ALCALDÍA MUNICIPAL DE CHÍA

SECRETARÍA DE GOBIERNO

030

Chía, de 2019 S.G.

CIRCULAR EXTERNA No. 001

DE: ALCALDÍA MUNICIPAL Y SECRETARÍA DE GOBIERNO

PARA: CIUDADANÍA DEL MUNICIPIO DE CHÍA

ASUNTO: PRECISIONES RESPECTO DE LA NATURALEZA Y ALCANCE DE LAS GRABACIONES OBTENIDAS POR EL CIRCUITO CERRADO DE TELEVISIÓN -CCTV- DEL MUNICIPIO Y SOBRE EL PROCEDIMIENTO PARA LA SOLICITUD Y EVENTUAL ACCESO A GRABACIONES, IMÁGENES Y CAPTURA DE DATOS

1. OBJETIVO

Precisar, dentro del marco legal vigente en esta materia, esto es, las disposiciones de las Leyes 1581 de 2012, 1712 de 2014, 1755 de 2015, y los Decretos 1074 y 1081 de 2015, así como las directrices trazadas por la Corte Constitucional, entre otros pronunciamientos, en la Sentencia T-114 del 3 de abril de 2018, aspectos relacionados con la naturaleza de las grabaciones de video vigilancia realizadas por las cámaras que integran el Circuito Cerrado de Televisión -CCTV- a cargo de la Alcaldía Municipal de Chía, ubicadas en espacios públicos definidos como puntos neurálgicos del municipio, así como el procedimiento para efectuar la solitud de acceso a su contenido por parte de la ciudadanía y usuarios de los servicios prestados por la entidad.

2. ANTECEDENTES Y MARCO NORMATIVO

El artículo 1° de la Carta Política le otorga a Colombia el carácter de un Estado social de derecho, que se organiza en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran, y en la prevalencia del interés general, esto es, en la búsqueda del bien común de la ciudadana y habitantes del territorio.

A su turno, el artículo 2° constitucional establece como fines esenciales del Estado, entre otros, servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo, y para esos efectos prevé que las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, así como para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.

Por su parte, los artículos 15, 10 y 23 de la Constitución Política, consagran los derechos fundamentales individuales de acceso a la información pública y privada y de petición, y señalan que éstas prerrogativas deben ser garantizados por todas las autoridades públicas de conformidad con las leyes que reglamenten su ejercicio, en armonía con el interés general y efectivo cumplimiento de los fines del estado.

Para desarrollar y regular dichas prerrogativas, en cuanto tiene que ver con la facultad que tienen todas las personas a conocer, actualizar y rectificar las informaciones y datos personales que se hayan recogido sobre ellas en bases de datos o archivos, así como para acceder a información pública o privada, el congreso expidió la Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*.

El artículo 3° literal c) de esa norma define el dato personal como *"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*, y señala que las personas naturales o jurídicas, públicas o privadas, que

recopilen y manejen este tipo de información se denominan encargados o responsables del tratamiento de datos. El mismo precepto se refiere al *"tratamiento"* de datos como *"Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Así mismo, el artículo 4° de la Ley 1581 de 2012, establece entre los principios que deben regir el tratamiento de datos personales, el de *"acceso y circulación restringida"*, que debe entenderse como la restricción para el uso y divulgación de la información derivada de este tipo de datos, de tal manera que su utilización sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley, y su contenido, salvo la información pública, no podrá estar disponible en internet u otros medios de divulgación o comunicación masiva, a menos que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados.

La disposición en comento consagra también el principio de *"seguridad"*, según el cual *"La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*.

De otra parte, la norma configura un principio de *"confidencialidad"*, referido al hecho de que *"Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."*

El artículo 5° de la Ley 1581 de 2012, en armonía con el artículo 2.2.2.25.1.1 del Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo, se refiere a los *"datos sensibles"*, vale decir, aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, entre los que se encuentran los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

De acuerdo con el artículo 6° de la Ley 1581 de 2012, los datos sensibles, por regla general, no pueden ser objeto de tratamiento o utilización por parte de las persona o entidades que los obtengan o recopilen, salvo con autorización de su titular, o cuando su manejo y entrega a otras autoridades se requiera para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

A su turno, el artículo 13 de la aludida ley, establece las personas y autoridades a quienes se les puede suministrar la información relativa a datos personales, precisando que la misma sólo puede ser entregada a *i)* sus titulares o representantes, *ii)* a las entidades públicas o administrativas en ejercicio de sus funciones legales, *iii)* por orden judicial, o *iv)* a terceros autorizados por el titular o por la ley.

Finalmente, los artículos 17 y 18 de la Ley 1581 de 2012, atribuyen a los responsables y encargados del tratamiento de datos, deberes respecto de la custodia y manejo de dicha información, así como en relación con el respeto y protección a los titulares de la misma, de los derechos a la intimidad, buen nombre y habeas data.

Dentro de ese contexto normativo, la información, imágenes y datos personales captados a través de sistemas de video vigilancia –SV-, esto es, mediante cámaras de seguridad, adquiere relevancia en la actualidad, pues tanto las personas naturales o jurídicas de carácter particular, como las entidades públicas en todos los niveles, buscan implementar este tipo de herramientas tecnológicas con el fin de garantizar la seguridad de bienes o personas en un lugar determinado, y en el caso de las autoridades administrativas, mejorar y optimizar la prestación de los servicios a su cargo, e incrementar los medios de protección a la ciudadanía, espacios y bienes públicos, con lo cual han venido incrementando su

presencia, al ser considerados como un medio idóneo para realizar el monitoreo y la observación de actividades en escenarios domésticos, empresariales, laborales y públicos.

Resulta entonces necesario señalar que la Real Academia Española de la Lengua RAE[1] define la video vigilancia como la actividad de "***1.*** *f. Vigilancia por medio de un sistema de cámaras fijas o móviles*". A su turno, la Guía de Video vigilancia de la Autoridad Española de Protección de Datos, amplía el concepto señalando las siguientes finalidades:

> *"La video vigilancia generalmente persigue garantizar la seguridad de los bienes y las personas o se utiliza en entornos empresariales con la finalidad de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Ambas finalidades constituyen bienes valiosos dignos de protección jurídica, pero sometidos al cumplimiento de ciertas condiciones. La utilización de medios técnicos para la vigilancia repercute sobre los derechos de las personas lo que obliga a fijar garantías"*[2].

Dicho lo anterior, debe concluirse que en el ámbito territorial, las grabaciones efectuadas a través del Circuito Cerrado de Televisión –CCTV- y demás medios tecnológicos al servicio de la Alcaldía Municipal de Chía, ubicadas en espacios públicos catalogados como puntos neurálgicos y estratégicos del municipio, tienen como finalidades principales: *i)* garantizar la seguridad de los bienes y las personas que habitan, permanecen y/o transitan en los lugares de cobertura de los dispositivos de vigilancia, así como *ii)* contribuir a la prevención del delito y ocurrencia de otras conductas que atenten contra la convivencia, o de hechos que perturben la tranquilidad e integridad física de los habitantes del territorio.

A través de la utilización de los sistemas de video vigilancia, se busca garantizar el cumplimiento de los referidos fines estatales, que corresponden a la misión, naturaleza y funciones de las autoridades y dependencias de la administración municipal, en especial las del Despacho del Alcalde y la Secretaria de Gobierno, actualmente establecidas por el Decreto 40 de 2019, acto administrativo cuyo artículo 38 le atribuye a esa última dependencia, facultades para *"Liderar, orientar y coordinar la formulación de políticas, planes y programas dirigidos a garantizar la convivencia pacífica, el respeto de los derechos humanos, la seguridad ciudadana y la preservación del orden público en el municipio."* (Literal a), competencias que soportan y justifican, el uso proporcionado y racional, por parte del municipio, de los sistemas de video vigilancia a través de cámaras de video vigilancia que efectúan grabaciones de personas y hechos, y capturan imágenes y datos.

Cabe anotar que la utilización del sistema de video vigilancia es uno de los mecanismos más efectivos para dar cumplimiento a las finalidades de la administración en relación proteger la integridad de los bienes y las personas que habitan, permanecen o transitan en las zonas de influencia de las cámaras de seguridad.

3. NATURALEZA DE LAS GRABACIONES CAPTADAS POR EL SISTEMA DE VIDEOVIGILANCIA –SV- DE LA ALCALDÍA MUNICIPAL DE CHÍA

Es preciso resaltar que si bien la Alcaldía Municipal de Chía es una entidad pública, ello no significa que las grabaciones que se efectúen por los medios tecnológicos instalados en distintos puntos del perímetro del municipio sean de naturaleza pública, ni que sobre el acceso a la información que contienen las mismas no pueda imponer la administración municipal restricciones o limitaciones.

Por el contrario, de acuerdo con el marco normativo al que se ha venido haciendo referencia, resulta jurídicamente viable y además necesario, que la Alcaldía, a través de la Secretaría de Gobierno, reglamente el trámite de solicitud y eventual obtención de información, grabaciones, imágenes y datos recopilados a través de los sistemas de video vigilancia, aún más, teniendo en cuenta que el contenido de las mismas puede eventualmente, poner en tensión y riesgo de vulneración, el derecho a la intimidad, buen nombre o *habeas data* de los sujetos que son monitoreados y arriesgar la integridad y aptitud del medio probatorio, en el marco de los procesos judiciales.

[1] Diccionario de la Lengua Española – 23ª Edición. Real Academia de la Lengua. Disponible en: <<https://dle.rae.es/?id=bmtXm9x>>
[2] Guía de Videovigilancia, Agencia Española de Protección de Datos. página 4. Disponible en: <<https://www.prevent.es/Documentacion/guia_videovigilancia.pdf>>

Al respecto, debe señalarse que la Ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*, se ocupó de regular el derecho de acceso a la información pública, así como los procedimientos para el ejercicio y garantía de éste derecho y las excepciones a la publicidad de información.

Es por ello que el artículo 6° de la Ley 1712 de 2014, se refiere al concepto de información, como un conjunto organizado de datos o imágenes contenido en cualquier documento, incluidos los que se obtiene o almacenan en medios tecnológicos o de captura en video, que los sujetos y entidades encargadas o responsables del tratamiento de datos generan, obtienen, adquieren, transforman o controlan, diferenciándola de la noción de *"información pública"*, al catalogarla como la obtenida y utilizada por entidades legalmente concebidas como públicas, e incluso, la norma alude a la *"información pública clasificada"*, esto es, aquella que estando en poder o custodia de un entidad o autoridad pública,

> *"...pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley."*. (Literal c)

La misma disposición alude a la *"información pública reservada"*, como aquella que *"...estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley."* (Literal d)

En armonía con estas definiciones de orden legal, la honorable Corte Constitucional, entre otros pronunciamientos, mediante la sentencias T-729 del 5 de septiembre de 2002, Magistrado Ponente Eduardo Montealegre Lynnet, T-407 del 31 de mayo de 2012, Magistrado Ponente Mauricio Gonzales Cuervo, y T-114 del 3 de abril de 2018, Magistrado Ponente: Carlos Bernal Pulido, ha sentado su postura en relación con la protección del derecho a la intimidad y buen nombre, y su correlación con el ejercicio del derecho de petición, en la modalidad de solicitudes de información, al abordar el contenido, clasificación y alcance del acceso a la información, en especial aquella obtenida mediante Circuitos Cerrados de Televisión –CCT-, a través de sistemas de video vigilancia –SV-.

Para tal efecto, dentro de la sentencia T-114 de 2018, la corporación acude a la definición doctrinaria del Circuito Cerrado de Televisión –CCTV-, como un:

> *"...conjunto de componentes directamente entrelazados, que crean un circuito de imágenes y, se les denomina circuito cerrado porque a diferencia de la televisión tradicional, este solo permite un acceso limitado y restringido del contenido de las imágenes a algunos usuarios. En efecto, el CCTV puede estar compuesto de una o varias cámaras de vigilancia conectadas a uno o más monitores o televisores, los cuales reproducen imágenes capturadas; estas imágenes pueden ser, simultáneamente, almacenadas en medios analógicos o digitales, según lo requiera el usuario."*

Igualmente, la providencia a la que se viene haciendo referencia, indicó que la naturaleza de la información recopilada por los sistemas de vigilancia –SV-, se determina a partir del lugar en el cual se encuentran instaladas las cámaras de seguridad que recogen y captan la información, para lo cual distinguió entre medios ubicados en: *i)* lugares privados, *ii)* establecimientos privados abiertos al público o, *iii)* establecimientos y/o instituciones públicas.

Y a partir de la anterior clasificación de los espacios privados o públicos donde se captura la información por medio de cámaras y SV, la Corte precisa que:

> *"(...) la información captada por las cámaras de seguridad instaladas en el domicilio de una persona es indiscutiblemente privada. De igual manera, la información captada por los equipos de vigilancia instalados en establecimientos privados abiertos al público también tienen la naturaleza de privada, debido a que continuamente se encuentra registrando información de las personas que frecuentan este tipo de lugares.*

Cosa distinta, ocurre con los dispositivos de seguridad instalados en establecimientos y/o instituciones públicas, debido a que, según la tipología establecida por la jurisprudencia de la Corte Constitucional, está captando imágenes en un lugar abierto al público"[3].

Como ya se indicó, esta postura se encuentra ligada con la interpretación y tesis que la Corte Constitucional había expuesto en la sentencia T-407 de 2012, mediante la cual definió los espacios en los cuales las personas realizan sus actividades cotidianas en las diferentes esferas de su desarrollo -personal, familiar, social y gremial-, señalando que además de la calle y del domicilio privado, calificados como espacio público y privado, respectivamente, existen unos espacios que por sus características propias y particulares, escapan a dichas definiciones, habida cuenta que dadas sus condiciones especiales, comparten características de las dos categorías antes definidas, como lo son las oficinas, los centros educativos, los colegios y las universidades, los restaurantes, los bancos y entidades privadas o estatales con acceso al público, los almacenes y centros comerciales, los cines y teatros, los estadios, los juzgados y tribunales, entre otros.

Es allí donde, de acuerdo con el pronunciamiento de la Corte, surge el concepto de espacios denominados *"semi-privados"* y *"semi-públicos"*, entendiendo los segundos como aquellos:

"...lugares de acceso relativamente abierto en los que diferentes personas se encuentran en determinado momento para realizar cierta actividad puntual dentro de un espacio compartido: un cine, un centro comercial, un estadio. A diferencia de los espacios públicos, en estos lugares puede exigirse determinada conducta a las personas y eventualmente requerirse condiciones para la entrada (...).

Aunque son sitios cerrados, hay gran flujo de personas y mayor libertad de acceso y movimiento, por lo cual las restricciones a la intimidad son tolerables por cuestiones de seguridad y por la mayor repercusión social de las conductas de las personas en dichos espacios"[4]. (resaltado extratexto)

De lo dicho por la Corte, puede concluirse que si bien la Alcaldía Municipal es una entidad estatal, de naturaleza pública, no puede predicarse lo mismo del espacio físico en el cual se desarrollan sus actividades misionales, pues como ya se vio, los lugares donde ello ocurren pueden considerarse en general, como espacios semi-públicos, que en tal virtud, permiten la exigencia de ciertos comportamientos, reglas de conducta e incluso, imponer algunas limitaciones a las libertades individuales de las personas que los frecuentan y/o permanecen en esos lugares, para lo cual resulta pertinente que la administración implemente sistemas de video vigilancia -SV-, que en los términos empleados por esa corporación, comportan *"... mayor tolerancia al control y vigilancia sobre las conductas de las personas con el fin de evitar y prevenir situaciones de riesgo ya que las repercusiones sociales son mayores"*[5].

En este orden de ideas, en el marco de las citadas disposiciones legales, las grabaciones, imágenes y captura de datos realizadas en el perímetro del municipio, a través de las cámaras de seguridad que hacen parte de los sistemas de video vigilancia SV, ubicadas en lugares previamente catalogados como neurálgicos y estratégicos en materia de seguridad y prevención del delito, corresponden, según el ya mencionado literal c) del artículo 6° de la Ley 1712 de 2014, a *"información pública clasificada"*, y de acuerdo con la jurisprudencia de la Corte Constitucional también analizada en esta circular, esos datos son recopilados y obtenidos en *"espacios semi públicos"*.

En efecto, si bien las grabaciones, imágenes y captura de datos personales en estos espacios eventualmente podría afectar los derechos fundamentales individuales a la intimidad, buen nombre, habeas data o dignidad de las personas que son monitoreadas y observadas través del CCTV con que cuenta el municipio, tal detrimento se justifica y por tanto, resulta razonable y proporcionado, porque su finalidad primordial es la de garantizar la seguridad y protección de las personas y bienes que residen en el municipio, y reducir la

[3] Corte Constitucional de Colombia. T. 114 de 2018. Magistrado ponente CARLOS BERNAL PULIDO. Bogotá, D.C., tres (3) de abril de dos mil dieciocho (2018).
[4] Idem
[5] Ibidem

ocurrencia de conductas que puedan constituir delitos, o atentar contra la convivencia pacífica de los ciudadanos.

Ahora bien, la administración municipal, en cabeza del Alcalde y la Secretaría de Gobierno, como dependencias encargadas y responsables del manejo de dichos datos, deben asumir la responsabilidad y deberes que consagra la Ley 1581 de 2012, por el uso y tratamiento de la información recolectada por este medio tecnológico, y por tal razón, resulta indispensable que el acceso a los datos e información personal, en la modalidad de consulta, solicitud de copias o información, de que trata la Ley 1755 de 2015, obtenidos a través de los SV, se restrinja con el ánimo de preservar los derechos a la intimidad, buen nombre, habeas data y dignidad de sus titulares, y se suministre sólo a las personas o autoridades habilitadas por el mencionado artículo 13 de la norma que regula la protección de datos, esto es, a quienes acrediten tal titularidad, a las entidades públicas en ejercicio de sus funciones, o a las autoridades judiciales, cuando medie orden que así lo solicite.

Al respecto, el artículo 18 de la Ley 1712 de 2014, como quedó corregido por el artículo 1° del Decreto 2199 de 2015, establece que la información pública clasificada, esto es, referida a datos privados o personales, puede ser denegada para su acceso o consulta a terceros, por acarrear una posible vulneración de los derechos de sus titulares, al prever que:

> *"**Información exceptuada por daño de derechos a personas naturales o jurídicas.** Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:*
>
> *a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011."*

Por su parte el artículo 2.1.1.4.1. del Decreto 1081 de 2015, Único Reglamentario del Sector Presidencia de la República, reitera lo siguiente:

> *"**Excepciones al Derecho fundamental de acceso a la información pública.** Los sujetos obligados garantizarán la eficacia del ejercicio del derecho fundamental de acceso a la información pública, sin perjuicio de su facultad de restringirlo en los casos autorizados por la Constitución o la ley, y conforme a lo previsto en los artículos 18 y 19 la Ley 1712 de 2014, en consonancia con las definiciones previstas en los literales c y d del artículo 6°, de la misma."*

En conclusión, el tratamiento de los datos personales obtenidos a través de las cámaras de seguridad que hacen parte del SV del municipio de Chía, que permiten la grabación de videos, captura de imágenes y datos, especialmente en cuanto a tiene que ver con su acceso y suministro como consecuencia del ejercicio del derecho de petición, debe ser regulado por la Alcaldía, a través de la Secretaría de Gobierno, con estricta sujeción a las disposiciones legales que restringen y limitan su entrega a personas distintas a los titulares de los datos, las entidades públicas en cumplimiento de sus funciones o las autoridades judiciales, previo requerimiento.

4. ALCANCE Y LIMITACIONES PARA EL TRATAMIENTO DE LAS GRABACIONES, IMÁGENES Y CAPTURA DE DATOS EFECTUADAS POR EL CCTV

Aclarado el punto anterior, dentro del marco normativo y jurisprudencial ya reseñado, pero además, siguiendo los lineamientos de la Guía denominada *"Protección de Datos Personales en Sistemas de Videovigilancia"* expedida en 2016 por la Superintendencia de Industria y Comercio, se advierte que el uso de los mencionados sistemas en las actividades de monitoreo y observación:

> *"...implican la recopilación de imágenes de personas, es decir, de datos personales de acuerdo con la definición contenida en el literal c) del artículo 3 de la Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", entendido como "(c)ualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*

En consecuencia, en el manejo o Tratamiento de esos datos se deben observar los principios establecidos en dicha norma, esto es, legalidad, finalidad, libertad, calidad o veracidad, seguridad, confidencialidad, acceso y circulación restringida, y transparencia, así como las demás disposiciones contenidas en el Régimen General de Protección de Datos Personales."[6]

La guía a la que se acaba de hacer referencia señala, con fundamento en la definición legal del tratamiento de datos personales efectuado por el artículo 3° de la Ley 1581 de 2012, a que ya se hizo referencia en esta circular externa, que: ***"En el caso de las imágenes de personas determinadas o determinables, operaciones como la captación, grabación, transmisión, almacenamiento, conservación, o reproducción en tiempo real o posterior, entre otras, son consideradas como Tratamiento de datos personales, y en consecuencia,*** *se encuentran sujetas al Régimen General de Protección de Datos Personales."*

Con fundamento en lo anterior, puede concluirse que las grabaciones, imágenes y captura de datos realizadas por el sistema de video vigilancia –SV- al servicio de la Alcaldia Municipal de Chía, que se opera a través del CCTV con que cuenta el municipio, tienen el carácter de datos personales, que como se ha indicado, se incorpora a la noción de *"información pública clasificada"*, por lo que se reitera que las dependencias administrativas encargadas de su obtención y recopilación a través del CCTV, adquieren el carácter de responsables del tratamiento de los mismos, asumiendo los deberes y responsabilidades consagrados en los artículos 17 y 18 de la Ley 1581 de 2012.

Al respecto, debe recordarse que la manipulación de estos datos puede afectar los derechos fundamentales a la intimidad, buen nombre, habeas data o dignidad de las personas que son observadas o monitoreadas a través de dichos medios tecnológicos, prerrogativas que si bien se ven razonablemente limitadas en aquellas espacios semi públicos a los que se refiere la Corte Constitucional, no pueden ser desconocidos totalmente, o injustificadamente amenazados con el actuar de la administración, circunstancias que ocurrían en el evento de permitir el acceso incondicional e ilimitado, por parte de cualquier particular, a las grabaciones del CCTV que opera el municipio a través de cámaras de seguridad.

Vale la pena puntualizar que los derechos constitucionales fundamentales a proteger en desarrollo de las grabaciones, imágenes y captura de datos personales efectuadas a través de los SV con que cuenta la Alcaldía de Chía, son esencialmente los siguientes:

- Derecho a la intimidad y privacidad: Entendido por la jurisprudencia nacional como *"la existencia y goce de una órbita reservada para cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural"*[7].

- Derecho a la imagen: Derecho fundamental y autónomo, íntimamente relacionado con la dignidad humana y concretado en tres aspectos, a saber: *"(i) la autodefinición del sujeto a partir de sus características físicas, esto es, cómo quiere verse y ser percibido por los demás; (ii) la potestad de la persona de decidir qué parte de su imagen será difundida y qué parte no, ya sea de manera onerosa o gratuita (aspecto positivo), así como la posibilidad de prohibir la obtención, utilización o reproducción no autorizada de la imagen de una persona (aspecto negativo); y (iii) la imagen social"*[8].

- Derecho al habeas data, al que la corte define, entre otras, en la sentencia T-077 del 2 de marzo de 2018, como *"un derecho fundamental autónomo que comprende las siguientes tres facultades: (i) el derecho a conocer las informaciones que a su titular se refieren; (ii) el derecho a actualizar tales informaciones; y (iii) el derecho a rectificar las informaciones que no correspondan a la verdad. En la sentencia T-527 de 2000 indicó que el titular de la información que obra en una base de datos cuenta con el mecanismo de la rectificación, que implica la concordancia del dato con la realidad, y el de actualización, que hace referencia a la vigencia del dato de tal manera que no se*

[6] Guía de Protección de Datos Personales en Sistemas de Videovigilancia. Superintendencia de Industria y Comercio. Pág. 4.
[7] Corte Constitucional. M.P. Jorge Pretelt. C - 881 de 2014. Bogotá D. C., diecinueve (19) de noviembre de dos mil catorce (2014).
[8] Corte Constitucional. M.P. José Reyes T - 454 de 2018. Bogotá D.C., veintidós (22) de noviembre de dos mil dieciocho (2018).

muestren situaciones carentes de actualidad. Mediante la Sentencia T-729 de 2002, añadió a la definición de este derecho la facultad que tiene el titular de datos personales, de exigir la certificación de la información y la posibilidad de limitar su divulgación, publicación o cesión."

- Derecho a la honra y buen nombre, que de acuerdo o con la jurisprudencia que ha expedido la Corte Constitucional, recientemente a través de la sentencia T-117 del 6 de abril de 2018, como *"...el concepto que se forman los demás sobre cierta persona. De esta manera, la jurisprudencia de esta Corte ha definido el derecho al buen nombre como "la reputación, o el concepto que de una persona tienen los demás" y "la estimación o deferencia con la que, en razón a su dignidad humana, cada persona debe ser tenida por los demás miembros de la colectividad que le conocen y le tratan".*

- Derecho a la Dignidad Humana: Especialmente en lo relativo a una de las facetas de su funcionalidad, determinada por la Corte Constitucional como la *"intangibilidad de los bienes no patrimoniales, de la integridad física y moral o, en otras palabras, la garantía de que los ciudadanos puedan vivir sin ser sometidos a cualquier forma de trato degradante o humillante"*[9].

De otra parte, conviene hacer referencia en la presente circular al tema relacionado con el manejo y custodia de las grabaciones, imágenes y captura de datos efectuadas por los sistemas de video vigilancia, cuando esta información tiene el propósito de ser usada en el marco de un proceso judicial, toda vez que de acuerdo con el artículo 275 del Código de Procedimiento Penal, la misma se considera como elemento material probatorio o evidencia física[10].

Es así como la norma en cita señala que:

> ***"Artículo 275**. Elementos materiales probatorios y evidencia física. Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes: (...)*
>
> *f) Los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público".*

En consecuencia, los elementos materiales de prueba y evidencias físicas recaudadas a través de los sistemas de video vigilancia del municipio, deben cumplir además con los procedimientos de *"cadena de custodia"* adelantados por la autoridad con funciones de Policía Judicial, para su debida recolección, preservación e introducción al proceso penal.

A tal efecto, de acuerdo con la jurisprudencia de la Corte Suprema de Justicia, debe entenderse como *"cadena de custodia"*:

> *"...el conjunto de procedimientos encaminados a asegurar y demostrar la autenticidad de los elementos materiales probatorios y evidencia física. Está conformada, entonces, por los funcionarios y personas bajo cuya responsabilidad se encuentren elementos de convicción durante las diferentes etapas del proceso; se inicia con la autoridad que recolecta los medios de prueba desde el momento en que se conoce la conducta punible, y finaliza con el juez de la causa y los diferentes servidores judiciales. Así, al momento de recolectar las evidencias -llamadas a convertirse en prueba en el juicio oral- es necesario registrar en la correspondiente acta la naturaleza del elemento recogido, el sitio exacto del hallazgo y la persona o funcionario que lo recogió, así como los cambios que hubiere sufrido en su manejo"*[11].

---

[9] Corte Constitucional. M.P. Luis Vargas C - 143 de 2015. Bogotá D.C., seis (6) de abril de dos mil quince (2015).
[10] Entendidos como cualquier objeto, instrumento o medio de conocimiento conducente al descubrimiento de la verdad, como son huellas, marcas o rastros de origen físico, químico, biológico o electrónico, perceptible a través de los sentidos o mediante la utilización de tecnología forense, cuyo análisis proporciona las bases científicas o técnicas para encaminar la investigación penal, lograr la identificación del autor o autores, y así confirmar o descartar la comisión de una conducta punible y la reconstrucción de los hechos. Manual del Sistema de Cadena de Custodia. Fiscalía General de la Nación. 2018.
[11] Corte Suprema de Justicia. Sala de Casación Penal. Sentencia 35127 de abril 17 de 2013. Magistrado Ponente. Dr. José Luis Barceló Camacho.

Adicionalmente, de conformidad con el *"Manual del Sistema de Cadena de Custodia"*, expedido en 2018, por la Fiscalía General de la Nación, este proceso se considera como el pilar fundamental para el hallazgo, recolección, embalaje, transporte, análisis y almacenamiento de los Elementos Materiales Probatorios y Evidencia Física (EMP y EF).

De acuerdo con dicho manual, la *"cadena de custodia"* está a cargo, de manera exclusiva y a prevención, de la policía judicial o quien haga sus veces, autoridades que deben dar inicio a los procedimientos anteriormente señalados, y tiene como propósito la garantía de autenticidad y capacidad demostrativa de dichos elementos, mientras que la autoridad competente ordena su disposición final.

Para tal fin, señala el manual que en desarrollo de los procedimientos de *"cadena de custodia"*, se deberá dar estricta observancia a los siguientes principios[12]:

a) Autenticidad
b) Capacidad demostrativa
c) Identidad
d) Integridad
e) Preservación
f) Seguridad
g) Almacenamiento
h) Continuidad
i) Registro

Igualmente, dentro del procedimiento de *"cadena de custodia"*, el funcionario de policía judicial encargado de dichas actividades debe ceñirse a los protocolos y condiciones de bioseguridad y protección y actuar conforme a los lineamientos que para llevar a cabo ese trámite han sido establecidos en la Ley 906 de 2004, el *"Manual Único de Policía Judicial"* y el *"Manual del Sistema de Cadena de Custodia"*.

Bajo éstas circunstancias, debe señalarse que no es posible para la Alcaldía Municipal-Secretaria de Gobierno, realizar la entrega del contenido de las grabaciones, imágenes o captura de datos realizadas por el sistema de video vigilancia a cargo de la administración, a los particulares o ciudadanía en general, cuando estos hayan sido obtenidos por orden de autoridad judicial o deban ser incorporados a un proceso, como quiera que dichos terceros no cuentan con la titularidad ni condición de idoneidad para fungir como autoridad de Policía Judicial, y por ende, tampoco poseen los conocimientos técnicos – científicos indispensables para adelantar los procedimientos de *"cadena custodia"* anteriormente expuestos, por lo cual, permitir el manejo de dichos elementos de prueba o evidencias físicas por parte de particulares, puede poner en riesgo la autenticidad de la prueba y su preservación, derivando en una eventual inadmisibilidad o invalidez del medio de prueba dentro del proceso judicial.

Por lo anteriormente expuesto, se hace necesario que la Administración establezca unas pautas y protocolo mínimo para que, mediante el ejercicio del derecho de petición de información o consulta, se autorice el acceso al material documental, captado mediante grabaciones, imágenes y captura de datos, por el sistema de video vigilancia –SV- que administra y opera el municipio a través de cámaras de seguridad enlazadas mediante un Circuito Cerrado de Televisión –CCTV-, aclarando que en cualquier caso, y por expresa disposición legal, para el tratamiento de datos personales, en relación con su manejo, reproducción, consulta o entrega a personas distintas al titular de los mismos, debe mediar orden judicial o requerimiento de autoridad administrativa en ejercicio de sus competencias.

5. PAUTAS Y PROTOCOLO PARA LA CONSULTA DEL MATERIAL GRABADO POR EL SISTEMA DE VIDEOVIGILANCIA DE LA ALCALDÍA MUNICIPAL DE CHÍA

5.1. ¿Quiénes pueden consultar el Sistema de Videovigilancia a cargo de la Alcaldía Municipal y al servicio del municipio?

De conformidad con las consideraciones expuestas, y en el marco de la normatividad vigente que regula la materia, a la cual se ha hecho referencia en esta circular externa,

[12] FISCALÍA GENERAL DE LA NACIÓN. Manual del Sistema de Cadena de Custodia. 2018. Pág 11.

solamente podrá emitirse y/o entregarse copia del material grabado, imágenes o captura de datos, a personas distintas a sus titulares -debidamente acreditados-, en el evento que se requiera como prueba dentro de un proceso adelantado por autoridad civil, penal, administrativa, fiscal o disciplinaria competente, siempre y cuando medie orden judicial que así lo solicite, o requerimiento de la entidad pública en ejercicio de sus competencias administrativas (artículos 6° y 13 de la Ley 1581 de 2012).

Así las cosas, en el evento en que algún habitante o transeúnte del municipio requiera el acceso a las grabaciones, imágenes o datos capturados a través del sistema de video vigilancia –SV- del municipio, con el propósito de que dicho material obre como prueba dentro de un proceso civil, penal, fiscal o disciplinario podrá solicitar a la Secretaría de Gobierno[13], en los términos previstos por la Ley 1755 de 2015, en concordancia con los artículos 24 y 25 de la Ley 1712 de 2014, y 2.1.1.3.1.1. del Decreto 1081 de 2015, que realice el *back up* o copia de seguridad en los mecanismos de almacenamiento (servidores y archivos) de datos con los que cuenta el SV, para que la misma sea puesta a disposición de la autoridad competente que la requiera, indicando con precisión la información relevante de la institución y/o funcionario de destino, así como la descripción de las circunstancias de tiempo, modo y lugar en las que ocurrieron los hechos, de conformidad con lo establecido en el numeral 5.2. del presente documento.

Lo anterior con el fin de delimitar tanto espacial, como temporalmente el contenido objeto del *backup*, siendo la Secretaría de Gobierno, la única dependencia autorizada para responder la solicitud de acceso, en los términos del numeral 1° del artículo 15 de la Ley 1755 de 2015, en armonía con el artículo 26 de la Ley 1712 de 2014, como fue corregido por el artículo 4° del Decreto 1494 de 2015, y el artículo 2.1.1.3.1.4. del Decreto 1081 de 2015, y de encontrarlo pertinente, de remitir a la autoridad competente el contenido del material.

Cuando se trate de solicitudes de acceso a grabaciones, imágenes o captura de datos obtenidos a través del SV del municipio, que tengan la calidad de información pública clasificada o reservada, presentadas por personas distintas a sus titulares, la respuesta por parte de la Secretaría de Gobierno se emitirá en los términos del artículo 2.1.1.4.4.1. del Decreto 1081 de 2015.

De otra parte, también se consideran legítimamente interesados en la consulta de las grabaciones, los entes y organismos de control interno y externo, las autoridades judiciales y de policía y las entidades públicas en ejercicio de sus competencias.

Deberá tenerse en cuenta que por políticas de seguridad y en cumplimiento a las recomendaciones emitidas por la Superintendencia de Industria y Comercio, a través de la *"Protección de Datos Personales en Sistemas de Videovigilancia"*, las grabaciones e imágenes obtenidas a través de las cámaras de seguridad que componen los SV operados y administrados por la Alcaldía Municipal de Chía, cuentan con un término máximo de almacenamiento en los servidores y de permanencia en los archivos custodiados por la entidad, que será establecido por la Secretaría de Gobierno con arreglo a la ley, por lo cual no se podrá facilitar el acceso a los mismos por fuera de dicho término.

En ningún caso la Alcaldía Municipal de Chía certificará las grabaciones o imágenes grabadas por los SV a cargo de la administración, ni realizará manifestación alguna respecto de su contenido.

5.2. ¿Cómo acceder a la consulta de los Sistemas de Videovigilancia de la Alcaldía Municipal de Chía?

Las personas que se encuentren incluidas en el numeral anterior y cumplan con los requisitos establecidos en la presente circular, pueden solicitar la consulta de las grabaciones, imágenes o captura de datos obtenidas a través de las cámaras de seguridad que hacen parte de los sistemas de video vigilancia –SV- del municipio, y son operados mediante Circuito Cerrado de Televisión –CCTV., para lo cual, a efectos de su seguimiento y control, el Despacho del Alcalde y la Secretaría de Gobierno encuentran necesario que la

[13] Como encargada de liderar, orientar y coordinar la formulación de políticas, planes y programas dirigidos a garantizar la convivencia pacífica, el respeto de los derechos humanos, la seguridad ciudadana y la preservación del orden público en el municipio, de conformidad con el numeral 1 del artículo 38 del Decreto 40 de 2019.

misma se efectúe mediante solicitud escrita dirigida a ésta última dependencia (correo electrónico y/u oficio radicado en la Dirección Centro de Atención al Ciudadano), indicando como mínimo la siguiente información:

a) Nombre e identificación del solicitante.

b) Dirección de notificación, indicando un correo electrónico como medio de comunicación.

c) Descripción del motivo de la solicitud de acceso a la grabación o imagen, con indicación del interés particular y/o legitimación que le asiste para conocer el contenido del material.

d) Descripción sucinta de las condiciones de tiempo (incluyendo año, mes, día y hora), modo y lugar en las que presuntamente ocurrieron los hechos o que motivan la solicitud de la grabación o imagen en la que se tiene interés para su acceso.

e) Información de la entidad, institución pública o autoridad judicial a la cual se deberá remitir el material, indicando datos de contacto del funcionario encargado del proceso o trámite en virtud del cual se requiere la grabación o imagen solicitada.

f) Datos generales de la investigación, proceso, radicación o trámite que motiva la solicitud.

El solicitante podrá aportar los documentos adicionales que considere pertinentes, pero en los términos de los artículos 15 y 17 de la Ley 1755 de 2015, la Secretaría de Gobierno se encuentra facultada para verificar que la petición reúna los requisitos mínimos previstos en el numeral 5.2 de la presente circular, necesarios para iniciar el trámite de estudio y decisión, y de ser el caso, para requerir al interesado a fin de aporte dichos soportes, de manera que el término de respuesta sólo se computara una vez se reúnan tales formalidades mínimas.

6. CONSIDERACIÓN FINAL

Se recuerda que la seguridad y la prevención del delito dentro del municipio es responsabilidad conjunta las autoridades y de sus habitantes, por lo cual se exhorta a la ciudadanía en general a mantener las precauciones necesarias para el cuidado de sus efectos personales, bienes e integridad personal, según sea el caso.

Sin otro particular,

Cordialmente,

LEONARDO DONOSO RUIZ
Alcalde

CORONEL (R) JOSÉ WILLIAM ARIAS GARCÍA
Secretario de Gobierno

Proyectó: Fernando Blanco Mojica- Profesional Especializado.
Revisó: Coronel (R) José William Arias García – Secretario de Gobierno
Revisó: Luz Aurora Espinoza Tobar- Jefe de la Oficina Asesora Jurídica
Revisó: Álvaro Ardila Mora- Profesional Especializado OAJ