UNIVERSIDAD DE VALPARAISO
FACULTAD DE DERECHO
PROGRAMA MAGÍSTER EN DERECHO
ESCUELA DE DERECHO

UNIVERSIDAD DE VALPARAÍSO
FACULTAD DE DERECHO Y CIENCIAS SOCIALES
ESCUELA DE DERECHO

MAGÍSTER EN DERECHO

"VIDEOVIGILANCIA Y SEGURIDAD PÚBLICA, UNA MIRADA CONSTITUCIONAL"

Tesis para optar al grado de Magíster en Derecho

ALEXIS FERNANDO GONZÁLEZ ACUÑA

Rodolfo Herrera Bravo
(Profesor Guía)

OCTUBRE 2021

RESUMEN

El presente proyecto abordará el uso de la videovigilancia como tecnología para la prevención y persecución de los delitos cometidos en el espacio público, y cómo la utilización de sistemas de televigilancia genera un conflicto con el derecho a la privacidad de las personas en el mismo, así como también desde la perspectiva de la protección de los datos personales, considerando que el almacenamiento de las imágenes captadas por los sistemas son tratamientos de datos personales realizados por los organismos públicos, especialmente por las municipalidades. Para ello se revisarán la regulación jurídica existente, la tecnología que se utiliza y la efectividad de la videovigilancia, para finalmente presentar los alcances en materia de protección de datos personales y el derecho a la vida privada, con ocasión del empleo de la videovigilancia en el espacio público, así como la labor que han desempeñado diversas instituciones relacionadas con la protección de datos en el contexto de la incorporación de estas tecnologías al espacio público.

PALABRAS CLAVES:

Privacidad, videovigilancia, espacio público, transparencia, protección de datos.

INDICE

INTRODUCCIÓN. -

Conocido es que en los dominios del sistema jurídico las disputas "reales" son ocasionales más que habituales, los problemas de cierta relevancia son, en rigor, la excepción más que la regla. El sistema está compuesto casi en su mayoría por mandatos simples de comprender y de aplicar, "por lo mismo una gran parte de la actividad litigacional es rutinaria - las premisas son indiscutidas y la declaración lógica es suficiente para solucionar la cuestión-, el problema surge cuando se rompe la rutina, las premisas son difíciles de hallar, las normas son difíciles de comprender o derechamente las reglas y principios se encuentran en colisión" (Morris, 2013: p.140). A medida que las sociedades se van desarrollando, la dinámica de convivencia se vuelve cada vez más compleja, en especial aquella relacionada con el ejercicio diario de los derechos de las personas. Ya se ha visto como el primer desarrollo industrial llevó a la discusión de los derechos de los trabajadores frente a la automatización primaria de fábricas y los procesos de producción en cadena.

En ese sentido, el avance tecnológico siempre se ha considerado una muestra del progreso de una sociedad, especialmente debido al desarrollo científico que implícitamente conlleva cada avance en la utilización de tecnologías. En la actualidad, y pese a la acelerada carrera de desarrollo tecnológico que existe, y que, debido a los procesos de globalización, ha permitido que la tecnología sea cada vez más popular en su uso, la utilización de estas tecnologías lleva implícito la conflictividad con el ejercicio de los derechos, en especial cuando en su contrapartida se trata de potestades ejercidas por el Estado.

Así, desde hace varias décadas se ha venido discutiendo acerca del conflicto que subyace en cuanto a la potestad de vigilancia en los espacios públicos y cómo esto representa un conflicto con el derecho constitucionalmente garantizado a la privacidad, especialmente cuando se trata del manejo de datos e información que genera la televigilancia (Figueroa, 2014: p.18)*;* conflicto que ha tratado de superarse en beneficio del resguardo de la seguridad pública y en el cual, no necesariamente, se ha sopesado en forma correcta las implicancias de tal desequilibrio hacía la justificación de beneficio razonado en política criminal sin el resguardo debido a la protección del legítimo ejercicio de un derecho, que puede ser afectado

en forma transversal e indiscriminada a cada miembro de la sociedad, y de cuya afectación, además, no parece dársele tanta importancia por el colectivo (Squella, 2019: p11)[1].

Así, en el presente trabajo pretendemos abordar el conflicto desde la mirada del ejercicio de la televigilancia en espacios públicos como parte de una política del Estado en relación con la seguridad pública y cómo esta televigilancia produce un conflicto con el derecho a la privacidad, principalmente desde que el uso de tecnologías de televigilancia ya no solo se circunscribe al momento, sino que propicia una recopilación, sistematización y almacenamiento de información proveniente de un conjunto de imágenes, cuya naturaleza consiste en ser datos personales.

De acuerdo a los significados otorgados por el Diccionario de la Lengua Española, la palabra "vigilar", se entiende como "*observar algo o a alguien atenta y cuidadosamente*" y "vigilancia" como "*cuidado y atención exacta en las cosas que están a cargo de cada uno*" y también como "*servicio ordenado y dispuesto para vigilar*" (Real Academia de la Lengua, 2016c: p. 2243). En cuanto a "Video" (que proviene el latín *video* que significa "yo veo") se define en su acepción n°1 como "*Sistema de grabación y reproducción de imágenes, acompañadas o no de sonidos, mediante cinta magnética u otros medios electrónicos*", así como también, "*grabación hecha en video*" en su acepción N°2 (Real Academia de la Lengua, 2016c: p. 2240). Por su parte, el mismo diccionario define la palabra "videovigilancia" como "*vigilancia por medio de un sistema de cámaras, fijas o móviles*" (Real Academia de la Lengua, 2016c: p.2241). Se puede entender que corresponde entonces a un sistema de grabación y reproducción de imágenes, acompañadas o no de sonidos, mediante cinta magnética u otros medios electrónicos cuyo objetivo se encuentra en el cuidado y atención exacta en las cosas que están a cargo .

[1] Un problema que ya ha sido avizorado por Agustin Squella, quien hace un paralelo entre el conocimiento e ignorancia de los derechos: "*los derechos humanos se invocan tanto como se ignoran, y se ignoran en un doble sentido: porque se los atropella y porque se sabe poco de ellos. Los derechos humanos se desconocen cuando no se los declara, respeta o protege, pero también cuando se ignora qué son, que historia tienen, como se garantizan (ídem)*".

Ahora bien, la videovigilancia del espacio público es una práctica fortalecida en las grandes urbes del planeta, y cuyos fines se originan no en un reciente desarrollo tecnológico, sino en la necesidad de ejercicio de control por parte del Estado y que pareciera ser común a todos los modelos de Estado (Rivero Ortega, 2002: p. 25).

En ese sentido, el argumento para la implementación de estos sistemas de televigilancia parece estar directamente relacionado con la posibilidad de ejercer una prevención eficaz respecto de la comisión de delitos, o por lo menos, una actitud reactiva inmediata que permita aminorar los efectos de la comisión de hechos ilícitos, especialmente aquellos cometidos en flagrancia, así como también servir de medio de prueba en los procesos judiciales en los que se persigue a estos delitos, cometidos y captados por estos sistemas de televigilancia. Sin embargo, la eficacia y efectividad no siempre resulta ser tal como lo plantea la autoridad política, y sus efectos nocivos para el conflicto con el legítimo ejercicio de ciertos derechos, en especial el derecho a la protección de la privacidad de las personas en los espacios públicos, de cuyo caso existe un legitima expectativa, no suele ser sopesado como debiera[2]. Es posible, además, identificar una afectación en el señalado derecho no solo en lo que se refiere a su ejercicio en espacios públicos, sino también, como un efecto colateral de la implementación de dichos sistemas con capacidad de captación hacia espacios privados.

A todas luces, el argumento de la seguridad pública parece ser meritorio y muchos ciudadanos parecen estar dispuestos a tal sacrificio. Pero ¿qué ocurre cuando el sistema implementado se traduce en una afectación no solo al momento inmediato vigilado, sino que se transforma en la posibilidad de almacenamiento continuo de imágenes que representan datos personales generando bases de datos complejas? ¿Cómo se cautela el cumplimiento de los parámetros admitidos para el ejercicio de esta modalidad de vigilancia? ¿Cómo se puede lograr reducir el impacto en la implementación de sistemas de tal forma que se reduzca su utilización solo a espacios públicos y no se produzca una afectación a los espacios privados?

[2] Para Gemma Galdon-Clavel lo que constatan estas evaluaciones internacionales es que los sistemas de videovigilancia en el espacio público pueden contribuir a la reducción de la delincuencia en dicho ámbito, pero de manera desigual: más en lugares de poca actividad social y poco control informal, como los aparcamientos aislados, por ejemplo, que en centros urbanos y zonas residenciales (Galdon-Clavel, 2015: p. 86).

¿Existe un organismo que pueda realizar un ejercicio potestativo de vigilancia y protección de los ciudadanos?

La idea de este trabajo es contextualizar lo más posible dicho problema para arrojar luces sobre cómo se requiere proceder, especialmente considerando las implicancias constitucionales desde la protección de uno de los derechos que entran en conflicto con la implementación de los sistemas de televigilancia, conflicto que no solo se circunscribe al ejercicio del derecho en espacios públicos, y que puede tener una repercusión en espacios considerados como privados (especialmente los residenciales adyacentes) donde también es posible identificar una afectación que debe ser analizada.

1. LA REGULACIÓN JURÍDICA DE LA VIDEOVIGILANCIA EN CHILE.

Para adentrarnos en el tema de discusión procederemos a establecer cuál es la base del uso de tecnologías para la implementación de los sistemas de televigilancia, considerando los requerimientos y orientaciones técnicas emanadas desde el Gobierno central hacia los distintos organismos del Estado, teniendo presente, además, la materialización de esta política pública en los espacios públicos y cómo se producen interacciones y conflictos entre las medidas de televigilancia, considerando el enfoque de prevención situacional, con el ejercicio del derecho a la privacidad en el espacio público.

1.1. Sobre la Tecnología Utilizada

Lo primero que debemos puntualizar es que la aplicación de la televigilancia, además de ser la medida de solución aplicada por los organismos del Estado a la problemática de la seguridad, se presenta como una de las 5 tipologías de Intervención Socioespacial que ha considerado la Subsecretaría para la Prevención del Delito de nuestro país, las cuales corresponden a: 1) la Recuperación de Espacios Públicos (como senderos peatonales seguros, plazas, equipamiento deportivo/recreativo, entre otros); 2) la Iluminación Peatonal; 3) El Equipamiento Público y Comunitario; 4) los Sistema de Alarmas Comunitarias; y 5) Sistemas

de Teleprotección, que implican la utilización de cámaras de televigilancia, aeronaves no tripuladas de televigilancia (comúnmente conocidos como "drones") y pórticos de televigilancia (Subsecretaria de Prevención del Delito, 2019: p. 32).

En ese sentido, según se ha entendido, la intervención socioespacial forma parte de la política de Prevención Situacional, entendiendo que "*la modificación de las circunstancias espaciales junto al componente comunitario, contribuyen a disminuir las oportunidades para la comisión de delitos y la violencia, y reducir la percepción de inseguridad de la población, convirtiéndose en un soporte para la recuperación y consolidación de las relaciones sociales existentes en él, las que son vitales para la sustentabilidad de la inversión en el tiempo*" (Subsecretaria de Prevención del Delito, 2019: p. 32).

Ahora bien, en lo que se refiere a estas formas de actuación, es posible distinguir dos enfoques: la Prevención Situacional y la Prevención de la Delincuencia Mediante el Diseño Ambiental[3]En ese sentido, la Prevención Situacional tiene una influencia inglesa, y surge en el ámbito de las ciencias sociales y está asociada a un alto uso de recursos tecnológicos (como cámaras de vigilancia) los cuales se enfocan en la protección de blancos vulnerables. Así, la Prevención Situacional tiene como característica centrarse en tipos de conductas específicas indeseables, ya sean incivilidades y/o delitos. Por otra parte, la Prevención de la Delincuencia Mediante el Diseño Ambiental es una disciplina que surge principalmente bajo la influencia de la arquitectura y el desarrollo urbano, examinándose la forma en cómo estas variables facilitan o dificultan el ejercicio del control social informal sobre un espacio determinado (Rau, 2016: p. 89-90).

Desde el aspecto criminológico, la Prevención Situacional busca, entre otras cosas, la priorización de la prevención del delito ante el control mediante políticas orientadas de una manera práctica y menos académica, un énfasis en las alteraciones del medio ambiente físico, la relevancia del proceso de control social informal y la agresión más que el agresor como el primer foco de atención, situada en un contexto espacial (Rau, 2016:p. 100).

[3] CPTED por sus siglas en inglés: Crime Prevention Through Environmental Design.

En el marco de las Orientaciones Técnicas en materia de Prevención Situacional entregadas por la Subsecretaria de Prevención del Delito, se cataloga a los sistemas de teleprotección como "*soporte y medio de prueba visual en eventuales procesos judiciales*" en los delitos de hurto, robo con intimidación, robo con violencia, delito de robo por sorpresa y lesiones, además de considerarlos como una estrategia de manejo de condiciones físicas y ambientales que facilitan la ocurrencia de delitos y percepción de temor en el delito de robo con fuerza, todo de acuerdo a un cuadro comparativo de las tipologías de Prevención Situacional (Subsecretaria de Prevención del Delito, 2019. p. 33).

Más allá de lo ya puntualizado, en cuanto a la breve referencia de la Prevención Situacional, pretendemos tomar como punto de partida estas Orientaciones Técnicas que han sido entregadas por el Estado para los efectos de aplicar tecnologías de televigilancia, y que están dirigidas a servir de base a la implementación y puesta en marcha de los señalados sistemas. Resultan, entonces, un marco ineludible (Subsecretaria de Prevención del Delito, 2019: p. 36).

En ese sentido, y de acuerdo a la conceptualización técnica, el sistema de televigilancia consiste en una serie de componentes que funcionan de forma integrada, lo que considera hardware, software y personal de monitoreo, debiendo todos ellos estar en completa operación para lograr un funcionamiento efectivo del sistema. Se entiende entonces que, ante la falla de cualquiera de ellos en su funcionamiento, se afectará la operación eficaz del sistema.

Así, de acuerdo a las Orientaciones Técnicas entregadas por la Subsecretaria de Prevención del Delito (Subsecretaria de Prevención del Delito, 2019: p. 36), el sistema de televigilancia deberá contar con al menos 3 subsistemas:

1. Sistema de cámaras de circuito cerrado de televisión (CCTV): El sistema consiste en una serie de cámaras que envían información gráfica hasta una sala de control y monitoreo mediante un sistema de transmisión que puede ser alámbrico, inalámbrico o ambos. La sala de control y monitoreo debe contar con equipamiento y dispositivos

necesarios para la gestión y almacenamiento de las imágenes que envían las cámaras en tiempo real, de esta forma se realiza un monitoreo del espacio público.

2. Sistema de transmisión de datos: corresponde a la plataforma encargada de transmitir información de un lugar a otro. Los medios de transmisión más ocupados son los inalámbricos, fibra óptica e híbrido (unión entre 2 o más sistemas distintos), presentando grandes diferencias de equipamiento y costos entre sí.
3. Sala de control y monitoreo: Lugar donde se administrará y visualizará las imágenes enviadas por las diferentes cámaras de televigilancia instaladas. Este sistema debe contar con equipos de concentración de datos, monitores para visualización y consolas de control con su respectivo personal de operación.

El ecosistema que forman estos tres componentes forma el sistema de televigilancia, pudiendo prever que son dos los subsistemas que se encuentran más propensos a generar un conflicto con el ejercicio del derecho a la intimidad: el subsistema de cámaras, que es la primera barrera en la captación de las imágenes, y el subsistema denominado sala de control, que es donde finalmente se produce el almacenamiento de los datos que forman las imágenes, y donde las mismas se convierten en datos personales.

1.2. Videovigilancia y Espacio Público.

La discusión que se nos avecina no consiste entonces en debatir acerca de sí resulta oportuno o no la utilización de sistemas de televigilancia, ya que esta discusión parece superada (sin siquiera darse en el ámbito público)[4], sino más bien parece orientarse en este punto a debatir el marco en el cual estos sistemas de televigilancia deberán implementarse

[4] Así incluso se ha informado como política pública por parte del Ministerio del interior: "*El proyecto Televigilancia Móvil, es una iniciativa enmarcada en el programa innovación tecnológica de la Subsecretaría de Prevención del Delito que, a través del uso de sistemas de aeronaves remotamente pilotadas, (RPAS) con cámaras de alta definición, permiten obtener información visual y transmitirla a centrales de monitoreo ubicadas en las Intendencias Regionales. Así, es posible detectar incivilidades, realizar patrullajes preventivos en el territorio y obtener medios probatorios ante delitos flagrantes*"; agregando que "*La iniciativa se enmarca en el Plan "Calle Segura" y contempla una inversión de 797 millones de pesos para implementar drones equipados con cámaras infrarrojas y centros de monitoreo*". En nota de prensa titulada "Sistema de Televigilancia Móvil se implementa en la Región Metropolitana" publicada el día 18 de marzo de 2019 en la página institucional del Ministerio del Interior y Seguridad Publica. Disponible en https://www.interior.gob.cl/noticias/2019/03/18/sistema-de-televigilancia-movil-se-implementa-en-la-region-metropolitana/. Fecha de última consulta: 30 de enero de 2021.

para la supervigilancia del espacio público y cómo esta implementación va generando una limitante al ejercicio del derecho a la privacidad en el espacio público.

Según señalan las Orientaciones Técnicas emanadas de la Subsecretaria de Prevención del Delito:

> "*Las intervenciones de sistemas de televigilancia responden a una estrategia que aborda el tema de la prevención de una manera más integral, como instrumento de apoyo a la gestión de seguridad y control en los territorios, dirigidos principalmente a aumentar la cobertura y ayuda en la vigilancia formal en zonas con condiciones de riesgo, además de ser utilizado como soporte y medio de prueba visual en eventuales procesos judiciales. El sistema debe captar, almacenar y proveer imágenes de alta definición y resolución necesaria para ser utilizada como medio preventivo, de prueba, soporte y ayuda en la vigilancia de los sectores donde se ubicarán las cámaras*" (Subsecretaria de Prevención del Delito, 2019: p. 35).

Al respecto se puede señalar que desde la perspectiva técnica del Estado, se busca un sistema que permita apoyar la gestión de seguridad en los espacios públicos tratando de actuar como un disuasivo, o permitiendo una reacción pronta ante hechos constitutivos de ilícitos que puedan observarse por los operadores del sistema, y que además, propicia ser un medio de prueba en los procesos judiciales, esencialmente en materias penales, derivados de los hechos ilícitos cometidos en espacios públicos y registrados por el sistema.

Así, el argumento de la seguridad publica viene a propiciar un escenario donde las medidas de televigilancia implementadas especialmente por los municipios parecen justificadas, tanto por lo beneficioso del uso de tecnologías como también por la responsabilidad que tienen estas corporaciones al ser el organismo público que entra en contacto directo con la ciudadanía en problemas que podrían denominarse como cotidianos. En palabras de Chacón

> "*Esta acción municipal para la seguridad pública es discutida por abundante bibliografía que indica que las municipalidades están en medio de la*

construcción de un relato nuevo de la prevención del delito y conforman un escenario que recibe dos tipos de presiones: desde arriba y desde abajo. Desde arriba, porque el Estado central se ha visto sobrepasado por el tema, no ha dado abasto y ha solicitado apoyos a entidades descentralizadas para abordar este fenómeno; y desde abajo, porque muchos municipios han reivindicado su capacidad para hacerse cargo del problema" (Chacón Romero, 2016: p.128),.

1.3. La Política Pública y la Videovigilancia.

La primera aproximación que realizamos es que, de acuerdo a lo dispuesto en los incisos 4° y 5° del artículo 1° de la Constitución Política:

"*El Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respeto a los derechos y garantías que esta Constitución establece*" considerando que "*Es deber del Estado resguardar la seguridad nacional, dar protección a la población y a la familia, propender al fortalecimiento de ésta, promover la integración armónica de todos los sectores de la Nación y asegurar el derecho de las personas a participar con igualdad de oportunidades en la vida nacional*".

Es aquí donde, por mandato constitucional, encontramos la funcionalidad y deber de actuación del Estado y de sus organismos integrantes, respecto del ejercicio de políticas públicas que, en el caso particular, se refieren a la seguridad y protección de la población.

Ahora bien, en la práctica, quienes han materializado la implementación de sistemas de televigilancia en mayor medida son las municipalidades[5], quienes han encontrado su

[5] Tal es así, que cuando el Consejo para la Transparencia, en uso de sus facultades legales, considera oportuno emitir Oficio N° 2309, de fecha 06 de marzo de 2017, que Formula recomendaciones respecto a la instalación

justificación en el mandato legal contenido en su Ley Orgánica Constitucional, añadiendo como argumento para su utilización la pretendida eficacia y la utilidad de los programas de videovigilancia en la prevención de delitos.

Interesante resulta lo señalado por Víctor Manuel Sánchez Valdés (Sánchez Valdés, 2016: p.164), para quien la efectividad pretendida en la prevención de los delitos no resulta de tanta significancia. Así, señala que

> "(…)*desde finales de la década de los años 90 se han llevado a cabo muchas investigaciones en varias ciudades del mundo, cuyo objetivo ha sido medir la capacidad de las cámaras urbanas de video vigilancia para disuadir a los posibles infractores de la comisión de delitos. Sin embargo, los diferentes estudios obtuvieron evidencia contradictoria, por un lado hay una serie de trabajos en donde se observa que la instalación de cámara ayudó a reducir la cantidad de delitos como es el caso de Griffiths (2003), que estudió el efecto de la vigilancia remota en Gillingham, Inglaterra, en donde la incidencia criminal disminuyó en un 35% en la zona de tratamiento, mientras que en la zona de control apenas hubo una reducción del 0.05%"*(Sánchez, 2016: p.164).

En el marco de la implementación de sistemas de televigilancia por parte de los municipios, de acuerdo a lo dispuesto en el artículo 1° de la Ley N°18.695, Orgánica Constitucional de Municipalidades, la Municipalidad es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, cuya finalidad es satisfacer las necesidades de la comunidad local y asegurar su participación en el progreso económico, social y cultural de las respectivas comunas, para lo cual, de acuerdo al artículo 5° de la misma ley, cuentan con una serie de atribuciones, entre las cuales se encuentra el administrar los bienes municipales y nacionales de uso público y elaborar, aprobar, ejecutar y evaluar el plan comunal de seguridad pública.

---

de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N° 19.628, lo hace teniendo como destinario a los 345 municipios existentes en nuestro país. Ver supra 2.4.

Adicionalmente, y en relación a lo que dispone el artículo 4º de la Ley N°18.695, las municipalidades, en el ámbito de su territorio, pueden desarrollar, directamente o con otros órganos de la Administración del Estado, funciones relacionadas con diversas materias, destacándose lo dispuesto en su Literal J) referente a

> "*El desarrollo, implementación, evaluación, promoción, capacitación y apoyo de acciones de prevención social y situacional, la celebración de convenios con otras entidades públicas para la aplicación de planes de reinserción social y de asistencia a víctimas, así como también la adopción de medidas en el ámbito de la seguridad pública a nivel comunal, sin perjuicio de las funciones del Ministerio del Interior y Seguridad Pública y de las Fuerzas de Orden y Seguridad*" (Ley Orgánica Constitucional de municipalidades, …" .

Es en ese contexto normativo que se ha llevado a cabo por parte de las municipalidades las políticas de seguridad ciudadana, que han incluido la implementación de sistemas de Televigilancia en el marco de las direcciones, departamentos o unidades a cargo de la Seguridad Publica.

Resulta interesante la posibilidad de enfocar el análisis en cómo dichas potestades normativas entregadas por la Ley Orgánica Constitucional a los municipios se logran armonizar con lo dispuesto en el artículo 19 n° 26 de la Constitución Política de la Republica, en cuanto ésta establece "*La seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio*"; especialmente cuando la materialización de dichas potestades públicas se traduce en posibles restricciones al ejercicio de derechos fundamentales. Vale decir, es posible conjugar armónicamente el sustento normativo que ha sido utilizado por los municipios con la realidad práctica que concibe una limitación al ejercicio de un derecho, debidamente amparado y protegido, o es suficiente permitir, sin considerar la interpretación restrictiva que deberían tener estas normas, la implementación de sistemas de televigilancia.

Como señaláramos anteriormente (supra 1.2.). La discusión se ha saltado un paso importante (resulta oportuno o no la utilización de sistemas de televigilancia), y hoy nos enfrentamos a debatir el marco en el cual estos sistemas de televigilancia deberán implementarse para la supervigilancia del espacio público, representándose recién en este punto las consecuencias de dichos sistemas, especialmente la limitante al ejercicio del derecho a la privacidad en el espacio público, la cual en apariencia pareciera estar sujeta a una aprobación ciudadana bajo el argumento de la seguridad.

Así, para Arturo Herrera Verdugo (2016), la función de seguridad ciudadana implementada por parte de las municipalidades responde a una exigencia práctica. Así, señala el autor que "*No hay que olvidar que en el caso chileno los municipios han creado departamentos o direcciones de seguridad ciudadana, que en la práctica ejercen funciones de seguridad preventiva en apoyo a la labor policial, motivo por el cual sus operadores deben tener plena conciencia no solo de sus limitaciones legales, sino que también, y sobre todo, de sus deberes morales*" (Herrera, 2016: p. 75).

1.4. Insuficiencia en la Habilitación Legal de los Municipios para la Implementación de Sistemas de Televigilancia.

Como extensión natural de la política de seguridad pública, no resulta extraño que cada municipalidad, especialmente aquellas de mayor relevancia, cuente con un sistema de televigilancia en diversos puntos estratégicos, para cumplir con sus fines establecidos en la ley (fines establecidos en una conceptualización bastante amplia), pero que no se condicen necesariamente con la función de prevención del delito (que podríamos señalar que es privativa de las Fuerzas de Orden y Seguridad como Carabineros o Policía de Investigaciones), pero si dentro de la función de "seguridad pública", concepto este último bastante abstracto, que debe ser llenado de contenido, y ese contenido vendrá determinado por el reflejo ciudadano de turno, por la mayor o menor preocupación de la comunidad y la forma en que ésta, manifestada como interés políticamente amparable, pueda ser abarcada por la autoridad de turno.

Samuel Malamud Herrera (2018), por ejemplo, ha planteado la insuficiencia y vaguedad de considerar como suficientemente habilitante en el marco del principio de legalidad a las disposiciones contenidas en la Ley Orgánica Constitucional de Municipalidades, especialmente considerando los conflictos constitucionales que suscita la implementación de dichas medidas. Así, para el autor:

> "*Contrario a lo que han exigido los reseñados fallos del Tribunal Constitucional, el cumplimiento del estándar habría implicado indicar qué derechos constitucionales se pueden perturbar por medio del ejercicio de estas potestades, junto con la indicación también de la clase de actividades que se asumen como tolerables para resguardar la seguridad, por medio, a lo menos, de una enumeración ejemplar, para permitir una interpretación de tipo analógica. De otro modo, se entiende que cualquier derecho puede ser afectado y que cualquier sacrificio es válido para resguardar la seguridad; asunción que, como se puede comprender, encierra un intolerable ámbito de amplitud, incerteza y discrecionalidad*" (Malamud, 2018: p. 153).

Es entonces que ante esta situación concurre la necesidad de creación de protocolos de seguridad en cuanto al acceso a la información que las imágenes proveen, para no desnaturalizar su función. Y es aquí donde se empiezan a vislumbrar los primeros problemas en torno a la videovigilancia y el derecho a la privacidad, sobre todo cuando se transforma en el fin, pese a que es un medio en el marco de las políticas de seguridad ciudadana que se han expandido a todos los organismos del Estado que pueden permitírselo. Ya George Orwell, en su clásica novela de ciencia ficción titulada *1984*, hablaba sobre un futuro distópico, en el cual se encuentra la omnipresencia vigilancia del Gran Hermano (coincidente con el Estado vigilante).

No resulta extraño entonces que existan autores que sostengan que en dicha actividad hay (y debe existir) un componente ético. Así lo plantea Arturo Herrera Verdugo (2016), para quien la ética no es contraria ni mucho menos un obstáculo para las acciones de seguridad pública y ciudadanas, considerando que "*es el fundamento esencial que permite que dichas acciones se realicen bajo estrictos criterios de prudencia, dotando así de legitimidad a cada*

una de las iniciativas planteadas y efectivamente implementadas" (Herrera, 2016: p. 54). Ahora bien, en el marco de la insuficiencia regulatoria en el ámbito legal respecto de la implementación de sistemas de televigilancia, especialmente sobre el conflicto con el ejercicio del derecho a la privacidad en espacios públicos, dichos vacíos han tenido que ser suplidos vía jurisprudencia de los tribunales superiores, los cuales en el conocimiento de acciones de protección derivadas de la utilización de estos sistemas han determinado parámetros para su implementación (y a los cuales nos referiremos más adelante).

Así, los tribunales superiores han ido marcando una clara tendencia en el análisis del conflicto que se ha generado con la implementación de los sistemas de televigilancia. Así, en Sentencia de fecha 1° de junio de 2016, de la E. Corte Suprema, en autos Rol N°18.481-2016 (que revoca la sentencia apelada de 4 de marzo de 2016 de la Corte de Apelaciones de Santiago, dictada en los autos Rol N°82.289-2015), en su considerando décimo tercero, ha establecido los parámetros a considerar en la filmación de espacios públicos especialmente respetando derechos como la intimidad personal, la inviolabilidad del hogar y el secreto de las comunicaciones, reconociendo el argumento de la seguridad pública y la videovigilancia como medida de prevención y persecución de hechos delictivos[6]:

> "***Décimo tercero:*** *Que, tratándose de la utilización de videocámaras para captar imágenes de lugares públicos, abiertos o cerrados, debe entenderse como un fenómeno en expansión que forma parte de las nuevas tendencias relativas a la seguridad ciudadana con el objeto de mejorar los dispositivos de control en los lugares públicos donde pueden tener lugar conductas delictivas. Efectivamente, el incremento de la video-vigilancia en tales lugares debe admitirse como una forma de mejorar la prevención y persecución de hechos delictivos, reduciendo las ocasiones en las se comete un delito sin ser descubierto y consiguiendo rapidez de actuación por parte de la policía y como*

[6] Argumento también reconocido y valorado en el análisis por la E. Corte Suprema en su Considerando Octavo: "*En este orden de ideas, la video vigilancia en el espacio público, donde no puede pretenderse una mayor expectativa de privacidad –exceptuándose actos de intrusión que pueden constituir ilícitos penales-, encuentra su legitimidad en pos de la protección de personas y bienes, como en la disuasión de posibles actividades delictivas, las que en caso de suceder, la grabación de imágenes posibilitará eventualmente la identificación de los autores, adquiriendo una aptitud probatoria*".

eventual prueba en un proceso penal. Se trata de una reacción lógica de la sociedad ante determinados fenómenos delictivos.

En cambio, el uso de videocámaras para captar imágenes de espacios privados podrá constituir una intromisión ilegítima en el derecho a la intimidad o a la propia imagen, desde que se trata de aquellos espacios donde se desarrolla la vida privada de una persona y respecto de los cuales la propia jurisprudencia de nuestros tribunales ha sido cuidadosa al momento de establecer los límites relativos al ejercicio de las actividades de los órganos investigadores.

Por consiguiente, la filmación sólo cabe hacerla en los espacios, lugares o locales públicos, pero no en domicilios o en lugares privados, pues de lo contrario dicha intromisión afectará bienes constitucionalmente protegidos, tornándose por tanto en ilegítima, salvo que exista autorización judicial para estos casos.

En consecuencia, la video-vigilancia debe ser utilizada por la autoridad encargada de manera tal que se respeten derechos como la intimidad personal, la inviolabilidad del hogar y el secreto de las comunicaciones".

En ese marco de discusión, se ha realizado un interesante análisis por parte de Samuel Malamud(2018) en relación a los conflictos jurídicos que generaron la implementación por parte de municipalidades de Santiago de dos medidas de televigilancia que llevaron a diversos vecinos de las comunas y organizaciones no gubernamentales a presentar recursos de protección (por una parte, una iniciativa conjunta de las municipalidades de Las Condes y Lo Barnechea, por medio de la cual se adquirieron tres globos aerostáticos de tres metros de diámetro cada uno, capaces de ascender hasta 150 metros y de mantenerse en el aire hasta por 72 horas; y por otra, la adquisición por parte de la Municipalidad de Las Condes de tres dispositivos aéreos no tripulados equipados con cámaras de alta resolución y con mayor capacidad de movilidad que los globos aerostáticos, pensados para la vigilancia de lugares públicos como plazas). En el artículo el autor analiza la argumentación de la I. Corte de Apelaciones de Santiago y la E. Corte Suprema al conocer de los Recursos de Protección que motivaron las acciones descritas, todo en el marco del conflicto seguridad frente a privacidad.

Se comparte la observación realizada por el autor en cuanto la (vaga) habilitación legal emanada del artículo 4° letra J) de la Ley N°18.695, en relación a la Seguridad Pública (Malamud, 2018: p. 153)[7].

La discusión se extiende además hasta qué punto la habilitación legal señalada permite la implementación de distintos tipos de programas de seguridad, que pueden ser vulneratorios de derechos, o incluso exceder competencias otorgadas a otros organismos, pudiendo afectar con ello el principio de legalidad. Así, indica el autor anteriormente referido, en sus palabras :

> "*la existencia de la norma no debe entenderse como una autorización para que las municipalidades implementen cualquier tipo de programa en materia de seguridad pública, puesto que la autorización, a su respecto, es subsidiaria, pues opera solo a falta o en desmedro de los órganos públicos que por mandato de la Constitución tienen asignadas prioritariamente estas funciones, a saber, el Ministerio Público (artículo 83 de la Constitución Política), las Policías y el Ministerio del Interior (artículo 101 de la Constitución Política)*" (Malamud, 2018: p. 154) que.

1.5. Establecimiento de Parámetros para Regular el Conflicto por vía Jurisprudencial: La labor de la Corte Suprema y del Consejo para la Transparencia.

Ahora bien, en cuanto a la referida Sentencia de fecha 1° de junio de 2016, de la E. Corte Suprema, en autos Rol N°18.481-2016, al revocar la sentencia apelada de 4 de marzo de 2016 de la Corte de Apelaciones de Santiago, dictada en los autos Rol N°82.289-2015, estableció además, en su considerando décimo quinto, un "***Régimen de Autorización***" para

[7] Señala el autor que "*Contrario a lo que han exigido los reseñados fallos del Tribunal Constitucional, el cumplimiento del estándar habría implicado indicar qué derechos constitucionales se pueden perturbar por medio del ejercicio de estas potestades, junto con la indicación también de la clase de actividades que se asumen como tolerables para resguardar la seguridad, por medio, a lo menos, de una enumeración ejemplar, para permitir una interpretación de tipo analógica. De otro modo, se entiende que cualquier derecho puede ser afectado y que cualquier sacrificio es válido para resguardar la seguridad; asunción que, como se puede comprender, encierra un intolerable ámbito de amplitud, incerteza y discrecionalidad*."

el empleo de medios de televigilancia, llenando así un vacío legal (por vía jurisprudencial), que resulta ser el parámetro base para la utilización de la televigilancia. Este *Régimen de Autorización* está integrado por cuatro requisitos:

1° **Delimitación del espacio a grabar**: "*El ámbito físico a grabar se delimita a los lugares públicos, y de los espacios privados abiertos cuando se trate del seguimiento de un hecho que pueda constituir la comisión de un ilícito*";
2° **Certificación de un delegado municipal**: "*Un inspector o delegado municipal deberá certificar, al menos una vez al mes, que no se hayan captado imágenes desde espacios de naturaleza privada como el interior de viviendas, de establecimientos comerciales o de servicios, jardines, patios o balcones*";
3° **Destrucción de grabaciones en el tiempo establecido**: "*La destrucción de las grabaciones se hará efectiva por parte del responsable de su custodia después de 30 días, salvo si la grabación ha captado un ilícito penal u otra falta, caso en el cual las municipalidades recurridas adoptarán las medidas para su pronta entrega a los órganos competentes*";
4° **Derecho de Acceso Ciudadano**: "*Todo ciudadano tendrá derecho de acceso a las grabaciones, para lo cual deberá dirigir una solicitud al funcionario municipal que designe la autoridad edilicia, debiendo indicar el día en que presumiblemente fue grabado, debiendo las municipalidades recurridas establecer un procedimiento que permita el efectivo ejercicio de esta atribución*".

Respecto de los parámetros que deben cumplir, manteniendo su análisis desde el derecho internacional, Domingo Lovera Parmo (2017) señala que estas intromisiones requieren de habilitación legal (considerando lo dispuesto en la Observación General N°16, adoptada en relación al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos). En segundo lugar, debe demostrarse que son "*estrictamente necesarias*" para poder satisfacer el fin legítimo que se busca, es decir, cómo es qué esas medidas en particular se encuentran conectadas racionalmente con el fin que persiguen. En tercer lugar, "*se deben especificar con detalle las circunstancias precisas en que podrán autorizarse*" injerencias en la vida privada de las personas, interpretándose en sentido restrictivo. Y cuarto, deben contemplar siempre

el derecho a la autodeterminación informativa, a saber, la posibilidad 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 (Lovera, 2017: p. 394-396).

De hecho, desde la perspectiva de la normativa internacional sobre la materia, en especial sobre el conflicto vigilancia versus derecho a la privacidad, se constata una problemática no menor cuando se reconducen dichos parámetros hacia las formas que se están utilizando en nuestro país (especialmente por los municipios, y también por gobiernos regionales, que en materia de seguridad han reforzado el enfoque de unidades de control de tránsito a través de sistemas de cámaras en puntos estratégicos). El autor plantea que las actuaciones de las personas en el espacio público se realizan bajo la una expectativa razonable de privacidad, por lo que cuando se implementan estas políticas públicas de televigilancia, las mismas deben estar sujetas a cumplir con los requisitos establecidos por la legislación, pues dichos sistemas representan intromisión en la esfera de privacidad de la persona (Lovera, 2017: p. 387). Entiende el autor que las personas son titulares del derecho a la privacidad también en el espacio público o espacios de libre acceso, considerando que "*hasta cierto punto, la vida en el espacio público asegura (o aseguraba) un cierto grado de privacidad. No es que las personas no se vean unas a otras, pero sí que se proteja una relativa conciencia de que allí, afuera, en medio de la masa, es (o era) posible obtener ciertas cuotas de anonimato*" (Lovera, 2017: p. 403).

En igual sentido se manifiesta Ana Gude Fernández (Gude, 2014: p.75), para quien "*El derecho a la intimidad no tiene que desaparecer en cuanto salimos de nuestros domicilios*" ya que, si bien "*Nadie discute que sea posible la existencia de un mismo nivel de privacidad en la calle que en la habitación de una casa, sin embargo, parece lógico que también podamos disfrutar de ella cuando realizamos nuestras actividades en la vía pública*". Agrega que "*Por sus propias características, la videovigilancia de estos espacios atenta contra este derecho de la personalidad, porque somos observados de forma constante cada vez que paseamos por la calle o accedemos a uno de esos locales vigilados.*" (Gude, 2014: p.75),.

Dicho ejercicio del derecho a la privacidad en espacios públicos ha sido reconocido como una expectativa legitima en la resolución de conflictos relacionados con la implementación de sistemas de televigilancia. Así, en Sentencia de fecha 21 de agosto de 2017 de la Corte de Apelaciones de Santiago, en Autos Rol N°34.360-2017, señala en su considerando vigésimo séptimo en cuanto a la expectativa de privacidad en espacio público y como ella se relaciona con la posibilidad del ejercicio de televigilancia en espacio público lo siguiente:

> "*Que en el caso que nos interesa, la vigilancia a través de los drones se desarrolla en determinados espacios públicos —y no privados— de la comuna de Las Condes, y dentro de esa perspectiva cabe analizar la expectativa de privacidad que el ciudadano tiene en dichos espacios. En efecto,* ***razonable es que al acceder a un lugar público cada persona aspire, entre otros aspectos, a que sus conversaciones no sean de acceso público, como también que en su desplazamiento no sea objeto de registro personal, o de seguimientos, es decir, pueda deambular libremente manteniendo su anonimato frente a quienes lo rodean, a menos que incurra en conductas ilegales o se vea involucrado en situaciones de emergencia, pues en tales casos, normal es que tales expectativas de privacidad se desvanezcan***. (Negrita del tesista)
>
> *Dentro de ese escenario, la implementación de una televigilancia no resulta atentatoria a la vida privada de los actores si ellos llegan a circular por los espacios públicos donde sobrevuelan drones, en atención a la forma como ha sido implementada la medida por el municipio, pues ha existido una regulación de la actividad que permite conocer en forma previa los lugares donde se realiza la actividad, el horario, las personas encargadas de ello, las situaciones en que se procederá a la grabación, la duración en su mantención y la forma que tienen los ciudadanos de acceder a ellas; se trata, además, de vistas panorámicas de dichos lugares*".

Lo anterior, viene a determinar un contenido de parte del derecho a la privacidad y cómo ste se ejercería en un espacio público. Lo interesante es que no contempla una exclusión

del ejercicio del derecho a la privacidad en el espacio público, sino más bien admite un ejercicio limitado. Existirían entonces, a lo menos, dos parámetros a los cuales deberían sujetarse las políticas de televigilancia, considerando la experiencia en la implementación por parte de los municipios, y las consideraciones de afectación al derecho a la intimidad: primero, las consideraciones establecidas por la Sentencia de fecha 1° de junio de 2016, de la E. Corte Suprema, en autos Rol N°8.481-2016, respecto del "***Régimen de Autorización***" (las cuales forman parte de la Jurisprudencia del máximo tribunal, no obstante el conocido efecto relativo de las sentencias).

En segundo lugar, se deben considerar las recomendaciones realizadas por el Consejo para la Transparencia a través de su Oficio N°2309, de fecha 06 de marzo de 2017, que formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628. Lo interesante en este punto es que si bien el Consejo para la Transparencia tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información, (de acuerdo al artículo 32 de la Ley N°20.285), según su propia normativa, su actividad se reduce a recomendaciones, según su propia ley, que no alcanzan a tener un mandato regulatorio obligatorio sobre los organismos que están sujetos a su "jurisdicción", entendiéndose por tales la compleja estructura a la que remite el literal e) del artículo 33 de la Ley N°20.285, en tanto dentro de sus funciones se encuentra "*e) Formular recomendaciones a los <u>órganos de la Administración del Estado</u> tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean*" (subrayado propio).

Esto va formando un marco regulatorio, un parámetro determinado por órganos colegiados que buscan, bajo el análisis jurídico que a cada uno le corresponde, realizar una protección del derecho que eventualmente pueda verse perturbado, amenazado o derechamente infringido.

Por otra parte, si bien lo anterior representa un parámetro mínimo, no deja de ser insuficiente ante el estricto sentido del principio de legalidad que establece nuestra Constitución, tanto en la actuación de los órganos del Estado, como en la garantía que establece el numeral 26 del artículo 19 de la Constitución Política, en cuanto se asegura a todas las personas "*La seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio*".

2. PROTECCIÓN DE DATOS PERSONALES Y LOS DERECHOS DE LA PRIVACIDAD.

Ya expuesto el problema de la implementación de los sistemas de televigilancia, nos referiremos en este apartado al contenido del derecho a la privacidad consagrado en el Articulo 19 N°4 de la Constitución Política de Chile, tratando de sintetizar su configuración y contenido y cómo se produce el problema constitucional subyacente. Además, incluiremos una mirada a la vertiente de este derecho que se refiere al resguardo y protección de datos personales, especialmente al cuerpo normativo que lo regula (Ley N°19.628 sobre Protección de la Vida Privada) así como el ejercicio de la acción de Habeas data y como esta resulta preponderante cuando se refiere al tratamiento y almacenamiento de imágenes captadas por los sistemas de televigilancia, y como se consideran datos personales de acuerdo a las definiciones que nos otorga la misma ley.

Enseguida revisaremos un apartado considerando la función que ha ejercido el Consejo para la Transparencia en la protección de datos, especialmente cuando se trata de aquellos generados por los sistemas de televigilancia que implementan los organismos públicos, especialmente las municipalidades, y como a través de su labor administrativa se ha tratado de generar recomendaciones a estas corporaciones para la implementación de estos sistemas, considerando el conflicto potencial relacionado al derecho a la privacidad y protección de datos (especialmente con la dictación del Oficio N°2309, de fecha 06 de marzo de 2017), finalizando con el criterio utilizado en su jurisprudencia administrativa, en donde

se ha podido evidenciar una actividad de protección de los datos personales generados a partir de sistemas de televigilancia, en la resolución de amparos interpuestos por la negativa a solicitudes de acceso a la información que han pretendido acceder a los datos que poseen los municipios que han implementados estos sistemas.

2.1. Garantía Constitucional del Derecho a la Vida Privada

De acuerdo a lo que establece el artículo 19 de la Constitución Política de Chile, la Constitución asegura a todas las personas: N°4º. "*El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley*".

A la normativa constitucional ya señalada se deben agregar las normas pertinentes de los Tratados Internacionales ratificados por Chile y que se encuentren vigentes, los cuales forman parte del denominado Bloque Constitucional de Derechos respecto de la protección de la vida privada, que debe guiar las decisiones legislativas que buscan materializar y concretar dicha protección (Nogueira, 2015: p.303). En ese sentido resultan relevantes el artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 11.2 de la Convención Americana sobre Derechos Humanos, y como parte del Derecho Internacional y como marco referencial, también lo dispuesto en el artículo 8.1 del Convenio Europeo de Derechos Humanos.

El numeral 4° del artículo 19 de la Constitución permite identificar, en principio, dos derechos fundamentales: el respeto y protección a la vida privada de las personas (derecho a la privacidad) y el respeto y protección a la honra de la persona y su familia (derecho a la Honra). Además, y junto a estos dos derechos se reconoce como un tercer derecho la protección de los datos personales, ya no subsumido como parte del derecho a la privacidad, sino como un derecho que, en armonía con los anteriores, protege un ámbito sensible de la persona relacionada con la información personal, la cual se vuelve un factor determinante en

esta era moderna donde las relaciones interpersonales, sociales, e incluso económicas, se basan en el uso de dicha información. Para los propósitos de nuestro trabajo nos enfocaremos en la conceptualización del Derecho a la Privacidad como parte del conflicto jurídico que hemos planteado.

En cuanto al respeto y protección a la vida privada de las personas, el contenido esencial de este derecho se basa en la relación que genera la dignidad y su proyección inmediata en la vida privada de una persona y de su familia, lo que incluye el derecho a la propia imagen. La protección a la privacidad se constituye entonces por un ámbito de autonomía de las personas, donde ésta forma su personalidad y proyecta su vida, tomando sus propias decisiones, lo que posibilita el libre desarrollo de su personalidad.

Para conceptualizar bien el contenido del derecho, debemos considerar que se entiende por privacidad y por intimidad. El Diccionario de la Lengua Española entiende por "privacidad" como "*cualidad de privado*" y como "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*" (Real Academia de la Lengua Española, 2016b: p. 1786). A su vez, Entiende que "intimidad" se refiere a "*zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*" (Real Academia de la Lengua Española, 2016a: p. 1258). A partir de lo anterior podemos trazar como idea que la vida privada se relaciona con la intimidad, y ésta es el ámbito en que el sujeto y su familia y gente de afecto conviven, donde planifican el presente y el futuro, donde incrementan sus virtudes y buscan superar sus defectos, donde fomentan sus potencialidades para su progreso integral, sin la intervención ni presencia de terceros. Para Nogueira la privacidad en su ámbito más profundo lleva al concepto de intimidad, ámbito reservado del individuo que no desea ser develado al conocimiento o acción de los demás. Este es necesario para mantener un mínimo de calidad de vida humana, comprendiendo que son elementos de la intimidad la concepción religiosa o ideológica de una persona, su vida sexual, estado de salud, su genoma, entre otros, los cuales se catalogan como datos sensibles.

De acuerdo a lo establecido en el artículo 2° literales f) y g) de la Ley N° 19.628, sobre protección de la Vida Privada, se entiende por ***Datos de carácter personal o datos***

personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables y por ***Datos sensibles***, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

De esta forma, el derecho a la intimidad es la facultad de todo sujeto para evitar injerencias de terceros en los ámbitos que la integran, salvo que medie su consentimiento y decida compartir con más personas, de su círculo cercano, o lo haga público. Esta esfera íntima no puede ser vulnerada, salvo en casos específicamente establecidos, tales como procesos criminales, donde se investiguen delitos vinculados a situaciones de la vida privada como la bigamia o el incesto, juicios civiles derivados de la Ley de Matrimonio Civil, como el divorcio vincular o la nulidad del matrimonio, y también en juicios de cuidado personal o de alimentos respecto de niños, niñas o adolescentes.

Entendemos que el derecho a la protección de la vida privada es la facultad de los sujetos de mantener un ámbito de su vida fuera del conocimiento público, donde un sujeto realiza acciones que inician y concluyen en él mismo, siempre que no dañe a otros, no sean delitos o no sean hechos relevantes públicamente, o que afecten al bien común.

Para esto debemos hacer una distinción respecto a los actos públicos, los que no pertenecen al ámbito de protección de la vida privada y que se traducen en actuaciones externas que trascienden a quien las ejecuta por afectar el orden moral o el bien común; así como también las actuaciones que tengan relevancia pública por virtud del acto mismo, o en atención a la persona que lo ejecuta, cuya difusión satisfaga la función de formación de una opinión pública. Así lo entiende Nogueira (2004) en tanto señala que "*En la regulación jurídica relacionada con el ejercicio del derecho a comunicar información en relación a la honra y a la* ***privacidad****, serán circunstancias relevantes en esta ponderación la materia de la información, su interés público, su capacidad de contribuir a la formación de una opinión*

pública libre, el carácter público o privado de la persona objeto de la información, así como el medio a través del cual se ha transmitido la información" (Nogueira, 2004: p.146),.

Debido a lo anterior es que, en un juicio de ponderación ante el conflicto suscitado tantas veces entre el ejercicio de la libertad e información y un eventual conflicto con el derecho a la privacidad de una persona, se ha optado por decantar en favor del derecho a la información bajo el argumento de consistir en hechos de relevancia pública. Así, en Sentencia de la E. Corte Suprema, de fecha 18 de julio de 2019, en autos Rol N°5.489-2019 (que conoce de apelación de sentencia de I. Corte de Apelaciones de Santiago de recurso de Protección Rol N° 63936-2018) se señala en su considerando quinto lo siguiente:

"Quinto: Que sobre el conflicto entre ambas garantías fundamentales la doctrina ha sostenido que "Entre derechos fundamentales no se puede hablar de jerarquía de derechos, sino de equilibrio y armonización de derechos. Tanto la honra, la ***privacidad****, la libertad de opinión y de información, se encuentran en el mismo nivel de derechos humanos y fundamentales protegidos por la Constitución y por el derecho internacional de los derechos humanos, los cuales cuentan con las mismas garantías. La regla de proporcionalidad de los sacrificios es de observancia obligada al proceder a la limitación de un derecho fundamental por un precepto legal. Toda la acción deslegitimadora del ejercicio de un derecho fundamental adoptada en protección de otro derecho fundamental que entre en tensión con él, debe ser armonizadora de ambos derechos y proporcionada con el contenido y finalidad de cada uno de ellos*".

De esta forma, considera el máximo tribunal, según expresa en su considerando octavo:

"Octavo: Que de acuerdo al mérito de los elementos de juicio aparejados al proceso, y por tratarse de hechos de relevancia pública, el derecho a la honra y la vida privada cede en este caso ante la necesidad de protección de que goza la libertad de información, considerando la necesidad de la ciudadanía de conocer hechos como aquellos de que se trata en autos".

Se observa un criterio similar a lo resuelto en la Sentencia de la E. Corte Suprema, de fecha 28 de enero de 2019, en autos Rol N°31.279-2018 (conociendo de Apelación de sentencia que rechaza recurso de protección por parte de la I. Corte de Apelaciones de Santiago en Rol N° 59.683-2018), la cual en su considerando octavo señala lo siguiente:

"*Octavo: Que, mediando en relación con el reportaje materia del presente recurso, el interés público asociado con una denuncia efectivamente formulada por conductas que han sido estimadas como delictuales, resulta justificado privilegiar, en la especie, a la libertad informativa del medio, ante un eventual conflicto de derechos con la honra del recurrente, más aún cuando la presunta afectación de esta última parece más bien artificiosa. Por tal razón, tal y como lo ha sostenido con anterioridad esta Corte (SCS de 17 de marzo de 2016 en causa Rol N° 26.753-2015) no cabe analizar, en el contexto descrito y en esta sede el reclamo del recurrente respecto a los eventuales efectos de la exhibición de los reportajes elaborados por la recurrida, en los que tuvo una participación voluntaria y que refieren a una materia que ya está siendo investigada en otra instancia y con lato conocimiento*".

La E. Corte Suprema ha indicado que por vida privada se entiende aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento.
Por su parte, Luis María Díez-Picazo (2008) señala que:

> "(…)*la existencia de una esfera privada, en la que los demás (poderes públicos o particulares) no pueden entrar sin el consentimiento de la persona, no implica solo un reconocimiento del altísimo valor que tiene la faceta privada de la vida humana, sino que constituye también una garantía básica de libertad: en un mundo donde toda la actividad de los hombres fuera pública, no cabría la autodeterminación individual. El constitucionalismo, así, exige diferenciar entre las esferas pública y privada y, por tanto, entre lo visible y lo reservado*" (Diez-Picazo, 2008: p. 297).

En ese sentido, si toda actividad humana fuese pública no cabría la autodeterminación individual. El constitucionalismo exige diferenciar entre las esferas públicas y privada, y así entre lo visible y lo reservado.

Por su parte, el Tribunal Constitucional ha señalado en Sentencia del Tribunal Constitucional, Rol N°389, de fecha 28 de octubre de 2003, en su considerando vigésimo, que "*La privacidad integra los derechos personalísimos o del patrimonio moral de cada individuo, los cuales emanan de la dignidad personal y son, por su cualidad de íntimos de cada sujeto, los más cercanos o próximos a esta característica, única y distintiva, del ser humano. Por tal razón, ellos merecen reconocimiento y protección excepcionalmente categóricos tanto por la ley como por los actos de autoridad y las conductas de particulares o las estipulaciones celebradas entre éstos*".

Para Díez-Picazo (2008) se integran en este derecho, por una parte, la intimidad, y por otra, además de la honra, el derecho a la propia imagen.

En cuanto a la intimidad, el bien jurídico que se protege es un ámbito propio o reservado para alcanzar una calidad mínima de vida, este ámbito viene dado por cuestiones de índole personal y familiar. Es la intimidad un derecho genérico en esta materia, siendo especies el derecho a la propia imagen o el derecho al honor. Este derecho consiste en la facultad de excluir del conocimiento ajeno los hechos comprendidos en el ámbito propio y reservado. Esto lleva al problema de determinar el alcance exacto de la esfera privada, en que formalmente privado será lo que una persona decida excluir del conocimiento de los demás; y materialmente es privado todo lo que, según las pautas sociales imperantes, se considera reservado o ajeno al legítimo interés de los demás. Ahora bien, si lo decisivo para determinar la esfera personal es la voluntad del interesado se corren dos riesgos: decir que pueden definir su esfera personal es afirmar que podrán renunciar a su intimidad; y las personas podrían excluir del conocimiento incluso del Estado de aspectos incuestionablemente de interés público (los políticos y sus cargos precedentes), lo cual como hemos visto se determina a través de un análisis que excluye esta voluntad. Así parece conveniente un criterio predominantemente material.

Como lo señaláramos anteriormente, y compartiendo la opinión de Domingo Lovera Parmo (2017), consideramos que las actuaciones de las personas en el espacio público se realizan bajo una expectativa razonable de privacidad, por lo que cuando se implementan políticas públicas de televigilancia, las mismas deben estar sujetas a cumplir con los requisitos establecidos por la legislación, así como al propósito inherente que justifica su aplicación, pues dichos sistemas representan una intromisión en la esfera de privacidad de la persona. Así, las personas son titulares del derecho a la privacidad también en el espacio público o espacios de libre acceso, considerando que "hasta *cierto punto, la vida en el espacio público asegura (o aseguraba) un cierto grado de privacidad. No es que las personas no se vean unas a otras, pero sí que se proteja una relativa conciencia de que allí, afuera, en medio de la masa, es (o era) posible obtener ciertas cuotas de anonimato*" (Lovera, 2017: p. 403).

Así también puede observarse en el criterio contenido en Sentencia de la I. Corte de Apelaciones de Santiago, de fecha 21 de agosto de 2017, en autos Rol N° 34.360-2017, que rechaza recurso de protección, y que en su considerando vigésimo séptimo expresa lo siguiente:

"*27)º Que en el caso que nos interesa la vigilancia a través de los drones se desarrolla en determinados espacios públicos -y no privados- de la comuna de Las Condes, y dentro de esa perspectiva cabe analizar la expectativa de privacidad que el ciudadano tiene en dichos espacios. En efecto,* ***razonable es que al acceder a un lugar público cada persona aspire, entre otros aspectos, que sus conversaciones no sean de acceso público, como también que en su desplazamiento no sea objeto de registro personal, o de seguimientos, es decir, que pueda deambular libremente manteniendo su anonimato frente a quienes le rodean*** (Negrita del tesista)***,*** *a menos que incurra en conductas ilegales o se vea involucrado en situaciones de emergencia, pues en tales casos, normal es que tales expectativas de privacidad se desvanezcan*".

De esta forma, la legítima expectativa de privacidad no finaliza al utilizar los espacios públicos por parte de los ciudadanos, pues en una sociedad compleja, dichos espacios existen

para posibilitar la interacción entre los distintos integrantes de la misma. Afirmar lo contrario presentaría la problemática que, por ejemplo, una conversación privada sostenida entre dos personas de confianza en que una le confía a otra una información sensible que bajo los parámetros expresados se entendería como intima, por el solo hecho de darse en un espacio público, debería ser considerada como excluida de la esfera de protección del ejercicio del derecho a la privacidad.

Por otra parte, en cuanto al derecho a la propia imagen, éste se refiere a la corriente corporal del ámbito reservado, donde imagen es el aspecto físico de la persona, en tanto pueda calificarse de íntimo o reservado, incluyendo la reproducción o utilización de la voz. Hoy este derecho se entiende como un derecho fundamental autónomo, considerando que el consentimiento al uso de la propia imagen puede ser revocado en todo momento, salvando los daños que ellos provocaren. Este último aspecto se relaciona con lo dispuesto en la Ley N°19.628 de Protección de la Vida Privada, considerando la generación de Datos Personales que se produce a través de la recopilación y almacenamiento de imágenes captadas por los sistemas de televigilancia, lo cual también se relaciona con el derecho a la protección de los datos personales. Ahora bien, el Tribunal Constitucional, en su Sentencia de fecha 24 de febrero de 1987, Rol N° 43-1987, en su considerando 21°, ha determinado que "*la esencia del derecho debemos conceptuarla, desde el punto de vista del ordenamiento positivo y dentro de este ámbito precisar el alcance de la norma constitucional en los términos más sencillos, para que sea entendido por todos y no sólo por los estudiosos de la ciencia jurídica. Desde esta perspectiva, debemos entender que un derecho es afectado en su "esencia" cuando se le priva de aquello que le es consustancial de manera tal que deja de ser reconocible y que se "impide el libre ejercicio" en aquellos casos en que el legislador lo somete a exigencias que lo hacen irrealizable, lo entraban más allá de lo razonable o lo privan de tutela jurídica"*.

De esta forma, para el objeto principal de esta investigación, será la utilización de la videovigilancia en el espacio público, su regulación jurídica y la tecnología utilizada, mostrando como la videovigilancia restringe el derecho a la vida privada y tensiona la protección de datos personales. Así, para Rodolfo Figueroa (2013), la privacidad no solo se

puede vulnerar por recolección de información o divulgación, sino también en una serie de casos que categoriza como de procesamiento, que tiene que ver con el uso, almacenamiento y manipulación de información que ya ha sido recolectada (Figueroa, 2013: p. 866). A través del correcto tratamiento de los datos obtenidos por los dispositivos de videovigilancia -instalados para la prevención, reacción y persecución de los delitos cometidos en el espacio público- y un marco jurídico apropiado, es posible evitar vulnerar garantías fundamentales como los derechos de la privacidad y la protección de datos personales.

2.2. Ley N° 19.628 Sobre Protección de la Vida Privada: Datos Personales y Habeas Data.

En lo que se refiere al resguardo y protección de datos personales, el cuerpo normativo que lo regula es la Ley N°19.628 sobre Protección de la Vida Privada, aunque de la lectura de su texto se puede inferir que la regulación que establece viene dada desde el punto de vista del tratamiento de datos y la creación de bancos de datos que desde la óptica de resguardar el ejercicio de los derechos de la persona en el ámbito de la creación de datos personales, aunque se podría argumentar que se busca proteger los derechos de los titulares de dichos datos al regular el tratamiento. Lo anterior se ve ratificado por lo que dispone el artículo 1° de la Ley en cuento señala lo siguiente:

"Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce".

No obstante lo anterior, la ley entrega un conjunto de derechos subjetivos a los titulares de datos personales que permiten sostener la existencia de un derecho a la

autodeterminación informativa en su artículo 13 en cuanto señala que "*El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención*".

¿Qué se entiende como contenido de este derecho? Para Gude Fernández (2014), y considerando el caso de Alemania y el derecho fundamental a la autodeterminación informativa establecido en su legislación, el mismo "*consiste en un poder de disposición y de control sobre los datos personales que habilita a la persona para decidir cuáles de ellos deben proporcionarse a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, permitiendo también al titular de los mismos saber quién los posee y para qué, pudiendo oponerse a esa posesión o uso*" (Gude, 2014: p. 71). Entiende, entonces, que este derecho contempla dos facultades que son su núcleo esencial: de disposición y control sobre los datos personales, las que se concretan jurídicamente en la potestad de consentir la recogida, la obtención y el acceso a los mismos, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Adiciona como un correlato lógico para el ejercicio del derecho (como un complemento indispensable) la facultad de saber en todo momento quién dispone de ellos y a qué uso los está sometiendo, y el poder oponerse a esas dos operaciones. Finaliza señalando que "*La videovigilancia es el clásico ejemplo del conflicto entre la técnica de la vigilancia y el derecho a la autodeterminación informativa: los afectados no saben, quién y qué se esconde detrás de la cámara de observación*" (Gude, 2014: p. 82).

Volviendo a nuestro ordenamiento, y reconociendo la posibilidad práctica de negativa al ejercicio del derecho a la autodeterminación informativa, la ley en comento establece un recurso legal que posibilita someter a conocimiento judicial la acción pretendida: el *Habeas Data*. Así, dispone el inciso primero del Artículo 16 de la Ley N°19.628 que "*Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas*

correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente".

Ahora bien, cabe señalar que la legislación nacional vigente no ha entregado a ningún organismo público facultades destinadas a aplicar o resguardar el cumplimiento de la Ley Nº19.628, con atribuciones suficientes para sancionar o compeler a las entidades privadas que hacen tratamiento, en orden a lograr un adecuado procesamiento de datos personales. Lo que existe es un régimen de acción particular, donde cada ciudadano, en el marco del ejercicio de su derecho a la autodeterminación informativa deberá accionar para resguardar su interés. Es decir, no existe una autoridad de control de la legalidad en el tratamiento de datos personales, la cual solo se garantizaría a través del procedimiento judicial dispuesto en la ley.

Por otra parte, a nivel de tratamiento de datos personales por organismos públicos, la Ley Nº20.285, sobre Acceso a la Información Pública, encomienda al Consejo para la Transparencia velar por el adecuado cumplimiento de la ley sobre de protección de datos de carácter personal en lo que se refiere a la actividad de los órganos de la Administración del Estado. En ese sentido, el Consejo para la Transparencia ha tenido un rol activo en lo que se refiere la protección de datos, de lo cual profundizaremos más adelante. La pregunta, entonces, que corresponde hacer, considerando la posibilidad de protección de los datos personales que entrega la Ley N°19.628, es ¿cómo la implementación de un sistema de televigilancia en espacios públicos, que ya hemos señalado propicia la afectación al ejercicio del derecho a la privacidad en dichos espacios, se traslada a una posibilidad de afectación desde el punto de vista de los datos personales de las personas?

Para responder es necesario señalar que tal como indicáramos anteriormente, los sistemas de televigilancia se componen de 3 subsistemas, dentro de los cuales encontramos el subsistema integrado por las cámaras propiamente tal que conforman un circuito cerrado de televisión, y además un subsistema de control y monitoreo, donde se administran las imágenes enviadas por las diferentes cámaras de televigilancia instaladas, y donde se realiza el procesamiento y almacenamiento. Aquí es donde es necesario entender que la imagen de

una persona grabada a través del sistema genera un conjunto de datos personales, según lo dispuesto en el artículo 2 letra f) de la Ley 19.628.

Puede constatarse que es precisamente la naturaleza de la información y no el lugar de captación el criterio que el legislador sigue en la Ley N°19.628 para revestir de una especial protección a aquellos datos que estima personales. Esto plantea el grave problema acerca de los límites del derecho a la privacidad o intimidad, de cómo se plantea el ejercicio de este derecho en los espacios públicos (no solo bienes nacionales de uso público), y si basta la sola justificación del argumento preventivo delictual y accesorio a la persecución de los delitos para limitar en tamaña intensidad el derecho a la privacidad y la forma en cómo se naturaliza esta situación de afectación. Puede ser que nos encontremos ante un fenómeno cultural de una sociedad que desconoce cuáles son sus derechos y está incluso dispuesta a sacrificar parte de ellos (ejercicio legítimo de uno de sus derechos) en pro de una medida (accesoria, por lo demás, a un fin, o un medio para un fin) que busca una utilidad que se encuentra (supuestamente) amparada en la seguridad pública, tan beneficiosa para todos.

Ahora bien, el problema no solo resulta ser parte de la dinámica conflictiva seguridad pública con derecho a la privacidad. Existe también un problema entre la libertad y la seguridad, problema sobre cuya dinámica existente, como un conflicto constante, ha sido planteado de una excelente forma por Ana Gude Fernández (2014) para quien

> "*La libertad es un derecho «débil» que se relativiza fácilmente de cara a la problemática de la inseguridad*", y que sintetiza sosteniendo que "*La libertad y la seguridad son bienes constitucionales de primer orden en la medida que constituyen un presupuesto indispensable para el efectivo disfrute y cumplimiento de todos los demás. Los textos constitucionales y las declaraciones de derechos afirman que toda persona tiene derecho a la libertad y seguridad, sin embargo, se trata de un principio de no fácil realización. En la práctica se presentan como un binomio en constante tensión, en donde siempre es necesario sacrificar en mayor o menor medida una de sus partes*" (Gude Fernández, 2014: p. 73).

Esto nos lleva a cuestionar acerca de si la videovigilancia es un factor decisivo a la hora de actuar como un disuasivo en materia de seguridad pública, y si es, aun siendo positivo, un fundamento de tal intensidad que permite limitar de forma grave la privacidad de las personas, aun cuando se trate espacios públicos, y especialmente cuando la afectación se traslada a la creación de bancos de datos a partir de las imágenes almacenadas. Es decir, se llegará a producir un efecto real, cuantitativo, o será solo un mero dato anecdótico en similitud a la cuantía de la pena, que cuando se trata de política criminal es naturalmente utilizada como recurso aparentemente infalible, al señalar que con el solo aumento de la pena asignada a tal delito su ocurrencia se verá reducida. Se hace necesario destacar que no se cuestiona la utilidad posterior que puede representar para contribuir a resolver diversas situaciones delictivas[8]. Son una prueba directa que permite suplir el relato de algún testigo (que puede ser bastante falible) y representa aquí una utilidad. Utilidad *ex post*, pero no necesariamente *ex ante.*

Incluso, en el ámbito de la producción probatoria generado en procesos penales a partir de medidas y diligencias intrusivas, existe una limitante clara y establecida en el marco de la Ley N°19.974 Sobre el Sistema de Inteligencia del Estado (Ley de Inteligencia). Así lo señalan Viollier Bonvin y Ortega Romo quienes concluyen que:

> "*El principio de reserva legal establece la necesidad que cualquier tipo de restricción de derechos fundamentales, como la inviolabilidad de las comunicaciones y el derecho a la intimidad, requiera la existencia de una habilitación legal expresa. Esta habilitación debe, además, ser restringida, contener parámetros objetivos y precisos, no ser discrecional, estar sujeta a control y no implicar que el afectado padezca detrimentos excesivos*" (Viollier y Ortega , 2019: p.106).

[8] Para Gude Fernández, "*En la actualidad, el uso de las modernas tecnologías y, en particular, la aplicación de los sistemas de videovigilancia para garantizar la seguridad han contribuido a la prevención y persecución del delito, pero al mismo tiempo, no cabe duda de que han sido una fuente generadora de problemas: sus indudables ventajas han supuesto en muchos casos un sacrificio excesivo de no pocos derechos y libertades*" (Gude Fernandez, 2014: p. 74).

Idea que si bien se enmarca en el estudio que realizan sobre medias intrusivas para investigaciones en procesos penales al amparo de la ley de Inteligencia, vale también como parámetro en el caso del producto de la televigilancia, especialmente cuando se argumenta que es una herramienta fundamental para la persecución de delitos cometidos en espacios públicos.

Por otra parte no puede negarse la incidencia que tiene hoy las formas de comunicación moderna que involucran dispositivos de comunicación inteligentes con acceso constante (y muchas veces permanentes) al internet, a cuya vulneración pareciéramos estar más expuestos, significando este acceso no consentido una clara vulneración el derecho a la privacidad[9].

Así lo plantea también Lovera Parmo (Lovera 2017.) para quien el desarrollo de la privacidad en el contexto de las nuevas tecnologías, están vinculadas no solo al uso de internet, sino que también a las nuevas herramientas con que cuentan los órganos estatales para efectos de llevar adelante actividades de vigilancia, indica que existe una preocupación especialmente sensible respecto a las formas en que los Estados se embarcan en actividades de recolección de información respecto de sus ciudadanos y ciudadanas, el tratamiento que se hace de esa información y los usos que se da a la misma.

2.3. La Función del Consejo para la Transparencia en Cuanto a la Protección de los Datos Personales.

La Ley N°20.285, sobre Acceso a la Información Pública (conocida como "Ley de Transparencia") tiene su origen en dos hitos fundamentales: Primero, la reforma constitucional llevada a cabo durante el año 2005 en la vigencia del mandato presidencial de

[9] Viollier Bonvin y Ortega Romo plantean que "*En vista de que cada día una parte más significativa de nuestras interacciones y comunicaciones privadas pasan por nuestros dispositivos electrónicos, una medida intrusiva de estas características entregaría un acceso casi absoluto a los aspectos más íntimos de la vida privada del afectado, lo que desvirtuaría las garantías fundamentales consagradas en la Constitución. Las autorizaciones de las medidas intrusivas reguladas en la ley de inteligencia son otorgadas en el marco de la inviolabilidad de las comunicaciones y del expreso mandato al legislador de regular la afectación de tal garantía. Sin embargo, como revisamos, dicha restricción es posible solo cuando el derecho fundamental no se vea afectado en su esencia*" (Viollier et al., 2019: p.104).

Ricardo Lagos Escobar; y segundo, en el año 2006 con la sentencia del Caso Claude Reyes y otros versus Chile de la Corte Interamericana de Derechos Humanos[10], sentencia de 19 de septiembre de 2016, que resolvió, en lo que nos interesa:

1. El Estado violó el derecho a la libertad de pensamiento y de expresión consagrado en el artículo 13 de la Convención Americana sobre Derechos Humanos, en perjuicio de los señores Marcel Claude Reyes y Arturo Longton Guerrero, en relación con las obligaciones generales de respetar y garantizar los derechos y libertades y de adoptar disposiciones de derecho interno establecidas en los artículos 1.1 y 2 de dicho tratado, en los términos de los párrafos 61 a 103 de la presente Sentencia.

7. El Estado debe adoptar, en un plazo razonable, las medidas necesarias para garantizar el derecho de acceso a la información bajo el control del Estado, de acuerdo al deber general de adoptar disposiciones de derecho interno establecido en el artículo 2 de la Convención Americana sobre Derechos Humanos, en los términos de los párrafos 161 a 163 y 168 de la presente Sentencia.

De esta forma, tal como lo describe su artículo 1°, la Ley de Transparencia "*regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información*".

Ahora bien, en el marco de lo que nos interesa, la Ley de Transparencia crea el Consejo para la Transparencia, como una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio (artículo 31 de la Ley), cuyo objeto es "*promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del*

[10] Sentencia disponible sitio institucional de la Corte Interamericana de Derechos Humanos en https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf. Adicionalmente, se puede acceder a la ficha técnica del caso en el sitio web institucional de la Corte, disponible en https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=332. Fecha de última consulta: 30 de enero de 2021.

Estado, y garantizar el derecho de acceso a la información" (Artículo 32). Para lo anterior, la ley le otorga una serie de atribuciones, descritas en el artículo 33, entre cuyas resultan importantes las descritas en sus literales e) y m)[11].

Es en el marco de dichas potestades, y considerando el contexto de las problemáticas surgidas en razón de la implementación de sistemas de televigilancia por parte de distintas municipalidades que el Consejo para la Transparencia dictó el Oficio N°2309, de fecha 06 de marzo de 2017, que formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628. Se Trata de un acto administrativo, que encuentra su origen en lo dispuesto en el artículo 33 letras e) y m) de la Ley N° 20.285, y su oportunidad radica en la implementación de distintos dispositivos de televigilancia con fines de seguridad comunal por parte de diversas municipalidades. En cuanto al contenido del Oficio, y en relación a los municipios que decidan instalar dispositivos de videovigilancia, recomienda implementar las siguientes medidas:

1. La grabación y captación de imágenes debe efectuarse con fines exclusivos de seguridad comunal; 2. Las imágenes sólo podrán ser captadas en lugares públicos. Excepcionalmente podrán ser captadas en lugares privados abiertos cuando se trate de la persecución por un hecho constitutivo de delito flagrante.; 3. El municipio es el responsable legal del tratamiento de las imágenes grabadas o capturadas; 4. Se deben implementar medidas de seguridad para la protección de imágenes, de forma de impedir que terceros accedan a su contenido; 5. Las imágenes deberán ser destruidas dentro de los 30 días desde que éstas hayan sido grabadas o captadas; 6. Un funcionario municipal deberá certificar que las imágenes hayan sido grabadas en los lugares permitidos; 7. La municipalidad deberá garantizar el ejercicio de los derechos de la persona grabada, como los de acceso y cancelación de datos, entre otros.; 8. La municipalidad deberá inscribir el banco de

[11] *Artículo 33.- El Consejo tendrá las siguientes funciones y atribuciones:*
e) Formular recomendaciones a los órganos de la Administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean.
m) Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado.

imágenes en el Servicio de Registro Civil e Identificación; 9. El municipio deberá informar al Consejo sobre las medidas adoptadas.

Del Oficio en cuestión resulta importante destacar unos cuantos aspectos que se relacionan directamente con lo que en este trabajo se discute. Primero, de acuerdo a la apreciación del Consejo para la Transparencia (y esto parece ser en el marco de las potestades que derivan de lo dispuesto en la letra m del artículo 33 de la Ley N°20.285) la imagen de las personas constituye un dato personal que es protegido por la Ley N° 19.628, en tanto de acuerdo a lo que dispone el artículo 2° letra f del señalado cuerpo legal, la imagen de las personas debe ser considerada un dato personal, toda vez que permite la visualización gráfica de las características físicas de personas naturales identificadas o identificables, y serian estas características las que, como grado de identificabilidad, explican su utilidad en fines de prevención del delito.

En segundo término, y como necesaria consecuencia de lo anterior, resulta que la grabación de la imagen de las personas, su almacenamiento, visualización, análisis, encriptación, alteración o destrucción, entre otras operaciones, constituyen tratamientos de datos personales, lo que trae como consecuencia que "*dicho tratamiento, para efectos de su legitimidad, sólo puede efectuarse cuando la Ley N°19.628 u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello*" (artículo 4, inciso 1°, Ley N° 19.628) y, en el caso de los organismos públicos debe hacerse en el marco de sus competencias establecidas por la ley (artículo 20, Ley N° 19.628).

Como tercer punto, resulta que el municipio es el responsable legal del tratamiento de las imágenes, aun cuando dicho tratamiento pueda ser encargado a un tercero. Acá debemos poner atención, ya que de acuerdo a la apreciación del Consejo, los municipios están facultados para proceder a la implementación de sistemas de televigilancia, por cuanto "*tienen competencias legales para tratar las imágenes de personas con fines de seguridad comunal*". Esto último, de acuerdo a una interpretación de los artículos artículo 4°, letra j) y 5°, letra I, ambos de la Ley N°18.695, Orgánica Constitucional de Municipalidades, por lo que concluye que "*una de las funciones que la ley les ha otorgado a las municipalidades es*

el resguardo de la seguridad comunal y control del orden público y, por tanto, en cumplimiento del artículo 20 de la Ley N° 19.628, estos órganos del Estado sólo pueden tratar las imágenes en el marco de sus competencias y con la finalidad allí descrita".

Respecto a este tercer punto es posible realizar dos apreciaciones: Primero, la interpretación que realiza de la normativa el Consejo, es una interpretación de carácter administrativo. Así, por más que tenga como función "*Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado*", dicha función debe enmarcarse siempre en lo que se refiere a la actividad de los órganos del Estado. Lo anterior fluye de la misma definición que otorga el artículo 33 de la Ley N° 20.285, en cuanto señala que "*El Consejo tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información*".

Como segunda apreciación, no resulta de lo anterior un estándar suficiente para la habilitación de un órgano del Estado para proceder a implementar sistemas de televigilancia que conllevan el tratar datos personales de un sinfín de ciudadanos que diariamente circulan por los espacios públicos de la ciudad, afectando directamente su derecho a la privacidad, y la consecuente expectativa[12].

Volviendo a la responsabilidad del municipio, es necesario puntualizar la problemática que genera la posibilidad de tratamiento por un tercero. El problema se produce cuando el municipio, según entiende el Consejo para la Transparencia, puede encargar a un tercero (que prestará el servicio correspondiente) el tratamiento de los datos personales. De esto inferimos que se produce una actividad económica cuya base son los datos de un

[12] Samuel Malamud Herrera (2018) ha planteado la insuficiencia y vaguedad de considerar como suficiente la normativa legal habilitante a las disposiciones contenidas en la Ley Orgánica Constitucional de Municipalidades, especialmente considerando los conflictos constitucionales que suscita la implementación de dichas medidas: "*Como puede apreciarse, la competencia que concede a las municipalidades el artículo 4 letra j) de la Ley 18.695 es, en materia de seguridad pública, absolutamente genérica e inespecífica,57 pues no menciona qué tipo de intervenciones de seguridad autoriza y, más importante aún, no menciona qué derechos pueden ser afectados en el desarrollo de tales actividades*" (Malamud Herrera , 2018: p. 153).

centenar de ciudadanos que no tiene la opción de concurrir a generar su autorización, produciendo una merma en la posibilidad de ejercicio del derecho a la autodeterminación informativa, y la posibilidad entonces de generar actividades económicas paralelas, con el subsecuente riesgo para la privacidad de las personas cuyas imágenes (que representan datos personales) son tratadas. Al respecto, el Consejo solo se limita a manifestar en su Oficio que "*En el evento que uno o varios de los tratamientos de las imágenes sean mandatados a un tercero —por ejemplo, empresas de seguridad o de almacenamiento de datos—, el municipio mantiene la responsabilidad sobre el cumplimiento de las obligaciones legales y las recomendaciones de este Consejo, aun cuando hubiese encargado el tratamiento de datos a un tercero*". Lo cual resulta insuficiente si se considera la magnitud del problema que subyace en la tratativa de datos personales de los ciudadanos.

2.4. Jurisprudencia del Consejo para la Transparencia en Amparos por denegación de solicitud de acceso a la información referente a municipios que mantienen sistemas de televigilancia.

No obstante, lo señalado, la labor del Consejo para la Transparencia no ha sido del todo negativa, más si se considera las limitaciones legales que posee dentro de sus actuaciones. Ahora bien, en donde se ha podido evidenciar una actividad de protección de los datos personales generados a partir de sistemas de televigilancia, es en la resolución de Amparos interpuestos por la negativa a solicitudes de acceso a la información que han pretendido acceder a los datos que poseen los municipios que han implementado estos sistemas. Para contextualizar, es necesario precisar que la Ley N°20.285 de Acceso a la Información Publica establece como regla general en materia de acceso a la información el principio de publicidad, admitiendo excepcionalmente el secreto o reserva de la información, asumiendo una interpretación restrictiva de las causales que la misma ley establece en su artículo 21[13], en concordancia con lo dispuesto en el artículo 8° inciso 2° de la Constitución Política.

[13] *Artículo 21.- Las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes:*

1. Cuando su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente:

De esta forma, en Decisión adoptada con fecha 29 de mayo de 2018, en Amparos Roles C4217-17, C385-18, y C775-18, caratulados Edgardo Dinamarca Toledo con Municipalidad de Concón[14], roles en los cuales el recurrente solicita "*Copia de grabación del día 12, a las 15:00 hrs de televigilancia municipal existente en Avda. Concón-Reñaca con calle Laura Barros*", es decir, copia de las grabaciones de las cámaras del sistema de televigilancia que utiliza la Municipalidad de Concón en un día y horas específicos, el Consejo para la Transparencia rechazó los amparos deducidos atendido que considera que la grabación de imágenes captadas por las cámaras de televigilancia implica por parte del órgano reclamado un tratamiento de datos personales y, eventualmente, de datos de carácter sensible, actividad que puede redundar en afectaciones concretas al derecho a la privacidad y al derecho a la propia imagen, de lo cual deriva la necesidad de garantizar la protección de dicho derecho conforme a nuestro ordenamiento jurídico, velando por el adecuado cumplimiento de la Ley sobre Protección de la Vida Privada. En ese sentido razona en su considerando tercero sobre lo siguiente:

"*Que, las cámaras de seguridad instaladas en el espacio público registran imágenes tanto del entorno o espacio público, o de los vehículos que transitan, como también de personas naturales y de inmuebles de propiedad privada. En tal sentido, cabe tener presente que de conformidad a lo preceptuado en la ley N° 19.628, sobre Protección de la Vida Privada, en su artículo 2° letra f), son datos de carácter personal "los relativos a cualquier información*

a) Si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales.

b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas.

c) Tratándose de requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales.

2. Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.

3. Cuando su publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública.

4. Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.

5. Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política.

[14] Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000036639.

concerniente a personas naturales, identificadas o identificables" y su literal g) define como datos sensibles "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.". Por tanto, de conformidad con lo expuesto, a juicio de este Consejo, la entrega de imágenes captadas por cámaras de vigilancia implica por parte del órgano reclamado un tratamiento de datos personales y, también, de datos de carácter sensible, actividad que puede redundar en afectaciones concretas al derecho a la privacidad y al derecho a la propia imagen, de lo cual deriva la necesidad de garantizar la protección de dichos datos conforme a nuestro ordenamiento jurídico, velando por el adecuado cumplimiento de la Ley N° 19.628"

Es posible identificar que el Consejo asume que "*la entrega de imágenes captadas por cámaras de vigilancia implica por parte del órgano reclamado un tratamiento de datos personales"*, por lo que asume una posición de garante ante "*la necesidad de garantizar la protección de dichos datos conforme a nuestro ordenamiento jurídico"*. Así, en su considerando decimo señala que "*Que, en lo que respecta a la directa vinculación del derecho a la privacidad con el derecho a la propia imagen, que en el presente caso se verían directamente afectados de accederse a la entrega de la información solicitada, este Consejo estima que no sólo estamos ante datos personales, relativos a la imagen de una persona, sino que además ante datos sensibles, que conforme a la definición legal, son los referidos a hechos o circunstancias de su vida privada o intimidad, pues las grabaciones que se captan no sólo dan cuenta de las características físicas de determinadas personas, sino que también de sus conductas o hábitos personales*". Decidiendo finalmente en su considerando duodécimo "*Que, divulgar la información solicitada vulneraría no sólo la vida privada de las personas captadas en los registros visuales en poder de la reclamada, sin mediar su autorización, ni orden judicial, en infracción de los cuerpos normativos precedentemente citados, sino también, conllevaría una transgresión del deber de resguardo que nuestra legislación ha impuesto a los diversos organismos públicos que hoy efectúan tratamiento de*

datos personales, y en virtud de ello, poseen bases de datos que les permiten el adecuado cumplimiento de sus tareas."

El mismo criterio expuesto ha adoptado el Consejo, y basado en los mismos argumentos, cuando se trata de amparos deducidos en relación a denegaciones de solicitudes de acceso a la información a través de transparencia por parte de municipios, cuando dichas solicitudes dicen relación con los datos resultantes de sistemas de televigilancia. Así en decisión adoptada con fecha 19 de junio de 2018 en Amparo Rol C67-18, Caratulado Manuel Jofré Figueroa con Municipalidad de Las Condes[15], amparo deducido por denegación de solicitud de acceso a la información de "*todos los videos y/fotografías captadas por los globos aerostáticos en la comuna desde su implementación. Así como también todas las denuncias o acciones legales iniciadas con ocasión de dicha información*". Idéntico criterio se manifiesta en decisión adoptada con fecha 29 de enero de 2019 en Amparo Rol C5026-18, caratulado Luis Armijo Barrera con Municipalidad de Providencia[16], amparo que se dedujo tras la negativa a la solicitud de "*la grabación correspondiente a la cámara de la intersección esquina calle nueva Lyon con avenida providencia, del día lunes 17 de septiembre del 2018 en un rango horario de 08:50 a 09:10*". Cabe destacar que en ambas solicitudes la negativa al acceso a la información por parte de los mencionados municipios se funda en el artículo 21 N°2 de la Ley de Transparencia, por cuanto las grabaciones de las cámaras de seguridad constituyen datos personales que se encuentran protegidos, tanto por la Constitución Política como por la Ley de Protección de Datos.

Por otra parte, distinto es el criterio, y así lo ha sabido diferenciar el Consejo para la Transparencia, respecto de las solicitudes de acceso a la información que buscan acceder a información diversa de los datos personales como resultado de actividades de televigilancia, y que se refieren a aspectos técnicos de estos sistemas de televigilancia. Así, en decisión de fecha 29 de septiembre de 2020 en Amparo Rol C3721-20 caratulado Alejandro López con Intendencia Región Metropolitana de Santiago[17], cuyo amparo se deduce ante la respuesta negativa de la autoridad a la solicitud de acceso a la información en que el recurrente

[15] Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000020844.
[16] Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000025730.
[17] Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000040261.

solicitaba a la Intendencia lo siguiente: "*En virtud del anuncio por parte del Intendente sobre la instalación de cámaras con tecnología de reconocimiento facial: 1. Solicito hacer envío de las ubicaciones exactas de todas las cámaras que cuentan con esta tecnología en la ciudad de Santiago; 2. Marca y modelo de las cámaras; 3. Empresa proveedora de este producto y empresa encargada de la instalación; 4. En caso de que exista, un documento que detalle los planes de expansión e instalación de esta tecnología en otros puntos de la ciudad; 5. Protocolo o reglamento interno que norme el uso de esta tecnología; 6. Especificar si serán funcionarios públicos los que se harán cargo del uso de esta tecnología o se ha contratado una empresa externa (si es así, enviar nombre de empresa externa)*". Es entonces, decisión del Consejo, acoger el amparo deducido en contra de la Intendencia Región Metropolitana de Santiago, ordenando la entrega de información sobre las cámaras de reconocimiento facial consultadas, atendido el carácter público de lo requerido, caso en el cual no resultaron suficientes las alegaciones del servicio en orden a no contar con cámaras con dicha tecnología.

Pese a la labor desplegada, se considera insuficiente en cuanto a la protección de datos se refiere, especialmente porque la labor del Consejo se circunscribe a los posibles conflictos que se presenten sobre datos personales en el contexto de solicitudes de acceso a la información en el marco de lo regulado por la Ley de Transparencia. Es el criterio de, por ejemplo, Lovera Parmo, quien realiza una crítica al contexto de actuación del Consejo para la Transparencia señalando que "*Es cierto que la Ley 20.285, sobre Acceso a la Información Pública, dispone que será misión del CPLT "velar por el adecuado cumplimiento de la ley N 19.628" (artículo 33 letra m) –en cuyo ejercicio dictó las recomendaciones antes identificadas–. Sin embargo, la actividad del CPLT a este respecto se juega –y esto no es responsabilidad del CPLT, precisamente– en la protección de datos personales en poder de organismos públicos y respecto de los que otros particulares requieran acceso. Fuera de las recomendaciones, que responden a situaciones más bien acotadas, el CPLT vela por el cumplimiento adecuado de la ley sobre datos personales en un contexto de acceso a la información y transparencia, lo que inevitablemente altera su acercamiento a las cuestiones sobre privacidad. De este modo, no es un organismo adecuado de conformidad a los estándares del derecho internacional de los derechos humanos para la defensa de datos personales frente al Estado*" (Lovera, 2017: p. 414-415).

Incluso, quienes creen que el Consejo para la Transparencia cuenta con el potencial para ser el ente protector de las disposiciones de la Ley Nº19.628 sobre Protección de la Vida Privada conciben la necesidad de una transformación para que ello ocurra. Así, por ejemplo, para Álvarez Valenzuela, quien sostiene que la discusión no se encuentra en la necesidad o no de contar con una autoridad de control en materia de protección de datos personales en Chile, sino que sobre qué órgano debiera ejercer esa función, proponiendo además dotar al Consejo para la Transparencia de nuevas competencias en la materia (Álvarez Valenzuela, 2016: p. 60)[18].

[18] Para el autor, además, el reconocimiento del CPLT como autoridad de control en materia de protección de datos personales en Chile, con los resguardos necesarios ya identificados, puede significar por una parte, una mejora en la protección del derecho a la vida privada sin desmejorar el derecho de acceso a la información pública, y, por la otra, una mejor solución de los conflictos que enfrenten ambas instituciones jurídicas, mediante el arbitraje interno de las tensiones identificadas, además de establecer un modelo más eficiente en la administración de los recursos fiscales involucrados ((Álvarez Valenzuela, 2016: p. 73).

CONCLUSIONES. -

1. La implementación de sistemas de televigilancia por parte de organismos del Estado encuentra su justificación en la protección de la seguridad pública, y viene a ser parte del enfoque de Prevención Situacional, asumida como política pública transversal, a tal punto que las directrices para su implementación técnica provienen desde la propia Subsecretaria de Prevención del Delito. Por su parte, la implementación de estos sistemas contiene un conflicto intrínseco con el ejercicio del derecho a la privacidad, constitucionalmente garantizado, especialmente cuando esta se ejercita en el espacio público, y a cuyo respecto existe una legitima expectativa de privacidad, es decir, que el ejercicio de este derecho no queda excluido del espacio público.

2. Se evidencia, además, una falta de regulación en cuanto a la implementación de los sistemas de televigilancia, los cuales han sido materializados principalmente por los municipios, al alero de lo dispuesto en la Ley N°18.695, Orgánica Constitucional de Municipalidades, especialmente lo dispuesto en sus artículos 4° letra J y 5°. Esta justificación no resulta suficiente para cumplir con los parámetros de resguardo del ejercicio propio de un derecho, pues resulta una habilitación legal con un contenido amplio que viene a ser llenado a través de actos administrativos afectando el principio de legalidad establecido en nuestra Constitución Política, especialmente la garantía establecida en el artículo 19 N° 26.

3. Por otra parte, la insuficiencia regulatoria en el ámbito legal respecto de la implementación de sistemas de televigilancia, especialmente sobre el conflicto con el ejercicio del derecho a la privacidad en espacios públicos, ha sido suplida vía jurisprudencia de los tribunales superiores, los cuales en el conocimiento de acciones de protección derivadas de la utilización de estos sistemas han determinado parámetros para su implementación; y también por las recomendaciones emanadas desde el Consejo para la Transparencia, siendo la actividad de estos órganos la que

ha venido a dar un marco regulatorio para la implementación de estos sistemas de televigilancia.

4. De esta forma, resulta trascendental la Sentencia de fecha 1° de junio de 2016, de la E. Corte Suprema, en autos Rol N°18.481-2016, que en su considerando décimo quinto estableció un "***Régimen de Autorización***" para el empleo de medios de televigilancia, llenando así un vacío legal, que resulta ser el parámetro base para la utilización de la televigilancia, integrado por cuatro requisitos. Asimismo, las recomendaciones realizadas por el Consejo para la Transparencia a través de Oficio N° 2309, de fecha 06 de marzo de 2017, que formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628, completan un marco de actuación que permite un resguardo para el ciudadano. Se convierten entonces estos actos en dos parámetros a los cuales deberían sujetarse las políticas de televigilancia, considerando la experiencia en la implementación por parte de los municipios, y las consideraciones de afectación al derecho a la intimidad.

5. Si bien lo anterior representa un parámetro mínimo, no deja de ser insuficiente ante el estricto sentido del principio de legalidad que establece nuestra constitución, tanto en la actuación de los órganos del Estado, como en la garantía que establece el numeral 26 del artículo 19 de la Constitución Política, en cuanto se asegura a todas las personas "*La seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio*".

6. Se destaca además la labor que ha tenido el Consejo para la Transparencia en cuanto a la protección de datos personales, ya que de acuerdo a la apreciación del Consejo, la imagen de las personas constituye un dato personal que es protegido por la Ley N°19.628, en tanto de acuerdo a lo que dispone el artículo 2° letra f del señalado

cuerpo legal, la imagen de las personas debe ser considerada como un dato personal, toda vez que permite la visualización gráfica de las características físicas de personas naturales identificadas o identificables, y serían éstas características las que, como grado de identificabilidad, explican su utilidad en fines de prevención el delito. De esta forma, y como necesaria consecuencia de lo anterior, resulta que la grabación de la imagen de las personas, su almacenamiento, visualización, análisis, encriptación, alteración o destrucción, entre otras operaciones, constituyen tratamientos de datos personales, lo que trae como consecuencia que "*dicho tratamiento, para efectos de su legitimidad, sólo puede efectuarse cuando la Ley N°19.628 u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello*" (artículo 4, inciso 1°, Ley N° 19.628) y, en el caso de los organismos públicos debe hacerse en el marco de sus competencias establecidas por la ley (artículo 20, Ley N° 19.628).

7. La labor del Consejo para la Transparencia no se agota en la dictación de recomendaciones, sino que también se plasma a través de su jurisprudencia, a través de la cual se ha podido evidenciar una actividad de protección de los datos personales generados a partir de sistemas de televigilancia, en la resolución de Amparos interpuestos por la negativa a solicitudes de acceso a la Información que han pretendido acceder a los datos que poseen los municipios que han implementados estos sistemas. Así, en las consideraciones realizadas por el Consejo se entiende que la grabación de imágenes captadas por las cámaras de televigilancia implica por parte del órgano reclamado un tratamiento de datos personales y, eventualmente, de datos de carácter sensible, actividad que puede redundar en afectaciones concretas al derecho a la privacidad y al derecho a la propia imagen, de lo cual deriva la necesidad de garantizar la protección de dicho derecho conforme a nuestro ordenamiento jurídico, velando por el adecuado cumplimiento de la Ley sobre Protección de la Vida Privada.

8. Finalmente, es posible vislumbrar la necesidad de creación de un organismo estatal con capacidad y competencias para realizar la protección de los datos personales de

los ciudadanos de acuerdo a las disposiciones de la Ley N° 19.628, así como la legislación pertinente para proteger eficazmente el derecho a la privacidad de las personas.

BIBLIOGRAFIA. -

JURISPRUDENCIA.-

Sentencia de la Corte Suprema de Chile (2016): Rol 18.481-2016.

Sentencia de la Corte de Apelaciones de Santiago (2017): Rol 34.360-2017.

Sentencia de la Corte Suprema de Chile (2019): Rol N° 31.279-2018

Decisión de Amparo de Consejo para la Transparencia (2018): Rol C67-18 Caratulado Manuel Jofré Figueroa con Municipalidad de Las Condes. Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000020844. Fecha de última consulta: 30 de enero de 2021.

Decisión de Amparo de Consejo para la Transparencia (2018): unifica ROLES C4217-17, C385-18, y C775-18 caratulado Edgardo Dinamarca Toledo con Municipalidad de Concón. Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000036639. Fecha de última consulta: 30 de enero de 2021.

Decisión de Amparo de Consejo para la Transparencia (2019): Rol C5026-18 caratulado Luis Armijo Barrera con Municipalidad de Providencia. Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000025730. Fecha de última consulta: 30 de enero de 2021.

Decisión de Amparo de Consejo para la Transparencia (2020): Rol C3721-20 caratulado Alejandro López con Intendencia Región Metropolitana de Santiago. Disponible en https://jurisprudencia.cplt.cl/cplt/decision.php?id=CPLT000040261. Fecha de última consulta: 30 de enero de 2021.

DOCUMENTOS.-

Consejo para la Transparencia (2017): Oficio N° 2309, que formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628.

Real Academia Española de la Lengua (2016a): Diccionario de la Lengua Española, Tomo VII, Vigésimo Tercera Edición (Edición del Tricentenario), Grupo Editorial Planeta, Argentina, pp. 1326.

Real Academia Española de la Lengua (2016b): Diccionario de la Lengua Española, Tomo XI, Vigésimo Tercera Edición (Edición del Tricentenario), Grupo Editorial Planeta, Argentina, pp. 1910.

Real Academia Española de la Lengua (2016c): Diccionario de la Lengua Española, Tomo XII, Vigésimo Tercera Edición (Edición del Tricentenario), Grupo Editorial Planeta, Argentina, pp. 2314.

Subsecretaria de Prevención del Delito (División de Gestión Territorial) (2019): Orientaciones Técnicas Prevención Situacional tipología sistema de teleprotección. Disponible en http://www.seguridadpublica.gov.cl/media/2019/07/Sistemas-de-Teleproteccion.pdf. Fecha de última consulta: 30 de enero de 2021.

ARTÍCULOS.-

Álvarez, D. (2016): "Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?", en Revista de Derecho Universidad Católica del Norte, Coquimbo. Nº 1, pp. 51-79. Disponible en https://scielo.conicyt.cl/pdf/rducn/v23n1/art03.pdf. Fecha de última consulta: 30 de enero de 2021.

Chacón, A. (2016): "Capacidades Municipales para la Gestión en Seguridad Pública en Chile", en Seguridad Pública en Chile: del fenómeno global a la acción local. Roberto Lagos Flores (Ed.), Ediciones Universidad Tecnológica Metropolitana, Santiago, 1° Edición, pp. 123 – 156. Disponible en http://www.amuch.cl/wp-content/uploads/2016/11/seguridad-publica-montaje-1.pdf. Fecha de última consulta: 30 de enero de 2021.

Figueroa , R. (2013): "El derecho a la privacidad en la jurisdicción de protección", en Revista Chilena de Derecho, Vol. 40, Nº 3, Santiago, pp. 859 – 889. Disponible en https://scielo.conicyt.cl/pdf/rchilder/v40n3/art05.pdf. Fecha de última consulta: 30 de enero de 2021.

Galdon-Clavel, Gemma (2015): "Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas", en EURE Revista Latinoamericana de Estudios Regionales, Santiago, Vol. 41, N°123, pp. 81-101. Disponible en https://scielo.conicyt.cl/pdf/eure/v41n123/art04.pdf. Fecha de última consulta: 30 de enero de 2021.

Herrera, A. (2016): "Ética para la Seguridad Comunal: ¿imperativo u obstáculo? reflexiones sobre su rol humanizante en las tareas de prevención del delito y seguridad local" en Seguridad Pública en Chile: del fenómeno global a la acción local. Roberto Lagos Flores (Ed.), Ediciones Universidad Tecnológica Metropolitana, Santiago, 1° Edición, pp. 51–86. Disponible en http://www.amuch.cl/wp-content/uploads/2016/11/seguridad-publica-montaje-1.pdf. Fecha de última consulta: 30 de enero de 2021.

Lovera, D. (2017): “Privacidad: La Vigilancia en Espacios Públicos”, en En Informe Anual sobre Derechos Humanos en Chile 2017. Tomás Vial Solar (Ed.), Centro de Derechos Humanos, Facultad de Derecho, Universidad Diego Portales; Santiago, pp. 383-417. Disponible en http://www.derechoshumanos.udp.cl/derechoshumanos/images/InformeAnual/2017/9-derecho%20a%20la%20privacidad.pdf. Fecha de última consulta: 30 de enero de 2021.

Malamud, S. (2018): “Videovigilancia y privacidad: Consideraciones en torno a los casos Globos y Drones”, en Revista Chilena Derecho y Tecnología, Volumen 7, N° 2, Santiago, pp. 137-162. Disponible en https://scielo.conicyt.cl/pdf/rchdt/v7n2/0719-2576-rchdt-7-2-00137.pdf. Fecha de última consulta: 30 de enero de 2021.

Nogueira, H. (2004): "Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada", en Revista de Derecho de Valdivia, Volumen XVII, pp. 145 y 146.

_____. (2015): “El Bloque Constitucional de Derechos en Chile, el parámetro de control y consideraciones comparativas con Colombia y México: doctrina y jurisprudencia”, en Estudios Constitucionales, Centro de Estudios Constitucionales de Chile Universidad de Talca, Año 13, Nº 2, pp. 301-350. Disponible en https://scielo.conicyt.cl/pdf/estconst/v13n2/art11.pdf. Fecha de última consulta: 30 de enero de 2021.

Rau, M. (2016): “Seguridad Urbana: el contacto humano y la confianza en espacios de flujos peatonales y vehiculares en el territorio municipal”, en Seguridad Pública en Chile: del fenómeno global a la acción local. Roberto Lagos Flores (Ed.), Ediciones Universidad Tecnológica Metropolitana, Santiago, 1° Edición, pp. 87 – 122. Disponible en http://www.amuch.cl/wp-content/uploads/2016/11/seguridad-publica-montaje-1.pdf. Fecha de última consulta: 30 de enero de 2021.

Viollier, P.y Ortega, V. (2019): “Cuando el Estado hackea: El caso de Operación Huracán”, en Revista Chilena de Derecho y Tecnología, Santiago, Volumen 8, N° 2, pp. 83-110. Disponible en https://scielo.conicyt.cl/pdf/rchdt/v8n2/0719-2584-rchdt-8-2-00083.pdf. Fecha de última consulta: 30 de enero de 2021.

LIBROS.-

Diez - Picazo, L. (2008): Sistema de Derechos Fundamentales, Editorial Aranzadi S.A., Navarra.

Figueroa, R. (2014). Privacidad. Santiago: Universidad Diego Portales

Morris, C. (2013) Cómo Razonan los Abogados, Editorial Limusa,

Rivero Ortega, R. (2002): El Estado Vigilante, Editorial Tecnos, España.

Squella, A. (2019): Derechos Humanos, Editorial UV de la Universidad de Valparaíso, Valparaíso.