Iniciativa con Proyecto de Decreto por el que se crea la **Ley que Regula la Videovigilancia en el Estado de Coahuila de Zaragoza.**

Planteada por el **Diputado Rodolfo Gerardo Walss Aurioles**, del Grupo Parlamentario "Carlos Alberto Páez Falcón", del Partido Acción Nacional, conjuntamente con las Diputadas que la suscriben.

Fecha de Lectura de la Iniciativa: **27 de Abril de 2021.**

Turnada a las **Comisiones Unidas de Gobernación, Puntos Constitucionales y Justicia y de Seguridad Pública.**

Fecha de lectura del dictamen:

Decreto No.

Publicación en el Periódico Oficial del Gobierno del Estado:

H. PLENO DEL CONGRESO DEL ESTADO
DE COAHUILA DE ZARAGOZA
PRESENTE. -

RODOLFO GERARDO WALSS AURIOLES, EN MI CARÁCTER DE DIPUTADO DE LA SEXAGÉSIMA SEGUNDA LEGISLATURA DEL HONORABLE CONGRESO DEL ESTADO, CONJUNTAMENTE CON LOS INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL "CARLOS ALBERTO PÁEZ FALCÓN", CON FUNDAMENTO EN LO ESTABLECIDO EN LOS ARTÍCULOS 59, FRACCIÓN I, 65 Y 67 FRACCIÓN I, DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO DE COAHUILA DE ZARAGOZA, Y EN EJERCICIO DEL DERECHO AL QUE HACEN REFERENCIA LOS ARTÍCULOS 21, FRACCIÓN IV Y 152, FRACCIÓN I DE LA LEY ORGÁNICA DEL CONGRESO DEL ESTADO, SOMETO A LA CONSIDERACIÓN DEL PLENO LA PRESENTE INICIATIVA CON PROYECTO DE DECRETO QUE CREA LA LEY QUE REGULA LA VIDEOVIGILANCIA EN EL ESTADO DE COAHUILA DE ZARAGOZA; AL TENOR DE LA SIGUIENTE:

EXPOSICIÓN DE MOTIVOS

Antecedentes

Como muchos de los grandes inventos de la humanidad, los albores de lo que hoy se conoce como videovigilancia tiene orígenes en la industria militar. En 1942, Alemania desarrolló un circuito de televisión cerrada con la finalidad de vigilar el lanzamiento de misiles. Prácticamente al mismo tiempo, en Estados Unidos, se desarrolló un sistema similar, pero para vigilar desde una distancia segura las pruebas nucleares. Eran cámaras en blanco y negro conectadas a monitores. Luego aparecerían los sistemas de cuadrante, que permitían la visualización de varias cámaras a la vez a través un mismo monitor.

Los retos iniciales de este tipo de sistemas estaban relacionados con el almacenaje de las imágenes, en un principio, una persona debía estar siempre atenta a las cámaras, ya que no se podía almacenar el contenido, o bien, era muy costoso hacerlo. Con la aparición del VHS este problema fue solucionado de momento; una buena cámara (para la época), una videograbadora y montones de casetes VHS permitían vigilar sin tener a una persona en horario 24/7 frente al monitor, y la información se podía respaldar para efectos de ser analizada después. La era digital fue un segundo paso en la constante lucha para mejorar el almacenaje y edición de imágenes, los discos duros y las tarjetas de memoria optimizaron el espacio, en lugar de muchas cajas o gavetas con VHS, una pequeña caja con dispositivos digitales reemplazaba todo lo anterior y, además, las imágenes podían mejorarse con programas especiales de computadora.

Antes del acceso del internet a toda la población, la videovigilancia se circunscribía a circuitos cerrados, y en algunos casos a redes de transmisión limitadas a una empresa o dependencia de gobierno, así como al llamado intranet.

Se debe aclarar que algunos historiadores de la tecnología sostienen que la videovigilancia nació antes de 1942, entre 1936 y 37, cuando Walter Broch (Alemania, 02 de marzo de 1908-05 de mayo de 1990) inventó la llamada cámara iconoscópica, presentada durante los Juegos Olímpicos de Berlín y confirmada como una cámara móvil cien por ciento funcional un año después.

Finalmente, en la actualidad predomina la vigilancia en tiempo real y a distancia con señales que se transmiten por internet y, sistemas de reconocimiento facial, de los que hablaremos más adelante en esta exposición de motivos.

Desde sus orígenes, la videovigilancia mostró su alto grado de eficacia en las tareas de seguridad, pues impacta en dos aspectos esenciales de esta: la prevención, al disuadir a potenciales infractores de la comisión de conductas delictivas; y el combate, al aportar las evidencias de los crímenes cometidos frente a la lente.

Videovigilancia en México

En México la videovigilancia se remonta a los años ochenta, en lo que hoy conocemos como Ciudad de México, antes Distrito Federal; las primeras cámaras de monitoreo urbano se colocaron en los semáforos, como apoyo al trabajo de estos. Con el paso del tiempo y ante la enorme demanda de mayor vigilancia y seguridad en la ciudad, las autoridades de la Secretaría de Seguridad Pública fueron instalando e implementado sistemas más modernos y extensos para vigilar amplias zonas, así como eventos masivos de tipo cultural.

El artículo "Video Vigilancia en el Centro Histórico", de Jordy Micheli y Laura Islas, refiere lo siguiente:

> *"…En resumen, bajo el Proyecto Ciudad Segura de la administración anterior (Marcelo Ebrard) se sembraron 8 mil cámaras, de las cuales cerca de 4 mil en las estaciones del Metro y 2,380 en los propios vagones del sistema de transporte colectivo. En la administración actual (Miguel Mancera), se anunció la expansión de la videovigilancia a 7 mil cámaras más: 3 mil para las zonas habitacionales de alta densidad demográfica, dos mil 331 para puntos con alta incidencia delictiva,*

500 para control de tránsito, 369 para instalaciones estratégicas, 200 para reconocimiento de placas vehiculares, 300 para el carril confinado del Metrobus y 300 más en zonas rurales y de conservación…" Fin de la cita.

Si bien la Ciudad de México posee el mayor número per cápita de cámaras de videovigilancia del país, para enero de 2019, una realidad se hizo presente: 1 de cada tres cámaras no funcionaba, los motivos eran variados, desde obras viales y sobre cargas de voltaje, hasta vandalismo y falta de mantenimiento. Uno de cada cuatro altavoces también sufrió un desperfecto, con lo que el porcentaje de fallos en el rubro se incrementó un 300% con relación al 2017.

Guadalajara, al presente año, se encuentra entre las 50 ciudades con más cámaras de videovigilancia del mundo, hay 14.7 cámaras por cada mil habitantes, lo que da un total de 76,943 dispositivos.

Pese al número de dispositivos en la ciudad de Guadalajara, la capital de Jalisco ocupa el sitio 62 del índice de criminalidad a nivel mundial. En este mismo ranking, la Ciudad de México se posiciona en el lugar 28, Tijuana en el sitio 33 y Puebla en la posición 40.

Esto deja en claro lo fundado de la polémica sobre las mediciones de efectividad de la videovigilancia, las cuales deben sujetarse a modelos de medición que en realidad no están disponibles.

Impacto de la Videovigilancia en el Mundo
Gobiernos Locales, Iniciativa Privada y Particulares

El número 15, del año 2015; de la revista "Astrolabio, Nueva Época", de la cual citamos la fuente digital: file:///C:/Users/mavig/Downloads/9903-Texto%20del%20art%C3%ADculo-35149-1-10-20151228.pdf; refiere lo siguiente:

En 1947, una década después de logrado el desarrollo de la tecnología para el servicio público de televisión, apareció la primera propuesta (si bien luego denegada) para que la policía inglesa pudiera evaluar las imágenes en vivo de la BBC durante la boda real y así asistir en las funciones de patrullaje (Norris, Mccahill y Wood, 2004). Pues bien, en las inmediaciones del nuevo siglo, la relación entre las imágenes, la policía y la seguridad pública se profundizó en dimensiones antes impensadas: las políticas de seguridad gubernamentales incorporaron sistemáticamente los circuitos cerrados de televisión (CCTV) para monitoreo del

espacio público entre sus tecnologías para el control social y la prevención situacional del delito.

…

Utilizada inicialmente en Europa y en América del Norte, la video-vigilancia se ha expandido hacia los cinco continentes, convirtiéndose en una de las principales herramientas al servicio de la seguridad ciudadana. Según Norris et al. (2004), la difusión de estos sistemas es una tendencia que se ha manifestado globalmente, cuyo crecimiento fue verificado en cuatro etapas: una difusión inicial en el sector privado; la introducción de la video-vigilancia en el transporte y la infraestructura pública; una utilización limitada en espacios públicos, que funcionó como el puntapié inicial para la migración a su uso gubernamental en la prevención del delito; y un último momento en el que el monitoreo urbano tiende a la ubicuidad, con sistemas a gran escala que cubren ciudades enteras y que integran cámaras de seguridad del sector público y privado. A partir de la década del '90 se produjo el pasaje del uso privado al ámbito público de las cámaras de seguridad, cuando numerosas ciudades de todo el mundo comenzaron a utilizar estos sistemas de video-vigilancia mediante CCTV para monitoreo de espacios públicos. Uno de los más sorprendentes desarrollos al respecto fue el de Gran Bretaña, país que se posicionó como líder y pionero mundial con el más extendido sistema de cámaras en espacios públicos del planeta (Lyon, 2004). Desde fines de la década de 1980, se instalaron más de cuatro millones de cámaras y actualmente el país concentra el 20 por ciento del total de las cámaras en uso de todo el mundo (Edwards, 2005). La emergencia de Gran Bretaña como líder mundial en el desarrollo de CCTV puede ser explicado, tanto por la ocurrencia de eventos dramáticos particulares como por problemas de larga existencia (como el terrorismo de IRA)…" Fin de la cita.

En el mundo entero, especialmente en Europa, Asia y América, la videovigilancia ha crecido de modo exponencial, algunas cifras apuntan a que el mercado de las cámaras y equipos para este fin crece un 40 % anual desde el año 2008 en forma sostenible. Son de modo especial los gobiernos locales: estados, provincias, municipios, condados, distritos, entre otros, quienes le apuestan a la videovigilancia para tareas que comprenden los aspectos siguientes:

I.- Tránsito de vehículos.

II.- Transportes terrestres, aeroportuarios y marítimos.

III.- Acceso a servicios públicos.

IV.- Seguridad en Edificios Públicos.

V.- Seguridad Bancaria.

VI.- Monitoreo de zonas militares o de acceso restringido para la población civil.

VII.- Control de prisiones.

VIII.- Vigilancia de zonas naturales protegidas.

IX.- Vigilancia de zonas culturales o históricas.

X.- Vigilancia de zonas de alta afluencia turística.

XI.- Monitoreo de zona de gran afluencia de personas, como en las concentraciones de transportes públicos como el metro, y los aeropuertos.

Por su parte, la iniciativa privada adquiere este tipo de equipos para:

I.- Seguridad en general.

II.- Control de accesos de entrada y salida.

III.- Identificación de personal que desempeña tareas de alto riesgo (para la empresa) o que debe acceder a áreas sensibles de la misma.

IV.- Monitoreo de la planta productiva.

V.- Monitoreo de sus transportes en tiempo real.

Los particulares adquieren videocámaras para:

I.- Seguridad.

II.- Vigilancia de los hijos menores.

III.- Monitoreo en tiempo real de sus bienes y propiedades.

América Latina encabeza la región del mundo con el mayor crecimiento del uso de videovigilancia, las razones saltan a la vista y no es necesario abundar en ellas. Brasil, Argentina, Colombia y México ocupan el mercado más creciente, y de 2011 a 2014 observaron un crecimiento sostenido del 60% anual, luego se mantuvo un ritmo menor debido a las crisis financieras de la región.

Lamentablemente, no existen estudios, análisis o censos confiables sobre el impacto de los sistemas de videovigilancia en América Latina que permitan medir los resultados de forma realista y evaluar sus fortalezas y debilidades.

En otros países, los estudios reflejan dos posiciones encontradas: el fracaso o el éxito relativo; la necesidad de la videovigilancia y sus efectos negativos más allá de la seguridad que aportan.

En Europa, especialmente en países como Inglaterra, Francia e Italia, diversos estudios, así como la opinión de especialistas en el tema, han permitido arribar a una posición consensuada o por lo menos mayoritaria, a fin de desmitificar y colocar en una posición justa y realista el uso de la videovigilancia. Entre otras cosas refieren que el poder de disuasión del delito que tienen las cámaras de videovigilancia es muy poco, debido a que el grueso de los potenciales infractores o delincuentes ignoran su existencia, suponen que no funcionan, se siente seguros si traen el rostro cubierto y conocen por los medios de comunicación que las imágenes suelen ser poco nítidas y por ende de eficacia nula o controversial en los procesos legales. Existe sí, un porcentaje de disuasión, pero es bajo y, en el mejor de los casos, moderado; y depende de factores múltiples como: la región donde se ubican las cámaras, la zona, el tipo de personas que se mueven en la zona, el tipo de delitos y delincuentes que operan en el lugar, la vigilancia de policías y patrullas que complementa a las cámaras.

Los especialistas consideran, en su mayoría, -desde luego con algunos detractores- que el uso de las cámaras de videovigilancia gubernamentales obedece más a una cuestión política en la que se pretende simular que se hace algo por la seguridad y que con ello se cumplen las exigencias de la sociedad en la materia. Para esto se basan en el hecho de que, ante múltiples encuestas y entrevistas, es unánime que en cualquier parte del mundo la gente asocia la instalación de cámaras de videovigilancia con una sensación de mayor seguridad, de sentirse a "salvo", de percibir que ahora nada les va a pasar, porque los delincuentes no harán nada al ver los dispositivos.

Por otra parte, señalan los expertos, están las limitaciones tecnológicas y de recursos que las autoridades y los políticos nunca mencionan en sus discursos, en concreto, las siguientes:

A) No se pueden instalar cámaras en todos los puntos de riesgo de una ciudad grande.
B) Las cámaras, en su mayoría, no son de máxima capacidad, pues son muy costosas, y se opta por capacidades medias y bajas en alcance y nitidez; lo que lleva a una captura de imágenes que no siempre son claras para identificar responsables.
C) En los países latinos es común que la falta de mantenimiento de los equipos hace que empiecen a fallar en el corto o mediano plazo, y se termina con una gran parte de ellos inservibles, pero se le oculta el hecho a la población, quienes ven las cámaras al pasar sin saber que no funcionan.
D) La corrupción; es común que los encargados de los equipos, su monitoreo, respaldo y compilación de datos, se corrompan para desaparecer o borrar evidencias o bien, apagar los equipos en ciertos horarios para favorecer la comisión de un delito, incluso averiándolos dolosamente.

Aspectos Negativos de la Videovigilancia y el Conflicto de Derechos

Además de los aspectos técnicos, financieros y humanos antes mencionadas, la videovigilancia ha enfrentado a los gobiernos a un gran dilema: el derecho a la seguridad, y el derecho a la privacidad. El conflicto surge al momento que, bajo el pretexto de fomentar la seguridad, en las grandes urbes se instalan cámaras en cruceros, calles, avenidas y en lugares de gran afluencia de personas; pero, dicha vigilancia debe limitarse a las áreas públicas, sin invadir los dominios privados y la intimidad de las personas. El ciudadano no quiere sentir que una cámara puede vigilar el patio de su casa, el traspatio, sus ventanas y en general su entorno privado e íntimo. Este principio es un derecho constitucional de todos, en este país y en la mayoría de las naciones con regímenes democráticos que reconocen los tratados internacionales en materia de derechos humanos.

Las cámaras de videovigilancia no solo entran en conflicto y probables violación de derechos humanos cuando se instalan en la vía pública, en todo el mundo existe un debate por el uso y el abuso de estas en centros de trabajo, en comercios y en empresas donde, so pretexto de la seguridad o de vigilar a los trabajadores, se les observa o se les graba no solo mientras trabajan, sino también al comer, al descansar, al departir con compañeros en horario de descanso, incluso hasta la entrada del sanitario.

Algunos países como España han establecido restricciones a este tipo de videovigilancia, prohibiendo que en los centros de trabajo se grabe y observe a los trabajadores en sus áreas de descanso, en los baños, en los vestidores, o que se escuchen o graben sus

conservaciones privadas. Los sindicatos y los trabajadores deben ser informados de la localización de las cámaras y de su finalidad; las grabaciones solo deben conservarse por 30 días y borrarse, a menos que sean parte de una investigación. En caso de darse el supuesto anterior, el trabajador tiene el más amplio derecho de acceder a la grabación para poder ejercer su derecho a una defensa adecuada.

Como referencia, la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, de España (texto vigente al año 2020) establece:

> ***Artículo 3. Autorización de las instalaciones fijas.***
>
> *…*
>
> *3. No podrá autorizarse la instalación fija de videocámaras cuando el informe de la Comisión prevista en el apartado segundo de este artículo estime que dicha instalación supondría una vulneración de los criterios establecidos en el artículo 4 de la presente Ley Orgánica.*
>
> *4. La resolución por la que se acuerde la autorización deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo, deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación.*
>
> *5. La autorización tendrá en todo caso carácter revocable.*
>
> ***Artículo 4. Criterios de autorización de instalaciones fijas.***
>
> *Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones*

útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes.

Artículo 5. Autorización de videocámaras móviles.

1. En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6.

2. También podrán utilizarse en los restantes lugares públicos videocámaras móviles. La autorización de dicho uso corresponderá al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6.

Artículo 6. Principios de utilización de las videocámaras.

1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

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

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artícu lo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las

imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.

Artículo 8. Conservación de las grabaciones.

1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.

3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.

4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados.

Artículo 9. Derechos de los interesados.

1. El público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.

2. Toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos podrá ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Esta legislación se considera de avanzada, pues fue uno de los primeros países del mundo en tratar de establecer límites y derechos en el uso de la videovigilancia, privilegiando el derecho de las personas a la privacidad y a la intimidad.

El 23 de abril de 2020, el gobierno de Perú publicó el Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1218, Decreto Legislativo que regula el uso de las cámaras de videovigilancia y de la Ley N° 30120, Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Videovigilancia Públicas y Privadas; en este se garantizan entre otras cosas:

Artículo 5. Limitaciones

5.1. Las cámaras de videovigilancia no deben captar o grabar imágenes, videos o audios del interior de viviendas, baños, espacios de aseo, vestuarios, vestidores, zonas de descanso, ambientes donde se realiza la atención de salud de las personas, entre otros espacios protegidos por el derecho a la intimidad personal y determinados por la norma de la materia. Dicha disposición cesa cuando exista una resolución judicial sobre la materia.

5.2. No está permitida la difusión o entrega por cualquier medio de las imágenes, videos o audios a personal no autorizado, según lo señalado en el presente Reglamento.

5.3. En el caso de imágenes, videos o audios que involucren a niños, niñas o adolescentes, prima el interés superior del niño, niña o adolescente y se ejecutan las medidas de protección de su identidad o imagen en materia de difusión a través de medios de comunicación, de conformidad con lo señalado en el artículo 6 del Código de los Niños y Adolescentes, aprobado mediante Ley Nº 27337.

Artículo 9. Estándares técnicos de cámaras de videovigilancia en bienes de dominio público

9.1. Las cámaras de videovigilancia en bienes de dominio público deben cumplir con los siguientes estándares técnicos:

a. Nitidez de las imágenes y videos que permita la visualización de personas y placa de vehículos.

b. Sistema funcional y operativo que permita la conectividad y transmisión de imágenes, videos y audios en tiempo real y de manera ininterrumpida.

c. Capacidad de conexión directa vía internet analógica o tecnología digital IP y compatibles con los diferentes protocolos abiertos de conexión o interconexión digital que garantice su interoperabilidad con el Centro Nacional de Videovigilancia, Radiocomunicación y Telecomunicaciones para la Seguridad Ciudadana (CENVIR) o el que haga sus veces.

d. Acceso mediante conexión de internet a las cámaras de videovigilancia, restringido solo a personal autorizado y contemplando las medidas de seguridad respectivas.

e. Instalación en lugares estratégicos que aseguren un campo visual despejado de obstáculos u objetos, evitando la existencia de puntos ciegos, y con una distancia proporcional entre su ubicación y el alcance del zoom, de manera que permita la identificación de personas y placa de vehículos.

f. Instalación como mínimo en las siguientes zonas: i) áreas externas de los bienes de dominio público, que aseguren la captación de imágenes de las personas al ingreso y/o a la salida del establecimiento, así como de su perímetro adyacente o área de influencia deportiva, para el caso de estadios; y, ii) áreas internas donde existe atención al público o con afluencia de público, según corresponda y conforme a las disposiciones señaladas en normativa de la materia.

VIDEOVIGILANCIA EN BIENES INMUEBLES DE PROPIEDAD PRIVADA

Artículo 12. Cámaras de videovigilancia ubicadas en la parte externa de inmuebles de propiedad privada

12.1. Las cámaras de videovigilancia ubicadas en la parte externa de inmuebles de propiedad privada constituyen un instrumento de vigilancia ciudadana, en los casos de presunción de comisión de un delito o de una falta; ubicándose preferentemente en el ingreso y salida de los inmuebles, así como en áreas comunes con afluencia de público.

12.2. Las cámaras de vigilancia ubicadas en la parte externa de inmuebles no deben obtener imágenes de espacios públicos, salvo que resulte imposible evitarlo. En este último caso, la cámara debe captar únicamente la sección de vía pública que resulte imprescindible para cumplir con los fines de seguridad.

Artículo 13. Tratamiento de información proveniente de cámaras de videovigilancia ubicadas en la parte externa de inmuebles de propiedad privada

El tratamiento de información proveniente de cámaras de videovigilancia ubicadas en la parte externa de inmuebles de propiedad privada se rige bajo las disposiciones señaladas en el Título III del presente Reglamento, con excepción de lo contemplado en los literales b y c del párrafo 17.2 del artículo 17.

Artículo 17. Captación y grabación de imágenes, videos o audios

17.1. Las personas comprendidas en el ámbito de aplicación del presente Reglamento deben seguir los siguientes lineamientos en materia de captación de imágenes, videos o audios:

a. Cuando se encuentre frente a hechos, en tiempo real, que presenten indicios razonables de la comisión de un delito o falta, o que constituyan un riesgo al orden interno, orden público y seguridad ciudadana, se informa a la Policía Nacional del Perú o Ministerio Público, según corresponda; y se habilita la visualización inmediata del personal policial especializado. Si adicionalmente se presenta alguna emergencia o siniestro, debe comunicarse con el Cuerpo General de Bomberos Voluntarios del Perú, el Ministerio de Salud u otras entidades responsables de la atención, según la naturaleza del evento presentado.

b. Cuando luego de la captación, se toma conocimiento de hechos que presentan indicios razonables de la comisión de un delito o falta que constituyan un riesgo al orden interno, orden público y seguridad ciudadana, se informa y hace entrega de tal información en un plazo máximo de veinticuatro (24) horas a la Policía Nacional del Perú o Ministerio Público, según corresponda, bajo responsabilidad administrativa o penal, según corresponda.

17.2. Las personas comprendidas en el ámbito de aplicación del presente Reglamento deben seguir los siguientes lineamientos en materia de grabación de imágenes, videos o audios:

a. Mantener reserva, confidencialidad y cuidado debido de las imágenes, videos o audios. En tal sentido, no se puede alterar o manipular los registros; ceder o copiar imágenes, videos o sonidos obtenidos a terceros no autorizados; o, reproducirlos con fines distintos de los previstos en las presentes disposiciones;

b. Almacenar las imágenes, videos o audios grabados por un plazo mínimo de cuarenta y cinco (45) días calendario, salvo disposición distinta en normas sectoriales.

c. Excepcionalmente, si la grabación contiene información sobre la comisión de delitos, faltas o existe una investigación de oficio o a solicitud de parte sobre los hechos grabados, esta puede ser almacenada durante un periodo mayor al establecido, haciendo de conocimiento esta situación a la Policía Nacional del Perú.

Esta ley y el reglamento que se muestran son el reflejo de la intención de dos naciones para avanzar hacia una regulación oportuna y precisa de la videovigilancia. Regulan aspectos que han sido tema central del debate en todos los foros sobre derechos humanos y videovigilancia, especialmente los que se refieren a los límites físicos que deben cubrir las cámaras para respetar la intimidad y la privacidad de las personas, los límites que deben observar a su vez los particulares y las empresas al instalar videovigilancia, los derechos que tienen las personas que son vigiladas por medio de estos sistemas y cuando son grabadas con fines de investigación, en especial el derecho a ser notificados, acceder a las grabaciones para contar con una defensa adecuada y el derecho que las grabaciones sean destruidas cuando no se justifique su conservación o cuando sus contenidos se hayan obtenido ilegalmente.

También, establecen el actuar y forma en que deben proceder las autoridades con respecto a la instalación de los equipos y en relación con los contenidos de las imágenes.

Privacidad, Intimidad y Protección de Datos Personales están ampliamente protegidos en los tratados internacionales de los que México es parte, así como en convenios y en declaraciones que también ha aceptado el Estado Mexicano.

En nuestra Legislación Interna, la Constitución Política de los Estados Unidos Mexicanos, se establece:

Artículo 6o…

…

A…

…

II. *La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*

> ***Artículo 16.*** *Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento…*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley…*

A su vez, La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, dispone:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
>
> …
>
> ***IX. Datos personales:*** *Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;*
>
> ***XVI. Evaluación de impacto en la protección de datos personales:*** *Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;*

El rostro de una persona obtenido mediante una grabación es un dato personal protegido, y por ende el ciudadano afectado debe gozar de todas las garantías que la ley le confiere.

Software de Reconocimiento Facial y Datos Biométricos

Con el avance de la tecnología, la videovigilancia ha presentado avances sustanciales en capacidad y alcance, una muestra de ello es el reconocimiento de datos biométricos o reconocimiento facial.

La identificación biométrica no es nueva, se remonta a los programas que permiten reconocer a una persona por su retina, su huella digital, incluso su voz, tomados estos

como elementos únicos e irrepetibles en todo ser humano. La aplicación es sobre todo para el acceso a edificios, oficinas y toda clase de lugares públicos o privados donde el acceso debe ser controlado por motivos de seguridad.

En este caso no se trata de una invasión a la privacidad o intimidad de la persona, pues el usuario está uno a uno con el aparato que lo identifica y se justifica para él la necesidad, es decir, existe un consentimiento expreso.

El Sitio WEB "Legal Today", refiere en un artículo escrito por Marta Castrillo de la Fuente, abogada experta en protección de datos y nuevas tecnologías, lo siguiente:

(8 de abril de 2020)

Fuente (https://www.legaltoday.com/opinion/blogs/nuevas-tecnologias-blogs/blog-prodat/la-doble-cara-del-reconocimiento-facial-entre-las-ventajas-de-su-uso-y-el-impacto-en-nuestra-privacidad-2020-04-08/)

> *"Que alguien pueda desbloquear su teléfono móvil personal o acceder a determinadas instancias gracias a sus rasgos faciales es un hecho que, en la sociedad que vivimos hoy día, de la biometría y la autenticación por fases, no sorprende a nadie. Es más, hasta nos resultaría extraño que determinados dispositivos no nos ofreciesen estas facilidades. Esta situación, a nuestras generaciones pasadas, hasta les hubiese parecido más propio de las películas de ciencia ficción. Sin embargo, existe una realidad tangible e innegable y es que, hoy día, hacemos uso de nuestra cara como llave de acceso a nuestra información personal. En definitiva, la cara se ha convertido en la huella digital del presente milenio, relegando, a un segundo plano, la contraseña al uso.*
>
> *Todo ello es claramente posible gracias a la técnica de reconocimiento facial, entendiendo por tal a la tecnología que permite la identificación de una persona mediante el análisis de las características biométricas de su rostro. Una tecnología que, lejos de ser novedosa, nace ya en la década de los años 60 de la mano de Woodrow Wilson Bledsoe y evoluciona de forma vertiginosa y de la mano del avance de las nuevas tecnologías, principalmente en los últimos años.*
>
> *Pero ¿cómo funciona, realmente, la técnica de reconocimiento facial? La podríamos resumir en cuatro fases:*
>
> *1. Detección del rostro de la persona que se va a identificar, en el dispositivo escogido al efecto.*

2. Extracción de características faciales que conforman el denominado patrón biométrico facial.

3. Cotejo de la información biométrica obtenida con la existente en ciertas bases de datos y que tiene, como resultado, la obtención de un porcentaje de similitud de la persona a identificar, con aquellas que se encuentran en la base de datos.

4. Toma de decisión en base al porcentaje de similitud obtenido.

Esta herramienta es comúnmente utilizada en investigaciones policiales y/o desapariciones de personas de tal manera que los sistemas de reconocimiento facial se sincronizan con bases de datos de personas desaparecidas o en busca y captura, permitiendo la resolución de casos en este ámbito.

Es decir, que esta técnica cuenta con una serie de ventajas, es algo innegable. Es más, al estudiarlas, nos damos cuenta de que los dos pilares sobre los que todas ellas se asientan son la seguridad y la rapidez. Parece claro entonces que, si pensamos en hacer uso del reconocimiento facial, con la finalidad de capturar a un terrorista, todo el mundo estaría de acuerdo en hacer extensible el uso de esta técnica, ¿no?

El problema viene cuando nuestro ámbito privado y personal se ve vulnerado por el inadecuado uso que puede realizarse de este tipo de herramienta. Y es aquí, donde nos encontramos la cara "b" del reconocimiento facial.

Si existen dos grandes valores vulnerados por esa tecnología son, claramente, los derechos humanos y la privacidad. Ya lo decía el actual Comité Europeo de Protección de Datos, antiguo Grupo de Trabajo del Artículo 29, en su Dictamen 3/2012 acerca del reconocimiento facial en los servicios en línea y móviles: el seguimiento, localización o establecimiento del perfil automatizados de las personas y, como tal, sus efectos potenciales sobre la intimidad y el derecho a la protección de datos personales son importantes.

Se plantea entonces un debate ético entre lo que queremos conseguir, lo que estamos dispuestos a dar, y qué sacrificamos a cambio.

Cercando los inconvenientes que tiene la herramienta de reconocimiento facial, nos encontramos con discriminaciones raciales, usos indebidos que se hagan de los datos recogidos, errores en la identificación de las personas…etc.

No obstante, el que más preocupa al día de hoy, y con razón, es la injerencia que este tipo de tecnología tiene en la privacidad de las personas cuyos rasgos faciales se tratan. Lo primero que parece oportuno aclarar es si la cara puede considerarse un dato de carácter personal.

Para dar respuesta a esta cuestión, nos hacemos eco de lo recogido en el Reglamento General de Protección de Datos (en adelante, RGPD), concretamente en su artículo 4 en el que se recoge que un dato de carácter personal es toda aquella información que permite identificar a una persona física. Si continuamos leyendo el referido artículo, la norma considera que persona física es toda aquella cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador cómo, por ejemplo, elementos propios de la identidad física, fisiológica, genética.

No necesitamos investigar más para concluir que, efectivamente, sí, el rostro de una persona sí constituye un dato de carácter personal.

Aun así, ahondando un poco más en la categorización de la cara como dato de carácter personal, nos encontramos con que esta parte tan personal de nosotros, tiene la consideración de dato biométrico entendiendo por tal, aquella tipología de dato personal obtenido a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos tal y cómo contempla el mismo artículo 4 del RGPD.

Recordemos, igualmente, que una de las novedades que trajo consigo la actual normativa vigente en materia de protección de datos, esto es, el RGPD y la Ley Orgánica Española de Protección de Datos y Garantía de los Derechos Digitales (en adelante, LOPDGDD) fue reconocer los datos biométricos como datos especialmente protegidos equiparando su categorización a los datos de salud, de ideología política, religiosa…etc.

Es el propio RGPD el que, en diferentes puntos de su articulado, recalca la especial defensa que merecen los datos personales especialmente protegidos al ser datos que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales. Su vulneración, podría suponer un riesgo para los interesados.

¿Qué implicación tiene esta categorización? Tanto en el considerando 51 como el artículo 9 del RGPD, se recoge que por regla general quedan prohibidos los tratamientos de esta categoría de datos salvo que dicho tratamiento se encuentre dentro de alguno de los supuestos de excepción recogidos en el artículo 9.2 RGPD:

Que exista un consentimiento explícito del interesado.

Que el tratamiento se lleve a cabo para cumplir con las obligaciones y derechos del responsable del tratamiento o del interesado.

Para proteger intereses vitales del interesado u otra persona física.

Que el tratamiento se efectúe por fundaciones o asociaciones sin ánimo de lucro siempre que el tratamiento se refiera a los miembros actuales o antiguos de tales organismos.

Tratamientos referidos a datos personales que el interesado ha hecho manifiestamente públicos.

Sea necesario por razones de interés público esencial y en el ámbito de la salud pública.

Que el tratamiento sea necesario para fines de medicina preventiva o laboral.

Tratamiento con fines de archivo en interés público, investigación científica o histórica o fines estadísticos.

Cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

Si amparándose en una de las excepciones anteriormente recogidas, una empresa o país procede a la captación y tratamiento de los rasgos faciales de una multitud de personas, deberán tenerse en cuenta las siguientes salvaguardas:

Será necesaria la realización de una evaluación de impacto en los términos establecidos en el artículo 35 del RGPD.

Deberán contar con una serie de medidas de seguridad y mecanismos destinados a mitigar los riesgos que pueda entrañar la recogida y tratamiento de los datos biométricos: almacenamiento cifrado, controles de acceso, supresión automática de los datos…etc.

Y, siempre, tendrá que tenerse en cuenta los principios de limitación de la finalidad del tratamiento, minimización de datos y proporcionalidad recogidos en el artículo 5 del RGPD.

Todas estas medidas se configuran como necesarias pues, en última instancia, los datos biométricos, a diferencia de otra tipología de datos especialmente protegidos, cuentan con una problemática añadida y es que los mismos pueden recogerse sin el consentimiento de la persona en cuestión, como no ocurriría, por ejemplo, con la huella dactilar. No nos olvidemos que la captación de nuestra imagen en la vía pública, puede decir mucho más de nosotros que una mera fotografía online; desde cuáles son nuestras ideologías religiosas, hasta cuales son nuestros gustos por las tiendas en las que compramos, entre otras cuestiones.

Qué dicen nuestros referentes mundiales al respecto.

Tal y como ocurre con las diferentes voces españolas que se pronuncian acerca de la tecnología de reconocimiento facial, existen disparidad de opiniones entre los países que hacen uso de ésta. Desde China, cómo país a la cabeza de la técnica del reconocimiento facial y cuyo uso se encuentra, cada vez más, en tela de juicio. Pasando por la India, uno de los países pioneros en el uso de esta tecnología en la lucha contra el tráfico de personas. Hasta desembocar en EEUU país que ha enfocado su uso en el ámbito policial.

No obstante, limitando el uso del reconocimiento facial a nuestro territorio, hemos de recalcar que, en Europa, no lo tenemos tan claro. La injerencia que este tipo de sistemas supone en la privacidad de los interesados ha llevado a la Comisión Europea a promover, en el marco de una estrategia digital hecha realidad a través de su futuro libro blanco de Inteligencia Artificial, el veto de este tipo de sistemas, durante un plazo determinado que permita avanzar en el desarrollo de soluciones que mitiguen los riesgos que este tipo de herramientas suponen y que permitan hacer uso del reconocimiento facial de tal forma que se respeten los valores y principios europeos.

Es por ello por lo que, en última instancia, tendremos que esperar a la aprobación definitiva del mencionado Libro Blanco, para comprobar qué marco normativo nos

plantea la Comisión Europea en lo que respecta al uso de la tecnología de reconocimiento facial.

Lo que es innegable es que el reconocimiento facial es una técnica que viene pisando fuerte y que, cada vez más, adquiere un protagonismo con una indudable repercusión en nuestra esfera más privada e íntima. No obstante, no nos olvidemos que la problemática de la técnica de reconocimiento facial no se encuentra en la existencia de la herramienta en sí misma, si no en el buen o mal uso que se haga de la misma por parte de los países o empresas responsables del tratamiento.". Fin de la cita textual.

Los Falsos Positivos y las Violaciones de Derechos Humanos que Genera el Reconocimiento Facial

El 11 de junio de 2020, Amnistía Internacional publicó en su sitio WEB lo siguiente: "Amnistía Internacional pide que se prohíba el uso de tecnología de reconocimiento facial con fines de vigilancia masiva".

Fuente (https://www.amnesty.org/es/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/)

El texto es alusivo a los casos de violencia de la policía contra afroamericanos en Estados Unidos; la publicación destaca que:

"…El uso policial de la tecnología de reconocimiento facial viola los derechos humanos de distintas maneras. En primer lugar, en el contexto de la actuación policial racialmente discriminatoria y la aplicación de criterios raciales contra las personas negras, el uso de esta tecnología podría exacerbar el riesgo de que la policía cometa violaciones de derechos humanos cuando actúa contra comunidades negras. Las investigaciones realizadas coinciden en que los sistemas de reconocimiento facial procesan algunos rostros con más precisión que otros, dependiendo de características clave como el color de la piel, la etnia y el género. Por ejemplo, el Instituto Nacional de Estándares y Tecnología (NIST) ha medido los efectos de la raza, la edad y el sexo en destacados sistemas de reconocimiento facial utilizados en Estados Unidos –según el Dr. Charles H. Romine, director del NIST, "el estudio midió tasas más altas de falsos positivos en las mujeres, las personas afroamericanas y, en particular, las mujeres afroamericanas"–.

Asimismo, un equipo de investigación de la Universidad de Georgetown ha advertido de que la tecnología de reconocimiento facial "afectará desproporcionadamente a las personas afroamericanas", debido en gran parte que, en las listas de personas bajo vigilancia de la policía de Estados Unidos, hay considerablemente más rostros negros que blancos. "Los sistemas de reconocimiento facial de la policía arrojan peores resultados con las personas afroamericanas, pero es que, además, éstas tienen más probabilidades de que se las incluya en ellos y de ser objeto del tratamiento que realizan"

En segundo lugar, cuando el reconocimiento facial se utiliza con fines de identificación y vigilancia masiva, al "solucionar" el problema de la tasa de precisión y mejorar las tasas de precisión en el caso de los grupos ya marginados o desfavorecidos no se aborda el impacto de la tecnología de reconocimiento facial en el derecho de manifestación pacífica y el derecho a la privacidad. Por ejemplo, las personas negras sufran ya una injerencia desproporcionada en la privacidad y otros derechos, por lo que "mejorar" la precisión puede suponer simplemente aumentar la vigilancia y el desempoderamiento de una comunidad ya desfavorecida.

La tecnología de reconocimiento facial comporta supervisión, recopilación, almacenamiento, análisis u otros usos de material y recopilación de datos personales sensibles (datos biométricos) de manera masiva y generalizada, sin sospecha razonable e individualizada de delito, lo que constituye vigilancia masiva indiscriminada. Amnistía Internacional cree que la vigilancia masiva indiscriminada no es nunca una injerencia proporcionada en los derechos a la privacidad y la libertad de expresión, de asociación y de reunión pacífica…" Fin de la cita.

El 25 de junio de 2019, El Relator Especial de las Naciones Unidas sobre la libertad de opinión y de expresión, David Kaye, "recomendó a los Estados una suspensión inmediata de la venta, la transferencia y el uso de sistemas de vigilancia hasta que se establezcan los correspondientes marcos legales que respeten los derechos humanos.

El relator también solicitó a las Naciones Unidas, y en particular al Consejo de Derechos Humanos, la creación de un grupo de trabajo o un cuerpo especial con mandatos interrelacionados que vigile y presente recomendaciones sobre las últimas tendencias y casos individuales de vulneraciones de los derechos humanos propiciados por los sistemas de vigilancia digital".

Entre los aspectos más sensibles que los expertos en derechos humanos consideran se deben abordar en un marco legislativo que los regule, destacan:

A) La admisión de que el reconocimiento facial no es una prueba cien por ciento eficaz y precisa para identificar a una persona y que, por ende, las autoridades no deben tomarla como un medio de "identificación certero y definitivo"; sino que, como en otros medios de pruebas, se debe cotejar con más instrumentos de valoración, con peritajes imparciales y con otros elementos de convicción. Concediendo además al presunto responsable el derecho de controvertir el reconocimiento facial en términos equitativos y con el acceso a los mismos medios tecnológicos y periciales con los que cuentan las autoridades de procuración de justicia y administrativas.
B) Que el reconocimiento facial no se utilice como una herramienta de control o acoso político, para vigilar y seguir a las personas en todos lados donde existen cámaras con este tipo de software.
C) Que no se realicen grabaciones, compilación y almacenaje de material de reconocimiento facial sin que medie una orden emitida por autoridad competente con la debida fundamentación y motivación.
D) Establecer mecanismos para que el material obtenido por este tipo de sistemas no sea entregado, vendido o comercializado con terceros como el crimen organizado o personas morales y particulares con algún interés en las imágenes de una persona.
E) Que el software de reconocimiento facial no pueda estar disponible y accesible a particulares y personas morales de forma libre y sin restricciones precisas y bajo control del Estado.

Aspectos Positivos de la Videovigilancia

En todo el mundo y desde sus orígenes es una verdad incuestionable que los sistemas de videovigilancia han contribuido de manera más que significativa a la prevención; pero, sobre todo, a la investigación y resolución de delitos, desde robos simples, robos con violencia, hasta homicidios y secuestros, así como delitos sexuales, solo por citar algunos.

Es verdad que como elemento de disuasión el impacto es un tema controversial, pero aun los expertos concuerdan en que tener instalada una cámara de vigilancia siempre hace que el potencial infractor piense dos veces en sus planes.

La videovigilancia también ofrece a las autoridades de procuración de justicia una herramienta formidable para documentar, investigar y castigar las conductas delictivas; muchos crímenes pudieron haber quedado impunes si una cámara de videovigilancia no hubiera captado los hechos en el momento en que ocurrieron.

En materia de tránsito y vialidad, todos los días, la videovigilancia permite que miles de accidentes de auto por todo el mundo se puedan resolver, determinando con precisión la responsabilidad de los infractores.

La videovigilancia privada, es también una herramienta poderosa y de alto impacto, cuando los particulares se suman y aportan los contenidos de sus cámaras para la resolución de los delitos y faltas administrativas.

En cuanto al reconocimiento facial, se debe destacar que, como lo señalan los expertos, sólo bajo una regulación estricta y con mecanismos que garanticen su uso con estricto respeto a los derechos humanos y con la absoluta garantía de que no será usado con fines corruptos, sería admisible como una herramienta de seguridad.

Además, se debe garantizar que la persona videograbada con este tipo de tecnología goce de todos los derechos necesarios para defenderse ante una imputación basada en un reconocimiento facial.

Legislación Nacional y Local en Materia de Videovigilancia

En México la regulación de la videovigilancia está en ciernes, y podemos contar que, a nivel federal, se cuenta con el siguiente ordenamiento:

A partir de 2016 la Secretaría de Gobernación, a través del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, presentó la Norma Yécnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Videovigilancia de Seguridad Pública del País.

En un recorrido por las legislaciones de las entidades federativas, pudimos constatar que varios estados cuentan con leyes de videovigilancia u ordenamientos similares, a saber:

Baja California Sur. Fecha de publicación: 31 de julio de 2014.

Colima. Fecha de publicación: 22 de agosto de 2009.

Zacatecas. Fecha de publicación: 22 de agosto de 2018.

Durango. Fecha de publicación: 15 de julio de 2012

Morelos. Fecha de publicación: 08 de diciembre de 2020

Estado de México. Fecha de publicación: 28 de octubre de 2013

Yucatán. Fecha de publicación: 26 de julio de 2018.

Estas leyes en su mayoría presentan la misma estructura, que se limita a regular aspectos como:

Principios básicos;

Deberes de las autoridades;

Límite de la videovigilancia privada;

Determinación de los lugares públicos susceptibles de ser videovigilados;

La creación de comités o comisiones estatales encargadas de regular y sancionar la videovigilancia;

Las reglas de la conservación y manejo de la información;

El uso y destino de la información relacionada con delitos videograbados;

Los derechos de los particulares, generalmente bajo una óptica muy general; y

La creación de los registros estatales de equipos de videovigilancia.

Y presentan deficiencias o ausencia de rubros como los derechos humanos de los particulares con respecto a la videovigilancia y en relación con el reconocimiento facial. La falta de límites físicos precisos para los alcances de la videovigilancia gubernamental y los límites de la vigilancia privada. Por otra parte, se carece de casos o supuestos de excepción a los límites antes mencionados, además de otros aspectos de gran importancia.

Conclusiones y Objetivos de la Presente Iniciativa

En primer lugar, a lo largo de esta exposición de motivos, tratamos de hacer un ejercicio de análisis objetivo e imparcial de los aspectos negativos y positivos de la videovigilancia, tanto en lo referente a los derechos humanos, la invasión a la intimidad y a la privacidad, como a los aspectos técnicos y tecnológicos;

Recabamos los aspectos legislativos que se consideran necesarios a contemplar en una ley que regule la videovigilancia y en su caso el reconocimiento facial;

Hicimos un repaso por las diversas opiniones con relación a los conflictos de derechos humanos que plantean la videovigilancia y el reconocimiento facial; y

Resaltamos el valor y el aspecto positivos de la videovigilancia como herramienta para combatir el crimen.

Por ello, en esta iniciativa planteamos no solo el marco legislativo para regular la videovigilancia en sus aspectos generales, sino que introducimos contenidos para:

I.- Regular los límites físicos de la videovigilancia, para impedir que las cámaras vigilen u observen al interior de los hogares, oficinas, patios, traspatios y jardines. Así como áreas públicas privadas, como los baños públicos;

II.- Establecer que la colocación de las cámaras y equipos deben obedecer a razones y motivos debidamente justificados por la autoridad, y no a meras ocurrencias o criterios "estándar";

III.- Establecer los derechos de los particulares con relación a la videovigilancia;

IV.- Asegurar que la videovigilancia no se use para fines corruptos de parte de la autoridad;

V.- Establecer los límites al uso de programas de reconocimiento facial; y

VI.- Fijar el deber de la autoridad para crear protocolos para la instalación de cámaras de videovigilancia y de programas de reconocimiento facial.

Por las consideraciones expuestas, sometemos a este H. Pleno, la presente iniciativa con Proyecto de Decreto que crea la:

LEY QUE REGULA LA VIDEOVIGILANCIA EN EL ESTADO DE COAHUILA DE ZARAGOZA

CAPÍTULO PRIMERO
DISPOSICIONES GENERALES

Artículo 1.- Las disposiciones de esta Ley son de orden público e interés social y de observancia general en el Estado de Coahuila y tienen por objeto:

I. En relación con las personas que son videograbadas en la vía pública:

a. Establecer el régimen legal para el respeto de los derechos humanos en el uso de sistemas públicos de videovigilancia y manejo de la información que se obtenga de los mismos.
b. Crear un marco jurídico que brinde certeza sobre el manejo de la información que se capte a través de la videovigilancia.
c. Establecer las bases legales en caso de que se vulneren los derechos de las personas, así como para sancionar el mal uso de la información obtenida por medio de la videovigilancia y en su caso, la reparación del daño.

II. En relación con las autoridades estatales y municipales:

a. Regular la instalación y utilización de equipos y sistemas tecnológicos de videovigilancia por los organismos y dependencias de la administración pública estatal y municipal.
b. Regular la utilización de la información obtenida por el uso de equipos y sistemas de videovigilancia públicos o privados cuando capten imágenes en la vía pública.
c. Establecer un registro de sistemas públicos de videovigilancia.
d. Establecer el registro de equipos y sistemas de videovigilancia instalados u operados por particulares y que estén orientados a captar imágenes o audio en la vía pública.

Artículo 2.- Tipos de videovigilancia:

I. En razón de quien las instala y opera:

a. Públicas, aquellas adquiridas, instaladas y operadas por organismos o dependencias de la administración pública estatal o municipal.
b. Privadas, aquellas adquiridas, instaladas y operadas por particulares, ya sean personas físicas o morales.
c. Privadas de uso público, aquellas instaladas en bienes que se utilicen para la prestación de algún servicio público que se haya concesionado a particulares, quedando los concesionarios obligados a instalar, además de las cámaras que consideren conforme a su objeto, todas aquellas que la autoridad les indique,

debiendo además estar conectadas al sistema de videovigilancia público en los casos que así les sea requerido por la autoridad competente.

II. En razón de los lugares que se videovigilen:

a. Videovigilancia en la vía pública
b. Videovigilancia en lugares privados

III. Por su movilidad:

a. Fijas
b. Móviles

Artículo 3.- La videovigilancia pública a que se refiere el inciso a de la fracción II del artículo 2 de esta Ley, deberá tener como finalidad:

I. La seguridad e integridad de las personas y sus bienes;
II. La prevención de hechos delictivos;
III. La investigación y persecución de delitos;
IV. El uso adecuado y pacífico de la vía pública;
V. La documentación de conductas ilícitas; y
VI. El control del tráfico vehicular o peatonal y la recopilación de la evidencia de los accidentes para deslindar responsabilidades.

Artículo 4.- Los particulares que cuenten con equipos o sistemas privados de videovigilancia que capten imágenes o sonidos en la vía pública, otorgarán a las autoridades, en los términos que señala la presente Ley, acceso a los mismos cuando así se requiera para el cumplimiento de los fines mencionados artículo 3 de este ordenamiento.

Para efecto de lo antes mencionado, la obtención de las imágenes de cámaras de videovigilancia privada se podrá tramitar y obtener de la siguiente forma:

a. Por solicitud libre e informal realizada por las autoridades administrativas y de seguridad públicas del estado y el municipio.

b. Mediante requerimiento formal y por escrito debidamente fundamentado de las autoridades antes mencionadas, cuando el particular así lo solicite.
c. Por requerimiento oficial del Ministerio Público en los términos de la legislación penal.
d. Por requerimiento de autoridades jurisdiccionales locales y federales.

Si un particular desea hacerse o conocer el contenido de la videovigilancia obtenida por otro particular, podrá solicitarlo de forma directa. El poseedor de la información no está obligado a entregar esta o permitir el acceso a su contenido.

Los particulares tendrán derecho a hacerse y conocer el contenido de la videovigilancia obtenida por los sistemas de videovigilancia públicos, siempre y cuando el solicitante aparezca en las imágenes. En tales casos, la autoridad deberá asegurarse de resguardar la identidad de otras personas que aparezcan en la misma secuencia de grabación.

Artículo 5.- El titular del Poder Ejecutivo del Estado, y los Ayuntamientos en el ámbito de sus respectivas competencias, expedirán las normas técnicas y protocolos para la instalación de las cámaras de video vigilancia pública y privada.

El Titular del Poder Ejecutivo deberá expedir el Reglamento de esta ley, y los municipios podrán expedir sus respectivos reglamentos para la regulación de la videovigilancia que se encuentra a cargo de su competencia.

Artículo 6.- Para los efectos de la presente ley, se entiende por:

Sistema de Videovigilancia. Conjunto organizado de dispositivos electrónicos o tecnológicos que cuenten con cámaras fijas o móviles que registren imágenes con o sin sonido y las almacenen en cualquier medio tecnológico, análogo, digital, óptico o electrónico; en general a cualquier sistema de carácter similar que permita la grabación de imagen y sonido utilizadas para la videovigilancia.

Software de reconocimiento facial. Programa de computadora diseñado para analizar los datos biométricos del rostro de una persona y compararlos con los almacenados en una base de datos, a fin de identificarla.

Videocámara. Cámaras fijas o móviles, equipos de grabación, o bien, todo medio técnico análogo, digital, óptico o electrónico y, en general, cualquier sistema que permita captar o grabar imágenes con o sin sonido,

Videovigilancia. Captación o grabación de imágenes con o sin sonido que se realicen en términos de la presente Ley.

Artículo 7.- La instalación y uso de equipos y sistemas públicos de videovigilancia deberá observar los siguientes principios:

I. Principios a observar en la toma de decisión para la instalación de equipos fijos o uso de equipos móviles:

a. IDONEIDAD. Podrá emplearse la videovigilancia cuando resulte adecuado en una situación concreta, en referencia a cierta periodicidad de hechos ilícitos, o la concurrencia o tránsito de personas y/o vehículos.
b. INTERVENCIÓN MÍNIMA. La ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho a la intimidad de las personas, al honor y a la propia imagen.
c. RIESGO RAZONABLE. La utilización de videocámaras cuando razonablemente se pueda prever la proximidad o posibilidad de un daño o afectación a la seguridad pública.
d. PELIGRO CONCRETO. La utilización de videocámaras por una contingencia inminente que provoque o pueda provocar algún daño o afectación a la seguridad pública.

Principios a observar en la operación de la videovigilancia y uso de la información obtenida:

a. INTEGRIDAD CIUDADANA. El Gobierno del Estado y los Ayuntamientos en el ámbito de sus competencias, garantizarán que los sistemas públicos de videovigilancia no vulneren derechos humanos.
b. RESPETO AL FIN. La instalación de equipos o sistemas de videovigilancia, así como las imágenes y audio captados, no podrán tener un uso distinto a los que persigue la Ley.
c. DIFUSIÓN JUSTIFICADA. Las imágenes o audios captados por sistemas de videovigilancia sólo podrán ser divulgados cuando fundada y motivadamente se justifique para los fines que establece el artículo 3 de la Ley.
d. CERTEZA DE CONFIDENCIALIDAD. El Gobierno del Estado y los Ayuntamientos deberán garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o

tratamiento no autorizado, y que permitan detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o por fallas técnicas.

e. TEMPORALIDAD. Las imágenes y audio solo podrán conservarse, en los casos donde no se documente la comisión de un delito o una falta administrativa, hasta por cuarenta y cinco días naturales. En todos los demás, el tiempo que sea necesario hasta que el proceso legal del que forma parte haya concluido plenamente o causado estado.

CAPÍTULO SEGUNDO
DE LA INSTALACIÓN DE VIDEOVIGILANCIA

Artículo 8.- La instalación de equipos o sistemas de videovigilancia por cualquier entidad u órgano público en la vía pública, deberá hacerse del conocimiento del Comité Técnico de Videovigilancia. El Comité podrá emitir recomendaciones respecto a la ubicación y tipo de tecnología utilizada. Sólo en caso de considerar que se violen los requisitos y principios de la Ley, podrá ordenar que no se instale o en su caso, el retiro de la videovigilancia.

Los particulares que instalen equipos de videovigilancia en propiedad privada, pero que capten imágenes o sonidos en la vía pública, deberán registrarlos ante Comité Técnico de Videovigilancia. El Reglamento de esta Ley proveerá un procedimiento para que el registro pueda ser en línea y sólo requiera de informar la ubicación y número de equipos instalados y designar una persona para contacto.

Los desarrollos inmobiliarios que cuenten con equipos o sistemas de videovigilancia en sus accesos y salidas o en las calles, banquetas, parques o áreas públicas del desarrollo, deberán realizar el mismo registro a que se refiere el párrafo anterior de este artículo.

Artículo 9.- La instalación de equipos y sistemas púbicos de videovigilancia deberá observar los principios a que se refiere el artículo 7 de la Ley; se hará en lugares en los que contribuya a prevenir, inhibir y combatir conductas ilícitas y a garantizar el orden y la tranquilidad ciudadana y su ubicación estará basada en los criterios siguientes:

I. Lugares determinados como zonas peligrosas.
II. Áreas públicas de concentración, afluencia o tránsito de personas que se cataloguen como de posible riesgo de incidencia delictiva.

III. Colonias, calles o avenidas que registran los delitos de mayor impacto para la sociedad.
IV. Intersecciones o cruceros viales considerados conflictivos o bien, de alta comisión de ilícitos.
V. Zonas escolares, recreativas, turísticas, comerciales, instituciones bancarias, estacionamientos públicos, y lugares de alta afluencia de personas.
VI. Las zonas registradas con mayor incidencia de infracciones administrativas.
VII. Las zonas con mayor vulnerabilidad a fenómenos de origen natural o humano identificados en los atlas de riesgo.
VIII. Las zonas con mayor índice de percepción de inseguridad.

Artículo 10.- Queda prohibida la colocación de propaganda, lonas, mantas, carteles, espectaculares, estructuras, o cualquier tipo de señalización que impida, distorsione, obstruya o limite el cumplimiento de las funciones de los equipos y sistemas de videovigilancia.

Artículo 11.- La instalación y operación de equipos o sistemas de videovigilancia podrá realizarse en lugares y espacios públicos abiertos y cerrados, sin que la sola instalación y operación se consideren intromisiones ilegítimas o trasgresoras del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Artículo 12.- Salvo que exista orden judicial, las autoridades no podrán utilizar videovigilancia cuando se dé alguno de los siguientes supuestos:

I. Para captar imágenes o sonido en lugares privados salvo consentimiento del propietario o de quien tenga la posesión.
II. Cuando se tenga como propósito obtener información personal o familiar o cuando se afecte de forma directa, grave e injustificadamente la intimidad de las personas.
III. Cuando se tenga como propósito grabar conversaciones de naturaleza privada.

Las imágenes y sonidos obtenidos accidentalmente en los casos señalados en este artículo deberán ser destruidas inmediatamente por quien las haya grabado o por quien tenga la responsabilidad de su custodia.

Artículo 13.- Las cámaras de videovigilancia públicas, en ningún caso, podrán instalarse cuando tengan como finalidad vigilar o grabar las áreas siguientes de las propiedades privadas:

I. Los patios o jardines ya sean frontales o traseros;
II. Los pasillos interiores;
III. Cocheras; y
IV. Puertas y ventanas.

Se exceptúan de lo anterior, aquellas cámaras de videovigilancia que, sin tener la finalidad específica de grabar en propiedad privada, indirectamente capten imágenes de inmuebles que tienen su puerta de acceso frontal, jardines, patios o ventanas a la misma altura de la acera, en cuyo caso el ángulo de visión de la cámara no puede evitar tomarlas parcialmente.

Tampoco podrán las cámaras apuntar a las azoteas de las viviendas, exceptuando los casos donde la cámara se ubique a una altura considerable sobre el nivel de suelo y resulte imposible evitar grabar la parte de la azotea más cercana a la calle, en cuyo caso el Comité deberá determinar la distancia de la azotea que cubrirá la cámara y las razones por las que no se puede evitar la toma, debiendo notificar a los afectados la situación, para que manifiesten su derecho y en su caso su oposición.

Las prohibiciones establecidas en el presente artículo solo podrán suspenderse en los casos donde medie una autorización judicial o ministerial para efectos de investigación delictiva.

En los casos donde un particular voluntariamente acepte que su propiedad sea vigilada, la vigilancia deberá afectar solo su inmueble, espacios de los alrededores y azotea.

Los particulares deberán sujetarse a todas las limitaciones establecidas en la presente al colocar equipos de vigilancia en sus inmuebles.

Artículo 14.- Las autoridades que concesionen servicios públicos a particulares, podrán solicitar a éstos la instalación de sistemas de videovigilancia en los bienes afectos al servicio público concesionado. Así mismo, podrán solicitar que tales sistemas se interconecten con los de las propias autoridades, y en todo caso, tendrán acceso en todo momento a la información que se genere, la cual deberá ser tratada en los términos que establece la Ley.

Artículo 15.- Los equipos de videovigilancia instalados al amparo de la presente Ley, no podrán ser retirados por ninguna circunstancia, con excepción de aquellos casos en los que la autoridad determine que los equipos por su ubicación y características:

I. Han dejado de cumplir con los objetivos para los cuales se instalaron.

II. Se determine el deterioro físico que imposibilite su adecuado funcionamiento, en cuyo caso deberá repararse o sustituirse.

III. Cuando no se encuentre información relativa a la autorización otorgada para la instalación de equipos en la vía pública.

Artículo 16.- Los servidores públicos que tengan a su cargo el monitoreo de las imágenes y sonidos captados por equipos o sistemas de videovigilancia, deberán reportar de inmediato al superior jerárquico las fallas que detecten en su funcionamiento para su inmediata reparación o sustitución. La omisión en emitir el reporte o la falta de reparación o sustitución sin causa justificada será sancionada en los términos del Capítulo Sexto.

CAPÍTULO TERCERO
DEL COMITÉ TÉCNICO DE VIDEOVIGILANCIA Y LAS COMISIONES MUNICIPALES DE VIDEOVIGILANCIA

Artículo 17.- El Comité Técnico de Videovigilancia será un órgano de la Secretaria de Seguridad Pública del Estado, con independencia técnica, de gestión y para emitir resoluciones. Estará integrado por un titular y un suplente que lo cubra en su ausencia, conforme a lo siguiente:

I. Un representante del Secretario de Seguridad Pública del Estado, que será su presidente;
II. Un representante del Secretario General de Gobierno del Estado;
III. Un representante de la Fiscalía General del Estado;
IV. Un representante del Poder Legislativo, que podrá o no ser diputado, nombrado por la Comisión de Seguridad Pública;
V. Un representante del Fiscal General del Estado;
VI. Un representante de la Comisión Estatal de los Derechos Humanos;
VII. Un representante del Instituto Coahuilense de Acceso a la Información Púbica;

VIII. Un representante de cada una de las secretarias o direcciones de seguridad pública o análogos de los Ayuntamientos, que realicen actividades de videovigilancia; y

IX. Cuatro representantes ciudadanos, dos de ellos del sector empresarial y dos del sector universitario, que serán nombrados en los términos que determine el Reglamento.

Artículo 18.- El Comité Técnico de Videovigilancia velará por el debido cumplimiento de esta Ley y tendrá las siguientes atribuciones y obligaciones:

I. Tomar conocimiento, llevar registro y, en su caso, negar la instalación fija o móvil de equipos o sistemas de videovigilancia a dependencias y organismos públicos Estatales o Municipales;

II. Llevar el registro de equipos de videovigilancia privados que capten imágenes o sonidos en la vía pública;

III. Ordenar el retiro de instalaciones fijas de videocámaras cuando se viole lo dispuesto en la presente ley.

IV. Emitir resoluciones respecto a solicitudes de información de las imágenes y sonidos grabadas en lugares públicos;

V. Elaborar y expedir normas técnicas, protocolos y manuales para la materialización de sus atribuciones y cumplimiento de sus obligaciones;

VI. Ordenar la destrucción de las imágenes y sonidos obtenidos conjunta o separadamente por el sistema de videovigilancia, que vulneren el derecho a la intimidad personal y familiar; al honor y a la propia imagen, a excepción de aquellas que sean solicitadas por la autoridad competente o sean parte de un proceso judicial que puedan ayudar al esclarecimiento de hechos delictivos;

VII. Autorizar la conexión de videocámaras privadas, al sistema de videovigilancia aplicado por cualquier cuerpo de Seguridad Pública Estatal o Municipal, sólo para que éstos reciban imágenes o sonido del prestador del servicio;

VIII. Certificar que el contenido de una videograbación fue obtenido en términos de la presente Ley;

IX. Determinar la custodia y destino temporal de las videograbaciones que estime oportuno;

X. Dar aviso al superior jerárquico que corresponda, del uso indebido que se esté dando a un sistema de videovigilancia;

XI. Gestionar y en su caso recabar las grabaciones realizadas por organismos o dependencias públicas de carácter Estatal y Municipal, así como de particulares, cuando sean solicitadas por una autoridad competente;

XII. Proteger el derecho a la intimidad personal y familiar; al honor y a la propia imagen, garantizando el respeto a los principios rectores establecidos por esta Ley;

XIII. Realizar visitas de inspección y supervisión a los sitios donde se encuentren instalados equipos o sistemas de videovigilancia o donde se reciba y procese la información que éstos generan; y

XIV. Las demás que señale la Ley.

Artículo 19.- Los Ayuntamientos que operen equipos o sistemas de videovigilancia, podrán constituir Comisiones Municipales de Videovigilancia, en cuyo caso, previa notificación al Comité, podrán asumir las funciones establecidas en el artículo anterior, con excepción de las establecidas en las fracciones I y II.

El Comité otorgará en todo momento a las Comisiones acceso para consulta a los registros de equipos y sistemas de videovigilancia que se encuentren dentro de su demarcación.

Artículo 20.- Las Comisiones Municipales de Videovigilancia deberán estar integradas por:

I. El director o secretario de seguridad pública municipal, por sí mismo o a través de un representante, quien presidirá la Comisión;
II. Un representante del presidente municipal;
III. Dos integrantes del ayuntamiento nombrados por el Cabildo;
IV. Un representante del delegado o su equivalente de la Fiscalía General del Estado;
V. Un representante de la Comisión Estatal de Derechos Humanos;
VI. Un representante del Instituto Coahuilense de Acceso a la Información Pública; y

VII. Cuatro representantes ciudadanos, dos de ellos del sector empresarial y dos del sector universitario, que serán nombrados en los términos que determine el Reglamento

Artículo 21.- Cada miembro del Comité o Comisión tendrá derecho a voz y un voto. En caso de empate en las votaciones, el Presidente del Comité tendrá voto de calidad.

Artículo 22.- El Comité y, en su caso, las comisiones nombrarán un Secretario Técnico que se encargará de dar seguimiento a las sesiones, llevar actas y registros, documentar los trabajos y archivos, así como de las demás funciones que señale el Reglamento. En las sesiones del Comité o Comisión en Secretario Técnico tendrá sólo derecho a voz.

CAPÍTULO CUARTO
RECONOCIMIENTO FACIAL

Artículo 23.- En el Estado de Coahuila y en sus municipios, solo podrá utilizarse software de reconocimiento facial y tecnologías similares de identificación biométrica por medio de las cámaras y sistemas de videovigilancia pública, cuando el fin sea única y exclusivamente la investigación y persecución de los delitos, cualquier otro objetivo distinto a éste se considera nulo de pleno derecho e importará todas las responsabilidades que la ley contemple para los infractores.

Se exceptúa de lo dispuesto en el párrafo anterior, el reconocimiento facial que las autoridades implementen para fines de control de personal en las dependencias, acceso a áreas restringidas y seguridad de las instalaciones gubernamentales y militares.

No podrá utilizarse ningún software de reconocimiento facial para realizar investigaciones de carácter administrativo, civil, fiscal, laboral ni de cualquier materia ajena al proceso penal y a la investigación de los delitos, siendo las autoridades de procuración de justicia y jurisdiccionales de materia punitiva las únicas autorizadas para ordenar investigaciones e identificaciones por medio de dicha tecnología.

Artículo 24.- Los particulares que, derivado de una identificación obtenida por medio de un software de reconocimiento facial, sean imputados como responsables de un delito, tendrán en todo momento los siguientes derechos:

I. A ser informados de inmediato acerca de que fueron identificados por medio de reconocimiento facial;

II. A que se les muestre la grabación donde se les identifica y el proceso tecnológico por medio del cual se arribó a dicha conclusión;
III. A tener acceso a la grabación para que puedan controvertir su veracidad y gozar de una defensa adecuada; y
IV. En caso de que se demuestre que la identificación es negativa, que la grabación sea destruida una vez que el proceso haya concluido.

Artículo 25.- El software de reconocimiento facial no hace prueba plena en el proceso de identificar a una persona y, en todo caso, sus resultados deberán convalidarse en los términos de la legislación penal con otras pruebas y elementos de convicción.

El valor probatorio de los sistemas de reconocimiento facial por medio de datos biométricos será el que determinen la legislación penal y los criterios de los juzgadores conforme a derecho.

El rostro de una persona obtenido mediante una grabación es un dato personal protegido y por ende el ciudadano afectado debe gozar de todas las garantías que la ley le confiere.

Los particulares y las personas morales privadas solo podrán utilizar software de reconocimiento facial para fines de control de personal, accesos restringidos y seguridad interna de sus instalaciones e inmuebles. Los datos que obtengan mediante dicho sistema deberán tratarse conforme a lo establecido en las leyes de protección de datos personales vigentes en el país y en el estado, y las personas afectadas gozarán de todos los derechos a ser notificadas, a oponerse, rectificar y cancelar lo que a su derecho convenga.

CAPÍTULO QUINTO
DEL MANEJO Y CONTROL DE LA INFORMACIÓN OBTENIDA POR EQUIPOS O SISTEMAS DE VIDEOVIGILANCIA

Artículo 26.- Las instituciones públicas de carácter estatal o municipal que tengan a su cargo equipos o sistemas de videovigilancia, deberán garantizar y serán responsables de la custodia, inviolabilidad e inalterabilidad de las imágenes y sonidos obtenidos, así como sobre su destino, incluida su inutilización o destrucción.

Artículo 27.- Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las imágenes o sonidos generados, deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas y darles el manejo que señala la

presente Ley y deberán abstenerse de obtener, guardar o transferir indebidamente el original o copia de dicha información.

Cualquier uso indebido de información deberá ser reportado de inmediato al superior jerárquico y a su vez, al titular de la institución o dependencia, quien deberá reportarlo bajo su responsabilidad al Comité o Comisión para que esta a su vez, procure y vigile que se sigan los procedimientos legales para sancionar a los responsables.

Artículo 28.- Las instituciones públicas deberán emitir mensualmente un informe al Comité o Comisión sobre la utilización que se haga de la información obtenida por los equipos o sistemas de videovigilancia.

Artículo 29.- La información obtenida por las instituciones públicas sólo podrá ser utilizada para los fines de esta Ley y deberá ser proporcionada a petición del Comité o Comisión o cualquier autoridad competente que la requiera. En ningún caso, las imágenes o sonidos obtenidos podrán ser proporcionados a autoridades no competentes para solicitarla o, salvo lo dispuesto en el párrafo siguiente, a particulares. Tampoco podrá divulgarse por cualquier medio las imágenes o sonidos captados, salvo que se justifique la necesidad de su divulgación para los fines que persigue la esta Ley.

Toda persona que figure en una grabación podrá tener acceso a la misma, en los términos que señale el Reglamento de esta Ley. Podrá solicitar su destrucción siempre que la imagen o sonido no esté relacionada con la posible comisión de un delito o falta administrativa o sirva para la investigación de alguno.

Artículo 30.- Cualquier información obtenida que se considere pueda presumir la comisión de algún delito o falta administrativa, deberá ser puesta a disposición del Comité o Comisión para que certifique su autenticidad y obtención legítima conforme a esta Ley y determine su remisión a la autoridad competente para la investigación o persecución del posible delito o falta.

Artículo 31.- Toda grabación será destruida en un plazo máximo de cuarenta y cinco días naturales, contados a partir de la fecha de su captación, salvo que estén relacionadas con hechos punibles descritos en alguna figura típica, investigaciones, estudios en materia de seguridad pública, faltas administrativas relacionadas con la seguridad pública o que formen parte de un procedimiento jurisdiccional.

Artículo 32.- Las instituciones públicas deberán crear protocolos para el manejo de toda la información obtenida mediante los sistemas de videovigilancia, estableciendo una secuencia de resguardo integrada por todas aquellas medidas necesarias para evitar que

las grabaciones sean alteradas, ocultadas o destruidas, así como para garantizar su autenticidad. Las grabaciones se mantendrán en lugar seguro y protegido, sin que puedan tener acceso personas no autorizadas en su manejo. Al momento de transferir o copiar una grabación, se debe dejar constancia de ello en un documento de resguardo, asentándose una reseña de la información contenida en la grabación, sus características específicas de identificación, fecha, hora, nombre, firma de quien autoriza la transferencia o copia, así como de quien la recibe y de quien entrega, y el lugar donde se depositará, el motivo de la transferencia o copia y la parte de la grabación de la que se haya expedido copia.

Artículo 33.- El Comité o Comisión podrá, excepcionalmente, autorizar la divulgación de imágenes o sonidos obtenidos por los sistemas de videovigilancia, cuando considere que el conocimiento público pueda servir para esclarecer hechos presuntamente delictivos o localizar personas de interés por sus conductas presuntamente delictivas.

Artículo 34.- La información recabada mediante sistemas de videovigilancia podrá ser suministrada o intercambiada con Instituciones de seguridad pública de los órdenes federal, estatal o municipal, mediando convenio de colaboración y de conformidad con la Constitución Política de los Estados Unidos Mexicanos, la Ley General del Sistema Nacional de Seguridad Pública, la Ley del Sistema Estatal de Seguridad Pública, el Código Nacional, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Morelos y la Ley de Transparencia y Acceso a la Información Pública del Estado de Coahuila de Zaragoza.

CAPÍTULO SEXTO
DE LAS SANCIONES

Artículo 35.- Se aplicarán a los servidores públicos que incumplan con la presente Ley, las sanciones siguientes:

I. Con multa de 50 a 500 el valor de la unidad de media y actualización y suspensión del cargo e inhabilitación para desempeñar cargos públicos hasta por tres años, al encargado de la custodia de las grabaciones que entregue a una persona no autorizada para ser difundidas o que no las entregue conforme lo marca la presente Ley o, que no haga el reporte a que se refiere el artículo 15 de esta Ley; y

II. Con multa de 150 a 1500 de la unidad de medida y actualización, y suspensión del cargo e inhabilitación para desempeñar cargos públicos hasta por cinco

años al funcionario o servidor público que difunda o participe en la difusión de grabaciones obtenidas al amparo de la presente Ley, sin autorización previa correspondiente de la autoridad competente.

Artículo 36. Cuando se cometan infracciones por particulares a lo dispuesto en la presente Ley, se aplicarán las siguientes sanciones:

I. Con multa de 50 a 500 veces la unidad de medida y actualización, que no las entregue conforme lo marca la presente Ley; y
II. Con multa de 150 a 1500 veces la unidad de medida y actualización, al particular que difunda o participe en la difusión de grabaciones obtenidas al amparo de la presente Ley en las que no se contengan ilícitos penales o infracciones administrativas o que no las entregue conforme lo marca la presente Ley.

Artículo 37. Las sanciones establecidas en la presente Ley serán independientes de las que resulten aplicables por la comisión de delitos en términos de la legislación penal, de los daños y perjuicios que se causen conforme a la legislación civil o de las responsabilidades que en su caso deriven de la Ley General de Responsabilidades Administrativas

Artículo 38. Las infracciones previstas en la presente Ley serán interpuestas en términos de lo dispuesto por la Ley de Responsabilidad señalada en el artículo anterior. Tratándose de los prestadores de servicio de seguridad privada se aplicarán conforme a los establecido en la Ley del Sistema Estatal de Seguridad Pública de Coahuila.

CAPÍTULO SÉPTIMO
DE LOS MEDIOS DE DEFENSA

Artículo 39. Contra las resoluciones dictadas en la aplicación de esta Ley, procederá el juicio de nulidad previsto en la Ley del Procedimiento Contencioso Administrativo para el Estado de Coahuila de Zaragoza.

Tratándose del ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el manejo de datos personales, procederá el recurso de revisión, en términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza.

TRANSITORIOS

PRIMERO. El presente decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado.

SEGUNDO. En un plazo no mayor a sesenta días naturales, contados a partir de la entrada en vigor del presente decreto, deberá crearse del Comité Técnico de Videovigilancia.

TERCERO. Los municipios que cuenten con sistemas de videovigilancia podrán crear las Comisiones a que hace referencia esta Ley en un plazo no mayor a ciento veinte días naturales, contados a partir de la entrada en vigor del presente Decreto, o bien, por acuerdo de Cabildo en los términos de la ley, coordinar sus sistemas con el del estado, por medio del Comité Técnico de Videovigilancia.

CUARTO. - Los municipios que opten por manejar con independencia sus propios sistemas de videovigilancia, deberán sujetarse a las bases establecidas en esta Ley y, además, crear sus reglamentos respectivos en un plazo no mayor a ciento cuarenta días naturales, contados a partir de la entrada en vigor del presente decreto. Dichos reglamentos deberán sujetarse a las bases, alcances y límites de este decreto en todo lo que no vulnere la autonomía municipal en materia de seguridad pública.

En el mismo plazo antes mencionado, los particulares y personas morales privadas con sistemas de videovigilancia instalados deberán ser notificados de la vigencia de esta Ley, para que conozcan sus alcances y realicen los ajustes pertinentes en sus equipos.

QUINTO. - Iniciada la vigencia de esta ley, las autoridades estatales y municipales contarán con un plazo improrrogable de cuarenta y cinco días naturales para ajustar todas las cámaras de videovigilancia existentes a los límites establecidos en el presente decreto.

SEXTO. - Se derogan todas las disposiciones que se opongan al presente decreto.

Saltillo, Coahuila; a 27 de abril de 2021.

ATENTAMENTE

"POR UNA PATRIA ORDENADA Y GENEROSA

Y UNA VIDA MEJOR Y MÁS DIGNA PARA TODOS"

GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL "CARLOS ALBERTO PÁEZ FALCÓN"

DIP. RODOLFO GERARDO WALSS AURIOLES

DIP. LUZ NATALIA VIRGIL ORONA

DIP. MAYRA LUCILA VALDÉS GONZÁLEZ

HOJA DE FIRMAS QUE AOCMPAÑA LA INICIATIVA CON PROYECTO DE DECRETO QUE CREA LA LEY QUE REGULA LA VIDEOVIGILANCIA EN EL ESTADO DE COAHUILA DE ZARAGOZA