Industria y Comercio
SUPERINTENDENCIA

PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA

Imagen: www.pixabay.com - WDnet Studio

MINCOMERCIO
INDUSTRIA Y TURISMO

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA

TABLA DE CONTENIDO

INTRODUCCIÓN

Los Sistemas de Videovigilancia[1] (SV) o cámaras de seguridad implementadas con la finalidad de garantizar la seguridad de bienes o personas[2] en un lugar determinado 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.

Estas tareas de monitoreo y observación realizadas a través de los SV, 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[3].

Por lo anterior, es importante brindar orientación a quienes implementen SV para que adecúen el uso de los mismos a las disposiciones que regulan la protección de datos personales. Es así como a través de esta guía se precisan algunos aspectos que deberán ser tenidos en cuenta para garantizar la protección de los derechos de los Titulares[4] de información cuyas imágenes son captadas mediante SV.

1. "*Vigilancia a través de un sistema de cámaras, fijas o móviles*", disponible en http://dle.rae.es/?id=bmtXm9x, Diccionario de la Real Academia de la Lengua Española, Edición del Tricentenario.

2. Concepto No. 13-102526 emitido por la Oficina Asesora Jurídica de la Superintendencia de Industria y Comercio, junio 24 de 2013, haciendo referencia a la Guía de Videovigilancia de la Agencia Española de Protección de Datos, página 4.

3. Ley 1581 de 2012 y sus decretos reglamentarios.

4. Ley 1581 de 2012, artículo 3, literal f): "***Titular:*** *Persona natural cuyos datos personales sean objeto de Tratamiento*".

1. ¿A QUIÉNES APLICA ESTA GUÍA?

Esta guía está dirigida (i) a las personas, compañías u organizaciones que utilizan SV recolectando datos personales, ya sea en calidad de Responsables[5] o Encargados[6] del Tratamiento de datos personales, por medio de cámaras, videocámaras, análogas o digitales, cámaras IP o mini-cámaras, circuitos cerrados de televisión (CCTV) y, en general, cualquier medio por el cual se realice el Tratamiento[7] de imágenes de Titulares de datos personales, en especial con fines de vigilancia, para orientarlos en el cumplimiento de sus deberes en materia de protección de datos personales, y (ii) a los Titulares de la información, para que tengan conocimiento de cómo ejercer sus derechos frente a los primeros, garantizando así el respeto por sus derechos fundamentales a la intimidad, al buen nombre y a la protección de datos personales, consagrados en el artículo 15 de la Constitución Política a partir del cual se desarrolla el derecho de habeas data en Colombia.

Las grabaciones que se realicen (i) dentro del ámbito exclusivamente personal o doméstico, (ii) con fines periodísticos, o (iii) que tengan como finalidad la seguridad nacional del Estado, no están cobijadas por lo señalado en esta guía.

2. ¿QUÉ ES CONSIDERADO COMO TRATAMIENTO DE IMÁGENES?

El Tratamiento de datos personales ha sido definido como "***(c)ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión***" [8]. 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.

5. Ibídem, literal e): "Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos".

6. Ibídem, literal d): "Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento".

7. Ibídem, literal g): "Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión".

8. Ibídem.

3. ¿QUÉ IMPLICACIONES TIENE SER EL RESPONSABLE Y/O ENCARGADO DEL TRATAMIENTO?

El Responsable del Tratamiento es, por definición, la persona natural o jurídica que decide sobre la base de datos y/o el Tratamiento de los datos. Es por esto que la ley ha dispuesto una serie de obligaciones[9] a su cargo, en particular, para garantizar la protección de los derechos de los Titulares de información respecto de la recolección, almacenamiento, uso y disposición de sus datos personales, en este caso, de su imagen.

El Encargado del Tratamiento es un tercero, persona natural o jurídica distinta del Responsable, que trata los datos personales por cuenta de este. Para mayor claridad, en los casos de videovigilancia, cuando la implementación de los SV se realiza por intermedio de un tercero, como son las empresas de vigilancia y seguridad privada que hacen uso, entre otros, de medios tecnológicos para la prestación de su servicio, estos terceros tienen la calidad de Encargados del Tratamiento y su cliente - llámense copropiedad, propietario de un establecimiento de comercio, empresa, etc. - la de Responsable del mismo.

Como ocurre con los Responsables del Tratamiento, los Encargados tienen unos deberes[10] señalados en la ley y están obligados a cumplir lo dispuesto en el Régimen General de Protección de Datos Personales.

Los Responsables del Tratamiento deben tener siempre en cuenta que no por el hecho de contratar a un tercero - Encargado - se pueden sustraer de sus obligaciones, ya que son los primeros llamados a garantizar que el Tratamiento de los datos personales se realice con arreglo a los principios establecidos en la ley y respete los derechos de los Titulares.

4. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

De acuerdo con el principio de libertad, que rige el Tratamiento de datos personales, "***(e)l Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular***"[11] . Así, por regla general se requiere que el Titular autorice el Tratamiento de sus datos personales. Es por esto que se deben establecer los mecanismos para obtener la autorización de los Titulares que se encuentran dentro de un área de videovigilancia, teniendo en cuenta para ello que el consentimiento se puede manifestar (i) por escrito, (ii) de forma oral, o (iii) mediante conductas inequívocas[12].

9. Ibídem, artículo 17.

10. Ibídem, artículo 18.

11. Ibídem, artículo 4, literal c).

12. Decreto Único 1074 de 2015, artículo 2.2.2.25.2.5.

Ya que los SV pueden implementarse en lugares como establecimientos de comercio, copropiedades, edificios, centros comerciales y parqueaderos, entre otros, en todos los casos se debe informar a los Titulares de datos personales que se encuentran en una zona de videovigilancia y obtener su autorización para el Tratamiento de los mismos. Para ello, se pueden utilizar señales o avisos distintivos en las zonas de videovigilancia, principalmente en las zonas de ingreso a los lugares que están siendo vigilados y monitoreados y al interior de estos. Incluso, se pueden emplear anuncios de audio, en los casos en que sea posible (por ejemplo en bancos, centros comerciales, grandes superficies, etc.). En los casos en que se realice grabación de audio también se debe informar sobre dicha situación a los Titulares.

Las señales o avisos implementados deben, como mínimo, cumplir con el contenido de un aviso de privacidad, a saber:

- Incluir información sobre quién es el Responsable del Tratamiento y sus datos de contacto.
- Indicar el Tratamiento que se dará a los datos y la finalidad del mismo.
- Incluir los derechos de los Titulares.
- Indicar dónde está publicada la Política de Tratamiento de la Información.

Adicionalmente, el aviso debe ser visible y legible teniendo en cuenta el lugar en el que opere el SV, por ejemplo, las señales en zonas de tránsito de vehículos, como los parqueaderos, deben ser apropiadas para informar a los conductores sobre el uso de las cámaras en dicha zona. Las señales no deben afectar la seguridad de peatones o conductores.

El uso de la señal o aviso no exime del cumplimiento de las demás obligaciones contempladas por el Régimen General de Protección de Datos Personales para los Responsables y Encargados del Tratamiento.

5. FINALIDAD DE LOS SISTEMAS DE VIDEOVIGILANCIA (SV)

Los SV son considerados como intrusivos de la privacidad al involucrar herramientas como el monitoreo y la observación de las actividades que realizan las personas a lo largo del día. Por estas razones, antes de tomar la decisión de implementar SV se debe tener en cuenta la necesidad de utilizarlos y considerar si esa necesidad se suple con la implementación de los mismos o si existen otros mecanismos que se puedan utilizar y que generen un menor impacto en la privacidad de las personas.

Lo anterior guarda relación directa con el principio de finalidad, que también rige el Tratamiento de datos personales, el cual impone que el fin perseguido con dicho Tratamiento sea legítimo en relación con la Constitución y la ley y que tenga un propósito específico, explícito e informado.

Así las cosas, de acuerdo con la normativa vigente, los desarrollos jurisprudenciales y los estándares internacionales en la materia, el principio de finalidad implica (i) un ámbito temporal, es

decir, que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la finalidad para la cual se han recolectado, y (ii) un ámbito material, que exige que los datos recaudados sean solo los necesarios para cumplir las finalidades perseguidas, lo que implica que los mismos se limiten a los que resulten adecuados, pertinentes y acordes con las finalidades para las cuales fueron recolectados.[13]

Los datos recaudados, en este caso, las imágenes, sólo podrán ser utilizadas para la (s) finalidad (es) previamente establecida (s). En caso de que las finalidades cambien o deban ser complementadas o suprimidas, se deberá solicitar la autorización de los Titulares para continuar tratando sus datos personales. De no ser esto posible, no se podrá continuar haciendo dicho Tratamiento.

6. PROCEDIMIENTOS OPERACIONALES QUE INVOLUCREN LA PROTECCIÓN DE DATOS PERSONALES

Los Responsables y Encargados del Tratamiento deben establecer de forma previa, los procedimientos relacionados con la recolección, mantenimiento, uso, supresión o disposición final de los datos personales y la atención de las peticiones, consultas y reclamaciones presentadas por los Titulares, entre otros, de acuerdo al propósito o finalidad del SV.

Los procedimientos deben ser documentados y socializados con el personal que tendrá acceso a los SV de forma previa al inicio de la operación. Es importante hacer seguimiento al cumplimiento de los procedimientos establecidos. Por esta razón, deben realizarse auditorias periódicas.

En línea con lo anterior, los Responsables y Encargados del Tratamiento deben observar las siguientes reglas:

- Solicitar y conservar prueba de la autorización de los Titulares para el Tratamiento de sus datos personales.
- Implementar SV sólo cuando sea necesario para el cumplimiento de la finalidad propuesta, respetando la dignidad y demás derechos fundamentales de las personas.
- Limitar la recolección de imágenes a la estrictamente necesaria para cumplir el fin específico previamente concebido.
- Informar a los Titulares acerca de la recolección y demás formas de Tratamiento de las imágenes, así como la finalidad del mismo.
- Conservar las imágenes sólo por el tiempo estrictamente necesario para cumplir con la finalidad del SV.
- Inscribir la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos. No será necesaria la inscripción cuando el Tratamiento consista sólo en la reproducción o emisión de imágenes en tiempo real, sin perjuicio del cumplimiento

13. Concepto No. 13-102526 emitido por la Oficina Asesora Jurídica de la Superintendencia de Industria y Comercio, junio 24 de 2013, haciendo referencia a la Guía de Videovigilancia de la Agencia Española de Protección de Datos, página 4

de las demás disposiciones del Régimen General de Protección de Datos Personales.

- Suscribir cláusulas de confidencialidad con el personal que accederá a los SV.

- No instalar SV en lugares donde la recolección de imágenes y, en general, el Tratamiento de estos datos pueda afectar la imagen o la vida privada e íntima de las personas.

7. MEDIDAS DE SEGURIDAD

El SV y la base de datos conformada deben contar con las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales, evitando su adulteración, pérdida, deterioro, consulta, uso o acceso no autorizado o fraudulento[14], mantener la integridad de la información y garantizar los derechos de los Titulares de los datos personales.

Para lo anterior, los Responsables y Encargados del Tratamiento deberán establecer las medidas que consideren efectivas y pertinentes para garantizar la seguridad de la información. Algunas de las medidas a implementar pueden ser: limitar el acceso a la información, cifrar la información y realizar auditorías periódicas a las medidas adoptadas. Las medidas implementadas deberán ser informadas a las personas que operen los SV para su puesta en práctica al operarlos. En los casos en que el Tratamiento se limite a la reproducción o emisión de imágenes en tiempo real, la visualización debe limitarse solamente al personal autorizado para ello. Las imágenes grabadas deben ser visualizadas en un área de acceso restringido que garantice la seguridad de las mismas.

De igual forma, se deben establecer medidas sobre la confidencialidad[15] y reserva de los datos personales y exigir su cumplimiento a todas aquellas personas naturales o jurídicas que tengan acceso y hagan Tratamiento de las imágenes recolectadas. Esta obligación se debe extender incluso después de finalizada la relación laboral o contractual de la que se derivó el Tratamiento de datos personales.

Los datos personales recolectados deberán mantenerse sólo por el tiempo que sea necesario, de acuerdo con la finalidad específica establecida por el Responsable del Tratamiento, al cabo del cual deberán ser eliminados. Es importante documentar los procesos de eliminación de la información.

En todo caso, las medidas de seguridad implementadas dependerán del análisis de riesgo que se realice en cada etapa del ciclo del dato tratado, es decir, desde el momento en que se recolecta hasta su disposición final. Dicho análisis debe tener en cuenta el impacto en caso de que se materialicen los riesgos, esto con el fin de que se identifiquen y adopten las medidas de mitigación respectivas.

14. Ley 1581 de 2012, literal g), principio de seguridad.

15. Ibídem, literal h), principio de confidencialidad.

Adicionalmente, se deben implementar protocolos de respuesta en el manejo de violaciones e incidentes de seguridad de los SV y, en caso de presentarse alguno, los Responsables o Encargados del Tratamiento deberán reportarlo a la Superintendencia de Industria y Comercio.

8. DIVULGACIÓN DE LA INFORMACIÓN

El acceso y divulgación de las imágenes debe estar restringido[16] y su Tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por solicitud de una autoridad pública en ejercicio de sus funciones. En consecuencia, la divulgación de la información que se recolecta por medio de un SV debe ser controlada y consistente con la finalidad establecida por el Responsable del Tratamiento.

9. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

Los Titulares de los datos personales tienen derecho[17] a conocer, actualizar, rectificar o suprimir sus datos personales; a revocar la autorización del Tratamiento; a ser informados acerca del Tratamiento de los mismos; a presentar quejas por infracciones al Régimen General de Protección de Datos Personales a acceder de forma gratuita a los datos personales que hayan sido objeto de Tratamiento, entre otros. Los Responsables y Encargados del Tratamiento deben garantizar el ejercicio de estos derechos por parte de los Titulares de datos personales, así como dar cumplimiento a las demás obligaciones que les impone el Régimen General de Protección de Datos Personales.

En línea con lo anterior y teniendo en cuenta las particularidades de los SV, se debe tener especial cuidado en el ejercicio del derecho de acceso por parte de los Titulares de los datos personales, adoptando medidas para no transgredir los derechos de terceros, igualmente Titulares de información, como se explica a continuación.

9.1. Acceso a las imágenes por parte de los Titulares de datos personales

Los Titulares de la información están facultados para ejercer su derecho de acceso a las imágenes tratadas mediante SV. En tal virtud, cuando un Titular ejerza este derecho, los Responsables y Encargados del Tratamiento deben adoptar los procedimientos y las medidas necesarias para proteger los derechos de los demás Titulares cuyos datos personales han sido objeto de Tratamiento junto con los de

16. Ibídem, literal f), principio de acceso y circulación restringida.

17. Ibídem, artículo 8.

quien solicita el acceso. Algunas de las medidas que pueden adoptarse son las siguientes:

- Establecer un procedimiento para acceder a las imágenes, que le permita a los Responsables y Encargados del Tratamiento verificar la calidad de Titular de quien solicita el acceso a la información.

- Requerir al Titular solicitante datos como fecha, hora, lugar, entre otros, para facilitar la ubicación de la imagen y limitar al máximo la exposición de imágenes de terceros.

- Si en la imagen aparece un (unos) tercero(s) Titular(es) de datos personales, se deberá contar con la autorización de dicho(s) tercero(s) para la entrega de la cinta o grabación.

- Si no se tiene la autorización de los terceros para divulgar la información contenida en la cinta o grabación requerida, los Responsables y Encargados del Tratamiento deben garantizar la anonimización del (los) dato (s) del (los) tercero (s), tomando medidas encaminadas a tal fin, como hacer borrosa o fragmentar la imagen de dicho (s) tercero (s).

9.2. Supresión de las imágenes

El Titular de los datos personales también se encuentra facultado para solicitar la supresión de sus imágenes[18] en la medida que no exista un deber legal o contractual que impida tal supresión, como sería por ejemplo el caso en que los datos personales recolectados mediante una grabación constituyan prueba de la presunta comisión de un delito. La solicitud de supresión, así como cualquier otra reclamación que se adelante ante los Responsables y Encargados del Tratamiento, deberá realizarse de acuerdo al procedimiento establecido por los artículos 15 y 16 de la Ley 1581 de 2012.

En todo caso, el término de retención de las imágenes debe ser limitado y razonable, en concordancia con la finalidad del Tratamiento de los datos recolectados.

10. CÁMARAS CON ACCESO A LA VÍA PÚBLICA

Una de las finalidades más comunes de los SV es garantizar la seguridad de bienes o personas en entornos públicos y privados. Garantizar la seguridad en entornos públicos es tarea que corresponde de forma exclusiva al Estado y en razón de la cual se encuentra legitimado para operar SV en la vía pública, excluyendo de este ejercicio a los particulares.

La operación de SV privados puede implicar, en algunos casos, la toma de imágenes en la vía pública por ser necesaria para alcanzar la finalidad establecida, por ejemplo, garantizar la seguridad de bienes y personas en entornos privados. De ser así, dicha recolección debe limitarse a aquella que no pueda evitarse para alcanzar el fin legítimo perseguido. El caso más común es

18. Ibídem, artículo 8, literal e).

la toma de imágenes en puntos de acceso, como porterías y entradas a propiedades privadas, la cual se debe restringir a las áreas más próximas al espacio objeto de vigilancia.

11. TRATAMIENTO DE IMÁGENES DE NIÑOS, NIÑAS Y ADOLESCENTES

El Tratamiento de imágenes de niños, niñas y adolescentes debe respetar los derechos prevalentes de los mismos y sólo se podrá realizar cuando (i) responda y respete su interés superior, y (ii) asegure el respeto de sus derechos fundamentales.

Un claro ejemplo del Tratamiento de imágenes de niños, niñas y adolescentes es el que realizan las instituciones educativas que operan SV con finalidades de seguridad en el desarrollo de las actividades ejecutadas al interior de la institución.

En todos los casos, los Responsables y Encargados que utilicen SV que involucren el Tratamiento de imágenes de niños, niñas y/o adolescentes deben observar las siguientes reglas, además de lo señalado previamente en esta guía:

- Contar con la autorización de los padres o representantes legales de los menores y con la aquiescencia de estos, teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto.

- Informar a los padres o representantes legales acerca de la finalidad y el Tratamiento al cual serán sometidos los datos personales de los menores, así como los derechos que les asisten.

- Limitar la recolección y demás Tratamiento de las imágenes, de acuerdo con lo que resulte proporcional y adecuado en consideración a la finalidad previamente informada.

- Garantizar la seguridad y reserva de los datos personales de los menores.

- Restringir el acceso y la circulación de las imágenes, conforme a lo establecido en la ley.

El padre y/o representante legal del niño, niña o adolescente solo podrá acceder a las imágenes de este. Así, en caso de que se pretenda dar acceso o circular imágenes de clases y/o actividades donde aparezcan otros niños, niñas o adolescentes, se deberá solicitar la autorización de los padres y/o representantes legales de todos ellos.

Siempre que la implementación de SV involucre también el Tratamiento de datos personales de otros Titulares, como directivos, personal docente o administrativo, padres de familia, etc., los Responsables y Encargados del Tratamiento deberán respetar los derechos de aquellos y cumplir las obligaciones que dicha calidad les impone.

12. RECOMENDACIONES GENERALES

- Consulte si hay normas que regulen los SV y revise las disposiciones contenidas en el Régimen General de Protección de Datos Personales, para dar cumplimiento a las mismas.

- Evalúe el impacto que un SV puede tener respecto de la intimidad y la protección de los datos personales de los Titulares de información y determine si realmente necesita la implementación del mismo para lograr la finalidad perseguida.

- Determine el período de tiempo que permanecerá la información en sus bases de datos teniendo en cuenta la finalidad para la cual se recolectó y documente la supresión de la misma.

- Limite la recolección de información, considerando lo que resulte proporcional y adecuado según la finalidad establecida.

- Obtenga la autorización o consentimiento del Titular de los datos personales para el Tratamiento de los mismos, adoptando los mecanismos necesarios para dar cumplimiento a lo establecido en el Régimen General de Protección de Datos Personales.

- Implemente medidas de seguridad y confidencialidad para el Tratamiento de la información recolectada mediante los SV.

- Diseñe políticas y protocolos para la recolección, uso, circulación, conservación y disposición final de la información que recolecta, así como para la atención de las peticiones, consultas y reclamos presentados por los Titulares e informe de estos al personal que opere los SV.

- Tenga en cuenta que el Tratamiento de imágenes de niños, niñas y adolescentes deberá responder a un interés superior de los menores y respetar sus derechos fundamentales.

- Recuerde que las bases de datos con fines de videovigilancia también deben inscribirse en el Registro Nacional de Bases de Datos –RNBD-, administrado por esta Superintendencia.

Industria y Comercio

SUPERINTENDENCIA