GUIA DE VIDEOVIGILANCIA

Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales.

Presentación

El objetivo de la presente guía es facilitar a los sujetos obligados las mejores prácticas en ciertos ámbitos de aplicación de la video vigilancia, en razón de hacer valer el derecho a la protección de los datos personales del titular del dato.

En los diferentes espacios, la utilización de imágenes que contienen personas identificables tiene una serie de implicaciones para el derecho a la protección del dato personal.

La captación de la imagen de una persona reconocible constituye un dato de carácter personal y por tanto, debe ser tratada de acuerdo a lo principios que sustentan el derecho a la protección del dato.

Recordar que la grabación de la vía pública y de los que transitan por ella está permitida en algunos supuestos por motivos de seguridad.

En los siguientes apartados se expondrán los bienes jurídicos afectados por esta práctica, los principios y reglas generales que se deben aplicar, las obligaciones de los responsables y los derechos de los ciudadanos cuya imagen es captada por un sistema de videovigilancia.

A partir de esta base, se recomiendan una serie de mejores prácticas en la captación de imágenes en determinados lugares.

I. IMAGEN COMO DATO PERSONAL.

La video vigilancia nos ha facilitado el tener mayor seguridad, sintiéndonos más protegidos y con esto responder una demanda constante de la sociedad para tener mayor protección.

Lo que persigue la video vigilancia es primeramente: la protección de bienes y personas, verificación de los trabajadores en sus labores asignadas en sus actividades laborales y responder a las demandas de la sociedad que requieren información visual de un hecho acontecido.

Los medios técnicos para la vigilancia repercuten sobre el derecho de las personas lo que obliga a que se fijen garantías ya que permite la captación, y en su caso la grabación, de información de carácter personal en forma de imágenes.

Uno de los principales objetivos de la Ley, es garantizar la protección de los datos personales en posesión de los sujetos obligados, así como su derecho de acceso, rectificación, cancelación y oposición mediante procedimientos sencillos y expeditos.

Por lo tanto, cuando la información es captada por cámaras que se encuentran en posesión de los Sujetos Obligados y afecta a personas identificadas o identificables constituye un dato personal y como tal debe ser protegido bajo el resguardo de la Ley en la materia.

Es importante mencionar que una de las obligaciones a las que están sujetas las autoridades es asegurar la protección de los datos personales en su posesión y permitir el acceso de los particulares a sus datos personales, y en su caso ejercer los derechos de acceso, rectificación, cancelación y oposición; siempre que así procediere.

Hay un sinfín de requisitos, que se deberán prever para llevar a cabo la debida protección de dicha información, como:

1. **Determinar el responsable de la base de datos,** conforme a la ley de transparencia se entiende que es el servidor público titular de la unidad administrativa responsable de las decisiones sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.
2. **El encargado del tratamiento,** es el servidor público o cualquier otra persona física o moral facultada por un instrumento jurídico o expresamente autorizado por el responsable, para llevar a cabo el tratamiento físico o automatizado de los datos personales, y
3. **El afectado,** interesado o titular del dato es la persona física titular de los datos personales que sean objeto del tratamiento.

II. CUESTIONES QUE SE RECOMENDARÁN EN LA PRESENTE GUÍA

Debemos de tener en cuenta que la video vigilancia es un medio particularmente invasivo, y resulta necesaria el conjunto de condiciones que legitimen dichos tratamientos, así como la definición de los principios y las garantías que deberán aplicarse.

Los principios de protección de datos deberán regir el tratamiento de las imágenes que son captadas a través de cámaras, video cámaras y cualquier medio técnico análogo, que capte y/o registre imágenes, ya sea con fines de vigilancia u otros en los supuestos en que exista grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquéllas.

VIDEOVIGILANCIA Y PROTECCIÓN DE DATOS

III. ¿QUÉ ES LA VIDEO VIGILANCIA?

De acuerdo al diccionario de la Real Academia Española, se define como la vigilancia que se lleva a cabo a través de un sistema de cámaras, fijas o móviles.

Por lo cual es toda actividad que presuma la colocación de una cámara de grabación, fija o móvil, con la finalidad de garantizar la seguridad de una instalación o de las personas, asegurar el correcto desempeño de las tareas en el entorno laboral o ser de utilidad en diversos ámbitos.

Un sistema de video vigilancia está integrado, de forma básica, por un elemento de captación de la imagen (cámara), visualización (la pantalla) y uno de almacenamiento (disco duro).

Para que la imagen captada sea utilizada de forma inmediata o en un momento posterior, debe ser transmitida al elemento de visualización y al elemento de almacenamiento, respectivamente.

Debido a que las autoridades quieren dar mayor protección a la sociedad en general y así mismo, la sociedad pide mayor seguridad por parte de las

autoridades, es por lo cual se está implementando la utilización de video cámaras para poder tener una seguridad que sea grabada y utilizada para los fines que se dispongan.

Sin embargo, es importante hacer notar que el rápido avance de la tecnología ha traído como consecuencia que ya no sean tan caros los sistemas de procesamiento y el desarrollo de los sistemas de vigilancia basados en vídeo, esto ha convertido a las cámaras en sistemas fácilmente distribuibles, accesibles e instalables, permitiendo su implantación de forma generalizada y muchas veces no cuenta con un ordenamiento jurídico que lo sustente.

Lo que es de preocuparse no es el costo del sistema de video vigilancia, sino que la gente que tenga el acceso a la operación de las mismas tenga conocimiento del tratamiento que debe darle por ley a las imágenes captadas en relación al derecho de la protección de los datos personales.

Los datos personales son toda aquella información numérica, alfabética, gráfica, **fotográfica,** acústica o de cualquier otro tipo concerniente a una persona física identificada o inidentificable, relativa al origen étnico o racial, las características físicas, morales o emocionales, a la vida afectiva y familiar, domicilio particular, número telefónico particular, cuenta personal de correo electrónico, patrimonio personal y familiar, ideología y opiniones políticas, creencias, convicciones religiosas o filosóficas, estados de salud físico o mental, las preferencias sexuales, la huella digital, ácido desoxirribonucleico (ADN), fotografía, número de seguridad social, y toda aquélla que permita la identificación de la misma.

Así como también define el concepto de sistema de datos personales, el cual se entiende como todo conjunto ordenado de datos personales que estén en posesión de un sujeto obligado, ya sea de forma física o automatizada como es el caso que nos ocupa.

Por lo cual, la imagen de una persona, en la medida que es identificable o susceptible de ser identificada, es considerada dato de carácter personal.

En el ámbito de la video vigilancia, deben aplicarse los principios sobre protección de datos siempre que se utilicen medios técnicos para grabar, captar, tratar, almacenar y reproducir imágenes de personas identificables, ya sea en tiempo real o en diferido.

Esta obligación no existe en los siguientes supuestos:

Al realizar grabaciones en el ámbito personal o familiar, esto es en situaciones de la vida privada de los titulares de los datos, ya sea en celebraciones familiares, siempre que se sigan manteniendo en ese ámbito.

Difundir grabaciones personales o familiares a través de Internet supone traspasar el ámbito doméstico.

En el desempeño de las labores de información realizado por profesionales de medios de comunicación, en base a la libertad de información.

NOTA: Aquellos Sujetos Obligados que instalen sistemas de video vigilancia para captar o tratar imágenes en las que puedan aparecer personas identificables, deben observar los principios sobre los que se sustenta el derecho a la protección del dato personal, ciertos principios generales de actuación de conformidad con lo dispuesto en la legislación de la materia.

IV. Principios de protección de datos que rigen el tratamiento de imágenes.

Se entiende por tratamiento de imágenes en la video vigilancia todo el proceso desde su captación, almacenamiento y reproducción hasta su cancelación.

De acuerdo con el concepto de tratamiento, es cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o físicos, y aplicadas a datos personales, como la obtención, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Por lo cual los sujetos obligados al tratar los sistemas de bases de datos que tienen en su posesión deberán observar los principios de: Principios de Consentimiento, Información, Finalidad, Licitud, Lealtad, Calidad, Responsabilidad, Proporcionalidad, y los deberes de Seguridad y Confidencialidad, mismos que se definen a continuación:

Principio de Consentimiento: Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales, sin embargo, dicho principio por ley tiene diversas excepciones:

No se requiere el consentimiento cuando:

1. Se recaben para el ejercicio de las atribuciones legales conferidas a los sujetos obligados, es decir si existe un ley que exima el consentimiento del titular del dato.
2. Se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. (como pudiera ser que la captación es

necesaria para su mantenimiento o cumplimiento, si la grabación forma parte de las funciones de los Sujetos Obligados o persigue el interés vital de los individuos grabados), es decir si existe una relación jurídica.

3. Sean necesarios para efectuar un tratamiento para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.

Principio de Calidad.- El principio por el cual la autoridad sólo podrá tratar los datos cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad para los que se hubieren obtenido.

Por lo tanto, las imágenes obtenidas deben ser adecuadas, pertinentes y nunca excesivas, en relación con la finalidad que haya motivado la instalación de las cámaras.

Principio de Proporcionalidad.- Principio por el cual el sujeto obligado se compromete a optar por el tratamiento que permita conseguir la finalidad pretendida, por el que menor incidencia tenga en el derecho a la protección del dato, es decir no se realice un tratamiento excesivo para la finalidad deseada.

El sujeto obligado deberá ponderar el objetivo buscado y la posible afectación de los derechos de las personas, de tal forma que no exista un medio menos invasivo que cumpla la finalidad perseguida.

El principio de proporcionalidad en la utilización de las video cámaras se deberá regir en su doble versión de idoneidad y de intervención mínima.

- **La idoneidad** establece que solo puede emplearse la video vigilancia cuando resulte adecuado en una determinada situación en concreto, como el mantenimiento de la seguridad ciudadana, de conformidad con lo que disponga la Ley en materia de Seguridad pública o en el reglamento que desarrolle el sujeto obligado, siempre y cuando se respete el derecho a la protección del dato que tiene el titular del dato.

- **La intervención mínima** exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al honor, a la propia imagen y a la intimidad de las personas.

Principio de Finalidad.- Principio por el cual se debe identificar de forma precisa los propósitos perseguidos en el tratamiento de los datos personales por lo que los sujetos obligados sólo deberán utilizar los datos personales para el fin u objetivo para el cual fueron recabados y tratados los mismos.

Principio de Licitud.- Principio el cual consiste en que la posesión y tratamiento del sistema de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada sujeto obligado y deberán obtenerse a través de medios previstos en dichas disposiciones.

O bien, contar con el consentimiento del titular del dato afectado para proceder a captar su imagen personal.

Principio de Información. - Principio que consiste en dar a conocer al interesado la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales, el cual se cumple a

través de los avisos de privacidad, de conformidad con los requisitos que prevé la Ley de protección de datos y demás marco normativo.

Los individuos cuya imagen vaya a ser utilizada por los sistemas de video vigilancia deben ser notificados de la grabación antes de que se produzca o se lleve a cabo la captación de la imagen o bien de forma simultánea, darle a conocer el aviso de privacidad.

La información en la recolección de los datos personales es un elemento esencial del derecho a la protección de datos y por tanto su cumplimiento resulta ineludible. Este viene contemplado en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se le conoce como **AVISO DE PRIVACIDAD**, en el cual las autoridades que soliciten datos personales como lo es la imagen, deberán informar al interesado de manera expresa y clara lo siguiente:

1. Que sus datos se incorporarán a un sistema de datos personales, su finalidad y destinatarios;
2. Del carácter obligatorio o facultativo de la entrega de los datos personales;
3. De las consecuencias de la negativa a suministrarlos;
4. De la posibilidad de que estos datos sean transmitidos, en cuyo caso deberá constar el consentimiento expreso de la persona;
5. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y
6. Del cargo y dirección del responsable, entre otros requisitos que establece el marco normativo.

Sin embargo, las especiales características que se dan en la video vigilancia comportan el diseño de procedimientos específicos para informar a las personas cuyas imágenes se capten. Para estos efectos, la colocación de los carteles de información (Aviso de privacidad) es obligatoria, ya que cada uno de los principios de protección de datos se traduce en derechos para los titulares de los datos y obligaciones para las autoridades.

Toda persona expuesta a la video vigilancia debe ser informada de modo expreso, preciso e inequívoco respecto a la colocación de los equipos, la zona que se monitoriza, el responsable de la base de datos y los derechos que tienen, los cuales se comentaran más adelante.

Es importante aclarar que los individuos que quieran consultar la información disponible sobre una instalación de vigilancia por video pueden encontrarla en los siguientes elementos:

1. En los carteles colocados en los accesos al recinto grabado, que notifica a las personas sobre la actividad que se está produciendo.
2. En los impresos informativos que debe proporcionar el sujeto obligado. Estos avisos de privacidad certifican la existencia de una base de datos con las imágenes tratadas por su consideración como datos de carácter personal, así como la identidad y datos de contacto del responsable del tratamiento de los datos.

Deber de Seguridad. - deber de todo responsable y encargado de llevar a cabo el tratamiento de datos personales, mantener y garantizar las medidas de seguridad administrativas, técnicas y físicas establecidas en el documento de

seguridad, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

El sujeto obligado debe garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados, puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

Es por lo cual el responsable del tratamiento debe establecer las normas, procedimientos y acciones que garanticen que la información contenida en las imágenes va a ser accesible únicamente para aquellas personas o autoridades autorizadas y deberá implementar las medidas de seguridad administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Deber de confidencialidad.- Principio el cual consiste en garantizar que exclusivamente la persona interesada pueda acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.

Es decir, toda persona que intervenga en el tratamiento de imágenes de otras personas captadas por los sistemas de video vigilancia está obligada a respetar la confidencialidad de los datos personales a los que tienen acceso durante este tratamiento.

En este contexto, existen algunos requisitos que se deberán tener en cuenta para la captación y tratamiento de imágenes de carácter personal.

V. REQUISITOS PARA LA UTILIZACIÓN DE LAS VIDEOCÁMARAS.

Para realizar un correcto uso de las instalaciones de cámaras y videocámaras se deben seguir ciertas reglas que rigen todo el proceso desde la captación de la imagen, almacenamiento, reproducción hasta su cancelación, es decir el tratamiento de las imágenes del mismo.

Las autoridades deberán tener en cuenta los siguientes principios:

- Debe informarse sobre la captación y/o grabación de las imágenes, por lo cual es importante comunicar el uso de instalaciones de cámaras o videocámaras y recordar que sólo es admisible cuando no exista un medio menos invasivo para logar la finalidad perseguida.
- Debe existir una relación de proporcionalidad entre la finalidad que se persigue y el modo en que se traten los datos.
- Se podrán tomar imágenes parciales y limitadas de vías públicas cuando resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas.
- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos o por lo menos se tratará de evitar la captación de tales espacios públicos.

- En cualquiera que sea el caso, el uso de sistemas de video vigilancia deberá ser respetuoso con los derechos de acceso y de cancelación de los titulares de los datos y el resto del Ordenamiento Jurídico de la materia.
- Las imágenes solo se conservarán por el tiempo imprescindible para cumplir con la finalidad establecida para la cual fueron recabadas.

No es admisible la captación de imágenes en espacios protegidos por el derecho a la intimidad como los interiores de viviendas cercanas, en baños, vestuarios o en espacios físicos ajenos al específicamente protegido por la instalación. Las imágenes se conservarán por el tiempo que sea imprescindible para la satisfacción de la finalidad para la cual se ha recabado.

V. REGISTRO DE BASES DE DATOS

Es de entenderse que la utilización de video cámaras nos lleva al tratamiento de datos personales, que no es otra cosa que un conjunto organizado de datos de carácter personal, en este caso imágenes de los titulares de los datos, los

cuales se almacenan en discos duros, o en cualquier otro soporte informático, y permite localizarlas atendiendo a ciertos criterios como el día y/u hora de grabación, el cruce de imágenes, el lugar registrado con listas de asistencia, entre otras.

Lo anterior se encuentra contemplado como atribución del Pleno de la Comisión en la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.

VII. ACCESO A LAS IMÁGENES CAPTADAS POR VIDEOCÁMARAS POR PARTE DE UN TERCERO.

La implementación de los sistemas de video vigilancia puede presentarse en diversas situaciones tales como, en el marco de una relación de negocios previamente establecida; que los datos recabados por el responsable deban ser comunicados a terceros, bien porque la comunicación tenga por objeto la satisfacción de un interés legítimo del responsable o del cesionario o bien por necesidades diferentes, como puede ser aquellas de índole privada.

En otras palabras es cuando el responsable de la instalación de video vigilancia (responsable del tratamiento), contrata a una empresa de seguridad para que realice la instalación y el tratamiento de las imágenes por lo tanto, esta última se convierte en encargada y la responsabilidad también recae sobre la empresa

externa. De manera que el encargado puede responder como responsable si las utiliza de forma indebida.

Al efecto, en atención a lo anterior, es posible que se puedan dar los siguientes casos:

Se pueden dar los siguientes casos:

- Cuando se contratan los servicios de instalación y/o mantenimiento técnico de los equipos y sistemas de video vigilancia sin acceso a las imágenes. En este caso la empresa no posee la condición de encargado del tratamiento, correspondiendo a la autoridad que la contrató, la adaptación de la instalación a los requisitos normativos.

- Sistemas de video vigilancia con utilización de los equipos o acceso a las imágenes. Cuando la prestación de servicios comporta la utilización de las instalaciones y/o el acceso a las imágenes, la empresa de seguridad deberá ser considerada encargado del tratamiento. Por ello, cuando se capten y/o registren imágenes con fines de seguridad privada y la empresa de seguridad contratada utilice las videocámaras y/o accesa a las imágenes por medio de su personal, resulta ineludible la celebración de un contrato de transferencia entre la autoridad y la empresa para la finalidad exclusiva que se especifique.

Cuando se capturan y almacenan imágenes para cualquier finalidad, y es una empresa externa la encargada del tratamiento de los datos, el responsable debe:

1. Velar porque la empresa externa encargada del tratamiento reúna las garantías para el cumplimiento de todas las obligaciones establecidas para la protección de los datos personales,

2. Celebrar un contrato que establezca esta prestación de servicio y la relación entre el responsable y encargado del tratamiento,
3. Cancelar las imágenes una vez cumplida la relación contractual, y
4. Evitar que el encargado subcontrate a su vez el tratamiento de la información, salvo que se le autorice expresamente.

El contrato que regula el tratamiento de las imágenes debe contener, entre otras obligaciones, lo siguiente:

I. Designación y obligación del responsable y de los encargados, de guardar la debida confidencialidad de los datos personales contenidos en el sistema de datos personales;
II. La posibilidad de incurrir en las responsabilidades y sanciones civiles o penales que correspondan por el uso inadecuado de los datos,
III. El nivel o niveles de protección requeridos para los datos de acuerdo con su naturaleza, y
IV. La obligación de permitir verificaciones a las medidas de seguridad adoptadas mediante la inspección de la información y documentación que se estimen necesarias.

VIII. MEDIDAS DE SEGURIDAD

El responsable de la instalación deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Por tanto quien haya contratado los servicios de una empresa de seguridad, pudiendo ser una autoridad, debe cumplir con el deber de garantizar la seguridad de las imágenes.

Por regla general, las bases de datos de video vigilancia deberán tener un nivel básico en relación con las medidas de seguridad que la Comisión emitirá como recomendaciones para todas las bases de datos, no solo para las de video vigilancia. No obstante, el responsable de la mencionada base de datos debe tener en cuenta que habrá de evaluar el nivel de seguridad de acuerdo con el contenido y finalidad de la base de datos.

Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos, deberá de observar la debida reserva, confidencialidad y secreto en relación con las mismas.

IX. CANCELACIÓN DE OFICIO DE LAS IMÁGENES.

La Ley, no contempla un plazo para la cancelación de los datos que se encuentran en la base de datos, sin embargo, va ligado o concatenado con la finalidad de la obtención de los mismos, si ya cumplió su finalidad y no hay ninguna obligación legal que requiera su conservación, se deberá dar de baja y eliminarla del sistema, asimismo, deberán tomar en cuenta lo establecido por el Catálogo de Disposición documental.

Por lo cual, será la autoridad quien determine el plazo para dar de baja el sistema de base de datos en relación a las imágenes captadas en el sistema de

video vigilancia. Por tanto una vez transcurrido dicho plazo las imágenes deberán ser canceladas.

En aquellos casos en los que el responsable constatase la grabación de un delito o infracción administrativa que deba ser puesta a conocimiento de una autoridad y la denunciase, deberá conservar las imágenes a disposición de la autoridad competente.

X. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

El ejercicio de los derechos de Acceso, Rectificación, Cancelación u Oposición se encuentra amparado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Toda persona tiene derecho a la protección de sus datos personales por lo cual la utilización de instalaciones de video vigilancia para captar, grabar o reproducir imágenes relativas a personas identificables constituye una práctica que puede afectar a la intimidad y privacidad de estas.

El titular del dato tiene derecho al Acceso, Rectificación, Cancelación y Oposición de sus datos personales, mismos que son conocidos por su acrónimo, como derechos ARCO.

Derecho de Acceso

El ejercicio del derecho de acceso reviste características singulares:
Requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y constatar la presencia del afectado en sus registros.

Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

Si se ejerciese el derecho de acceso ante el responsable de un sistema que únicamente reproduzca imágenes sin registrarlas, deberá responderse en todo caso indicando la ausencia de imágenes grabadas.

Derecho de Rectificación.

No resulta posible el ejercicio del derecho de rectificación ya que por la naturaleza de los datos, las imágenes tomadas de la realidad que reflejan un hecho objetivo, se trataría del ejercicio de un derecho de contenido imposible.

Derecho de Cancelación.

Por lo que respecta al derecho de cancelación, se debe señalar que la cancelación solicitada por el afectado se rige por lo previsto en la normativa de protección de datos.

El interesado tiene derecho a cancelar sus datos personales cuando:

I. El tratamiento de los mismos no se ajuste a lo dispuesto por la Ley, sus reglamentos o los lineamientos respectivos; o

II. Hubiere ejercido el derecho de oposición y éste haya resultado procedente.

Cuando se ejerce el derecho de cancelación dará lugar al bloqueo de los datos, el cual es un periodo que no tiene tiempo definido para investigar si la información ya no se requiere resguardar, por lo cual durante ese periodo de bloqueo solo estará a disposición de las autoridades, para la atención de posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas para que una vez que se haya cumplido el mismo se proceda a su supresión.

No debe olvidarse que conforme a las previsiones de la normativa de protección de datos, en caso de denegación de un derecho, deberá indicarse expresamente la posibilidad de iniciar un procedimiento de recurso de revisión ante el INFONL.

Derecho de Oposición

Por otro lado, el ejercicio de oposición también plantea enormes dificultades. Si este se interpreta como la imposibilidad de tomar imágenes de un sujeto concreto en el marco de instalaciones de video vigilancia vinculadas a fines de

seguridad privada, no resultaría tampoco posible su satisfacción en la medida en la que prevalecería la protección de la seguridad.

"Los derechos de rectificación y oposición son prácticamente de ejercicio imposible"

XI. VIDEO CÁMARAS COMO SEGURIDAD PÚBLICA

Respecto al uso de las videocámaras en relación con la seguridad pública, es importante comentar que estos aparatos se utilizan en lugares como calles y espacios públicos generalmente con la finalidad de afirmar que hay una mejor convivencia ciudadana, así como para prevenir delitos, faltas e infracciones relacionados con la seguridad pública, los cuales se deben regir por disposiciones específicas, ya sea por reglamento que desarrolle el Sujeto Obligado o por la ley.

El tratamiento de las bases de datos personales procedentes de las imágenes obtenidas cuando es utilizado en cámaras y videocámaras por Seguridad Pública deberá también cumplir con el marco normativo en materia de protección de datos personales.

XII. DEBERES

- No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus entradas, salvo consentimiento del titular o con autorización judicial, ni en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave a la intimidad de

las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada.

- Poner las imágenes captadas a disposición de la autoridad administrativa o judicial competente.
- Establecer periodos de conservación de las imágenes y destrucción de las mismas.
- Señalización de las zonas vigiladas.
- Ejercicio de los derechos de acceso y cancelación.

En cualquier caso, se debe de aplicar plenamente el derecho a la protección de los datos que se estipula el marco normativo en la materia, en particular en lo relativo a:

1. La Creación de la base de datos,
2. La adopción de medidas de seguridad de las mismas; y
3. Comunicaciones de datos a cesionarios distintos de las autoridades administrativas competentes en relación con las infracciones o delitos eventualmente registrados. (Transferencias)

LA SEÑALIZACIÓN GARANTIZARÁ EN TODO CASO LOS DERECHOS DE LOS AFECTADOS.

XIII. LAS VIDEO CÁMARAS CON FINES DE CONTROL DE TRÁFICO

La instalación y uso de videocámaras y de cualquier otro medio por el cual se capten y reproduzcan imágenes para el control, regulación, vigilancia y

disciplina del tráfico se debe efectuar por la autoridad encargada de regular el tráfico y de conformidad con la protección de los datos personales.

Se debe tener en cuenta que las cámaras deberán utilizarse con respeto al principio de proporcionalidad en cuanto a la idoneidad y de intervención mínima y corresponderá a las administraciones públicas con competencia para la regulación del tráfico, autorizar la instalación y el uso de estos dispositivos.

El acuerdo o la resolución que ordene la instalación y uso de los dispositivos fijos de captación y reproducción, deberá contener lo siguiente:

a) Identificará genéricamente las vías públicas o los tramos de aquellas cuya imagen sea susceptible de ser captada.
b) Las medidas tendientes a garantizar la preservación de la disponibilidad, confidencialidad e integridad de las grabaciones de registros obtenidos.
c) El sujeto obligado encargado de su custodia y de la resolución de las solicitudes de acceso y cancelación.

En lo mencionado anteriormente resulta de plena aplicación los derechos por los cuales se rige el derecho a la protección del dato personales.

XIV. ACCESO A EDIFICIOS

El acceso a edificios públicos puede requerir la captación de imágenes personales mediante la utilización de cámaras y video cámaras.
Estos procesos de control de acceso generalmente se articulan mediante controles en los cuales el interesado se identifica, se obtiene su imagen

(fotografía) y se emite un pase o tarjeta de identificación. En estos casos, los datos de carácter personal son recabados por servicios de seguridad tanto en edificios públicos como privados, en establecimientos, espectáculos y convenciones.

Al implementar estos servicios de seguridad, se debe tener en cuenta lo siguiente:

1. El responsable del sistema de datos asumirá el cumplimiento de todas las obligaciones en relación al derecho a la protección del dato.
    - La obtención de los datos efectuada se limitará a la finalidad de realizar controles de acceso.
    - Debe informarse del tratamiento de los datos personales.
    - Los datos personales no podrán ser utilizados para otros fines ni cedidos fuera de los casos expresamente establecidos en la ley, salvo consentimiento del interesado.
    - Los datos serán cancelados cuando se haya cumplido la finalidad de la obtención que generó el recopilado de datos personales.
    - El responsable de la base de datos garantizara la adopción de las medidas de seguridad que correspondan.

XV. CÁMARAS CON ACCESO A LA VÍA PÚBLICA

La prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva al Estado. Por tanto, la regla general es la prohibición de captar imágenes de la calle desde instalaciones privadas.

Sin embargo, en ciertas ocasiones la protección de los espacios privados sólo es posible si dichas cámaras se encuentran ubicadas en espacios como los frentes de los inmuebles. A veces, también resulta necesario captar los accesos, puertas o entradas, de modo que, aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta.

De este modo las cámaras y video cámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de las cámaras.

Pero en todo caso deberá evitarse cualquier tratamiento de datos que sea innecesario para la finalidad que se persigue.

Debe tenerse en cuenta que la utilización de las instalaciones de video vigilancia en la vía pública es para los cuerpos de seguridad del Estado.

XVI. CAPTACIÓN DE IMÁGENES EN SECTORES ESCOLARES Y DE MENORES

El tener la necesidad de colocar cámaras de seguridad con el fin de poder controlar conductas que lleguen a afectar a la seguridad, tendría que ser proporcional en relación con la infracción que se pretende evitar y en ningún caso, esta no debe suponer el medio inicial para llevar a cabo las funciones de vigilancia.

Se sugiere se tomen en cuenta las siguientes sugerencias:

1. Sea una medida apta para conseguir el objetivo propuesto;
2. No haya otra medida más idónea para la consecución de tal propósito con igual eficacia;
3. Y que sea equilibrada, ya que de ella se derivaran más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto

Los menores de edad merecen una especial protección por lo que el principio de proporcionalidad debe aplicarse al máximo.

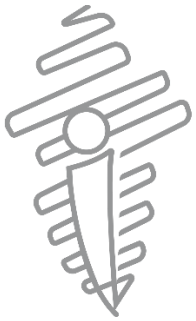
En entornos como colegios y guarderías, cuyo objetivo son los menores de edad, deberán en particular tomar en cuenta lo siguiente:

1. La zona que será objeto de la video vigilancia será la mínima imprescindible abarcando espacios públicos como entradas, salidas y pasillos.
2. No se podrán instalar cámaras en espacios como baños, vestuarios o aquellos en los que se lleven a cabo actividades cuya captación de la imagen de los menores pueda afectar la imagen o la vida privada como los vestidores de gimnasios.
3. Salvo circunstancias excepcionales, no es admisible la captación de imágenes para llevar a cabo el control de asistencia escolar.

XVII. CONCLUSIONES

- Cuando las imágenes se refieren a personas que son identificadas o pueden ser identificables, se deben observar los principios en materia de protección de datos personales:
- Si se trata de entornos laborales en los que pueden captarse imágenes de trabajadores, debe tenerse encuentra que las normas laborales contienen criterios y garantías respecto de sus derechos y deberes.
- Se informará de la existencia de instalaciones destinadas a captar las imágenes y su finalidad turística o promocional y no podrán utilizarse para finalidades distintas.
- Se adoptarán medidas oportunas de seguridad.
- Las imágenes se conservarán por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron.

- En los casos en los que las imágenes sean libremente accesibles en internet, es recomendable establecer políticas de privacidad estableciendo, de modo particular, las condiciones de uso para los terceros.
- Cuando las imágenes captadas y/o reproducidas no permitan la identificación de los individuos, ni cualquier aspecto personal como números de matrícula de coches, no serán aplicadas las normas sobre protección de datos.
- La utilización de video cámaras para captar, grabar o reproducir imágenes relativas a personas identificadas o identificables constituye una práctica habitual, pero puede afectar los derechos fundamentales y en particular el derecho a la protección de datos personales.
- El principio de proporcionalidad es básico para la elección de este tipo de medios, descartándose la video vigilancia cuando existan medidas menos lesivas para los derechos fundamentales.
- El responsable, debe ser diligente en la elección de la empresa de seguridad que le preste servicios, ya que debe reunir todos los requisitos legales para ello.
- En el ámbito laboral deberá garantizarse el respeto de los derechos de los trabajadores.
- Deberá de comunicarse por medio de un aviso de privacidad, que la zona es video grabada.



info·nl
INSTITUTO ESTATAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Visita nuestra página

https://infonl.mx/

Av. Constitución 1465-1 Pte.

Zona Centro, Monterrey, N.L. 64000

Llama a los teléfonos

(81) 10 01 78 00