. La

¹ (Sentencia Peck contra Reino Unido 2003)

revelación de las imágenes del señor Peck, no correspondían a la comisión de un delito y, por lo tanto, la difusión de las mismas era una intromisión en la vida privada del demandante¹.

Después de siete años de litigio, el TEDH reconoció la violación al derecho de vida privada que sufrió el señor Peck y ordenó al Estado inglés a pagar por los daños ocasionados a Peck. Aunque los CCTV contribuyeron a salvar su vida, meses después la hizo un poco más miserable. Este caso es muy reluciente, porque el TEDH se tomó la tarea y señaló una diferencia sustancial para determinar cuándo un sistema de videovigilancia podía considerarse intrusivo en la vida privada de un individuo:

“...el seguimiento de las acciones de un individuo en un lugar público por utilización de equipo fotográfico que no registra los datos visuales, como tal, no da lugar a una injerencia en la vida privada del individuo. Por otro lado, la grabación de los datos y el carácter sistemático o permanente del registro pueden dar lugar a tales consideraciones”.

En cuanto a los límites de las garantías individuales en materia de videovigilancia, el TEDH ha señalado que *“la revelación y publicación en los medios de comunicación, en el marco de campañas de lucha contra el crimen, de imágenes obtenidas por medio de sistemas de videovigilancia emplazados en la vía pública y a espaldas de la persona filmada, violan el artículo 8.43”* del Convenio².

En el asunto ***Frantisek Rynes contra República Checa***³, el TJUE analizó varios aspectos: primero, se trataba de un sistema de CCTV que almacenaba datos personales, y la finalidad del CCTV que era para videovigilancia privada, pero tenía acceso a un lugar público.

El señor Rynes en múltiples ocasiones le habían quebrado las ventanas de su hogar debido a esto decidió instalar una cámara bajo el techo de su casa. El dispositivo de videovigilancia enfocaba la entrada de su casa, parte de la vía pública y el inmueble enfrente de su casa. Con la instalación de las cámaras fue posible identificar a los agresores y las

¹ (Llanera Conde s.f., 22-23)

² (Sentencia Peck contra Reino Unido 2003) mencionado por (Lim 2010, 91)

³ (Rynes contra Republica Checa 2013)

grabaciones obtenidas fueron aportadas como prueba en el proceso penal. Uno de los acusados pugnó la legalidad de la grabación argumentando que el dispositivo de la videovigilancia violaba las reglas de protección de datos establecidos por la agencia protectora de datos personales del país. Se acusó al señor Rynes de haber infringido varios enunciados de la Directiva 95/46 CE, primero, porque no se obtuvo el consentimiento previo de los titulares de esos datos mientras estaba en vía pública; segundo, no se les informó sobre el alcance y finalidad de la grabación, y tercero, no se le comunicó a la agencia sobre el tratamiento de los datos como corresponde.

El TJUE interpretó que, efectivamente, el sistema de videovigilancia utilizado por el señor Rynes permitía el tratamiento de datos personales y el caso era aplicable al régimen legal de la Directiva 95/46/CE, al no tratarse de una actividad exclusivamente personal o doméstica. Cita: *“La noción de datos personales en el sentido del artículo 2 de la Directiva, abarca toda información sobre una persona física identificada o identificable, entendiendo por identificable todo individuo que pueda ser reconocido, directa o indirectamente, por referencia a alguna de sus características físicas. De esta manera, la imagen de una persona registrada por una cámara es un dato personal, ya que por medio de la misma puede identificarse a un individuo”*¹.

Dado que el sistema de videovigilancia utilizado por el señor Rynes captaba imágenes en un espacio público, no podían acogerse a la excepción del artículo 3, inciso 2, párrafo segundo *“no se aplicarán al tratamiento de datos personales: efectuado por una persona física en el ejercicio de actividades, exclusivamente, personales o domésticas”*. El TJEU determinó que esa exención debía interpretarse en sentido estricto, y que las cámaras de uso doméstico deben limitarse a captar el espacio privado de las zonas de la casa. Otro aspecto importante que se conjuga de la sentencia es que, si el sistema de videovigilancia tiene capacidad de guardar o recopilar imágenes, se está frente al tratamiento de datos personales. Si las imágenes quedan almacenadas en un soporte, se está frente a un tratamiento automatizado de datos personales².

¹ (Sentencia 2014)

² (López Nalda y Boulat 2015)

El TJUE manifestó que el consentimiento no siempre es obligatorio, pues la Directiva 95/46 permite evaluar el interés legítimo del responsable del tratamiento. Tratándose de un sistema de videovigilancia de uso doméstico, el propietario puede alegar interés legítimo de proteger su propiedad, su salud, su vida privada y la de su familia, según el artículo 7 inciso f) los jueces consideraron que el procesamiento de datos personales puede hacerse sin el consentimiento del interesado “...cuando sea necesario para la realización del interés legítimo del responsable del tratamiento o si recabar esa información resulta imposible o supone un esfuerzo desproporcionado de conformidad con el artículo 11, inciso 2 de la Directiva” (López Nalda y Boulat)

Otro caso similar sucedió en Alemania. Un vecino implementó una cámara en la entrada de casa. Cada vez que sonaba el timbre, la cámara se activaba y transmitía una imagen aproximadamente por un minuto, sin almacenar ninguna imagen. En la **Sentencia del Tribunal Supremo del 8 de abril del 2011**:

“se consideró conforme a derecho la colocación de la cámara en este espacio de acceso público, porque tenía como objetivo salvaguardar la propiedad del propietario, y no existía otro medio técnico menos invasivo con los derechos de los transeúntes. Las imágenes obtenidas se utilizaban de manera temporal limitada y restringida, únicamente para que el propietario pudiera identificar a los visitantes de la casa y así poder autorizar o impedir su entrada” (Gude Fernández 2014).

En el asunto **Carmelo, G. contra Gunter, R.**¹, ocurrido en España, uno de los vecinos instala dentro de su propiedad unas cámaras por motivos de seguridad, aunque las cámaras no graban sonido capturan las tres puertas de acceso al domicilio del vecino. El Tribunal Supremo resolvió que, si hubo una afectación al derecho de intimidad porque las cámaras de seguridad permitían ver y grabar las puertas de la casa del vecino y, consideró que para garantizar la seguridad de su vivienda, no era necesario enfocar las puertas del inmueble del vecino y que la medida de instalar una cámara era desproporcional al fin pretendido².

¹ (Sentencia No. 7549/2010 2010)

² (El Supremo sentencia que las cámaras no pueden grabar a los vecinos 2011)

“No se ha acreditado que exista una situación de inseguridad que justifique la colocación de las cámaras, pudiendo establecerse otros medios menos invasivos para garantizar la seguridad”. Se condenó al demandado a quitar las cámaras y a pagarle una indemnización por daños morales al vecino.

En el asunto ***P.G y J.H contra Reino Unido***, del 25 de setiembre del 2001, el TEDH analiza la obtención ilícita de un dato personal (la voz) de unos supuestos sospechosos de robo por parte de los cuerpos policiales. En un supuesto de conspiración para la comisión del delito de robo, la policía procedió a instalar micrófonos ocultos para grabar las conversaciones mantenidas en el piso de uno de los conspiradores. Así mismo, procedieron a grabarlos, mientras se encontraban detenidos en la estación de policía. El material recolectado de ambos lugares (las voces) fue sometido a análisis de comparación.

El Tribunal concluyó una violación del artículo 8 del CEDH respecto a la instalación de los aparatos de escucha en ambos lugares, concretando que no existía base legal para regular el uso de aparatos de escucha por la policía dentro de sus propias instalaciones. El Tribunal estimó que: *“la grabación de la voz de una persona en un soporte permanente para su análisis posterior perseguía manifiestamente, en combinación con otros datos personales, facilitar la identificación de esta persona. Concluye el registro de las voces de los demandantes para dicho análisis ulterior había vulnerado su derecho al respeto de la vida privada”*¹.

Como se mencionó anteriormente, los datos sensibles como la imagen o la voz permiten identificar a la persona. La revelación de cualquier dato sensible puede afectar, directamente, el desarrollo de la personalidad del individuo, la cual forma parte de la vida privada de la persona. En este caso particular, el TEDH reconoció que la recopilación y el almacenamiento sistemático o permanente de datos sensibles atenta contra la vida privada de la persona². En otras sentencias, el TEDH ha establecido algunos criterios que deben seguirse para la recolección de datos sensibles: su uso debe estar limitado en el tiempo, en el espacio y debe haber una sospecha previa de los involucrados en la comisión del delito.

¹ (Sentencia P.G y J.H contra Reino Unido 2001)

² Entiéndase por sistemático cualquier aparato o medio de recolección de datos personales que es indefinido en el tiempo y en el espacio.

Los siguientes casos establecieron jurisprudencia en materia laboral, pero también sientan un precedente del uso de CCTV como medio de prueba para ejecutar un despido justificado por la comisión de delitos como robo o faltas graves por parte de los trabajadores.

En el asunto *Köpke contra Alemania*¹, el TEDH valoró la proporcionalidad en el uso de los CCTV cuando la recopilación de imágenes se hizo por medio de cámaras ocultas, es decir, sin el consentimiento de la persona; el uso de los CCTV tenía como finalidad identificar al supuesto ladrón de un supermercado, en este sentido, el TEDH consideró que las cámaras eran la única herramienta que tenía el dueño para dilucidar los hechos.

Los propietarios de un supermercado en Alemania se percataron de unos faltantes de dinero en uno de sus sucursales. Instalaron provisionalmente un equipo de videovigilancia en la tienda y lograron identificar a la trabajadora que les estaba robando, quien fue despedida. El tribunal laboral alemán confirmó que la instalación de las cámaras era justificada porque no existía otra manera de identificar al responsable y, además, la vigilancia había sido bien delimitada. La trabajadora recurrió la resolución al Tribunal Constitucional alemán y al Tribunal Europeo, pero ninguno de los dos admitió la demanda al estimar que “no había motivo alguno que permitiera suponer que la ponderación hecha por la autoridad laboral hubiera representado una violación a ese derecho fundamental de vida privada.”

El TEDH concluyó que: *“la injerencia en la vida privada del solicitante se limitó a lo necesario para alcanzar los objetivos perseguidos por la videovigilancia. Los tribunales nacionales habían considerado además que el interés del empleador en la protección de sus derechos de propiedad solo podía salvaguardarse eficazmente mediante la recopilación de pruebas a fin de demostrar la conducta delictiva del solicitante en los procedimientos judiciales. Además, la videovigilancia encubierta del solicitante había servido para despejar la sospecha de otros empleados. No había habido ningún otro medio igualmente eficaz para proteger los derechos de propiedad del empleador que hubiera interferido en menor medida con el derecho de la demandante al respeto de su vida privada. En resumen, nada indicaba que las autoridades nacionales no hubieran alcanzado un equilibrio justo, dentro de su margen de apreciación, entre el derecho de la demandante al respeto de su vida privada y el*

¹ (Köpke contra Alemania 2010)

interés de su empleador en la protección de sus derechos de propiedad y el interés público en la correcta administración de justicia”.

Para este caso en particular, se consideraron dos aspectos importantes para considerar la grabación oculta válida: la grabación oculta se realizó sobre la base de una sospecha previa, sobre los trabajadores que existía tal sospecha, y el tiempo de grabación fue de forma temporal¹.

En el asunto ***López Ribalda y otros contra España***, sucedió lo contrario. A pesar de que se trataba igualmente de cámaras ocultas en el trabajo, el TEDH consideró que el patrono había atentado contra el artículo 8 de CEDH, porque la recopilación se había realizado de manera permanente e indiscriminada y, además, sin el consentimiento de los trabajadores, considerando la prueba del despido ilícita.

Una compañía de supermercados instaló en una de sus sucursales un sistema de cámaras visibles y otras ocultas pues detectaron irregularidades entre las ventas y los inventarios de los productos. El patrono informó a los trabajadores sobre la instalación de las primeras cámaras, pero no de las segundas, las cuales se ubicaron encima de las cajas registradoras. Tiempo después se comprobó que varios trabajadores no cobraban algunos productos cuando compraban para ellos mismos o para alguno de sus compañeros. La empresa despidió al grupo de trabajadores que estaban implicados, pero cinco trabajadores inconformes procedieron a impugnar el despido alegando que se había violentado el deber de información previa (el dueño no les había informado la instalación de las cámaras ocultas), y por tanto alegaban una violación al derecho a la privacidad consagrada en el artículo 8 del CEDH, artículo 5 de la LOPD y la Instrucción 1/2006 de la Agencia de Protección de Datos.

Los despidos fueron validados por los tribunales laborales y superiores de Catalunya, al considerar lícita y proporcionada la prueba de los vídeos aportados por el patrono. Los trabajadores elevaron el caso al TEDH, argumentando que la falta de información de las cámaras ocultas, el tiempo ilimitado de su uso (instalación fija y no temporal) suponía la vulneración de los artículos 6 y 8 de la CEDH. El TEDH confirmó “...*que la imagen de los*

¹ (Sánchez Migallón y Monclús Ruíz 2018)

trabajadores debe considerarse incluida dentro del concepto de dato de carácter personal que establece la vigente Ley Orgánica 15/199”.

El TEDH entra a analizar el deber de información cuando se recopilan datos personales, derecho que se materializa con un cartel amarillo de “zona vigilada”, según se abstrae del artículo 5 de la LOPD y de la Instrucción 1/2006 y concluye que en este caso no se cumplió con esta obligación. A diferencia del caso Köpke, considera el TEDH que las cámaras ocultas grabaron de manera indiscriminada a todo el personal y no exclusivamente a los sospechosos, durante varias semanas, sin límite de tiempo y durante todo el tiempo de la jornada laboral, medida que considero desproporcional¹. La jurisprudencia previa exigía para la instalación de las cámaras fijas el deber de información previa y la finalidad de la colocación de estas.

“No puede instalarse cámaras que graben indiscriminada y permanentemente sin esa información previa. Distinto sería el caso cuando la monitorización se hace de manera exclusiva, específica y temporal, constatada la existencia de una sospecha sólida de la comisión de una infracción laboral grave, del personal responsable de la comisión de esos ilícitos”. Cabe “la posibilidad de monitorizar sin información previa, cumpliendo los principios de idoneidad, proporcionalidad y razonabilidad, en el caso de que se den los requisitos antes expuestos: la existencia de una fundada sospecha previa, la vigilancia temporal y exclusiva del personal –en la medida de lo posible, en el sentido de no indiscriminada- sobre el cual se tienen la fundada sospecha”².

En este caso, el Tribunal condenó al gobierno español y a la empresa al pago de daños y perjuicios para cada uno de los afectados³. En este caso particular se estableció la obligación de informar a cualquier persona sometida a videovigilancia en su lugar de trabajo de la existencia de cámaras y satisfacer el deber de información para garantizar el derecho a la privacidad y a los derechos de acceso, rectificación, cancelación y oposición⁴.

¹ (Sentencia 1874/13 y 8567/13 2018)

² (Bercós Tomás 2018)

³ (El TEDH obligue a España a indemnizar cinco cajeras filmadas robando por no informarlas de las cámaras ocultas 2018)

⁴ (Saiz y Saborit 2018)

El caso a continuación, no existe la comisión de un delito de por medio como en los casos anteriores, pero la sentencia viene a establecer el respeto al principio de proporcionalidad en la recopilación y grabación de imágenes y voces con fines de seguridad en material laboral. El Tribunal Constitucional español en la **STC 98/2000, del 10 de abril**, determinó que, si bien es cierto, los patronos tienen el derecho de proteger su propiedad, los medios para llevarlo a cabo deben ser proporcionales al fin y no pueden menoscabar los derechos de los trabajadores.

El dueño del casino La Toja instaló unos micrófonos en dos zonas concretas del lugar, en el área de cajas y en la ruleta francesa, el empleador señaló que la finalidad de estos grabadores era por seguridad. Santiago Aldazábal Gómez en representación de los trabajadores interpuso un recurso de amparo alegando una vulneración del derecho a la intimidad de los trabajadores. La empresa empleadora alegaba que en el centro de trabajo no era posible ejercer el derecho a la intimidad¹, pero el Tribunal consideró que la instalación de dichos micrófonos era una intromisión ilegítima en el derecho a la intimidad dentro del lugar de trabajo, por falta de indispensabilidad de la medida, ya que existía un sistema de seguridad de videocámaras.

“...el sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por el empresa”².

La sentencia de la **Sala Primera del Tribunal Constitucional español número 29/2013, de 11 de febrero**, los tribunales españoles analizaron el deber de información que establece la legislación española en el uso de los sistemas de videovigilancia, entre ellos el

¹ (De la Cuadra 2000)

² (Sentencia 98/2000 2000)

cumplimiento del deber de información previa a los trabajadores acerca del contenido y el objetivo específico del uso de los sistemas de cámaras de vigilancia y control.

Un profesor de la Universidad de Sevilla es suspendido temporalmente de su trabajo y sancionado con su sueldo por irregularidades y ausencias injustificadas en su jornada laboral. Por medio de los CCTV logró comprobarse la información y se aportó como prueba para efectuar las sanciones correspondientes. El profesor recurrió a los tribunales alegando la AEPD no había autorizado de modo expreso el uso de las imágenes para fines de control laboral, ni había sido comunicada formalmente a los trabajadores de la Universidad. Los tribunales laborales rechazaron los alegatos del profesor. Insatisfecho recurrió la sentencia al tribunal constitucional: *“Lo que se discutía fundamentalmente en el recurso era si la utilización de las grabaciones hechas por las cámaras de seguridad para controlar el cumplimiento de las obligaciones laborales debía ser o no previa y expresamente comunicada a los trabajadores interesados”*¹.

El Tribunal Constitucional acogió el recurso y le dio razón al recurrente declarando la obligación que tiene el patrono de informar en forma previa, clara, expresa e inequívoca que las grabaciones podrán ser utilizadas con la finalidad de imponer sanciones disciplinarias por incumplimientos laborales (Casino Rubio 2013). La sentencia aporta varios aspectos. Primero, se reconoció que el derecho a la protección de datos consagrado en el artículo 18.4 CE es un derecho autónomo e independiente (se reconoce expresamente). Segundo, que, dentro de las obligaciones empresariales, el trabajador tiene derecho a ser informado sobre el uso y fin de las cámaras, sin ser necesario su consentimiento. Y, por último, que el empleador no puede cambiarle la finalidad al uso de las cámaras. Es decir, si las cámaras en un principio fueron instaladas para controlar los accesos de ingresos o egresos de personal al campus universitario, no podía variar el destino de las imágenes recabadas, utilizándolas para control laboral.

En el asunto **De La Flor Cabrera contra el Reino de España**, la obtención de las imágenes no se obtuvieron por medio de CCTV; sin embargo, se rescata el criterio del TEDH

¹ (Casino Rubio 2013)

referente al derecho a la propia imagen y vida privada, donde se consideró que la toma de imágenes en vía pública y sin el consentimiento de la persona no constituyen una violación a su vida privada ni al derecho a la imagen cuando la finalidad de dichas fotografías se utilizan como medio de prueba dentro de un proceso judicial.

El señor Cabrera sufrió un accidente de tránsito, mientras paseaba en su bicicleta fue arrollado por un auto. Posteriormente, interpuso una acción civil por daños y perjuicios contra el conductor y la compañía aseguradora, argumentando que a raíz del accidente sufría de secuelas de neurosis post traumática que le acarreó un miedo intenso para continuar conduciendo. La compañía de seguros aportó como elementos de prueba unos vídeos que fueron tomados en la vía pública donde se apreciaba al demandante conduciendo una moto. El objetivo de estos vídeos era desmentir el miedo que alegaba el demandante, y para eso la compañía aseguradora había contratado a una agencia de detectives privados para que realizarán este trabajo. Aunque se indemnizó al demandante, este no quedó satisfecho y recurrió a instancias superiores, además, interpuso una demanda contra la aseguradora argumentando que su derecho a la vida privada y el derecho a la imagen habían sido vulnerados, así mismo exigía que la aseguradora le devolviera todas las grabaciones originales y copias de los vídeos concernidos. Los Tribunales Nacionales españoles desestimaron la prueba alegada por el demandante y consideraron que la prueba cumplía con el objetivo legítimo, las imágenes se tomaron en vía pública, y nunca fueron difundidas públicamente¹

El TEDH señaló que el presente caso “no trata de la difusión de imágenes relativas a la vida cotidiana del demandante, sino exclusivamente de la toma y la posterior utilización de tales imágenes como medio de prueba en el marco de un proceso civil (...) asimismo, las imágenes litigiosas no estaban destinadas a ser publicadas, no habiendo sido realizada su toma de una manera sistemática o permanente”. Además, que la conducción de una moto en vía pública es una actividad susceptible de ser grabada y, las imágenes sólo se utilizaron en el proceso como medio de prueba, por lo tanto, no existió ningún riesgo de explotación posterior.

¹ (Asunto De La Flor Cabrera contra España. 2014)

Para el TEDH, el uso de los vídeos dentro del debate judicial era razonables y legítimos pues las imágenes grabadas tenían la intención de desmentir los supuestos padecimientos e incapacidades del demandante, a partir de los cuales se fundaba la solicitud de indemnización. El TEDH no se alejó del enfoque de los Tribunales Nacionales, y desestimó los alegatos de violación a la vida privada y al derecho de propia imagen del demandante.

De los análisis jurisprudenciales se desprende una corriente orientada a la protección de la vida privada del ciudadano y el respeto de los principios rectores de la videovigilancia. Los Tribunales europeos, tanto nacionales como internacionales, han reflexionado sobre la incidencia que tienen los CCTV sobre la vida privada del ciudadano y sus datos personales. Han procurado establecer los límites temporales y espaciales para su funcionamiento, conciliando los fines de la viodevigilancia (seguridad) con las libertades civiles de los ciudadanos.

A continuación, se analizará el caso de la videovigilancia en Costa Rica. Los proyectos concretos y legislativos que existe en nuestro país, el uso que actualmente le están dando las fuerzas policiales, así como los aspectos relacionados con su funcionamiento operativo.

Sección segunda: Análisis de la videovigilancia en Costa Rica.

En el año 2007, el Ministerio de Seguridad Pública (en adelante MSP) publicó en La Gaceta, el Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos (Decreto 34 104-G-MSP), y su posterior reforma el Decreto 35 532-MSP, en el año 2009 mediante el Sistema Nacional de Video protección Ciudadana. A partir de esa fecha se regula normativamente la video-vigilancia en nuestro país.

Inicialmente, las expectativas del proyecto, era la colocación de cámaras en puntos estratégicos de nuestra capital con la finalidad de prevenir, mejorar y reducir la delincuencia; el proyecto reglamentario estaba diseñado para que fuera el Ministerio de Seguridad (Fuerza Pública) el encargado de administrar y operar estos sistemas en espacios públicos, incluyendo la instalación de las cámaras y la creación de un centro operativo de comando donde llegarían las imágenes. Posteriormente, se sumó la Municipalidad de San José, y otros municipios.

“La idea de colocar cámaras de vigilancia nació en el 2004, pero dos años después, el alto costo de los equipos (de ¢1,5 millones a ¢5 millones) limitó el proyecto gubernamental. Empero, municipios como el de San José, Alajuela, Belén, Cartago y Heredia, entre otros, retomaron la idea y emprendieron la colocación de visores electrónicos manejados por las policías municipales, pero cuyas imágenes son facilitadas a la Fuerza Pública”¹.

A raíz del panorama anterior, se realizaron algunas consultas y entrevistas a la Municipalidad de San José y a la Agencia de Protección de Datos de los Habitantes referentes al funcionamiento de las cámaras de seguridad y al tratamiento de datos que se deriva de estos. A continuación, se desarrolla la información suministrada por ambas instituciones, en conjunto con un análisis del decreto que rige dicha actividad, con la finalidad de determinar si la norma se cumple en la realidad práctica y, finalmente, la jurisprudencia constitucional que existe en nuestro país en relación con la materia.

¹ (Arguedas 2016)

2.1 Sobre el Ministerio de Seguridad Pública (MSP).

En el decreto que regula la videovigilancia en los espacios públicos de nuestro país, el Ministerio de Seguridad de Gobernación, Policía y Seguridad Pública, se legitima como la autoridad competente para llevar a cabo esta actividad. En dicha norma se le otorgan algunas facultades (atribuciones) y responsabilidades a la institución que se detallan a continuación, unas de índole técnica y organizativa y otras de índole legal:

- Son los encargados para planificar, instalar, operar y administrar el sistema de videovigilancia y los centros de captación y almacenamiento de imágenes (centros operativos).

- Son los responsables de custodiar la información sustraída y obtenida de las cámaras de vigilancia, quiere decir, que es el responsable de los datos personales que se obtienen por medio de los CCTV. A esto se le conoce como el deber de confidencialidad y seguridad que básicamente establece accesos controlados a los centros operativos, discreción de la información que obtienen (imágenes) y el resguardo de la información, evitando cualquier fuga o difusión de información personal de los ciudadanos.

- Tiene la atribución de celebrar convenios con otras instituciones para ubicar las cámaras. De igual manera, es el responsable de colocar y mantener los letreros de aviso de las zonas bajo vigilancia.

- Tiene la responsabilidad de darle mantenimiento técnico a los equipos de vigilancia, deben asegurarse que los equipos estén funcionando adecuadamente sin desperfectos o anomalías, solucionar las fallas que se presenten (directamente o por un tercero) a la mayor brevedad.

- Aunque no lo menciona expresamente es importante que el personal conozca a la perfección todos los procedimientos y protocolos de seguridad, especialmente ante la detección de un delito¹.

En resumen, al ser el MSP el responsable de operar y administrar estos sistemas, también lo es de los datos que se obtienen por medio de las cámaras; tiene una legitimidad que le es conferida por medio de la norma, expresamente atribuciones y obligaciones de fondo o procedimientos que debe cumplir la institución para llevar a cabo su función.

¹ (Castellón Sossa 2016)

2.2 Sobre la Municipalidad de San José

El proyecto municipal de videovigilancia inició con veinticinco cámaras de seguridad. Para el año 2016 la red de CCTV contaba con ciento setenta cámaras instaladas, ciento treinta y uno instaladas por el Consejo Municipal de San José y treinta y nueve por el Ministerio de Seguridad Pública. Al día de hoy, el proyecto cuenta aproximadamente con 200 cámaras y es el ente municipal quien opera la mayoría de cámaras capitalinas, pues las que instaló el Ministerio de Seguridad no se encuentran en funcionamiento, según informó la licenciada Mónica Coto, jefa del Departamento de Seguridad Electrónica de la Municipalidad de San José en la entrevista llevada a cabo el 25 de octubre del 2017. En opinión de la licenciada Coto el decreto se creó con la finalidad de que fuera el Ministerio de Seguridad el encargado de operar los CCTV e incluso utilizaron parte de su presupuesto en la infraestructura tecnológica de algunas cámaras instaladas en San José. Sin embargo, el Ministerio Público no pudo llevar a cabo la parte operativa del proyecto.

Las cámaras municipales están ubicadas a lo largo de los distintos distritos de Merced, Carmen, Paseo Colón, Avenida Segunda, Hospital, Catedral, San Sebastián, Zapote, San Francisco, Hatillo, Pavas y La Uruca tiene como principal objetivo detectar la comisión de delitos como hurtos, asaltos, escenas obscenas en las vías públicas, ventas ambulantes o ilegales en las aceras, entre otros. Aunque la inversión es millonaria, dentro del proyecto municipal se desea aumentar el número de cámaras y ampliar la extensión de éstas a parques, boulevares, hospitales, plazas, entre otros. Para la municipalidad, la cantidad de cámaras que operan hasta hoy son pocas, y consideran que se requiere de la instalación de más cámaras para poder mejorar la seguridad pública y ciudadana¹.

“Las cámaras de vigilancia electrónica, son una de las tecnologías de punta que la Policía Municipal de San José está implementado, con el fin de tener un mayor control urbano, con un uso eficiente de los recursos materiales y humanos de los que dispone”².

¹ (Granados 2016)

² (Arias 2011)

Actualmente la Municipalidad es la propietaria de las cámaras y quien administra los sistemas de vídeo-vigilancia. Aunque el artículo 1 permite la colaboración de otras instituciones estatales en la persecución de ese fin, no se faculta expresamente a las municipalidades a ejercer la función y operación completa de estos sistemas, función que le fue concedida en un principio al Ministerio de Seguridad¹. A pesar que la Licenciada Coto afirma que en los centros de comando operativo se cuenta con la presencia de uno o dos oficiales de la Fuerza Pública, a mi criterio, no sólo refleja la poca participación e intervención del MSP en el tema de la videovigilancia, sino que demuestra las contrariedades práctico-legales de estos sistemas: por un lado, la norma faculta al MSP como la autoridad competente pero incapaz de llevar a cabo el proyecto y la Municipalidad de San José, institución que intervino y acaparó un proyecto, que si bien es cierto lo faculta a participar, no le acredita la realización absoluta de esta actividad.

Para la municipalidad josefina, el proyecto de las cámaras es una iniciativa interinstitucional en conjunto: *“En el esfuerzo de coadyuvar, desde el reforzamiento de la prevención, con la Fuerza Pública, la Policía Municipal y el Ministerio del ramo colaboran en el intercambio de información e, incluso, en la verificación cruzada de los datos que generan tanto las cámaras instaladas por el ayuntamiento, como por las que han sido dispuestas por otras entidades públicas y privadas. En el proyecto de vigilancia electrónica (...) participan, a su vez, otras entidades públicas y privadas, que con un espíritu de colaboración, en beneficio de la seguridad ciudadana y de mejorar la calidad de vida de la ciudadanía, han realizado importantes inversiones en tecnología de vigilancia y han confiado en la Policía Municipal para dar buen uso a estos modernos recursos de lucha contra la delincuencia y otras patologías sociales que amenazan el tejido social y el desarrollo económico y humano de la capital”*².

¹ Debe comprenderse que los sistemas de videovigilancia, son una iniciativa que generalmente los promueve los gobiernos locales, así ha pasado en muchas ciudades y capitales de Europa y Latinoamérica. El asunto primordial es que esa facultad debe ser conferida de manera expresa en la norma. En Costa Rica, puede observarse que, aunque existe una norma que faculta a una institución específica, en la práctica la realiza otra entidad.

² Municipalidad de San José, Boletín Informativo de la Dirección de Seguridad Ciudadana y Policía Municipal, 2011c. Mencionado por (Durán Segura 2012, 81)

Vale la pena diferenciar la legitimidad que tiene el MSP como responsable de los datos obtenidos por estos sistemas y la colaboración interinstitucional. El decreto incentiva la participación de instituciones con funciones policiales o judiciales a colaborar en la consecución del fin del decreto. Sin embargo, tratándose de datos personales de carácter sensible, las pautas de competencia y responsabilidades de cada institución deben establecerse claramente, principalmente cuando existe un tratamiento de datos. Una de las preocupaciones que se genera cuando existen varias instituciones que manejan y operan estos sistemas, es el trasiego de la información y los usos que eventualmente se les dé. En el caso de las cámaras con fines públicos orientados a la seguridad, tiene por responsables a los cuerpos policiales, quienes son los que administran, maneja y operan estos sistemas, y en todo caso, los responsables de asumir los problemas que se deriven del tratamiento de datos.

Dado que el Decreto 34 104-G-MSP, solo faculta al Ministerio de Seguridad. Pública, para la vigilancia electrónica de los espacios públicos, se le consultó a la Municipalidad de San José, el fundamento legal que les permitía operar los sistemas de videovigilancia, a lo que contestaron que: *“A la luz de la misma Constitución Política, nacen las Municipalidades y estas a su vez se rigen por una norma especial que es el Código Municipal en el mismo nos encontramos facultados con patrimonio propio y personalidad y capacidad jurídica plena para ejecutar todo tipo de actos y contratos necesarios para cumplir la administración de la jurisdicción territorial. Por lo anterior, dentro del plan de Gobierno se han impulsado como soluciones alternas al eje de seguridad la implementación de seguridad electrónica en espacios públicos y privados con el propósito de satisfacer las necesidades de seguridad de la colectividad afecta a la jurisdicción territorial”*¹.

Aunque existe un decreto que establece la competencia del Ministerio de Seguridad en el manejo de los CCTV, es el ente municipal quien los opera, basándose en la autonomía que la Constitución Política les da a los gobiernos locales. Las atribuciones que la municipalidad se está confiriendo para participar en este proyecto carecen de fundamento y competencia legal, pues lo que están haciendo es una interpretación extensiva de un artículo constitucional, y están pasando

¹ (Coto 2017)

por alto el otorgamiento legal dado expresamente al Ministerio de Seguridad. También, se les consultó acerca de los usos y fines que se les daban a los CCTV:

“EN ESPACIO PRIVADO: Ofrecemos a nuestros habitantes MSJ ALARMAS y dicho servicio consiste en la suscripción voluntaria de un servicio de alquiler y monitoreo de alarmas, cuya finalidad es controlar mediante dispositivos electrónicos los accesos a los bienes inmuebles y promoviendo la respuesta policial cuando se reciba una señal de alerta o de auxilio.

EN ESPACIO PUBLICO: las cámaras de videovigilancia tienen dos finalidades claramente definidas en nuestra Policía Municipal:

1. La Prevención a la ciudadanía: Cuando una imagen se constituye en una ALERTA PREVENTIVA para la ciudadanía, cuya finalidad es informar a la colectividad de un hecho que afecta su libre tránsito o el incumplimiento de la legalidad en espacio público este elemento se constituye en una alerta preventiva. En este caso, la primicia es el informar para que el ciudadano y ciudadana tome las previsiones del caso. El mundo ha evolucionado muchísimo y nuestro país no ha quedado atrás, gracias a esa evolución tecnológica hoy tenemos formas de advertir a nuestros ciudadanos de hechos.

2. La evidencia de un delito: En el caso de la segunda finalidad de la videovigilancia, cuando una imagen se constituye en Evidencia de un Delito, nos encontramos frente a un hecho que solo al Tercer Poder de la Republica - Poder Judicial- (según nuestra Constitución Política) debe conocer y ventilar; por lo tanto, es ahí donde debemos constituirnos en garantes del cumplimiento de la cadena de custodia de un hecho que es regulado por el tercer Poder y es ahí donde lo entregamos cumpliendo un protocolo determinado en conjunto con ese tercer Poder.

2.3 Sobre la Agencia de Protección de Datos de los Habitantes (Prodhab)

Ahora bien, la PRODHAB es la Agencia encargada de proteger los datos personales de los ciudadanos en nuestro país. Mediante la Ley No. 8968 del 7 de julio del 2011 y las nuevas reformas al Reglamento de la misma Ley en el 2016, se crea la Agencia de Protección de Datos de los Habitantes (Prodhab) en nuestro país. De acuerdo con la información obtenida en el sitio oficial la Agencia es un institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, su principal objetivo es garantizar el respeto al derecho a la

autodeterminación informativa de cualquier persona en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Asimismo, orienta al ciudadano a ejercitar sus derechos y a las entidades públicas y privadas que manejan bases de datos, a cumplir con las obligaciones que establece la Ley No. 8 968, de Protección de Datos de la persona frente al Tratamiento de sus Datos Personales”¹.

La Agencia de Protección de Datos de los Habitantes, de conformidad con la Ley N° 8968 y su Reglamento, no posee las atribuciones de un Órgano Consultivo, sino más bien, las de uno de naturaleza resolutoria, por medio de los procedimientos de Protección de Derechos; en consecuencia, sus señalamientos u opiniones jurídicas no son vinculantes.

Además de la Ley No. 8968 y su Reglamento, la Agencia se fundamenta en resoluciones que sobre la materia ha dictado la Sala Constitucional; algunos pronunciamientos que se emite por medio de la Red Iberoamericana de Protección de Datos de la cual es miembro la Prodhav, los cuales pueden “tropicalizarse” al contexto de nuestro ordenamiento jurídico.

Se conversó con la Coordinadora del Departamento de Registro de Archivos y Bases de Datos, la licenciada Karla Quesada Rodríguez con la finalidad de conocer si actualmente la Agencia tiene alguna injerencia o participación en los proyectos de videovigilancia pública de la Municipalidad de San José, pero la respuesta fue negativa, pues no existe proyectos, programas o convenios en común entre la Municipalidad de San José, el Ministerio de Seguridad y la Agencia de Protección de Datos².

También se le consultó sobre la existencia de una base de datos global o interinstitucional en nuestro país, pero la Prodhav desconoce si en los centros penitenciarios, sistemas de cédulas del Registro Civil, el sistema de licencias del Consejo de Seguridad Vial, controles migratorios de los aeropuertos, entre otros, existe una base que recopile datos personales de los ciudadanos.

¹ (Agencia de Protección de Datos de los Habitantes 2017)

² (K. Q. Rodríguez 2017)

La Agencia reconoce que la imagen es el dato personal que más identifica a la persona y es considerado un dato sensible, que debe manejarse con apego a todos los parámetros que la ley establece. Los artículos 3 y 9 de la Ley No. 8968.

El Reglamento de la Ley No. 8968 establece el plazo de diez años para la conservación de los datos personales, periodo que empieza a regir desde la fecha de terminación del objeto de tratamiento, salvo disposición de una norma especial que establezca un plazo distinto o medie interés público para conservar el dato; así las cosas, el mismo es de aplicación en aquellos procesos que lo ameriten, ya que es de observancia obligatoria (ver artículo 11)

Para la Prohab, los presupuestos que limitan el derecho a la protección de datos personales y la autodeterminación informativa son: “la seguridad del Estado, el ejercicio de la autoridad pública y la prevención, persecución, investigación detención y represión de las infracciones penales” (artículo 8 de la Ley No. 8968).

De acuerdo con el Decreto 34104-G-MSP y sus reformas, es posible utilizar las imágenes obtenidas por medio de los CCTV con fines de investigación o persecución policial, como medio de prueba para dilucidar los hechos o la identidad de los sospechosos, sin incurrir en una violación de los derechos civiles, siempre y cuando la fuente de la prueba se haya obtenido lícitamente sin menoscabar los derechos fundamentales de las personas involucradas, buscando el límite entre el principio de la libertad probatoria y la búsqueda de la verdad material¹.

También, se le consultó a la Prohab si hasta el momento existía alguna queja por parte de un ciudadano en relación con el funcionamiento de los CCTV en espacios públicos. A lo que contestaron que no se ha presentado ninguna denuncia que involucre quejas por parte de los ciudadanos respecto al funcionamiento de los sistemas de videovigilancia y el tratamiento de sus datos personales (imagen) en la cual aleguen una invasión a su vida privada; solo se dio una consulta por parte del hospital psiquiátrico sobre el tema, pero el

¹ (Vargas Acuña 2017)

asunto no trascendió a más pues como se mencionó, las opiniones de la Agencia no son vinculantes.

La agencia aún no ha entrado a analizar la viabilidad de crear una ley o un reglamento específicamente sobre videovigilancia; lo que si le corresponde es velar por el cumplimiento de la Ley No. 8968 y su Reglamento; no obstante, debe tenerse en cuenta de que como lo indica el Decreto N° 34 104-G-MSP, establece los parámetros a valorar entre los derechos individuales (derecho a la intimidad) y las garantías de la generalidad, donde obviamente se considera el derecho a la seguridad de los ciudadanos, para poder hacer uso de los mecanismos tecnológicos existentes en la protección de la ciudadanía (buscando proteger el uso de imágenes personales captadas en calles y avenidas públicas).

A continuación, se realizará un análisis del reglamento en mención, tomando en cuenta las causas que justifican la utilización de estos sistemas, se mencionarán algunas críticas que han surgido en la práctica u operación de los mismos, tomando en cuenta las entrevistas que se realizaron en la Municipalidad de San José y la Prodhab, lo anterior a partir del análisis comparativo con Europa.

2.4 Decreto 34 104-G-MSP: Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos

El **Considerando 1** del decreto en mención explica la problemática que sufre nuestro país en cuanto al aumento de la inseguridad y la percepción del problema delictivo. Dos críticas mencionan Cornelis Ramírez en relación con este considerando. Primero, no se citan ni se adjunta en el texto, cuáles fueron los estudios que llevaron a cabo para llegar a esa conclusión, “...lo que evidencia una falta de argumentación necesaria para su instalación”. Segundo, que se toma en cuenta la opinión pública como fuente de derecho, interviniendo los medios de comunicación colectiva. Muy particular del Populismo punitivo que se alimenta del efecto mediático de los medios de comunicación sobre los hechos violentos de los últimos años. Estas formas morbosas de narrar los hechos delictivos han hecho que la inseguridad individual se convierta en una colectiva, haciendo que el ciudadano se sienta cada vez más

inseguro. Resulta muy peligroso dejar que las leyes o las instituciones de derecho se construyan a partir de criterios tan subjetivos como la opinión pública o los medios de comunicación, dejando de lado la objetividad científica (Cornelis Ramírez 2015, 15).

Para Huhn, el discurso de criminalidad en nuestro país carece de objetividad científica y rebosa la opinión de los medios de comunicación. El autor menciona que los medios de comunicación emiten una opinión que carece de fuentes investigativas y, por el contrario, se da por un hecho o por una realidad que la criminalidad existe, que va en aumento y que todos están apercibidos de esta gran problemática¹.

Huhn menciona que cuando se tienen estadísticas o números de criminalidad, se comete otro error: la malversación o mala interpretación de las estadísticas que se usan de manera multidimensionalmente generalizada. El autor menciona que en las estadísticas de criminalidad se deben analizar los diferentes grupos de delitos (individualmente: homicidios, robos, violaciones, narcotráfico, etc.), el lugar donde se comenten (geográficamente), entre otros aspectos. El autor argumenta “...*que las tasas de criminalidad son usadas como un arma poderosa por aquellos interlocutores en el discurso de violencia y criminalidad, para distorsionar la proporción del problema*”².

Los medios de comunicación desempeñan un papel muy influyente en la percepción de seguridad del ciudadano, no obstante, los proyectos o medidas en que incurra la Administración Pública, deben tener una base científica-objetiva que las fundamente y no un simple discurso de opinión pública.

En el **Considerando 2** del decreto también se habla de una reacción institucional positiva, donde los tres poderes de la República se comprometen en la lucha contra la delincuencia. Una de las críticas que hacen al respecto Llobet y Chirino, es que la represión es ligeramente trasladada hacia la prevención, es decir, se previene investigando. Dicen:

¹ (Huhn, Criminalidad y discurso en Costa Rica: reflexiones críticas sobre un problema social 2012, 29)

² (Huhn, Criminalidad, miedo y control en Costa Rica: estadísticas de criminalidad y seguridad pública 2010)

“...la policía ya no tendrá que esperar la existencia de una sospecha para reaccionar (...) Tampoco será necesario, por ejemplo, esperar a que el peligro concreto sea imputado directamente a alguna persona para que el mecanismo de la justicia sea puesto en marcha. La policía y el sistema de justicia penal, en general, asumen sus tareas en lo que con razón llama Kniesel una forma de tutela preventiva de peligros. Esta reacción en una etapa contingente a la producción del peligro implica por cierto, una nueva dimensión operativa del trabajo policial que es en realidad una mezcla verdaderamente exótica de prevención de peligros, defensa frente a riesgos e investigación criminal”¹.

Dado la videovigilancia es generalizada e indiscriminada (no diferencia el criminal del que no lo es) se usan las redes tecnológicas para “hacer visible” al delincuente sin importar la esfera íntima del inocente. En este Considerando, también se habla de la participación del Ministerio de Seguridad Pública como a la autoridad competente para llevar a cabo el funcionamiento de estos sistemas. En el artículo 4 se establece la autoridad competente de estos sistemas.

En relación con el **Considerando 3** del decreto se manifiesta que la seguridad ciudadana es un esfuerzo de todos y se requiere la participación de la ciudadanía. Señala que a raíz del problema de inseguridad, cada vez más ciudadanos y empresas de nuestro país invierten en estos sistemas. Con estas afirmaciones puede percibirse lo lejos que estamos de una cultura reflexiva en el uso de la videovigilancia. Nuestro país está iniciando con la incorporación de nuevas tecnologías en el ejercicio de la función pública, y se demuestra el largo camino que queda por delante. En nuestro país, la legislación e instituciones públicas fomentan la proliferación de estos sistemas, sin percatarse de los resultados y las consecuencias peligrosas que pueden generar.

“Es menester agradecer la confianza de dichas instituciones y empresas y hacer un llamado para que otras entidades se unan en este proyecto de monitoreo electrónico de cámaras de vigilancia, de manera que seamos capaces de vigilar más sectores de la capital y, de este modo, prevenir la criminalidad” (Arias 2011)

¹ (Llobet Rodríguez y Chirino Sánchez, Principio de oportunidad y persecución de la criminalidad organizada (Problema prácticos e ideológicos de un proceso penal “eficiente”) 2000, 172-173)

En nuestro país, se ha manifestado que este tipo de medida es necesaria y efectiva para reducir o prevenir los actos delictivos en nuestras ciudades. Las autoridades estatales han manifestado que la tecnología vendría, sin necesidad de realizar una investigación exhaustiva, a solucionar el problema.

En el **Considerando 6** la imagen se constituye como un derecho conexo a la privacidad, y como tal, es un derecho dual ante sí mismo y ante los demás. Se está frente a dos supuestos. Primero, el Estado puede recopilar la imagen del ciudadano bajo ciertos supuestos; cuando se está frente a la comisión de un delito, la injerencia debe estar prevista por ley, y debe necesariamente, cumplir con los requisitos de legalidad, proporcionalidad y control judicial. Cuando las imágenes son obtenidas bajo estos supuestos, y son utilizadas dentro de un proceso judicial, los derechos de intimidad e imagen no son afectados.

El otro supuesto es cuando se obtiene imágenes que no cumplen con el objetivo previsto o su obtención no cumple con la valoración de legitimidad y licitud, en ese caso, pueden ser manipuladas arbitraria y eventualmente ser utilizada para el ejercicio del poder. En el texto se argumenta la posibilidad de reducir la presencia policial cambiándola por los sistemas de videovigilancia, pues cumplen el mismo propósito:

“Esta conclusión que responde a una lógica jurídica, se confirma y fortalece si establecemos el símil entre la percepción mediante el ojo humano, —el oficial de policía que vigila a los que transitan en una calle pública—, y la captura de esa misma imagen, mediante un instrumento o dispositivo tecnológico, para exactamente el mismo propósito del caso de la presencia humana policial”¹.

En el mismo enunciado se afirma que el recurso humano cayó en desuso, y que hoy en día las grandes ciudades, utilizan y consideran a los CCTV la herramienta más adecuada para llevar a cabo la seguridad:

“(...) la vigilancia mediante el ciudadano policía era, o es, posible en ciudades de limitada

¹ Considerando 6 del (Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos de Costa Rica 2007)

población y de concentraciones geográficas de corta dimensión. Actualmente, en nuestras grandes ciudades, esto se dificulta al punto de hacerla imposible, y se debe acudir a las nuevas tecnologías. Uno de estos mecanismos son las cámaras de toma y proyección de imágenes”

La afirmación de reemplazar el recurso humano por el recurso tecnológico es muy peligrosa por varios motivos. Primero, la tecnología carece de elementos subjetivos como la intuición, que le permite al policía estar alerta ante una determinada situación o determinadas personas que a su criterio podrían llevar a cabo el iter criminis; el razonamiento lógico o capacidad de análisis (psicología policial) que se logra mediante la observación y la experticia. La psicología policial le permite al oficial analizar las conductas, los comportamientos, los movimientos e incluso las respuestas de un posible sospechoso. A modo de ejemplo: los policías de control de aduanas en los aeropuertos tienen la posibilidad de observar y entrevistar a una persona. En ese lapso pueden observar si la persona está nerviosa (sudoración, tics nerviosos, ansiedad, etc.), si se comporta de manera sospechosa, si las respuestas son coherentes o no, entre otras cosas; en el supuesto del delito de tráfico internacional de drogas la presencia policial y la interacción personal entre el policía y el sospechoso es insustituible (a pesar de que los aeropuertos tienen gran cantidad de cámaras). Gracias a la presencia policial se genera la sospecha y, con ello, la detección del delito.

Segundo, a diferencia de las cámaras los policías tienen capacidad de reacción ante la comisión de un delito o ante situaciones de crisis y urgencia. Recordemos que la efectividad de los sistemas de videovigilancia para la prevención del delito depende de varios factores como, la buena comunicación entre el personal del centro de cámaras y los cuerpos policiales, y la rapidez en el despliegue policial. Si se cuenta con un sistema integrado de cámaras, pero falta la reacción policial, las cámaras se convierten en una herramienta que simplemente registra, invalidándose la función preventiva.

Contrario a la presencia policial que sí cumple con la función preventiva; difícilmente el delincuente vaya a cometer el delito si tiene cerca al policía, o bien, si el policía llega durante la comisión del delito puede interrumpir el mismo, evitando la finalización de este y

constituyéndose una simple tentativa del delito. Durante la comisión de un delito, las cámaras únicamente reproducen o registran un evento o personas, corresponde a los cuerpos policiales intervenir para interrumpir el mismo, desde esta perspectiva, los sistemas de videovigilancia se acercan más a un mecanismo punitivo que preventivo.

Finalmente, la información suministrada por las cámaras de seguridad requiere de la interpretación del sujeto. Los CCTV documentan y/o reproducen un hecho o evento específico, el cual se interpreta de manera aislada, y, finalmente, es una “*interpretación óptica subjetiva de los fenómenos observados*”¹, es decir, un desdoblamiento del principio de realidad.

No se está menospreciando la utilidad de los sistemas de videovigilancia para documentar un hecho delictivo, pero no se puede afirmar que las cámaras de seguridad son más efectivas que el recurso humano o que pueden sustituir la presencia policial de los espacios. Sería irresponsable de nuestra parte, dejar el peso de la seguridad pública y ciudadana a cargo de una herramienta tecnológica que solo reproduce o registra delitos, y que está imposibilitada para prevenir o reaccionar ante la comisión del mismo. Si bien es cierto, los sistemas de videovigilancia tienen un mayor aporte en la función punitiva, aun así, presentan problemas en este aspecto. Se piensa en el supuesto del delincuente que toma las precauciones de cubrirse por completo el rostro, y se muda con ropa poco descriptible. En este caso, resulta imposible la identificación del delincuente. Entonces, no puede afirmarse que los sistemas de video-vigilancia siempre aportan un resultado positivo para la persecución del delito en la identificación del sospechoso.

La presencia de los cuerpos policiales en los espacios públicos, es la estrategia policial que previene en mayor grado la comisión de delitos. Es indudable que las cámaras facilitan las funciones de cuidado y vigilancia de la policía, pero la efectividad de estas depende necesariamente de la presencia y reacción policial. No puede afirmarse que las cámaras pueden sustituir el recurso humano del policía. Debe conceptuarse los sistemas de video-

¹ VIRILIO PAUL. La máquina de visión. Documento HTML, obtenido el 16 de mayo de 2010 en <http://www.nodopsicoanalitico.com.ar/virilio.html>. Mencionado por (Cornelis Ramírez 2015, 17)

vigilancia como una herramienta más que se integra a las estrategias policiales de cada ciudad o país; y que como medio de prueba digital tiene un aporte útil y veraz dentro del proceso judicial.

El **Considerando 7** pone de manifiesto que el orden público, en su sentido más amplio, es una limitante de los derechos fundamentales, limitación que es conferida por la Constitución Política. La conservación del orden público constituye una de las causas que justifica el uso de los CCTV en espacios públicos y una limitación de los derechos constitucionales, en este caso derechos como la privacidad o la imagen.

El uso de las cámaras debe responder a fines de investigación policial. Sin embargo, una de las preocupaciones que se mencionó en el primer capítulo es la utilización de éstos sistemas como mecanismo de control social y espacial; esto es, cuando la Administración en el resguardo del orden público vigila sin distinción a todos los ciudadanos, aunque las cámaras deben enfocarse en la prevención y persecución de las conductas delictivas, la vigilancia se hace de manera general, indiscriminada y sin previa sospecha alguna.

Es cierto de que una de las funciones del Estado es velar por el bienestar del colectivo. En el ejercicio de sus potestades de imperio puede limitar las libertades civiles. Sin embargo, entre la función de cuidado/vigilancia y control social hay un hilo muy delgado que se debe evitar caer, límite que recae en el principio de legalidad y el cumplimiento de los principios rectores que rigen la actividad. La legalidad faculta a la Administración y establece los límites a sus potestades de imperio.

Aun cuando el Estado impone medidas para mantener el orden público como es el uso de los CCTV, paralelamente, la ley debe dotar de garantías al ciudadano, que lo protejan de los abusos de poder de la Administración Pública. En el caso de la videovigilancia, los derechos o garantías son conferidas también por ley, tales como el derecho de información: saber de la presencia de las cámaras, los lugares que están bajo vigilancia, conocer los fines de la recopilación de datos, la institución encargada de la videovigilancia; otros derechos como el acceso a la información, derecho de rectificación o cancelación de sus datos personales; y la

existencia de una institución donde el ciudadano pueda hacer valer estos derechos y atienda las consultas y quejas de los ciudadanos relativas al tema. Muchos de los ciudadanos desconocen el funcionamiento de las videocámaras, las repercusiones que pueden tener sobre la esfera privada y las consecuencias de la proliferación de estos sistemas en el futuro.

A nuestro criterio, el **Considerando 8** amplía el rango de discrecionalidad por parte de la administración en relación con el procedimiento de instalación de las cámaras, pues no se establecen los parámetros legales que fundamentan la instalación de la cámara en un lugar público. La importancia de definir un procedimiento para instalar una cámara radica en delimitar la discrecionalidad de los cuerpos policiales, e implícitamente establecer los motivos que justifican la implementación de las cámaras como medida administrativa. El reglamento lejos de definir un procedimiento objetivo para la instalación de las cámaras, empodera a los cuerpos policiales para que estos, bajo criterio propio, decidan sobre la instalación o no de las cámaras en los lugares públicos. No se define las condiciones de temporalidad y espacio, como el plazo de funcionamiento de la cámara o si el lugar permite o prohíbe la instalación de la cámara, respectivamente.

Las medidas administrativas que limitan las libertades civiles del ciudadano, deben cumplir, además, con el principio de necesidad, requieren un fundamento, una justificación para ser implementadas. “*Los motivos de orden público administrativo*” o la “*...perturbación de la pacífica convivencia*” son justificantes muy amplias y ambiguas de interpretar. De la misma manera, aplica el principio de necesidad cuando se trata de la escogencia entre una y otra medida, más o menos lesiva, acorde para que debe cumplir.

A diferencia de nosotros, la legislación española exige la realización dos análisis para la instalación de la cámara, uno *a priori* y otro *a posteriori*. En el primero, se verifica la viabilidad de instalar la cámara en el lugar, así como la necesidad de ubicar la cámara; y el segundo análisis, es para corroborar la efectividad de la cámara para la prevención, reducción o persecución del delito. Además de definir la necesidad y la efectividad de la cámara en un lugar determinado, es importante analizar las condiciones de proporcionalidad bajo las que va a funcionar la cámara: si el lugar es apto para instalar la cámara o bien estudiar la posibilidad

de incorporar una medida menos intrusiva que cumpla el mismo fin (por ejemplo, mejorar la iluminación del lugar, tener más presencia policial, mejorar el control de los accesos, etc.)

Parte de la reflexión que se abstrae de la doctrina y jurisprudencia europea, es que las videocámaras deben instalarse en lugares públicos cuando sea estrictamente necesario y no exista otra medida para cumplir con el fin. Al considerarse los sistemas de videovigilancia una medida administrativa lesiva e intrusiva en la esfera privada del ciudadano, la instalación de los mismos debe ser la *última ratio* de los cuerpos policiales. En esto radica la importancia del análisis previo a la instalación de una cámara, en que le permite a la Administración valorar la necesidad de ubicar la cámara y decidir en instalar la misma o implementar otra medida menos lesiva.

En el mismo considerando se establece que la finalidad de la seguridad es evitar la comisión de delitos, y por medio de la vigilancia es posible comprobar la conducta de los administrados conforme a la ley. Se debe tener claro cuáles son los objetivos de la videovigilancia y definir a quién está dirigida. En la buena teoría debe enfocarse en controlar el fenómeno del delito; utilizar las cámaras para “comprobar la conducta de los administrados” convierte a estos sistemas en dispositivos de gobernanza neoliberal que posiciona la violencia, el delito y los riesgos como núcleo de la actividad política porque opera como mecanismo de control poblacional mientras satisface la demanda de seguridad ciudadana (Zolezzi y Valenzuela Herrera 2017). Ejercer un control social generalizado e indiscriminado, constituye una violación al principio de proporcionalidad y afecta directamente los derechos de vida privada e imagen de la persona, pues se está sometiendo al ciudadano a cierto grado de exposición y escrutinio por parte de la Administración, y que a su vez permite registrar datos sensibles del ciudadano de forma masiva, muchas veces hasta sin el consentimiento.

Finalmente, se menciona que la vigilancia destinada a mantener el orden público, cuyo mandato es preventivo y de control en nuestro país, le corresponde en exclusiva al Ministerio de Seguridad Pública. Y *“no les corresponde a otros sistemas policiales por cuanto el judicial se concentra en la investigación de un delito cometido y el municipal es un sistema*

auxiliar de la policía de cobertura nacional”. Entonces, los sistemas de videovigilancia municipal deberían ser solo un soporte o apoyo en caso de que la red de vigilancia del Ministerio no funcionará o no captarán un delito. Se deja muy en claro de que las cámaras destinadas a la prevención y control de los espacios le corresponden exclusivamente al Ministerio de Seguridad, no a la municipalidad como sucede actualmente.

El **Considerando 9** del reglamento hace alusión al uso de las cámaras por parte del sector privado. Manifiesta que cada vez son más las instituciones públicas y privadas, las que recurren al uso de estos sistemas con la finalidad de resguardar la propiedad privada y la seguridad de la ciudadanía. Es una realidad que los CCTV se han ido incorporando paulatinamente en nuestra sociedad por empresas privadas e incluso en los hogares de los particulares. Gran parte de comercios o industrias utilizan las cámaras para controlar y vigilar el desempeño de los empleados, también por motivos de seguridad son colocadas en accesos de ingresos, parqueos, vestíbulos, incluso en los medios de transporte como los buses. También los utilizan los particulares en sus hogares, condominios o apartamentos, principalmente por motivos de seguridad privada y protección de la propiedad privada.

A diferencia de España (la Instrucción 1/2006, de 8 de noviembre), Costa Rica carece de una norma específica que regule el uso o la prestación de servicios de cámaras de seguridad por parte de empresas privadas de seguridad o vigilancia electrónica. Aunque la seguridad con fines privados no se ha establecido en nuestra legislación, existe jurisprudencia de la Sala Constitucional, donde se analiza la posible afectación al derecho a la intimidad, refiriéndose a la instalación de cámaras en lugares privados. En las primeras sentencias, la Sala consideró que no existía una afectación del derecho a la vida privada de los involucrados; los pronunciamientos más recientes han sido más proteccionista con los derechos civiles del ciudadano.

En otra línea de ideas, para que el derecho a la privacidad del ciudadano sea asegurado, se debe anunciar la presencia de las cámaras “*mediante rótulos suficientemente visibles*”. En la práctica, la gran mayoría de lugares públicos o privados que están siendo monitoreados no tiene esta señalización que la ley impone como obligación, específicamente

en el artículo 7 del decreto, se indican que debe ser en lenguaje claro y sencillo, y establece las dimensiones métricas del mismo, textualmente: *“CIUDADANO: PARA SU SEGURIDAD PERSONAL Y LA DE SUS BIENES, ESTE SECTOR ESTÁ CUBIERTO POR CÁMARAS DE VIGILANCIA. MINISTERIO DE SEGURIDAD PÚBLICA”*

La Municipalidad de San José, rotula las cámaras con una placa pequeña donde se indica que la cámara es propiedad de la municipalidad de San José. Sin embargo, la placa no cumple con las especificaciones que indica el reglamento, ni en el tamaño ni en la visibilidad de las letras, lo que trasgrede el principio de legalidad y de información del ciudadano. La importancia de cumplir con las especificaciones técnicas del rótulo (tamaño grande, con letras visibles y de color llamativo) es informar al ciudadano de la presencia de las cámaras, con ello se obtiene el consentimiento expreso, preciso e inequívoco del ciudadano, es decir, se está dando por informado y acepta implícitamente la reproducción o recopilación su imagen.

Actualmente, se carece de una institución que se encargue de analizar la finalidad, necesidad y ubicación de la cámara en determinado lugar, cerciorando que se cumpla la normativa y determine si la instalación de una cámara viola o afecta algún derecho del ciudadano. Actualmente, no existe un procedimiento de priorización de los lugares a monitorear; es la Municipalidad josefina quien determina, a criterio propio, la ubicación de las cámaras. Para ello, toma en consideración la peligrosidad de la zona, la concurrencia o afluencia de tránsito, o bien por solicitud de algún interesado. Aunque tenemos la Prodhav, la agencia no tiene injerencia alguna en el funcionamiento de los CCTV. Mientras que en España, la AEPD se ha encargado de adaptar las cámaras a la normativa referente a la protección de datos: supervisa que el uso de las cámaras esté en apego a los principios y normas del tratamiento de datos personales, atiende consultas y quejas de los ciudadanos, impone sanciones, lleva un registro de inscripción de ficheros (de las cámaras) y del responsable del tratamiento de datos¹.

No se trata solo de instalar cámaras por doquier con la intención de proveer seguridad pública y ciudadana, desconociendo los alcances, límites o consecuencias que tiene la tecnología sobre la vida cotidiana de las personas. Es necesario, que los gobiernos locales

¹ (Gil 2012)

analicen las repercusiones que implican las medidas administrativas, entre ellas, los sistemas de videovigilancia pública y privada.

En el **Considerando 10** se indica que las imágenes tomadas únicamente para investigaciones policiales no se considerará una transgresión o amenaza de violación de derechos fundamentales; únicamente el Ministerio Público o al Organismo de Investigación Judicial tendrán acceso a los registros de vídeos o imágenes de la persona sospechosa de cometer un delito, mediante orden judicial previa.

En relación a la ilicitud en la obtención de datos personales por medio de grabaciones (imágenes o voz), nuestra legislación indica que se debe de analizar el quién (quién obtuvo las grabaciones) y el cómo (qué medios utilizó). En el caso de las imágenes y tratándose de un delito, los medios de comunicación masiva como las cadenas televisivas, acostumbran a difundir la información, sobre todo, cuando existe un interés de parte del emisor en que se difunda la información; por ejemplo, empresas privadas que han sido víctimas de robo o asaltos, y difunden la noticia por los medios de comunicación televisiva. Para las voces nuestra legislación manifiesta que se puede incurrir en un delito si la captación se hace en desconocimiento del titular¹.

La captación indebida de la voz o de la imagen (datos personales) pueden acarrear para la víctima una violación del derecho al secreto de las comunicaciones e incluso al derecho a la intimidad; las implicaciones para el imputado podrían ser beneficiosas dentro del proceso penal, pues si la captación del dato personal se hizo de manera ilegal, se podría prescindir de la prueba procesal; la captación indebida del dato puede trascender en la afectación de uno o más derechos. Por ejemplo, existe una intromisión indebida al secreto de las comunicaciones, cuando la grabación y su posterior reproducción no cuentan con el consentimiento de la persona, los mecanismos de obtención no cumplen con las pautas establecidas por ley, y no acontece a un acto público. Pero, si las imágenes o la voz trascienden al ámbito público, los derechos de imagen, privacidad e incluso el honor podrían verse afectados.

¹ Artículo 198 del Código Penal de Costa Rica.

En palabras de Cornelis Ramírez “...este ilícito opera en principio si se logra demostrar que la afectación a la intimidad no es superior al perjuicio que podría sufrir si quien captura la grabación es víctima y sea para la demostración de un delito por parte del ofendido” (Cornelis Ramírez 2015, 11). Implica una valoración de las posibles afectaciones que se puedan generar por motivo de las grabaciones. Por ejemplo, en el caso de un secuestro que los familiares del ofendido graben las conversaciones que mantuvo con el secuestrador. En un proceso judicial es más importante identificar al sospechoso, que la afectación del derecho a la privacidad que este pueda alegar (por la ilegalidad de la captación)¹. En criterio de la Sala no se viola el derecho a la intimidad, cuando la persona que obtiene las grabaciones está siendo víctima de un delito, las que podría, eventualmente, aportar al proceso judicial como medio de prueba legítima.

En el **Considerando 11** se retoma la importancia de advertir a la ciudadanía de las áreas que están siendo monitoreadas. El deber de información es de vital importancia porque le permite al ciudadano ejercer su derecho a la autodeterminación informativa en relación al consentimiento en la obtención de los datos, así como el procesamiento, que incluye conocer los fines y usos de dicha recolección, la institución encargada del tratamiento y verificar la transparencia en el tratamiento de sus datos. Si no se cumple con este deber el ciudadano no tiene manera de saber que sus datos personales están siendo recopilados por la administración, desconoce la finalidad y el uso que le pueden dar a estos.

Una de las preocupaciones que manifiesta Cornelis Ramírez en relación con **artículo 1** párrafo segundo es la autorización que se le da al sector privado para colaborar en los fines del decreto, pues se generan dudas “sobre la obtención, manipulación y archivo de las imágenes y filmaciones obtenidas en lugares públicos” (Cornelis Ramírez 2015, 24).

Como se ha mencionado, en nuestro país no existe una normativa específica que regule los sistemas de videovigilancia con fines privados, por ende, una invitación como lo sugiere el texto es ambigua. Hemos dicho que toda injerencia del Estado en la vida privada de los ciudadanos debe estar prevista por ley (principio de reserva de ley), esto implica necesariamente la existencia de una norma que otorgue facultades, deberes y

¹ (Voto No.48-2001 2001)

responsabilidades a la institución que lleve a cargo la actividad. El tratamiento de datos sensibles como la imagen requieren un fuero de protección especial que minimice eventuales riesgos o daños a la privacidad, honor o dignidad de la persona, de ahí la necesidad de que la participación de instituciones o empresas privadas está determinada por una norma (la competencia, facultades, deberes, responsabilidades, etc.).

Para el autor, es necesario que se determine hasta dónde llega la participación de las empresas privadas en el uso de estos sistemas, debe especificarse si es para alquiler o compra, mediante licitación o contratación de servicios privados de videovigilancia. Lo anterior por cuanto en la compra, no habría mayor participación que la de un proveedor comercial. Sin embargo, en el caso de alquiler del equipo, licitación o contratación de servicios por parte de la empresa privada, la participación podría involucrar el acceso a la información y el tratamiento de datos personales. El texto actual es impreciso y ambiguo, pues no determina los límites de dicha participación. Cuando la participación de la empresa privada interfiere con el procesamiento de datos personales, es preferible que se regule en una norma dicha la prestación.

Además, esta extensión o participación de la empresa privada, se torna una vez más contradictoria con lo establecido en el artículo 4 del decreto, donde se manifiesta que el Ministerio de Gobernación, Policía y Seguridad Pública es la autoridad competente y legítima para llevar a cabo esta actividad.

El **artículo 2** del decreto determina que la finalidad de los sistemas de vídeo-vigilancia es utilizar las imágenes obtenidas a través de los CCTV dentro del proceso penal como medio de prueba, incrementando la efectividad de las investigaciones y persecución judicial de los delitos ocurridos en vía pública. El principio de legitimación del fin establece que:

“las intervenciones o injerencias secretas en los derechos fundamentales, a través de las ya mencionadas medidas de investigación deben servir para la protección, por medio de la persecución penal, tanto de bienes jurídicos individuales como la vida, la salud y la libertad, así como de bienes jurídicos como el Orden Constitucional Democrático y Liberal, la Existencia y Seguridad del Estado o de intereses políticos de defensa del Estado u otros

intereses de valor significativo, cuyo mantenimiento es mandato constitucional (Schwabenbauer, 2013)”¹

En este contexto las imágenes obtenidas por las cámaras tendrían la finalidad de identificar a los sospechosos de cometer un delito o bien esclarecer los hechos acontecidos; esta prueba digital tendría que cumplir con los principios probatorios que rigen el proceso penal, los requisitos de admisibilidad procesal y la cadena custodia de las imágenes. Los operadores de estos sistemas, deben cumplir con los deberes de confidencialidad y seguridad, asegurando que el uso de las imágenes sea acorde a los fines preestablecidos.

Otro aspecto ligado a la efectividad que debe considerarse es la relación costo-beneficio. Las cámaras de seguridad conllevan una gran inversión económica y tienen un alto costo empezando por la compra, el mantenimiento, la capacitación del personal, entre otros aspectos. Antes de adquirir estos sistemas es importante que la Administración Pública valore la efectividad que tienen los mismos en las mejoras de las condiciones de seguridad pública y ciudadana; evidenciar si existen otras medidas menos costosas y más efectivas, o bien, un complemento de la tecnología en las funciones policiales.

En el **artículo 5** se indica que las cámaras deben estar posicionadas en lugares altos de poca accesibilidad a la mano humana, y aunque no se especifica podrían ser fijas o móviles. Una de las críticas que Cornelis Ramírez hace en relación con el posicionamiento de las cámaras es que cubren una extensión espacial muy grande.

“No se especifican los criterios para la selección de los lugares, lo que deja abierta la posibilidad de que puedan violar el derecho a la intimidad al capturar imágenes en domicilios particulares o recintos públicos destinados a fines particulares, hasta el ámbito intangible de la intimidad (...) si dejamos únicamente a la policía la facultad de valorar dónde se instalan las cámaras sin ninguna posibilidad del ciudadano de cuestionar la ubicación, se estaría violentando también el derecho a recurrir las decisiones estatales”²

¹ (Romero Sánchez 2015, 329)

² (Muñoz Conde 2005) Comentarios a la sentencia del 3 marzo de 2004 del Tribunal Constitucional Alemán mencionado por (Cornelis Ramírez 2015, 26)

Además, el enunciado indica que la información obtenida de las cámaras se podrá conservar por el tiempo que ellos estimen necesario. Sin embargo, uno de los aspectos más importantes que deben respetarse en la actividad de la videovigilancia pública es la temporalidad de su uso, es decir, la fijación de su uso por un período de tiempo determinado, a partir del cual se analice la necesidad y procedencia de la cámara.

En el tratamiento de datos personales debemos recordar que la imagen es un dato sensible, como tal, debe tener la garantía de un plazo establecido por ley, una vez cumplido el plazo la información debe eliminarse cualquier resguardo (disco duro, memorias o bases de datos). En cuanto al plazo de conservación de la imagen surgen varias disparidades. Primero, la Prodhab indica el plazo de 10 años de almacenamiento, refiriéndose a datos personales en general y no solo a la imagen. Por otro lado, la Municipalidad de San José, señala el plazo de 7 días de almacenamiento de las imágenes y posteriormente son guardadas en un disco duro (se desconoce por cuanto tiempo). Y, finalmente, el artículo en mención establece un plazo indefinido que queda a criterio de la Administración. Considero que este enunciado constituye una violación a los principios rectores del tratamiento de datos personales, debido a que la legislación debe definir un plazo durante el cual las imágenes serán resguardar y, posteriormente, debe garantizar la eliminación de estas. Este problema surge por la falta de integración normativa e institucional en Costa Rica.

De acuerdo con la legislación española, los datos como la imagen serán almacenados por el plazo de 30 días salvo cuando “estén relacionada con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto”¹; fuera de esas excepciones y pasado el tiempo de un mes, las imágenes deberán ser eliminadas. Para Cornelis Ramírez:

“si no se estipula cuánto tiempo va a estar almacenadas las capturas realizadas por los equipos de videovigilancia, puede utilizarse hasta más allá de los límites legales necesarios

¹ Artículo 8 de la (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

para la puesta de denuncias, lo que influiría en la prescripción de algunos tipos penales, sobre todo los de menor rango punitivo como los hurtos. Igualmente, el mantener por largos períodos información personal capturada en sitios públicos, sería considerado una violación al derecho a la intimidad, al no perseguir ningún fin más que el de su existencia” (Cornelis Ramírez 2015, 27)

El **artículo 6** del decreto refiere a la ubicación física de las cámaras. Según lo conversado con la Municipalidad de San José para la ubicación física de las cámaras se toma en cuenta ciertos aspectos: primero, las zonas rojas o puntos calientes. Estos son áreas de nuestra capital que son consideradas peligrosas por el alto índice de criminalidad, las cuales tiene identificadas la policía por la comisión de delitos como asaltos, narcotráfico, prostitución, entre otros. Otro aspecto que se toma en consideración para la ubicación de una cámara es por petición de los ciudadanos o particulares, por ejemplo, cámaras que son ubicadas en paradas de autobuses o en algunos barrios capitalinos a solicitud del interesado. Finalmente, otro factor para ubicar una cámara es el aprovechamiento para la actividad delictiva. Es decir, si la cámara no capta o capta poca actividad delictiva en determinada zona se reconsidera el traslado de la misma a un lugar más aprovechable para la persecución del fin.

Nuestro reglamento no contempla la duración o vigencia de la captura de imágenes. Cornelis Ramírez indica que queda abierta: “...a- al tipo de contrato que realice el Ministerio de Seguridad (alquiler o compra de los equipos de videovigilancia), b- a la vida útil de los aparatos, c- a la renovación tecnológica (si se encuentra una mejor forma de vigilar) o d- de manera indefinida sin tener que justificarse ante otra institución más que a sí misma”. Una vez más, la falta de un plazo determinado viola el principio de temporalidad de la videovigilancia. Por ejemplo, en España la Ley 4/1997 establece el plazo máximo de un año para la ubicación física de una cámara, plazo que podrá renovarse considerando si las circunstancias que originaron la instalación de la cámara se han modificado o no¹.

¹ Artículo 3 inciso 4 de (Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 1997)

En España, la AEPD es la encargada de llevar la inscripción de los ficheros de videovigilancia y quien autoriza la instalación de las cámaras en los espacios públicos y privados, por medio de un análisis previo y posterior de la ubicación física de la cámara, donde se analiza el aprovechamiento de la cámara para la prevención y persecución del delito; y si la cámara representa o no un peligro para la vida privada de algún ciudadano. De conformidad con el artículo 3 inciso 4, la resolución que aprueba la instalación de la cámara: *“deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes”*.

Aunque la participación del juez o magistrado sea únicamente consultiva, con ello se cimenta de manera extensa y adecuada el uso de las videocámaras en lugares públicos tanto para la instalación, desinstalación o limitación del espacio físico. El punto de vista judicial garantiza la no afectación de un derecho fundamental.

El **artículo 8 y 9** establecen que los dos usos de las imágenes son para investigaciones policiales y en procesos judiciales.

“La restricción de un derecho fundamental con fines de investigación requiere de la existencia de una ley previa que autorice la medida, de manera que se exige la previsión legislativa de una tal injerencia, por ello corresponderá, pues, al legislador valorar los intereses en conflicto, siendo el público representado por el ius puniendi y el individual de mantener el derecho de que se trate libre de injerencias injustificadas- y determinar en qué supuestos y bajo qué condiciones puede tolerarse una restricción del derecho”¹

¹ (Choclán Montalvo 1995)

Nuevamente el **artículo 8** menciona que los usos que se le den a las imágenes obtenidas por medio de las cámaras deben ser orientadas a la persecución del delito, principalmente en la identificación de los sospechosos.

Cornelis Ramírez haciendo alusión a Foucault¹ señala que dentro de los procesos judiciales “...ya no importan los límites de la verdad, debe llegar a ella a toda costa y si es de procedimientos y garantías, los unos superan las otras, y despacio pero cierto, la tecnología relativiza los derechos, sobre todo, los que comprenden a la intimidad”. Los usos de la tecnología ligadas a las actividades policiales con fines preventivos y represivos se han intensificado y son cada vez más sofisticados; bajo un concepto de lucha contra la delincuencia los ciudadanos hemos cedido una parte de nuestra libertad y privacidad a cambio de una seguridad que pareciera no llegar, seguimos creyendo y apoyando políticas de control y represión que, aunque están dirigidas al delincuente también perjudican al ciudadano. Esos mismos esfuerzos represivos (del Estado y apoyados considerablemente por la población) se reflejan en los procesos penales enfocados en la incriminación del delito, la búsqueda del culpable y el encarcelamiento del responsable.

Es importante que la ley establezca, de manera puntual, los límites y los usos que se le vayan a dar a las imágenes, sean por infracciones penales y/o administrativas. En este sentido, recordamos las cámaras de seguridad vial que instalaron sobre algunas carreteras de nuestro país, con la finalidad de controlar los límites de velocidad en nuestras vías. Si las cámaras detectaban un exceso de velocidad, se generaba una multa para el propietario registral del vehículo. El proyecto que inició en el año 2011 estuvo unos meses en funcionamiento y después se suspendió por motivos de inconstitucional, donde se alegaba falta de razonabilidad y desproporcionalidad en los montos de las multas. Este es un ejemplo, de un proyecto de cámaras cuya finalidad es llanamente para infracciones administrativas.

¹ Foucault menciona que la investigación era un poder soberano que le correspondía al Estado y a partir de ella se establecía la verdad, textualmente dice “La investigación, en efecto, ha sido la pieza rudimentaria, sin duda, pero fundamental para la constitución de las ciencias empíricas; ha sido la matriz jurídico-política de este saber experimental”. Foucault Michel. “Vigilar y Castigar”, Siglo Veintiuno Editores. Buenos Aires, 2003, p. 208. Mencionado por Cornelis Ramírez, M., p. 32

Se le consultó a la Municipalidad de San José sobre el procedimiento señalado en el artículo 9, a lo que confirmaron que las grabaciones de las imágenes únicamente serán entregadas, previa orden de un juez, a funcionarios públicos del Poder Judicial, como OIJ, Fiscalía o Ministerio Público¹.

Para la valoración de las imágenes obtenidas por medio de CCTV por parte de los tribunales deben considerarse tres aspectos, según Cornelis Ramírez:

1. La incorporación de vídeo al juicio: para el autor las imágenes obtenidas por medio de CCTV son *“medidas de investigación con posible función probatoria”*, y aunque son una *“pieza de convicción (...) no es propiamente en sí mismo un medio de prueba si constituye una fuente de prueba a introducir en el juicio oral por medio de la prueba documental de ordinario”*, por eso debe comprobarse la autenticidad de la prueba videográfica, y debe de complementarse con otras pruebas, como la documental o testimonial.

2. Peritaje del vídeo: el autor se refiere a verificar la legitimidad de las grabaciones, ya que las mismas pueden ser susceptibles de manipulación. Lo que se quiere constatar es la integridad del material y la apropiada cadena custodia de las imágenes o vídeos.

3. Declaración en juicio del operador del equipo de videovigilancia: el autor señala que la *“...grabación obtenida solo tiene el valor de mera denuncia, debiendo, para alcanzar eficacia probatoria, incorporarse al juicio oral, y corroborarse allí, mediante la correspondiente contradicción, con la declaración de los agentes que la realizaron”*. Para Senés la prueba carece de autonomía funcional y más bien tiene carácter complementario respecto a otros medios de prueba, pues la filmación es *“una técnica que permite transferir las percepciones sensoriales a un instrumento mecánico que complementa y toma constancia de lo que sucede ante los que en su día deponen como testigos”*. En caso de duda o inconsistencias, lo ideal es complementar el material videográfico con las declaraciones de los intervinientes.

4. Exclusividad jurisdiccional: el autor señala que únicamente el juez o el tribunal colegiados es el órgano encargado de determinar si la persona que se observa en el vídeo es el acusado.

¹ (Llobet Rodríguez, Código Procesal Penal Comentado 2009)

Para Cornelis Ramírez “...el valor de la denuncia no produce en las grabaciones un valor probatorio en sí mismas, hasta que logre determinarse por otros medios, su adveración, mediando el proceso penal y las reglas de inmediatez, oralidad y contradictorio” (Cornelis Ramírez 2015, 32).

El **artículo 11** del decreto garantiza el deber de confidencialidad del personal que opera en los centros de comando de las cámaras. Dichos funcionarios tienen la obligación de mantener el secreto profesional acerca del contenido y el funcionamiento del sistema.

El **artículo 12** prohíbe el ingreso de personal no autorizado a los centros operativos de comando y el **artículo 13** impone el deber de cuidado que deben tener aquellas personas encargadas de la instalación, mantenimiento y operación de estos sistemas. Una de las críticas que hace al respecto Cornelis Ramírez es que no se menciona expresamente cuáles autoridades o con qué fines pueden ingresar personas no autorizadas en las salas de comando operativo. En cuanto a las sanciones por incumplimiento del personal una vez más el reglamento no las especifica. En España la Disposición adicional séptima de la Ley 4/1997 enumera las faltas e infracciones en las que puede incurrir un operador de las cámaras.

2.5 Sobre Jurisprudencia de la Sala Constitucional en materia de videovigilancia

Los pronunciamientos de la Sala Constitucional en materia de videovigilancia han sido pocos y cambiantes. En las tres sentencias emitidas por la Sala, se analizan diferentes argumentos relacionados para la cámara, el área de captación de las cámaras principalmente sobre espacios privados y si dicha ubicación afectación los derechos de privacidad de los recurrentes.

La línea jurisprudencial en nuestro país ha cambiado en relación al uso de los sistemas de videovigilancia. En la **Sentencia 1650 del 14 de febrero del 2006**, se refiere al uso de videocámaras con fines privados, donde el Tribunal consideró que no existía una violación al derecho a la intimidad. Se trata de un conflicto entre vecinos de un condominio; una de ellas

procedió a instalar dos cámaras de seguridad, que según acta notarial una captaba imágenes de la entrada principal del apartamento y la segunda ubicada en una ventana de la planta alta del inmueble con vista a la calle¹. El Tribunal considero que la cámara al estar “*dirigida hacia la vía pública del frente de su casa por razones de seguridad, y no tiene el alcance, ni la intención de verificar, lo que sucede dentro de la casa de la habitación de los recurrentes o del taller que está ubicado al frente*”, y por este motivo desestimó el alegato del recurrente concluyendo que no hubo transgresiones al derecho de privacidad.

Aunque esta jurisprudencia data ya de algunos años atrás, se puede observar lo distante que se encuentran nuestros tribunales de los criterios europeos. Varios aspectos por rescatar. Primero, la videovigilancia utilizada en espacios comunes con fines privados requiere, necesariamente, del consentimiento de los involucrados. La captación de imágenes sin el consentimiento del titular es una intromisión ilegítima a la intimidad del ciudadano, ya que se desarrollan aspectos íntimos de su vida. Segundo, la presencia de las cámaras debe manifestarse a las personas que ingresan o vivan en el condominio, por medio de carteles informativos. Finalmente, la captación espacial de las cámaras, cuyo fin es la seguridad de una propiedad privada, debe limitarse al espacio privado, no debe captar imágenes de la vía pública. Retomando el caso español, pareciera que la mejor opción es considerar la creación de una normativa que reúna las condiciones y requisitos para la prestación o concesión de este servicio o actividad privada, principalmente con el objetivo de resguardar el tratamiento de datos personales de los ciudadanos.

Posteriormente, en la Sentencia número **15 953 del 26 de setiembre del 2014** del mismo tribunal se declara con lugar el recurso de amparo; sin embargo, existen dos votos salvados donde se manifiesta que la vía procesal para resolver el recurso es vía contravencional, y no por la Sala Constitucional.

Los recurrentes interponen recurso de amparo contra su vecino, alegando que el accionado instaló cinco cámaras de vigilancia en su propiedad que enfocaban hacia las casas de habitación y los patios traseros de los recurrentes. Que la presencia de las cámaras y el monitoreo

¹ (Sentencia 01650 2006)

al que están expuestos han afectado a las personas que viven en la casa, ocasionándoles temor de ser observados, se sienten intimidados y les ha provocado daños psicológicos y trastornos de la personalidad. A pesar de que levantaron los muros y tapias para no ser captados y obstaculizar el enfoque de las cámaras; el recurrido elevó las cámaras. “Si bien es cierto el accionado tiene derecho a proteger o vigilar su propiedad, debe hacerlo dentro del propio límite del inmueble y con dirección directa hacia la calle pública de ser necesario, no así hacia sus casas”.

Afirman que la constante vigilancia de la que son objeto, amenaza el sano equilibrio emocional y armónico de los vecinos de la Calle Villalobos. Acusan que, tales hechos lesionan sus derechos a la intimidad, privacidad y propiedad. El Tribunal acogió el recurso principalmente porque el recurrido no aportó prueba que desvirtuara lo sostenido por los recurrentes. El Tribunal obligó a reubicar las cámaras de seguridad y colocarlas en un lugar que no afecte la privacidad e intimidad de los amparados.

En el voto salvado lo que se dice es que, por tratarse de una instalación de cámaras de seguridad con fines privados, la vía apropiada es la sede contravencional. Que, si se tratase de una invasión a la privacidad por parte del Estado por realizar vigilancias ilegítimas, si le correspondería resolver al Tribunal Constitucional¹.

A diferencia de las primeras dos sentencias, la **Sentencia número 03575, del 14 de marzo del 2014** del Tribunal Constitucional, interviene como parte el Estado y un particular.

La accionante interpone un recurso de amparo contra el Ministerio de la Presidencia ubicado en San José, Zapote, porque se había instalado una cámara de seguridad que giraba en 360° entre el edificio de Casa Presidencial y su propiedad y a su criterio, las captación de imágenes sobre su propiedad, lesionaban su derecho a la intimidad. La afectada conversó con el Jefe de Seguridad de Casa Presidencial y le solicitó que retiraran las varillas y la cámara de seguridad que daba hasta su propiedad. Aunque removieron las varillas, la cámara se instaló en el poste metálico, siendo que la misma ahora giraba solo 180° sobre sí misma. El Tribunal señaló que hubo una violación al derecho a la intimidad de la accionante durante el tiempo que el cámara giró los 360° enfocando su propiedad; ella “*tuvo que soportar una injerencia en*

¹ (Sentencia 15 953 2014)

su ámbito privado que devino en una lesión a ese derecho fundamental”. Aunque la cámara ya no captaba imágenes de su propiedad, declararon con lugar el recurso únicamente para efectos indemnizatorios porque, por un periodo de tiempo efectivamente se lesionaron los derechos fundamentales de la amparada¹.

Es evidente de que existe un problema de inseguridad en nuestro país que la Administración Pública debe resolver, llevando a cabo medidas eficientes y adecuadas para contrarrestar las causas y efectos de la delincuencia. En el discurso de la seguridad, la Administración Pública presenta los sistemas de videovigilancia como un instrumento efectivo y necesario para prevenir, reducir y perseguir la actividad delictiva, sin antes evaluar la efectividad de estos, y esta tarea la debe llevar a cabo el Estado.

2.6 Propuestas para el mejoramiento de la videovigilancia pública en Costa Rica.

Costa Rica tiene un largo camino que recorrer en la videovigilancia. El desarrollo legislativo, jurisprudencial y doctrinal ha sido escaso, y la experiencia práctica poca. Es una realidad que los CCTV cada día van en aumento, y no se está proyectando los efectos que pueden traer a futuro en la vida privada de las personas. Es cierto de que la privacidad ha cedido campo a la seguridad, pero la garantía de un derecho no puede ir en detrimento de otro. Es necesario adecuar el buen funcionamiento de las cámaras, controlar la proliferación de estos en los espacios públicos y privados, y regular los vacíos legales que existen ahora que estamos a tiempo. A continuación, se sugieren algunos aspectos importantes a partir de los cuales se puede mejorar y adecuar el funcionamiento de estos sistemas acorde a la legislación de protección de datos de nuestro país.

A. Regulación de la videovigilancia de acuerdo al principio de reserva de ley.

Una de las propuestas que consideramos importante es regular la videovigilancia con fines públicos bajo el principio de reserva de ley (sin excluir la colaboración reglamentaria). Hemos mencionado que el funcionamiento de las cámaras de videovigilancia no es neutral y

¹ (Sentencia 2014003575 2014)

pueden generar conflictos sobre los derechos fundamentales de los ciudadanos, específicamente con los derechos de imagen, privacidad, protección de datos personales y autodeterminación informativa.

Uno de los regímenes jurídicos que le corresponde al principio de reserva de ley, son los derechos constitucionales y los límites a derechos fundamentales, sin perjuicio de la existencia de reglamentos ejecutivos¹. La función garantista del principio de ley consiste en que, a través de la reserva se tutelan los derechos de los ciudadanos contra las intromisiones del poder ejecutivo, evitando que el mismo órgano que crea la norma sea el que la ejecute². Aunque la Constitución Política costarricense faculta al Ejecutivo a crear normas, consideramos que, por tratarse de una medida administrativa altamente intrusiva por sus capacidades de registro y captación de datos de los ciudadanos, así como las limitaciones que presenta sobre los derechos fundamentales ya mencionados, lo mejor es reservar el tema de la videovigilancia a la ley.

En nuestro país existe una ley de protección de datos (Ley No. 8968) y tenemos un decreto que regula la videovigilancia en espacios públicos, sin embargo, el decreto es breve, escueto y deja al aire aspectos importantes relacionados al tratamiento de las imágenes (temporalidad, participación de la Agencia de datos, videovigilancia con fines privados, etc.) y la participación institucional de los encargados o responsables de los datos.

Aunque el derecho a la imagen, la protección de datos personales y la autodeterminación informativa no se encuentran expresamente reconocidos en nuestra Constitución Política son derechos considerados fundamentales que hoy en día son amenazados por el acelerado avance tecnológico. La creación de una ley específica en la materia de videovigilancia pública vendría a garantizar el respeto de éstos derechos fundamentales, además reuniría las condiciones o pautas técnicas, operativas, organizativas y legales del uso de los CCTV, evitando los vacíos legales que existen actualmente y definiría de manera expresa las competencias de cada institución involucrada, sean en la etapa de

¹ Artículo 19 de la Ley General de la Administración Pública, Costa Rica.

² (Línea 2013)

recolección, procesamiento y almacenamiento de los datos, o bien en la etapa de investigación policial y proceso judicial.

Una ley referente a la materia vendría a designar un responsable competente de operar y administrar estos sistemas, esto le permite al ciudadano saber en manos de quién están sus datos y adonde puede acudir en caso de posibles afectaciones a sus derechos civiles. Algo muy particular que ocurre en nuestro país, es que el decreto expresamente indica que el Ministerio de Seguridad es el encargado de operar estos sistemas, pero en la realidad quien los utiliza y administra es la Municipalidad de San José, una situación como esta le genera al ciudadano inseguridad jurídica.

Por el contrario, cuando el ciudadano tiene claro quién es el responsable de los datos, cual es la finalidad del tratamiento, y tiene conocimiento de lo que ocurre con su información personal, se garantiza el libre ejercicio de la autodeterminación informativa, pudiendo el ciudadano controlar su propia información, ello le da seguridad de que sus datos están siendo debidamente resguardados, se evita el trasiego de los mismos y se delimitan las obligaciones y alcances del responsable u operador de los datos.

B. Participación institucional en el tema de la videovigilancia.

La vigilancia pública de los espacios, es una actividad que necesariamente requiere la participación coordinada de las distintas instituciones, esto implica una participación de los operadores de estos sistemas con los cuerpos policiales (despliegue policial), con las Agencias de datos y con las entidades encargadas de la investigación y persecución penal (Ministerio Público, OIJ, Poder Judicial, etc.), e incluso la participación de la ciudadanía en aspectos que les atañe. De igual forma la ley que rige la materia, establecería las competencias y responsabilidades de cada institución, así como los procedimientos que hubiera entre ellas para la consecución del fin.

Vale la pena diferenciar la participación de las instituciones en dos etapas: la etapa preventiva y represiva de los sistemas de videovigilancia. Sabemos que las funciones de orden y prevención les corresponden a los cuerpos policiales que finalmente son los encargados de

operar y administrar estos sistemas. En el decreto de nuestro país esta actividad le corresponde al Ministerio de Seguridad. Así mismo, se le faculta como responsable de las imágenes obtenidas por medio de las cámaras.

Uno de los aspectos que no considera el decreto es la participación de la Prodhab, sobre todo cuando se trata de una actividad que comprende tratamiento de datos. Es importante, que la Prodhab como institución encargada de velar por el cumplimiento de la legislación en materia de protección de datos, se involucre en los proyectos de videovigilancia pública (eventualmente con la de fines privados) que operan en nuestro país.

Su participación puede ser consultiva e incluso resolutive. En otros países, las Agencias de Protección de datos tienen a su cargo la inscripción de los ficheros de los encargados de las cámaras, verifican que las áreas bajo vigilancia cumplan con los requisitos informativos, ofrecen su opinión en cuanto a la ubicación física de las cámaras, atienden peticiones y resuelven quejas de los ciudadanos en caso de que las cámaras afecten la privacidad de los mismos, ofrecen recomendaciones para adecuar la actividad de la videovigilancia acorde a los principios de protección de datos e incluso tienen potestades sancionatorias en caso de afectaciones a derechos o incumplimientos de la normativa, entre otros aspectos.

La Prodhab no ha tenido ninguna clase de participación con los proyectos de vigilancia pública que operan actualmente en nuestro país. El funcionamiento de las cámaras carece de supervisión y control por parte de la agencia. Algo tan importante como lo es el derecho a ser informado de las zonas bajo vigilancia no se cumple a pesar de que el decreto en el artículo 7 lo establece como un requisito que en efecto no se cumple.

La Municipalidad josefina solo coloca a las cámaras una placa o distintivo para indicar que le pertenece; la importancia de ser informado radica en la posibilidad que tiene el ciudadano de ejercer su derecho a la autodeterminación informativa, evidentemente la “clandestinidad” de las cámaras menoscaba el libre ejercicio de este derecho fundamental. Es de vital importancia la participación de la Prodhab como institución supervisora y garante del

buen funcionamiento de las cámaras de seguridad acorde a los derechos de autodeterminación informativa y protección de datos personales de los ciudadanos¹.

En la función preventiva los operadores de estos sistemas deben participar activamente con otros cuerpos policiales o de seguridad, como lo son los policías municipales y de tránsito (en caso de una persecución vial). Uno de los aspectos prácticos y organizativos que mejora la efectividad preventiva de estos sistemas es la rapidez del despliegue policial ante la comisión de delitos *in fraganti*. Los operadores de estos sistemas deben mantener coordinación y comunicación con otros cuerpos de seguridad para darle efectividad a estos sistemas, porque por sí solos únicamente registran un hecho delictivo, no tienen la capacidad de interrumpir o evitar su comisión.

La etapa de persecución del delito se pueden identificar dos procesos, el primero de investigación policial y el segundo, el proceso penal. Con menos frecuencia se detecta la comisión de un delito de manera inmediata por medio de las cámaras. La mayoría de las veces las imágenes o vídeos son solicitados por las autoridades cuando el hecho delictivo ya transcurrió o existe una denuncia judicial por parte de algún ciudadano. A los cuerpos de investigación judicial (OIJ en nuestro país) le corresponde, primeramente, determinar si hay presencia de cámaras, si los hechos son captados por las mismas y obtener la copia de la información para ser analizada e incorporada en la causa penal. Un factor muy importante cuando las cámaras registran un delito, es la posibilidad de identificar a los involucrados del hecho delictivo, esto está relacionado con la calidad de las imágenes. En un supuesto que las imágenes o vídeos sean de mala calidad, difícilmente se tome en cuenta la prueba dentro del proceso penal, o bien el proceso sea desestimado.

En este sentido se le consultó a la Municipalidad de San José el procedimiento para la obtención de imágenes o vídeos captados por las cámaras del municipio cuando se está frente a la investigación de un delito: *“Para solicitar video de cámaras en espacio público es*

¹ La participación ciudadana también es importante. Algunas comunidades organizadas han incluido sistemas de videovigilancia en sus barrios que en la mayoría de las veces corre por presupuesto de la comunidad, estas iniciativas pueden unirse con los proyectos de vigilancia pública.

necesario cumpla con el siguiente procedimiento:

1. Debe contar con el número de la denuncia interpuesta en el Juzgado pertinente.

2. Cédula que demuestra que es parte involucrada de la denuncia.

3. Una vez constatado lo antes indicado se le atenderá en el Centro de Monitoreo para que pueda observar el video, si el mismo evidencia el hecho denunciado se extraerá el video de los servidores municipales, bajo el número de causa seguida en la entidad pertinente.

4. Posteriormente el ciudadano le indica a la entidad -OIJ- que consta en nuestros servidores video bajo el número de causa indicada, lo anterior a fin de que sea retirada la Evidencia Judicial de forma directa por el personal de investigaciones del OIJ y con ello garantizar la cadena de custodia conforme lo dicta la norma.

La Jefe de operaciones señaló que este procedimiento únicamente se realiza para fines de persecución del delito, he indicó que las grabaciones se conservan por 7 días y se resguarda la información en un servidor con los controles de seguridad requeridos.

Propiamente en el proceso penal, las imágenes o videos que se deseen incorporar al proceso penal deberán cumplir con las reglas legales y procesales de su obtención, con los requisitos de admisibilidad y cadena custodia de la prueba digital. Debido a que la prueba digital es un poco vulnerable de manipulación, lo ideal es someterla a un análisis perital para descartar que ha sido modificada por un tercero.

Una adecuada cadena de custodia garantiza la autenticidad y pureza del material que se va a utilizar como prueba. Una ruptura en la cadena de custodia convierte a la prueba inidónea que no se puede entrar a valorar pues atenta con las reglas de la sana crítica. La Sala Constitucional indicó que la cadena de custodia puede referirse a aspectos de legalidad de la prueba tales como si fue recopilada por sujetos con competencia para ello y si se cumplieron las formalidades procesales previstas para ello, etc.)¹.

¹ (Voto No. 5831, de las 9:12 horas 1996)

“Normalmente las pruebas que se obtuvieron en detrimento de las reglas legales y procesales de obtención se les llama prueba inidónea o prueba irregular (...) como lo ha indicado la Sala Tercera, una prueba que contenga un defecto en el manejo de la cadena de custodia de prueba también puede ser considerada prueba ilícita, si, -además de los yerros en el manejo de la cadena de custodia- se violentó en la obtención de la misma derechos y garantías fundamentales -además del debido proceso”¹.

La cadena de custodia debe respetarse en cuatro fases básicas en sede policial “en las que debe garantizarse la autenticidad del elemento o material a utilizar como prueba, a saber: el momento de la extracción o recolección de la prueba; el momento de la preservación y empaque; la fase del transporte o traslado; y, finalmente, la entrega apropiada de la misma”²

La problemática que se plantea con la incorporación de la prueba videográfica al proceso penal y su incidencia a posibles afectaciones a derechos fundamentales de la persona gira en torno al cómo se obtiene o produce la prueba, cómo se preserva y utiliza, la correcta introducción al proceso y la eficacia probatoria que proporciona, básicamente son los controles y garantías que se sitúan en torno a la captación de las imágenes y el grado de idoneidad, licitud y pertinencia que tienen dentro del proceso penal³.

En materia penal se pueden puntualizar tres aspectos importantes acerca de la prueba videográfica y son los límites constitucionales de las filmaciones, las garantías procesales que deben respetarse para incorporar válidamente las imágenes al proceso y la eficacia probatoria que tienen esas imágenes para destruir la presunción de inocencia del imputado (Navajas Ramos 1998, 153)

El primer punto se refiere a las fronteras que no pueden traspasarse para la obtención de las imágenes, y en este aspecto se distinguen la “prueba ilícita” que tiene que ver con la vulneración de derechos fundamentales recoocidos constitucionalmente (inviolabilidad del domicilio y las comunicaciones, *in dubio pro reo*, etc.), ante este supuesto la prueba no podrá

¹ (Voto No. 412, de las 15:30 horas 2006) mencionado por (Vargas Acuña 2017, 58)

² (Sentencia 368 1992)

³ (Navajas Ramos 1998, 151)

tomarse en cuenta dentro del proceso y la “prueba irregular” cuando hay vulneración de normas procesales ordinarias, en este caso, se pueden acreditar los hechos por otros medios de pruebas, con la finalidad de subsanar el defecto procesal en el que se incurrió.

Algunos de los límites constitucionales que podemos mencionar con respecto a las cámaras relación a su ubicación y su función. Las cámaras con fines policiales deben circunscribirse al ámbito de las vías públicas, espacios abiertos o lugares de tránsito públicos, no pueden captar imágenes en ámbitos privados, como la esfera domiciliar (salvo previo mandato judicial). Y el límite funcional es que las grabaciones de las imágenes ocurran dentro del contexto de investigación criminal dirigidas a personas sospechosas de la comisión de delitos graves.

En relación al segundo aspecto, lo que se procura es darle valor probatorio a la prueba lícita sin vulnerar ningún derecho fundamental, lo que implica un adecuado control judicial del material grabado y aportar las grabaciones en el momento procesal oportuno, que es el inicio de la investigación judicial.

“Las imágenes deben acompañar siempre al atestado como plasmación de la investigación llevada a cabo y dándoles el tratamiento de una auténtica pieza de convicción, tanto si se tomaron por decisión policial y en el curso de la investigación” del OIJ o el Ministerio Público.

Es importante recalcar la fuerza probatoria que tienen las imágenes dentro del proceso, pues permiten vincular la participación de los sospechosos en una supuesta actividad delictiva. *“Esta aportación inmediata del material videográfico permite un escrupuloso respeto a los principios procesales de igualdad y contradicción y proscribire toda posibilidad de indefensión al permitir, a los que pudieran verse involucrados en actividad supuestamente delictiva, como consecuencia de las filmaciones, a intervenir en la prueba ajena y proponer cuantos medios de prueba estimen pertinentes para combatir la fuerza probatoria de las imágenes”* (Navajas Ramos 1998, 160).

Una vez concluida la investigación policial, los soportes originales del material probatorio son entregados al juez, y al juez le corresponde acreditar la legitimidad de las imágenes considerando que se hayan obtenido en cumplimiento de las normas procesales y sin vulnerar derechos fundamentales (control judicial)¹.

Una vez comprobado que la prueba se obtuvo de manera lícita y fue aportada correctamente al proceso con todas las garantías procesales y de fondo, lo que corresponde es la proposición de la parte interesada y la valoración que el juez vaya hacer de ella. En este sentido, es importante tener claro que “la validez probatoria de la prueba videográfica no es absoluta” y por sí misma, “la prueba videográfica carece de eficacia absoluta para quebrantar la presunción de inocencia”. En palabras de Damian Moreno:

“la fuerza probatoria de estos medios de reproducción de imágenes puede llegar a ser tan intensa en cuanto se refiere a la fiabilidad de los hechos que representan, que no sería del todo descabellado pensar en el riesgo que comporta el que algunos Jueces sintieran la tentación de considerar la posibilidad de despreciar el resto del material probatorio, lo cual, si eso fuera así, supondrá la quiebra de todo el conjunto de principios sobre los que descansa la esencia misma del proceso y, en particular, la teoría general de los medios de prueba”².

Idealmente el juez deberá tomar en consideración otros medios de pruebas como las declaraciones de los acusados, peritajes, testimonios y prueba documental aportada al proceso, dándole mayor credibilidad al criterio judicial (sentencia condenatoria) y evitando darle autonomía propia a prueba videográfica.

¹ Con el material videográfico lo que se procura es el respeto íntegro de la prueba, sin manipulaciones o alteraciones que afecten el debido proceso. Puede ser que el juez requiera de la totalidad del material original o eventualmente pida una selección de las imágenes más importantes y clarificadoras del delito y los involucrados, siempre y cuando se garantice la legitimidad y verdad de la filmación.

² (Damián Moreno 1997)

C. Realización de estudios investigativos enfocados en mejorar el funcionamiento de estos sistemas y evaluar su efectividad.

Los sistemas de videovigilancia pueden convertirse en un instrumento muy valioso para los cuerpos de seguridad y llegar a ser un instrumento efectivo en la prevención y persecución del delito. Como hemos mencionado a lo largo del trabajo, estos sistemas deben funcionar en un marco legal que brinde protección al ciudadano respecto a sus datos personales, privacidad y autodeterminación informativa; a su vez, que cumpla con los objetivos propuestos en el tema de seguridad pública y ciudadana.

En Latinoamérica, a los sistemas de videovigilancia se les ha atribuido un gran peso como medida de seguridad y prácticamente, su proliferación se debe a una política criminal que los fomenta casi de manera aislada, sin tomarle importancia al grado de efectividad que tienen sobre la delincuencia y bajo qué condiciones secundarias se puede mejorar el funcionamiento de los mismos.

Llevar a cabo evaluaciones o experimentos prácticos permiten identificar las deficiencias que presentan estos sistemas, y una vez identificados es posible incluir las mejoras que sean necesarias. Otros países que han llevado a cabo estas investigaciones han logrado incluir otro tipo de medidas menos costosas como mejoras en la iluminación, mayor control en las salidas e ingresos de ciertos lugares de alto tránsito y aumentar el patrullaje policial en ciertas zonas.

Otra manera de mejorar la efectividad de las cámaras es por medio de la ubicación estratégica. La evaluación del lugar físico de las cámaras le permite a las autoridades tener un criterio del efecto que tienen los CCTV sobre la delincuencia. Por ejemplo, valorar la incidencia delictiva en un determinado lugar, determinar si la presencia de la cámara ha influido en la reducción de delitos o si más bien ha ocurrido un desplazamiento de la delincuencia a zonas no vigiladas, tomar en consideración si es necesario cambiar la ubicación de la cámara para otro lugar, puntos ciegos, etc.

Una de las principales críticas que han recibido los promotores de estos sistemas (autoridades policiales) es que han hecho un gran esfuerzo por expandir su uso, pero no se han preocupado en estudiar el efecto disuasorio que le atribuyen en la prevención y persecución del delito. En Costa Rica al igual que en otras partes del mundo, las mismas instituciones estatales que promueven el uso de estos sistemas desconocen la efectividad de estos para reducir o prevenir el delito.

Por ejemplo, la Municipalidad de San José facilitó información en relación con el número de vídeos o imágenes que solicitaba el OIJ para la investigación o persecución de un delito; no obstante, se desconoce el número de procesos judiciales que se resolvieron gracias al aporte de las pruebas digitales (fotografías o vídeos) obtenidas por las cámaras. El cuadro a continuación detalla la información: en la primera fila del cuadro se demuestra la cantidad de solicitudes que hizo el OIJ a la Municipalidad para la obtención de imágenes o videos que pudieran captar información del delito. La segunda fila indica la cantidad de veces que la Municipalidad pudo responder efectivamente a la solicitud (los videos o imágenes eran óptimas, porque aportaban información valiosa de la comisión de un delito).

INFORME DE CAMARAS 2017										
MES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	TOTAL
SOLICITUDES	145	112	64	102	160	194	111	152	152	1192
OIJ	75	83	50	75	109	135	76	89	82	774

A pesar de los datos suministrados por la Municipalidad de San José, no existe información estadística completa o investigaciones científicas que comprueben la efectividad de estos sistemas acorde con el fin que persiguen.

Las autoridades estatales han invertido miles de dólares en la adquisición de estos sistemas que, hasta la fecha en nuestro país, se desconoce los efectos positivos que puede tener en la prevención y persecución del delito; han sido fuertemente promovidos por las autoridades dentro de un discurso de lucha contra la delincuencia callejera y la represión del delito. Idealmente, el apogeo de estos sistemas debería ir de la mano de datos reales que respalde su funcionamiento y reorientar su uso en un marco garantista del derecho penal.

CONCLUSIONES.

1. Los antecedentes terroristas, la violencia y la delincuencia en general, son las causas principales que han alimentado el discurso político de la seguridad, y con ello los mecanismos de control y gestión de poder del Gobierno sobre sus habitantes. El acelerado avance tecnológico que existe hoy en día desafía a los Estados a considerar el uso de la misma, no sólo por una cuestión de seguridad o necesidad, sino también por criterios de eficiencia en sus funciones. Con la videovigilancia las autoridades públicas han podido extender los parámetros de alcance de la seguridad física.

2. Tanto en el continente americano como en Europa, los sistemas de videovigilancia se han proliferado aceleradamente convirtiéndose en una herramienta muy popular para mitigar los actos delictivos. Las cámaras de vigilancia ubicadas en los espacios públicos, tales como parques, calles, avenidas, plazas, estaciones y aeropuertos, son utilizadas por la policía con el fin de advertir los comportamientos y actividades ilícitas; y para revitalizar la confianza de los espacios comunes que son blancos de la delincuencia.

3. La video vigilancia plantea una discusión válida entre el derecho a la seguridad pública y la protección a los derechos concernientes a la vida privada del individuo. Los defensores de estos sistemas afirman que las cámaras de seguridad son una herramienta útil y eficaz para prevenir y perseguir la actividad delictiva. Quienes rechazan el uso de estos sistemas argumentan que son un mecanismo de control social y espacial, que afectan los derechos civiles de los ciudadanos. La falta de regulaciones, el uso desmedido o abusivo de las cámaras, la falta de información de los ciudadanos, la poca efectividad de las cámaras sobre la delincuencia y la inexperiencia generalizada de las autoridades son algunos de los motivos que dificultan la conciliación entre el derecho a la seguridad y a los derechos de vida privada del ciudadano.

4. A los sistemas de videovigilancia pública se le atribuyen dos fines, el de naturaleza preventiva tiene dos argumentos: primero, se cree que la presencia de las cámaras disuade las conductas delictivas, pues el delincuente al sentirse observado desistirá de cometer el delito y el segundo, que por medio de las cámaras los cuerpos policiales advierten actitudes sospechosas previas a un delito. El de naturaleza punitiva,

dirigido a la persecución del delito; las grabaciones obtenidas a través de las cámaras son un medio de prueba que permiten la identificación de los sospechosos y la aclaración de los hechos delictivos.

5. Las investigaciones científicas llevadas a cabo en otros países para determinar la efectividad de los CCTV arrojan los siguientes resultados. En los espacios vigilados hay una reducción poco significativa de los delitos y en los índices de victimización; la reducción del delito se manifiesta principalmente en los delitos contra la propiedad y delincuencia premeditada; también se comprobó un desplazamiento de la delincuencia a zonas no vigiladas; se detectó que la efectividad de los CCTV depende del número de cámaras, el alumbrado de la zona, el tiempo de respuesta policial, y su funcionamiento mejora en lugares cerrados y con accesos controlados. En la persecución del delito los CCTV han demostrado ser una herramienta muy útil dentro del proceso penal, para la identificación de los sospechosos.

6. Los detractores de la videovigilancia sostienen que las cámaras de seguridad son una peligrosa herramienta de control social. Algunos usos como la exclusión de minorías en algunos espacios públicos, análisis conductuales sin previa sospecha, seguimiento de personas por su apariencia física, vigilancia generalizada e indiscriminada, la omisión de informar la presencia de las cámaras, entre otros aspectos, constituyen una violación a los derechos privados de la persona, distorsionan la finalidad de las cámaras de seguridad, y lejos de proveer seguridad se convierten en un instrumento de control social y espacial por parte de los cuerpos policiales.

7. La presencia de las cámaras de seguridad en los espacios públicos influye sobre los derechos de vida privada, imagen y protección de datos personales. Con la vigilancia de los espacios públicos el anonimato del individuo se pierde mientras transita; los niveles de privacidad se pierden porque las cámaras captan imágenes o acciones que son personales y corresponden al ámbito de autonomía de la persona (decidir ser o no grabada), la vigilancia mediante cámaras es más intensa, prolongada, generalizada e indiscriminada pues se ejerce de igual manera sobre el que delinque como el que no lo hace, los datos personales como la imagen, son recopilados en muchas ocasiones sin el consentimiento del titular, y si las imágenes son almacenadas estamos frente al tratamiento de datos personales.

8. Los sistemas de videovigilancia tiene la capacidad de reproducir y recopilar la imagen, la cual constituye un dato personal sensible, y está protegida por una serie de garantías en el tratamiento de datos, como el consentimiento del titular (autodeterminación informativa), la conservación de la imagen a un tiempo limitado, y el uso exclusivo de la misma para la finalidad establecida. Así mismo, la legislación dota de los derechos de información, rectificación y cancelación al ciudadano respecto a sus datos personales.

9. La normativa y jurisprudencia europea consolidaron las bases legales para el adecuado funcionamiento de las cámaras y los derechos civiles de los ciudadanos, en los convenios se establecieron varios aspectos, como los principios que rigen la videovigilancia (legalidad, proporcionalidad, necesidad, eficiencia, eficacia); limitaciones espaciales y temporales en el uso de las cámaras (la conservación de las imágenes tienen un plazo fijo y se excluyeron lugares que no permiten la instalación de cámaras); derechos que pueden ejercer los ciudadanos en relación a los datos que le conciernen (derechos de acceso, información, rectificación y cancelación) y deberes que tiene quienes administran y operan las cámaras de seguridad (deber de informar, deber de confidencialidad y secreto en el tratamiento de datos).

10. El buen funcionamiento de los sistemas de vídeo vigilancia requiere del cumplimiento de tres factores fundamentales: primero, una buena regulación, es decir, una normativa congruente e integral; segundo, un sistema de garantías judiciales, donde el ciudadano pueda hacer valer sus derechos; y finalmente, estar sometida al control judicial. Si bien es cierto los sistemas de video vigilancia se incrementa la seguridad y el nivel de protección de los bienes y libertades de las personas, esta seguridad pretendida por medio de la utilización de la videovigilancia requiere de un sistema de garantías para que el ejercicio de los derechos y libertades constitucionales sea máximo, y no sea perturbado por un exceso de defensa de la seguridad pública.

11. Los sistemas de videovigilancia deben integrarse como una herramienta tecnológica más que da soporte a los cuerpos policiales, no como único recurso. Por sí solos, los sistemas de videovigilancia presentan algunos problemas en relación a la función preventiva, pues no tiene la capacidad de reacción, sino que únicamente registran el hecho delictivo. A diferencia de la presencia policial, se puede interrumpir la comisión de un delito, e incluso disuadir al delincuente de llevarlo a cabo.

12. En cuanto a la función punitiva la crítica gira en torno a que no siempre es posible la identificación del sospechoso; el delincuente puede cubrirse completamente el rostro, o bien, las imágenes suministradas pueden tener mala calidad, dificultando la identificación del mismo. Aunque existen cámaras de vigilancia en funcionamiento, finalmente, no aportan ningún resultado positivo para identificar a los involucrados. Siendo así, resulta válido cuestionar cuáles son los verdaderos aportes que generan estos sistemas en la reducción, prevención y persecución del delito.

13. En nuestro país, a diferencia de otros países como España o Inglaterra, no existen estudios, investigaciones o estadísticas que determinen la efectividad de estos sistemas o que indiquen cuales son las condiciones que se deben adaptar para mejorar la efectividad de los mismos. El análisis de los resultados investigativos, es decir, los resultados que determinan que tan efectivas son las cámaras de seguridad en los espacios públicos, permite que los Estados valoren la relación costo-beneficio de estos sistemas, pues representan una alta inversión económica de la que se espera obtener altas expectativas de mejoramiento en el tema de la seguridad pública y ciudadana.

14. En nuestro país la incorporación de cámaras con fines públicos y privados es cada vez mayor, es necesario una reforma legal que alinee el funcionamiento de las cámaras, acorde a los principios de la actividad y derechos civiles, se colmen los vacíos e incumplimientos legales que existen, actualmente, y se reorganicen las funciones de cada institución. Además, la instalación de las cámaras debe estar supeditada a análisis previos que verifiquen la necesidad y viabilidad de las cámaras, así como estudios posteriores, que determinen la efectividad de la cámara para la prevención y persecución del delito.

15. En Costa Rica, la normativa referente a los sistemas de videovigilancia se debe regular bajo el principio de reserva de ley, y no por decreto ejecutivo como sucede en la realidad. Debido a que la actividad recae sobre derechos protegidos a nivel constitucional, como el derecho a la vida privada y la imagen, e incluso la protección de datos personales, consideramos que la mejor opción.

16. Existe una falta de organización institucional en nuestro país. Por un lado tenemos la Agencia de Protección de Datos, que no participa ni tiene injerencia en los proyectos de videovigilancia. Existe un reglamento que establece la competencia del Ministerio de Seguridad Pública para llevar a cabo esta actividad, pero son las

municipalidades quienes están a cargo de estos proyectos. Y la Sala Constitucional que ha actuado como órgano resolutorio en caso de disputas relacionadas al funcionamiento de las cámaras. Esto implica una falta de coordinación entre las autoridades competentes, un desorden en las funciones que debe desempeñar cada una, hay un incumplimiento de la normativa existente y, finalmente, el ciudadano, que desconoce dónde puede hacer valer sus derechos, quejas o dudas. Debe ser la legislación quien determine las competencias de las instituciones involucradas en lo referente a los sistemas de video-vigilancia.

17. La poca jurisprudencia constitucional que existe sobre videovigilancia en nuestro país, dista de los pronunciamientos europeos. Los tribunales europeos han sido más proteccionistas sobre los derechos del ciudadano que sobre las potestades administrativas de los policías, son conscientes de las repercusiones que tienen la proliferación de estos sistemas sobre la vida privada de la persona y han sido contundentes en establecer los límites espaciales y temporales del funcionamiento de estos sistemas.

18. De los criterios de la Sala Constitucional es poco lo que se puede abstraer, se han analizado asuntos como el espacio de captación de las cámaras donde se ha ordenado la reubicación de las mismas, y el asunto de la finalidad de la cámara por motivos de seguridad. Finalmente, en un voto salvado la Sala concluye que los problemas que surjan entre vecinos por el uso de videocámaras deben resolverse en la sede contravencional y no en la Sala Constitucional. Pareciera que la participación de la Sala se limita a aquellos casos donde existen invasiones ilegítimas a la privacidad del ciudadano por parte del Estado. No entraría a resolver cualquier invasión a la privacidad de disputas que surgen entre particulares que involucre vigilancia con fines privados.

19. La presencia de los CCTV en los espacios públicos y los derechos privados del ciudadano pueden convivir en armonía sin conflicto alguno. Para ello es necesario reorientar políticas de seguridad que han incentivado la proliferación de estos sistemas, complementar la legislación con garantías para el ciudadano y delegar a una institución que se encarguen de supervisar el adecuado uso de las cámaras implementando mejoras prácticas en la vídeo vigilancia.

BIBLIOGRAFÍA

Libros:

- Arenas Ramiro, Mónica. 2006. *El derecho fundamental a la protección de Datos Personales en Europea*. 1ra edición; Valencia España: Editorial Tirant lo Blanch.
- Arzoz Santisteban, Xavier. 2010. *Videovigilancia, seguridad ciudadana y derechos fundamentales*, España: Civitas - Thomson Reuters.
- Azurmendi Adarraga, Ana. 1997. *El derecho a la propia imagen: su identidad y aproximación al derecho a la información*". Madrid, España: Editorial Civitas.
- Azurmendi Adarraga, Ana. 1998. *El derecho a la propia imagen: su identidad y aproximación al derecho a la información*. 2da. Edición. México, D.F: Universidad Iberoamericana.
- Baratta, Alessandro. 1996. *Criminología crítica y crítica del derecho penal*, México: Siglo XXI Editores.
- Borges Frías, Jorge Luis; Arias Gayoso, Grethel. 2009. *Discrecionalidad y Legalidad*. Argentina: Editorial El Cid Editor.
- Cabezuelo Arenas, Ana Laura. 1998. *Derecho a la intimidad*. Valencia, España: Editorial Tirant Lo Blanch.
- Castel, Robert. 1997, *Las metamorfosis de la cuestión social*, Buenos Aires: Paidós.
- Chirino Sánchez, Alfredo. 1997. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica*. San José: CONAMAJ.
- Cordero Vega, Luis. 2007. *El control de la Administración del Estado*. Santiago, Chile: Lexis/Nexis.
- Da Agra, Cândido; Domínguez, José Luis; García Amado, José Antonio; Hebberecht, Patrick y Recasens, Amadeu. 2003. *La seguridad en la sociedad del riesgo: un debate abierto*. España: Atelier.
- De Verda y Beamonte, José Ramón. 2007. *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Pamplona, España: Editorial Thomson-Aranzadi.
- Foucault, Michel. 2003. *Vigilar y Castigar*. Buenos Aires, Argentina: Siglo Veintiuno Editores.

- Garriga Domínguez, Ana. 2016. *Nuevos retos para la protección de datos personales. En la era del big Data y de la computación ubicua*, 1ra ed., Madrid, España: Dykinson, S.L.
- Herrán Ortiz, Ana Isabel. 2003. *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao: Cuadernos Deusto de Derechos Humanos No. 26.
- Huhn, Sebastian. 2012. *Criminalidad y discurso en Costa Rica: reflexiones críticas sobre un problema social*. 1ra edición San José, Costa Rica: Flacso.
- Llácer Matacás, María Rosa. 2001. *Protección de Datos personales en la sociedad de la información y la vigilancia*, 1ra ed. Universidad de Barcelona, España: Editorial La Ley.
- Llobet Rodríguez, Javier y Chirino Sánchez, Alfredo. 2002. *Principio de oportunidad y persecución de la criminalidad organizada. Problemas prácticos e ideológicos de un proceso penal eficiente*. San José: Ediciones Jurídicas Areté.
- Lorenzetti, Ricardo. 2014. *El arte de hacer Justicia. La intimidación de los casos más difíciles de la Corte Suprema*. Argentina: Penguin Random House Grupo Editorial.
- Norris, C., J. Moran, y G. Armstrong. 1998. *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate.
- Pérez Luño, Antonio Enrique. 1987. *Problemas Actuales de la Documentación y la informática Jurídica*". Madrid, España: Fundación Cultural Enrique Luño Peña.
- Pouillet, Yves, Pérez Asinari, María Verónica y Palazzi Pablo. 2009. *Derecho a la intimidad y a la protección de datos personales*. Buenos Aires, Argentina: Editorial Heliasta.
- Puccinelli Óscar R. 2004. *Protección de Datos de Carácter Personal*. Buenos Aires, Argentina: Editorial Astrea.
- Rivera Ortega, Ricardo. 2002. *El Estado Vigilante*. España: Editorial Técnos.
- Rodríguez Ruíz, Blanca. 1997. *El secreto de las comunicaciones, tecnología e intimidad*. Madrid, España: McGraw Hill.
- Serbín, Andrés; Sojo, Carlos y Salomón, Leticia. 2001. *Gobernabilidad democrática y seguridad ciudadana en Centroamérica*. Managua, Nicaragua: CRIES
- Sernaqué, Silva y Alfonso, Santos. 2002. *Control social, neoliberalismo y derecho penal*. Lima, Perú: UNMSM Fondo Editorial.
http://sisbib.unmsm.edu.pe/BibVirtual/libros/Sociologia/control_social_neo/indice.htm
 consultada el 21 de julio de 2018
- Simón, Jonathan. 2011. *Gobernar a través del delito*. España: Editorial Gedisa

Whitaker, Reg. 1999. *El fin de la privacidad: como la vigilancia total se esta convirtiendo en realidad*. España: Paidós Ibérica.

Revistas:

Arzoz Santisteban, Xavier. “Video vigilancia y derechos fundamentales: análisis de la constitucionalidad de la Ley Orgánica 4/1997”. *Revista Española de Derecho Constitucional*, No. 64 (Enero – Abril 2002): 133-176.

Carvajal Pérez, Marvin, y Alfredo Chirino Sánchez. “El camino a la regulación normativa del tratamiento de datos personales en Costa Rica”. *Revista de Derecho Constitucional*, (2003): 1-53.

Chirino Sánchez, Alfredo. “Protección de datos y moderno proceso penal. Aspectos constitucionales y legales”. *Revista de Ciencias Jurídicas de la Universidad de Costa Rica*, (1999): 9-41.

Choclán Montalvo, José Antonio. “La prueba videográfica en el proceso penal: Validez y límites”. *Revista No. 38 del Consejo General del Poder Judicial de España* (1995): 47-78.

Damián Moreno, Juan. “Reflexiones sobre la reproducción de imágenes como medio de prueba en el proceso penal”, *Revista Vasca de Derechos Procesal y Arbitraje*, (1997). Tomo IX.

Daroqui, Alcira. “Las seguridades perdidas”, *Argumentos*, Vol. 2 (mayo 2003): 1-8. dialnet.unirioja.es/descarga/articulo/3991762.pdf Consultada el 13 de agosto de 2018.

Estrada Alonso, Eduardo. “El Derecho a la imagen en la LO 1/1982, de 5 de mayo”. *Actualidad Civil*, No. 25 (1990): 365-376.

Izu Belloso, Miguel José. “Los conceptos de orden público y seguridad ciudadana tras la Constitución de 1978”. *Revista Española de Derecho Administrativo*, No. 58 (Abril – Junio 1988): 1-20

Sirovich, L. y Kirby, M. “Low-Dimensional Procedure for the Characterization of Human Faces”, *Journal of the Optical Society of America*, Vol. 4, No.3 (1987): 519-524.

Turk, Mathew. A. y Pentland, Alex. P. “Face Recognition Using Eigenfaces”. Vision and Modeling Group, The Media Laboratory Massachusetts Institute of Technology (1991): 586-591.

Revistas Digitales:

- Aba Catoira, Ana. “La videovigilancia y la garantía de los derechos Individuales: su marco jurídico”. *Anuario de la Facultad de Derecho de la Universidad de Coruña*, No. 7 (2003): 13-35. Consultado el 19 de enero, 2018. <http://ruc.udc.es/dspace/handle/2183/2251> DOI: <http://hdl.handle.net/2183/2251>
- Arteaga Botello, Nelson. “Video-vigilancia del espacio urbano: Tránsito, seguridad y control social. *Andamios. Revista de Investigación Social*, vol. 7, No. 14, (Setiembre - Diciembre 2010): 263-286. Consultada el 17 de diciembre del 2017. <http://www.redalyc.org/articulo.oa?id=62819897011>
- Arteaga Botello, Nelson. “Regulación de la video-vigilancia en México. Gestión de la ciudadanía y acceso a la ciudad”. *Espiral Guadalajara*. Vol. 3, No. 66 (Mayo - Agosto 2016): 193-238. Consultada el 17 de diciembre, 2017. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193#B49
- Betancourt, Andrea. “La Video vigilancia: un Sistema de seguridad que requiere de control y regulación”. *Repositorio Digital FLACSO Ecuador. Boletín Ciudad Segura*, No. 25 (2008): 3. Consultada el 8 de agosto, 2017. <http://www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=20859>.
- Caballero Julián, Franco Gabriel, Vidal Reyes, Martín, López Sánchez, Antonia, Jerónimo Ríos y Carlos Alberto. “Reconocimiento facial por el método de Eigenfaces”, *Pistas Educativas*, vol. 39, No. 127 (diciembre 2017): 69-81. Consultada el 3 de agosto de 2018. <http://www.itcelaya.edu.mx/ojs/index.php/pistas/article/view/1068>
- Cadenas Moreano, José Augusto, Montaluisa Pulloquina, Raúl Humberto, Flores Lagla, Galo Alfredo, Chancúsig Chisag, Juan Carlos y Guaypatín Pico, Oscar Alejandro, “Reconocimiento facial con base en imágenes”. *Revista Boletín Redipe*. Vol 6-5 (mayo 2017), 143-151. Consultada el 03 de Agosto de 2018. <https://webcache.googleusercontent.com/search?q=cache:P9ayH0xtPIoJ:https://revista.redipe.org/index.php/1/article/download/267/264/+&cd=2&hl=es&ct=clnk&gl=cr>

- Carrión, Fernando. “La inseguridad ciudadana en la comunidad andina”, *Iconos, Revista de Ciencias Sociales*, No. 18 (enero 2004): 109-119. Consultada el 4 de Julio, 2018. <https://dialnet.unirioja.es/descarga/articulo/4823159.pdf>
- Carrión, Fernando. “La inseguridad ciudadana en América Latina”, *Quórum. Revista de pensamiento iberoamericano*, No. 12 (2005): 29-52, <http://www.redalyc.org/pdf/520/52001204.pdf>
- Carrión, Fernando. “Ojo: le estamos filmando”. *Repositorio Digital FLACSO Ecuador. Boletín Ciudad Segura*, No. 25 (2008): 4-9. Consultada el 8 de setiembre, 2017. <http://www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=20859>
- Célida Godina Herrera, “El panóptico moderno”. *A parte Rei. Revista de Filosofía*, No. 46, (Julio 2006), 1-11. Consultada el 18 de diciembre del 2017. <http://serbal.pntic.mec.es/~cmunoz11/godina46.pdf>
- Cordero Vega, Luis. “Videovigilancia e intervención administrativa: las cuestiones de legitimidad”. *Revista de Derecho Público*, Vol. 70 (noviembre 2015): 359-376. Consultada el 02 de febrero, 2018. <https://revistas.uchile.cl/index.php/RDPU/article/view/37768/39415> DOI: 10.5354/rdpu.v0i70.37768
- De Dienheim Barriguete, Cuauhtémoc M. “El Derecho a la intimidad, al Honor y a la Propia Imagen”. *IUS Revista Jurídica. Universidad Latina de América*. (Julio 2001): 59-65. Consultada el 20 de noviembre, 2017. <https://revistas-colaboracion.juridicas.unam.mx/index.php/derechos-humanos-emx/article/view/23885/21367>
- De Terwangne, Cécile. “Privacidad en Internet y el derecho a ser olvidado / derecho al olvido”. *IDP: Revista de Internet, derecho y política*. No. 13 (Febrero de 2012): 53-66. Consultada el 13 de junio, 2018. <http://www.redalyc.org/articulo.oa?id=78824460006>
- Díez Ripollés, José Luis y Cerezo Domínguez, Ana Isabel. “La prevención de la delincuencia callejera mediante videocámaras. Regulación jurídica y eficacia”. *Polít. Crim*, No. 7 (2009): 171-196. Consultada el 15 de junio, 2018. http://www.politicacriminal.cl/Vol_04/n_07/Vol4N7A6.pdf
- Díez Ripollés, José Luis y Cerezo Domínguez, Ana Isabel. “La videovigilancia en las zonas públicas: su eficacia en la reducción de la delincuencia”, *Boletín Criminológico del*

- Instituto andaluz interuniversitario de Criminología*, No. 121 (Junio-julio 2010), 1-4.
Consultado el 25 de julio 2018.
<http://www.boletincriminologico.uma.es/boletines/121.pdf>
- Durán Segura, Luis A. “Lo que la ciudadanía anhela ver. Desarrollo urbano, nuevas tecnologías y espacios públicos en San José”, *Revista Universidad Santo Tomás*, No. 81 (12 de Junio, 2012): 117-144. Consultada el 9 de marzo, 2017.
<http://revistas.usta.edu.co/index.php/analisis/article/viewFile/1274/1472> DOI:
10.15332/s0120-8454
- Espinola Frausto, Dolly. “La video vigilancia en el discurso modernizador de la seguridad”. *Revista Ação midiática. Estudos em Comunicação, Sociedade y Cultura*. No. 6 (2013): 1-11. Consultada el 17 de marzo, 2017.
<https://revistas.ufpr.br/acaomidiatica/article/view/34413> DOI:
<http://dx.doi.org/10.5380/am.v0i6.34413>
- Fayos Gardó, Antonio. “¿Tienen las personas públicas derecho a la intimidad y a la propia imagen?”. *Revista de los Estudios de ciencias de la Información y de la Comunicación*, No. 35 (julio de 2014). Consultada el 14 de junio, 2017.
<http://comein.uoc.edu/divulgacio/comein/es/numero35/articles/Article-Antonio-Fayos-Gardo.html>
- Galdon-Clavell, Gemma. (Setiembre 2009). “Espacios públicos urbanos, prostitución y ordenanzas cívicas”. *Sin permiso*. <http://www.sinpermiso.info/printpdf/textos/espacios-pblicos-urbanos-prostitucin-y-ordenanzas-cvicas> Consultada el 03 de julio de 2017.
- Galdon-Clavell, Gemma. “Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas”. *Revista Latinoamericana de Estudios Urbanos Regionales (EURE)*. Vol 41. No. 123 (Mayo de 2015). Consultada el 19 de enero, 2018.
<http://www.eure.cl/index.php/eure/article/view/678/813>
- Gaytán Santiago, Pablo. “Vigilar y negociar. Imaginario sociomediático de la seguridad pública y campo vacío ciudadano”, *El Ciudadano*, No. 151 (mayo-junio 2010), 13-22.
Consultada el 7 de noviembre de 2018.
<http://www.redalyc.org/articulo.oa?id=32513865003>

- Gude Fernández, Ana. “Videovigilancia Privada en lugares de acceso público y derecho a la protección de datos: el caso Alemán”. *Revista de la Facultad de Derecho Estudios de Deusto*, Vol. 61, No. 1 (Enero-Junio 2014): 73-116. Consultada el 9 de marzo, 2018. <http://revista-estudios.revistas.deusto.es/article/viewFile/231/360>
- Huhn, Sebastian. “Criminalidad, miedo y control en Costa Rica: estadísticas de criminalidad y seguridad pública”. *Cuadernos de Sociología*, No. 10 (2010): 21-43, consultada el 4 de abril del 2017, http://www.academia.edu/771330/Criminalidad_Miedo_y_Control_en_Costa_Rica_Estadísticas_de_Criminalidad_y_Seguridad_Pública
- Ibarra Sánchez, Ernesto “Videovigilancia. Punto de colisión entre derechos fundamentales, seguridad y protección de datos personales en México”. *Acervo de la Biblioteca Jurídica Virtual de la UNAM* (5 de julio de 2010): 231-269, consultada el 03 de enero, 2018. <https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/17.pdf>
- Koskela, Hille. “Cam Era — the contemporary urban Panopticon.” *Surveillance & Society*, no. 3 (setiembre 2003). 292-313, consultada el 1 de setiembre, 2018 <http://www.surveillance-and-society.org> DOI: <https://doi.org/10.24908/ss.v1i3.3342>
- Lara Gamboa, Fernando. “El Derecho fundamental a la propia imagen y la publicación de Fotografías”. *Revista de Ciencias Jurídicas de la Universidad de Costa Rica*, No. 105 (2004): 187-214, consultada el 15 de marzo, 2017. <https://revistas.ucr.ac.cr/index.php/juridicas/article/view/13348/12620>
- Lio, Vanessa. “Cámaras de seguridad y prevención del delito. La utilización de la videovigilancia en la ciudad de Buenos Aires”. *Visioni LatinoAmericane e la rivista del Centro Studi per l’America Latina. Revista Pensamiento Penal*, No. 13 (2015): 33-46, consultada el 1 de diciembre, 2017. <http://www.pensamientopenal.com.ar/doctrina/41974-camaras-seguridad-y-prevencion-del-delito-utilizacion-video-vigilancia-ciudad-buenos>
- Lio, Vanessa. “Ciudades, cámaras de seguridad y video-vigilancia: Estado del arte y perspectiva de investigación”. *Astrolabio*, No. 15, (2015): 273-302. Consultado el 20 de julio de 2018 <https://revistas.unc.edu.ar/index.php/astrolabio/article/viewFile/9903/13441>
- Löfberg, Sara. “Ojos de águila: una primera aproximación al sistema de video vigilancia en Quito”, *Repositorio Digital FLACSO Ecuador. Boletín Ciudad Segura*, No. 25 (2008): 4-

- 9, consultada el 02 de octubre de 2017.
<http://www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=20859>
- Martínez de Pisón Cavero, José. “Vida Privada e intimidad: implicaciones y perversiones”. *Anuario de Filosofía del Derecho*, Vol. XIV, (1996-1997): 717-738.
https://www.researchgate.net/publication/315799058_Vida_privada_e_intimidad_implicaciones_y_perversiones Consultada el 01 de junio, 2018.
- Morales Godo, Juan “El derecho a la intimidad y la publicidad del registro en el Estado Democrático”. *Revista Boliviana de Derecho*, No. 4 (2007): 59-79.
<http://www.redalyc.org/pdf/4275/427539904004.pdf> Consultada el 04 de abril de 2018.
- Morenilla, José María. “La actividad del Tribunal Europeo de Derechos Humanos en relación con la seguridad ciudadana”. *Seminario Duque de Ahumada*, Vol. 14, (2002): 53-68.
http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/UBICACIONES/06/DUQUE_AHUMADA/14/4_JOSE%20MARIA%20MORENILLA%20RODRIGUEZ.PDF Consultada el 13 de abril, 2018.
- Muñoz Conde, Francisco. “Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal”. *Lusíada Direito*, No. 4/5 (2007): 29-76.
<http://revistas.lis.ulusiada.pt/index.php/ldl/article/viewFile/678/766> Consultada el 02 de febrero, 2018.
- Navajas Ramos, Luis. “La prueba videográfica en el proceso penal: su valor y límites para su obtención”, *EGUZKILORE*, No. 12 (diciembre de 1998): 147-169.
<https://www.ehu.eus/documents/1736829/3342827/Eguzkilore+12-13.+Navajas+Ramos.pdf> Consultada el 1 de diciembre de 2018
- Nogueira Alcalá, Humberto. “Aspectos de una Teoría de los Derechos Fundamentales: la delimitación, regulación, garantías y limitaciones de los Derechos Fundamentales”. *Revista Ius et Praxis*, Vol. 11, No. 2 (2005): 15-64.
<http://www.revistaiepraxis.cl/index.php/iepraxis/article/view/536/401> Consultada el 20 de febrero, 2018.
- Nogueira Alcalá, Humberto. “El derecho a la propia imagen como derecho fundamental implícito. Fundamentación y caracterización”. *Revista Ius et Praxis*. Vol. 13 No. 2 (2007): 245-285. http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000200011 Consultada el 2 de enero, 2018.

- O'Malley, Pat. "Repensando la penalidad neoliberal", *Delito y sociedad*, vol. 24, No. 40 (diciembre 2015), http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S2468-99632015000200002 Consultado el 21 de julio de 2018
- Pace, Alessandro "El derecho a la propia imagen en la sociedad de los mass media", *Revista Española de Derecho Constitucional*, No. 52 (enero / abril 1988): 33-52, https://www.jstor.org/stable/24882902?seq=1#page_scan_tab_contents Consultada el 20 de marzo de 2017
- Pérez-Cruz Martín, Agustín Jesús. "Videovigilancia y derecho a la intimidad: ¿Un nuevos ejemplo de conflicto entre el Derecho a la seguridad pública y el derecho fundamental a la intimidad?". *Anuario de la Facultad de Derecho de la Universidad de Coruña*, No. 1, (1997): 401-412. <http://ruc.udc.es/dspace/bitstream/handle/2183/1942/AD-1-21.pdf?sequence=1> Consultada el 4 de febrero, 2018.
- Quirós Camacho, Jenny. "La protección de datos personales y le habeas data: elementos para iniciar una discusión en Costa Rica". *Revista de Ciencias Jurídicas de la Universidad de Costa Rica*, No. 103 (2004): 141-187. <https://revistas.ucr.ac.cr/index.php/juridicas/article/view/13370> Consultada el 14 de agosto, 2017.
- Ramírez Hernández, Rebeca y Mena García, Sergio. "Recomendaciones para la Elaboración de Reglamentos", *Revista Jurídica de Seguridad Social*, No. 9 (Abril de 1999) 37-46, <http://www.binasss.sa.cr/revistas/rjss/juridica9/art7.pdf> Consultada el 02 de noviembre de 2017.
- Riquert, Marcelo Alfredo. "América Latina: modelos de política criminal y derecho penal del enemigo", *Panóptica*, A. 3, No. 18 (Marzo-Junio 2010): 154-175. http://www.panoptica.org/seer/index.php/op/article/view/Op_5.1_2010_154-175/288 Consultada el 21 de Julio de 2018.
- Roccatti, Mireille Velázquez. "La Seguridad Pública como Instrumento Esencial para el Ejercicio de los Derecho Humanos". *Instituto de Investigaciones Jurídicas UNAM*, No. 17 (1996): 141-146. <http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/17/pr/pr8.pdf> Consultada el 9 de setiembre, 2017.

- Romero Sánchez, Angélica. “Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán”, *Revista Criminalidad* 57 (2), 319-333. <http://www.scielo.org.co/pdf/crim/v57n2/v57n2a10.pdf> Consultada el 15 de noviembre de 2018.
- Santillán, Alfredo. “Los Dilemas de la Video vigilancia”. *Repositorio Digital FLACSO Ecuador. Boletín Ciudad Segura*, No. 13 (2007): 11. <http://repositorio.flacsoandes.edu.ec/bitstream/10469/2318/1/BFLACSO-CS25-06-Santillán.pdf> Consultada el 9 de octubre, 2017:
- Soto Urpina, Carles. “La Medición del desplazamiento y la difusión de beneficios: Aplicación del método Bowers y Johnson (2003) a la investigación de Cerezo y Díez Ripollés (2010)”. *Revista Española de Investigación Criminológica*. Vol. 11 (marzo, 2013): 1-26. <https://reic.criminologia.net/index.php/journal/article/view/74> Consultada el 02 de febrero, 2018.
- Téllez Valdés, Julio Alejandro. “La regulación jurídica de la videovigilancia bajo una perspectiva de Derecho Comparado”. *Instituto de Investigaciones Jurídicas de la UNAM*, (2012): 767-784. https://www.researchgate.net/publication/242421144_LA_REGULACION_JURIDICA_DE_LA_VIDEOVIGILANCIA_BAJO_UNA_PERSPECTIVA_DE_DERECHO_COMPARADO Consultada el 23 de febrero, 2018.
- Toledo Báez, María Cristina. “Aproximación a la protección de datos personales en España, Inglaterra y Francia como ejercicio de Derecho Comparado previo a una traducción”, *Contribuciones a las Ciencias Sociales EUMEDNET*, (Marzo, 2010) <http://www.eumed.net/rev/ccss/07/mctb.htm> Consultada el 23 de febrero, 2018.
- Valverde Espinoza, Ida Maurelia. “Régimen Legal de la Video vigilancia”. *Revista Jurídica Virtual* Año III, No. 4 (Marzo 2013). <http://docplayer.es/23572938-Regimen-legal-de-la-videovigilancia.html> Consultada el 9 de marzo, 2017.
- Vozmediano Sáenz, Laura, Vergara Iraeta, Ana Isabel y San Juan Guillén, César. “El estudio científico del miedo al delito: algunas reflexiones sobre un fenómeno urbano, mediático y político”, *International E-Journal of Criminal Sciences*, No. 4 (2010),

<http://www.ehu.eus/ojs/index.php/inecs/article/view/924> Consultada el 6 de noviembre de 2018.

Zavaleta Betancourt, José Alfredo y Bielefeldt Astete, Alberto. “Los retos de la seguridad ciudadana”, *Estudios de Seguridad y Defensa*, No. 1 (junio 2013), 91-113. <https://www.fundacionhenrydunant.org/images/stories/biblioteca/ddhh-segciudadana-violenciaurbana/Los%20Retos%20de%20la%20Seguridad%20Ciudadana%20-%20Jose%20Alfredo%20Zavaleta.pdf> Consultada el 07 de Agosto de 2018.

Sitios de Internet:

Agencia de Protección de Datos de los Habitantes. “Quienes somos?” Disponible en: <http://prodhab.go.cr/quienesomos/>

Agencia Española de Protección de Datos, “Informe jurídico de Videovigilancia”. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2007-0035_Deber-de-informar-en-videovigilancia.pdf

Arias F, Rafael (Marzo, 2011). “Seguridad ciudadana: prioridad para la nueva gestión”. Boletín Informativo de la Dirección de Seguridad Ciudadana y Policía Municipal. https://www.msj.go.cr/informacion_ciudadana/seguridad/San%20Jos%20Seguro/2011-03%20%20San%20José%20Seguro.pdf Consultada el 23 de abril, 2018.

Arias, Patricia; Rosada Granados, Héctor y Saín, Marcelo Fabián. (Octubre de 2012). “Reformas Policiales en América Latina. Principios y lineamientos progresistas”. Programa de Cooperación en Seguridad Regional. Bogotá, Colombia. <http://library.fes.de/pdf-files/bueros/la-seguridad/09383.pdf> Consultado el 17 de noviembre de 2017.

Aznar Gómez, Hugo. (1996). “Intimidad e información en la sociedad contemporánea”. Fundación Universitaria San Pablo CEU. <http://dspace.ceu.es/handle/10637/7161> Consultada el 17 de junio, 2018.

Beltrane, Florencia. “Seguridad ciudadana, inseguridad, políticas públicas, delito, Sistema penal”, IX Jornadas de Sociología, Facultad de Ciencias Sociales, Universidad de Buenos Aires, (2011), 1-15, <http://cdsa.aacademica.org/000-034/313.pdf> Consultada el 6 de agosto de 2018

- Berning Prieto, Antonio David (mayo, 2008). “Régimen jurídico de la videovigilancia. La captación y grabación de imágenes y sonidos con fines de investigación criminal”. Noticias Jurídicas. <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4374-regimen-juridico-de-la-videovigilancia-la-captacion-y-grabacion-de-imagenes-y-sonidos-con-fines-de-investigacion-criminal/> Consultada el 21 de abril, 2018.
- Calfa, Roxana; Sebastian, Sperber y Bourgeois, Nathalie. (Junio de 2010). “Ciudadanos, ciudades y video vigilancia. Hacia una utilización democrática y responsable de la videovigilancia”. Foro Europeo para la Seguridad Urbana”. Impreso por STIPA-Montreuil. http://efus.eu/files/2013/05/CCTV_ESPAGNOL.pdf Consultada el 01 de marzo, 2017.
- CANIETI. “Estudio de autorregulación en material de privacidad y protección de datos personales en el ámbito de las Ti” Prosoft. s.f. https://prosoft.economia.gob.mx/Imágenes/ImágenesMaster/Estudios%20Prosoft/FREF_04.pdf Consultada el 26 de Febrero, 2018.
- Carli, Vivien. (Diciembre de 2008). “Valoración de la video-vigilancia como una herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes”. Centro Internacional para la prevención de la Criminalidad. http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/Valoracion_del_CCTV_como_una_Herramienta_efectiva_de_manejo_y_seguridad_ESP.pdf Consultada el 02 de octubre, 2017.
- Comité de Derechos Humanos. “Examen de los Informes presentados por los Estados Partes de conformidad con el artículo 40 del Pacto” (1o. de noviembre del 2006). Sexto informe periódico Reino Unido de Gran Bretaña e Irlanda del Norte del Pacto Internacional de Derechos Civiles y Políticos, <http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsg%2F0K3H8qae8NhIDi53MecKx8EqSqfKWwnDvfDoWF2J8CGVEVjoLzczwwZdjKPMVPEBxCaaygxW8UbzmCU0847buNI%2Bg0iyXoJgD51eTIueIvfPMPwepSg2FDmPw9d9Rqw%3D%3D>
- Cornelis Ramírez, Martín (2015). “La videovigilancia en Costa Rica como medio de control social”. Pensamiento Penal.

<http://www.pensamientopenal.com.ar/system/files/2015/05/doctrina41187.pdf>

Consultada el 2 de junio de 2018.

Dammert, Lucía. (marzo, 2008). “Seguridad pública y privada en las Américas: Desafíos del análisis institucional”. Departamento de Seguridad Pública de la Organización de los Estados Americanos. <https://www.oas.org/dsp/documentos/publicaciones/seg%20pub-%20lasamericas.pdf> Consultada el 03 de febrero, 2017.

De Lamo Merlini, Olga. “Consideraciones sobre la configuración del derecho a la propia imagen en el ordenamiento español”. Biblioteca Digital de la Universidad Complutense de Madrid. http://eprints.ucm.es/10972/1/Lamo_Merlini_derecho_a_la_propia_imagen.pdf Consultada el 30 de junio, 2017.

Dirección General de Mercado Interior de la Comisión Europea. Grupo del artículo 29 sobre protección de datos. “Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara”. 25 de noviembre del 2002. Bruselas, Bélgica. Disponible en: Sitio web: www.europa.eu.int/comm/privacy

El grupo de protección de las personas en lo que respecta al tratamiento de datos personales. (11 de febrero, 2004). “Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara”, https://www.apda.ad/system/files/wp89_es.pdf Consultada el 23 de octubre de 2017

Enciclopedia Jurídica, “Orden Público”. Edición 2014. Disponible en: <http://www.encyclopedia-juridica.biz14.com/d/orden-público/orden-público.htm> (consultada el 21 de setiembre de 2017)

Gamboa Montejano, Claudia y Ayala Cordero, Arturo. (2009). “Datos Personales. Estudio teórico conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia”. Centro de Documentación, Información y análisis de México. <http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf> Consultada el 1 de octubre, 2017.

García Falconi, José C. (24 de Noviembre del 2005). “Derechos Constitucionales a la intimidad, privacidad y la imagen”. Universidad Central de Ecuador. Ecuador. <https://www.derechoecuador.com/derechos-constitucionales-a-la-intimidad-privacidad-y-la-imagen> Consultada el 15 de octubre, 2017.

- Informe Anual de la Comisión Interamericana de Derechos Humanos (2016). “Informe de la Relatoría Especial para la Libertad de Expresión”. Organización de los Estados Americanos. Disponible en: <http://www.oas.org/es/cidh/expresion/docs/informes/anuales/InformeAnual2016RELE.pdf>
- “Informe Anual sobre Derechos Humanos en Chile 2017” (noviembre, 2017). 1ra edición, Ediciones Universidad Diego Portales. Disponible en: <http://www.derechoshumanos.udp.cl/derechoshumanos/images/InformeAnual/2017/9-derecho%20a%20la%20privacidad.pdf>
- Insecurity. “Advances in CCTV” s.f., <http://www.insecurity.eu/index.php/news/archives/advances-in-cctv-can-offer-peace-of-mind> (último acceso: 28 de Agosto de 2018).
- Instituto Interamericano de Derechos Humanos. (2011). “Módulo instruccional: Derechos humanos, seguridad ciudadana y funciones policiales”. IIDH. San José, Costa Rica. <https://www.iidh.ed.cr/IIDH/media/1556/acceso-justicia-modulo-2011.pdf> (consultado el 18 de setiembre del 2017)
- Interpol. “Acerca de la INTERPOL, Historia”, s.f. <https://www.interpol.int/es/Acerca-de-INTERPOL/Historia> Consultada el 9 de marzo de 2017.
- Llanera Conde, Pablo. (2016). “Libertad y Seguridad en el Espacio Público: La Videovigilancia”. Sala Segunda del Tribunal Supremo. <https://es.scribd.com/document/139560702/LIBERTAD-Y-SEGURIDAD-EN-EL-ESPACIO-PUBLICO-LA-VIDEOVIGILANCIA> Consultada el 03 de enero, 2018.
- López Ávila, Viridiana. (18 de Marzo de 2014). “El derecho a la propia imagen en e derecho mexicano y su contexto de violencia”. Observatorio Iberoamericano de Protección de Datos. Disponible en: <http://oiprodat.com/2014/03/18/el-derecho-a-la-propia-imagen-en-el-derecho-mexicano-y-su-contexto-de-violencia/> Consultado el 1 de junio, 2017
- Macarena Rau V. y Paola Prosser L., “Estudio de evaluaciones de impacto de estrategias en CPTED y prevención situacional”, <http://www.leemira.cl/biblioteca/download.php?id=72> (consultada el 03 de octubre de 2018)

- Mertz, Catalina. “Delincuencia: la principal preocupación de los chilenos”. En *95 propuestas para un Chile mejor*, 1-70. Chile: 2013. <http://95propuestas.cl/site/wp-content/uploads/2013/05/delincuencia-en-chile-diagnostico-y-propuestas-catalina-mertz.pdf> Consultada el 15 de febrero, 2018.
- Mieres Mieres, Luis Javier (2014). “Derecho al olvido digital”. Laboratorio de Alternativas. http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf Consultada el 15 de abril, 2018.
- Millán Gómez, Agustín. (15 de marzo de 2013). “La videovigilancia y la protección de los datos personales en la Ciudad de México”. Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado. Última modificación. <https://itaipue.org.mx/articulos/2013/1503invitado.html> Consultado el 9 de junio, 2018.
- Murriá, Marta y González, Carlos. “La seguridad ciudadana: instrumentos de análisis”, trabajo presentado en el X Congreso Español de Sociología “Sociología y sociedad en España, Treinta años de sociedad, treinta años de sociología”, organizado por la Federación Española de Sociología (FES) en Navarra, 1,2 y 3 de julio de 2010. Instituto de Estudios Regionales y Metropolitanos de Barcelona, Universidad Autónoma de Barcelona, <http://www.fes-sociologia.com/files/congress/10/grupos-trabajo/ponencias/631.pdf> (consultada el 17 de agosto del 2018)
- Parrilli, Roberto (12 de octubre del 2011). “Doctrina del día: los sistemas de video vigilancia, el derecho a la privacidad, la imagen y la protección de datos personales”. Thomson Reuters. <http://thomsonreuterslatam.com/2012/02/22/doctrina-del-dia-los-sistemas-de-video-vigilancia-el-derecho-a-la-privacidad-la-imagen-y-la-proteccion-de-datos-personales/#sthash.5YG2f6AO.dpuf> Consultada el 27 de junio, 2017.
- Pérez Valdés, Damian. (26 de octubre de 2007). “Que son las bases de datos?” Maestros del web. <http://www.maestrosdelweb.com/que-son-las-bases-de-datos/> Consultada el 18 de junio, 2017.
- “Privacy by design para fomentar la figura del encargado”, Tercera entrega: Entrega Final, 47, disponible en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FRE_F_23.pdf (consultado el 18 de setiembre de 2018)

- Programa de las Naciones Unidas para el Desarrollo (Noviembre, 2013). “Informe Regional de Desarrollo Humano 2013-2014, Seguridad Ciudadana con Rostro Humano: diagnóstico y propuestas para América Latina”. PNUD, Nueva York, EEUU. <https://es.slideshare.net/gracielamariani/informe-regional-de-desarrollo-humano-20132014-seguridad-ciudadana-con-rostro-humanodiagnostico-y-propuestas-para-amrica-latina-del-pnud-programa-de-las-naciones-unidas-unidas-para-el-desarrollo> Consultado el 17 de diciembre, 2017.
- Programa Estado de la Nación, “I Informe Estado de la Justicia”, 1ra ed., E Digital ED S.A, Costa Rica, (abril 2015), 35, <http://www.estadonacion.or.cr/justicia/assets/estado-de-la-justicia-1-baja.pdf> (consultada el 25 de julio de 2018)
- Prosoft. “Privacy by design para fomentar la figura del encargado” *PROSOFT*. 2013. https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_23.pdf (último acceso: 18 de Setiembre de 2018).
- Quisbert, Ermo. (21 de junio de 2018). “Derecho La Intimidad O Vida Privada”, Apuntes Jurídicos. <http://jorgemachicado.blogspot.com/2013/01/dvp.html> Consultada el 03 de diciembre, 2017.
- Ranguni, Victoria. “Nuevas formas de problematización de la in/seguridad”, *Actas XXVII Congreso ALAS*, Buenos Aires, 2009: Facultad de Ciencias Sociales, UBA
- Sagant, Valérie y Shaw, Margaret. (2010). “Informe Internacional Prevención de la Criminalidad y Seguridad Cotidiana: Tendencias y Perspectivas”. Centro Internacional para la prevención de la Criminalidad. Montreal, Canadá. Disponible en: http://ovsyg.ujed.mx/docs/biblioteca-virtual/Prevencion_de_la_criminalidad_seguridad_cotidiana.pdf Consultado el 9 de marzo del 2017.
- Sánchez Migallón, Rubén y Monclús Ruíz, Jorge. (15 de enero del 2018). “¿Supone la reciente sentencia del TEDH un cambio en los requisitos para la videovigilancia de los trabajadores?”. Blog Cuatrecasas. <https://blog.cuatrecasas.com/laboral/sentencia-tedh-cambio-video-vigilancia-trabajadores/> Consultada el 13 de mayo, 2018.
- Secretaría de Economía de México. “Estudio de autorregulación en material de privacidad y protección de datos personales en el ámbito de las Ti. 5ta entrega: Versión Final”, Proyecto de Desarrollo de la Industria de las Tecnologías de la Información. Disponible

en:

https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

Secretaría de Seguridad Pública, “Informe anual de resultados 2010”, Ciudad de México (abril 2011), 4, http://www.ssp.df.gob.mx/TransparenciaSSP/Documents/2013/Art_15/SSP_Informe_Anual_2010.pdf (consultada el 2 de noviembre de 2017)

Secretaría General del Consejo. Bruselas. “Conclusiones del Consejo Europeo EUCO13/10 (17 de junio del 2010)”. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/115349.pdf

Secretaría General Organización de los Estado Americanos (Diciembre, 2008). “La Seguridad Pública en las Américas: retos y oportunidades”, 2da edición, SGOEA, Washington, EEUU. <https://www.oas.org/dsp/documentos/Observatorio/FINAL.pdf> Consultada el 01 de diciembre, 2017.

Soto, Carlos. (2015, 05 de Enero). “Videovigilancia. un negocio con grandes expectativas en 2015”. SecuriTIC. <http://www.securitic.com.mx/reportaje-especial/33-videovigilancia/reportaje/1397-videovigilancia-un-negocio-con-grandes-expectativas-en-2015>. Consultado el 1 de junio, 2017.

Varona Martínez, Gema. (2012, Diciembre). “Estudio exploratorio sobre los efectos del uso policial de la videovigilancia en lugares públicos. Propuesta criminológica de un sistema de indicadores sobre su adecuación y proporcionalidad en materia de seguridad”. Instituto Vasco de Criminología. Disponible en: <https://addi.ehu.es/bitstream/handle/10810/15269/USWEB138205.pdf?sequence=1&isAllowed=y>

Vida Fernández, José. (12 de Febrero de 2016). “La Seguridad Ciudadana y el Orden Público”. Lección 3, Universidad Carlos III de Madrid. <http://ocw.uc3m.es/derecho-administrativo/accion-administrativa-sectores-especificos/resumenes-de-contenidos-1/Leccion-3.pdf> Consultada el 3 de abril, 2017.

“Vigilancia, privacidad y seguridad”, SurPRISE Project, Surveillance Privacy Security, <http://surprise-project.eu/wp->

[content/uploads/2014/05/B3_CSIC_Information_Magazine_Spanish.pdf](#) (consultada el 21 de setiembre de 2018)

Tesis:

Gómez Calderón, Adriana Alejandra. “Autodeterminación informativa y derecho probatorio en materia penal”. Tesis para optar por el grado de Magíster, Universidad Nacional Estatal a Distancia, 2013.

<http://repositorio.uned.ac.cr/reuned/bitstream/120809/1232/1/Autodeterminacion%20informativa%20y%20derecho%20probatorio%20en%20materia%20penal.pdf>

Inácio Thomé, Henrique. “Victimización y cultura de la seguridad ciudadana en Europa”. Tesis doctoral en Sociología, Universidad de Barcelona, 2004.

<https://www.tdx.cat/bitstream/handle/10803/2866/TOL356.pdf>

Lozano Jiménez, José Luis. “Arte Panóptico: control y vigilancia en el Arte Contemporáneo”. Tesis doctoral de la Facultad de Bellas Artes, Granada. Universidad de Granada, 2012.

Moya Jiménez, Paulina Alejandra. “El derecho a ser informado como sustento fundamental del control de datos personales”. Tesis para optar el grado de licenciatura en Ciencias jurídicas y sociales, Universidad de Chile, 2010.

Palacios Huerta, Patricio. “Análisis crítico del Régimen Jurídico de Videovigilancia de las Fuerzas de Orden y Seguridad Pública”. Tesis de Maestría en Derecho Público. Universidad de Chile, 2007.

<https://www.tdx.cat/bitstream/handle/10803/2866/TOL356.pdf>

Peña Ortiz, Paola y Achío Gutiérrez, Catalina. “El derecho al olvido”. Tesis para optar por el grado de Licenciatura en Derecho. Universidad de Costa Rica, 2011.

Ramírez Zolezzi, Julio Ernesto y Valenzuela Herrera, Pecky Daniela. “Videovigilancia en el espacio público: el monitoreo de la ciudad como dispositivo del control poblacional”. Tesis para optar por el grado de licenciatura en Ciencias Jurídicas y Sociales. Universidad de Chile, 2017.

<http://repositorio.uchile.cl/bitstream/handle/2250/146569/Videovigilancia-en-el-espacio-p%C3%BAblico-el-monitoreo-de-la-ciudad-como-dispositivo-del-control-poblacional.pdf?sequence=1&isAllowed=y>

- Rodríguez Steller, Sara (2016). *Los derechos de intimidad y protección de datos personales. Estudio comparado en los sistemas jurídicos Mexicano, Español, Costarricense y análisis de las principales debilidades de la Agencia de Protección de Datos Costarricense*. Tesis para optar por el título de Licenciatura en Derecho. Universidad de Costa Rica. San Ramón, Alajuela.
- Soto Urpina, Carles. “Las dos caras de la prevención situacional: el desplazamiento y la difusión de beneficios”. Tesis doctoral de la Universidad Nacional Estatal a Distancia, 2015.
- Soto Vega, Francisco (2011). *Uso consentido de información personal en contratos comerciales de adhesión en Costa Rica*. Tesis de Licenciatura. Universidad de Costa Rica.
- Vargas Acuña, Daniela. (2017). *Vulnerabilidades en la incorporación y admisibilidad de la prueba electrónica en el proceso penal costarricense*. Tesis para optar por el grado de Licenciatura en Derecho, Universidad de Costa Rica.

Investigaciones Científicas:

- Gill, Martin y Spriggs, Angela. (2005). *Assessing the Impact of CCTV*. Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate.
- Hempel, León y Töpfer, Eric. (2004). *CCTV in Europe: final report*. Proyecto Urbaneye. Berlín: Centro de Tecnología y sociedad. Universidad de Berlín. Mencionado por
- Hempel, León y Töpfer, Eric. (2009). *The Surveillance Consensus*. European Journal of Criminology, 6 (2), pp. 157-177.
- Lomell, Heidi Mork. (2004). *Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo*, Norway, *Surveillance and Society*, 2, 2/3, 346-60.
- Norris Clive (2003), “From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control”, en David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Londres: Routledge, pp. 249-281.
- Von Hirsch, A. (2000), “The Ethics of Public Television Surveillance” in von Hirsch, A., Garland, D. and Wakefi eld, A. (eds.) *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing: Oxford)
- Welsh, Brandon C. y Farrington, David P. (2002). *Crime prevention effects of closed circuit television: a systematic review* en: Home Office Research Study Number 252, London:

- Home Office, 2002; & Martin Gill y Angela Spriggs. (2002). *Assessing the Impact of CCTV* en: Home Office Research Study Number 252 , London: Home Office.
- Welsh, Brandon C. y Farrington, David P. (2007). *Improved Street Lighting and Crime Prevention*. The Swedish National Council for Crime Prevention. Edita Västerås.
- Welsh, Brandon C. y Farrington, David P. (2008). *Effects of Closed Circuit Television Surveillance on Crime*, Campbell Collaboration.

Normativa:

- Convenio No 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con con respecto al Tratamiento automatizado de Datos de Carácter Personal.
- Decreto 34 104-G-MSP: Reglamento regulador de la vigilancia de calles, avenidas, carreteras y caminos mediante dispositivos tecnológicos o técnicos.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas cámaras o videocámaras, España.
- Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Ley No. 8968, del 5 de setiembre del 2011, Costa Rica.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, del 5 de Julio del 2010, México.
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, España.
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos, España.
- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), España.
- Manual de legislación europea en materia de la Protección de Datos. Agencia de los Derechos Fundamentales de la Unión Europea, 2014, Consejo de Europa.

Observaciones Generales aprobadas por el Comité de Derechos Humanos, Observación General No. 16, párrafo 8. Disponible en: https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html

Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de Desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, España. Disponible en; http://noticias.juridicas.com/base_datos/Admin/rd596-1999.html#cpau

Reglamento General de Protección de Datos, del Parlamento y del Consejo Europeo del 27 de abril de 2016, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Regulation of Investigatory Powers Act 2000, Reino Unido. Disponible en: https://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

Jurisprudencia nacional:

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 678-91, de las catorce horas y dieciseis minutos del veintisiete de marzo de mil novecientos noventa y uno.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 1026-94, de las diez horas cincuenta y cuatro minutos del dieciocho de febrero de mil novecientos noventa y cuatro.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 5376-94, de las once horas y cincuenta y cuatro minutos del dieciseis de setiembre de mil novecientos noventa y cuatro.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 4819-96, de las diez horas cuarenta y cinco minutos del trece de setiembre de mil novecientos noventa y seis.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 5831-96, de las nueve horas y doce minutos del primero de noviembre de mil novecientos noventa y seis.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 01650, de las dieciséis horas y treinta y ocho minutos del catorce de febrero del dos mil seis.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 03575, a las nueve horas cinco minutos del catorce de marzo de dos mil catorce.

Sala Constitucional de la Corte Suprema de Justicia. San José, resolución número 9412-2015, de las nueve horas y cinco minutos del veintiseis de junio de dos mil quince.

Tribunal de Casación Penal de San José, resolución número 368-F-92 de las ocho horas y cincuenta y cinco minutos del catorce de agosto de mil novecientos noventa y dos.

Jurisprudencia de Tribunales de España y Europa:

Corte Europea de Derechos Humanos, Sentencia Handyside contra Reino Unido, de 7 de septiembre de 1976.

Corte Europea de Derechos Humanos, Sentencia Huvig y Kruslin, de 24 de abril de 1990.

Corte Europea de Derechos Humanos, Sentencia Observer y Guardián contra Reino Unido, de 26 de noviembre de 1991.

Corte Interamericana de Derechos Humanos, Sentencia Velásquez Rodríguez contra Honduras, No. 4/1988, del 29 de Julio de 1988.

Tribunal de Justicia de la Unión Europea, Sentencia Rynes contra Republica Checa, No. C-212/13, de 20 de marzo del 2013.

Tribunal de Justicia de la Unión Europea, Sentencia Tele 2, Sverige AB contra Post-och Telestyrelsen y Secretaría del Departamento de Estado contra Watson, Brice and Lewis, 21 de diciembre de 2016.

Tribunal Europeo de Derechos Humanos, Sentencia Coster contra Reino Unido, de 18 de enero de 2001.

Tribunal Europeo de Derechos Humanos, Sentencia P.G y J.H contra Reino Unido, No. 44 787/19 98, 2001.

Tribunal Europeo de Derechos Humanos, Sentencia Peck contra el Reino Unido, No. 44.647/98, de 28 de enero de 2003.

Tribunal Europeo de Derechos Humanos, Sentencia Hannover contra Alemania, de 26 de junio de 2004.

Tribunal Europeo de Derecho Humanos, Sentencia Weber & Saravia contra Alemania, 29 de junio de 2006.

Tribunal Europeo de Derechos Humanos, Sentencia Köpke contra Alemania, No. 420/07, de 5 de octubre de 2010.

Tribunal Europeo de Derechos Humanos, Sentencia De La Flor Cabrera contra España, No. 10764/09, de 27 de mayo de 2014.

Tribunal Europeo de Derechos Humanos, Sentencia Sommer contra Alemania, del 27 de abril del 2017.

Tribunal Europeo de Derechos Humanos, Sentencia número 1.874/13 y 85.67/13, dictada el 9 de enero del 2018.

Sentencia número 170/1987, FJ. 4 del Tribunal Constitucional, España.

Sentencia número 11/1990, FJ. 5 del Tribunal Constitucional, España.

Sentencia número 55/1990, FJ. 5, del Tribunal Constitucional, España.

Sentencia número 94/1998, FJ. 4 del Tribunal Constitucional, España.

Sentencia número 98/2000 del 10 de abril del Tribunal Constitucional, España.

Sentencia número 292/2000, FJ. 5 del 30 de noviembre del Tribunal Constitucional, España.

Sentencia número 81/2001, de 26 de marzo del Tribunal Constitucional, España.

Sentencia número 14/2003, de 28 de enero del Tribunal Constitucional, España.

Sentencia número 127/2003, de 30 de junio del Tribunal Constitucional, España.

Sentencia número 7549/2010 de la Sala Civil del Tribunal Supremo, España.

Sentencia número 29/2013, FJ. 6 del 11 de febrero del Tribunal Constitucional, España.

Entrevistas:

Entrevista con la Licenciada Mónica Coto, jefa del Departamento de Seguridad Electrónica de la Municipalidad de San José, el 25 de octubre de 2017

Entrevista con la Licenciada Karla Quesada Rodríguez, Coordinadora del Departamento de Registro de Archivos y Bases de Datos de la Agencia de Protección de Datos de los Habitantes (Prodhab), el 13 de octubre de 2017.