Iniciativa con Proyecto de Decreto por el que se crea la **Ley que Regula el Uso de las Cámaras de Video Vigilancia y Video Inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza.**

Presentada por el **Ing. Miguel Ángel Riquelme Solís, Gobernador Constitucional del Estado de Coahuila de Zaragoza.**

Informe en Correspondencia el día **23 de Diciembre de 2020.**

Turnada a la **Comisión de Gobernación, Puntos Constitucionales y Justicia.**

**Lectura del Dictamen:**

**Decreto No.**

Publicación en el Periódico Oficial del Gobierno del Estado:

**INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE CREA LA LEY** **QUE REGULA EL USO DE LAS CÁMARAS DE VIDEO VIGILANCIA Y VIDEO INTELIGENCIA PARA LA SEGURIDAD PÚBLICA DEL ESTADO DE COAHUILA DE ZARAGOZA, SUSCRITA POR EL GOBERNADOR CONSTITUCIONAL DEL ESTADO DE COAHUILA DE ZARAGOZA, ING. MIGUEL ÁNGEL RIQUELME SOLÍS.**

El que suscribe, Gobernador Constitucional del Estado de Coahuila de Zaragoza, en ejercicio de las facultades que me confieren los artículos 59 fracción II y 82 fracción I, de la Constitución Política del Estado de Coahuila de Zaragoza; 2, 6, 9 apartado A fracción I, de la Ley Orgánica de la Administración Pública del Estado de Coahuila de Zaragoza y 152 fracción II y 153 de la Ley Orgánica del Congreso del Estado Independiente, Libre y Soberano de Coahuila de Zaragoza, me permito someter a la consideración de este Honorable Congreso la presente Iniciativa con Proyecto de Decreto por el que se crea la Ley que Regula el Uso de las Cámaras de Video vigilancia y Video Inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza, al tenor de la siguiente:

**E X P O S I C I Ó N D E M O T I V O S**

Atendiendo al mandato conferido por el artículo 21, párrafo noveno de nuestra Constitución Federal, correspondiente a que la Seguridad Pública es una función que está a cargo de la Federación, las Entidades Federativas y los municipios, la oferta política de esta Administración, se ha cimentado sobre el compromiso con la sociedad coahuilense, de mantener la paz y la seguridad en el Estado.

Para darle rumbo a esta visión dentro del ejercicio de gobierno, en el marco del Plan Estatal de Desarrollo Coahuila 2017 - 2023, construimos el eje rector “Seguridad y Justicia” a fin de orientar las políticas públicas encaminadas a lograr que la población confíe en las autoridades del Estado, a partir del debido cumplimiento de la ley y sancionando sus transgresiones.

Asimismo, con propósito de definir las estrategias idóneas para combatir la violencia y el delito, creamos el Programa Estatal de Seguridad Pública 2017 - 2023, promoviendo un sistema de coordinación y cooperación entre los tres órdenes de gobierno, situándonos como referencia nacional y ejemplo de corresponsabilidad[[1]](#footnote-1), en el combate a la delincuencia.

Del mismo modo, bajo la indubitable premisa de que dichos esfuerzos serían en vano sin una agenda de estado que promueva, respete, proteja y garantice los Derechos Humanos, con el apoyo de la Universidad Autónoma de Coahuila, la Academia Interamericana de Derechos Humanos y la Sociedad Civil, se diseñó el Programa Estatal de Derechos Humanos 2019 - 2023, a fin de transitar hacia una política garantista, que nos permita materializar los ideales de contar con Ciudades Seguras, en Paz y Libres de Violencia, que nuestras fuerzas del orden actúen respetando los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los Derechos Humanos y Ciudades Inteligentes con Protección de Datos Personales.

En este contexto, con el firme propósito de continuar los esfuerzos que nos permitan salvaguardar la vida, las libertades, la integridad y el patrimonio de todos los coahuilenses, así como contribuir a la generación y preservación del orden público y la paz social, es que le expresamos a este Honorable Congreso, la necesidad de contar con un marco normativo que responda a las necesidades puntuales que la materia de seguridad exige, particularmente en lo que obedece a la Video vigilancia.

La Video Vigilancia, puede definirse como una herramienta tecnológica que, a través de cámaras de video localizadas estratégicamente e interconectadas entre sí, permiten apoyar la operación y despliegue policial, la atención de emergencias, la prevención del delito y la procuración de justicia[[2]](#footnote-2). La adecuada implementación de los sistemas de video vigilancia, mejora, a su vez, la seguridad de la ciudadanía mediante el monitoreo de ambientes abiertos y cerrados, tales como calles y avenidas, bancos, supermercados, áreas de estacionamiento, edificios, entre otros.

Esto permite ampliar la capacidad de reacción de las fuerzas del orden en casos que amenazan la integridad de las personas, como accidentes, incendios u otro tipo de eventualidades.

De igual manera, la video vigilancia aumenta las fortalezas institucionales, puesto que incrementa la capacidad de supervisión a prácticamente 24 horas por 365 días. En ese sentido, sus efectos pueden entonces catalogarse en dos dimensiones principales: como un disuasor de delitos y como coadyuvante en la investigación y prevención policial.

La instalación de los sistemas de video vigilancia, se rige bajo el principio de que, si el delincuente percibe mayor certeza de ser capturado, disminuirán las posibilidades de involucrarse en alguna actividad criminal.[[3]](#footnote-3) Es decir, la video vigilancia puede funcionar de manera positiva para reducir el riesgo de incidencia de un delito, a la vez de que permite que las autoridades cuenten con material que sirva como evidencia para una denuncia futura. Derivado de la reducción de la criminalidad, un incremento en la sensación de seguridad puede acarrear impactos benéficos para la cohesión social en una comunidad, e incluso, en una ciudad o un estado.

En comparación con otros mecanismos, los sistemas de video vigilancia representan, asimismo, una alternativa con un mejor balance entre costo y beneficio en el manejo de la seguridad pública. La video vigilancia es una mejor inversión que el personal de seguridad en términos de eficiencia.[[4]](#footnote-4) A diferencia del recurso humano patrullando las calles, un sistema de video vigilancia no es susceptible de fatiga o pérdida de concentración, lo que implica un esfuerzo ininterrumpido, constante y consistente. A pesar de que el gasto hecho en un sistema de video vigilancia podría parecer mayor, en el largo plazo representa una forma de ahorro en comparación con la contratación de oficiales de policía adicionales.

Del mismo modo, la video vigilancia tiene un efecto positivo no solamente en la disuasión del delito, sino también en las propias tareas de los elementos de policía en tierra. Cuando la video vigilancia opera en coordinación con los organismos de mantenimiento del orden, la policía percibe una mayor certidumbre en el desempeño de su labor. Así, la inversión no sustituye a las capacidades del elemento humano, sino que extiende sus posibilidades y le brinda mayor seguridad para la realización de su trabajo.

La creación de esta Ley, obedece a la necesidad de un ordenamiento que no solo garantice un mejor uso de los recursos públicos para seguridad, sino que también permita establecer criterios en la planeación, diseño, implementación y operación de los sistemas de video vigilancia con base en la necesidad, proporcionalidad e integralidad de las medidas de prevención y contención del delito. Esta medida coadyuva a contemplar una visión multifactorial de la problemática a resolver.

A pesar de las ventajas que se han enumerado anteriormente, los sistemas de video vigilancia, representan un debate continuo con la sociedad civil sobre el balance que debe existir entre la seguridad pública y derechos como la privacidad, la transparencia o la proporcionalidad.

Especial relevancia cobra el aspecto correspondiente a la tecnología de Reconocimiento Facial. Por un lado, si bien es cierto que el Estado debe ser capaz de utilizar la tecnología a su alcance, el mismo tiene la obligación de hacerlo en un marco objetivo de legalidad.

Por ende, el presente proyecto contempla como base, los casos de éxito de las experiencias europeas en la implementación de sistemas de video vigilancia y reconocimiento facial.

En primer lugar, al retomar los precedentes legales y jurisprudenciales del Tribunal Europeo de Derechos Humanos, que reconocen que recolectar datos biométricos de las personas constituye un acto de molestia,[[5]](#footnote-5) podemos crear las bases legales para sustentar, conforme a los criterios establecidos en nuestra Constitución Federal, la validez de los actos de molestia, que, de acuerdo a estándares internacionales, comprende una dimensión dual: contar con fundamentación en el orden jurídico local y prever garantías y sanciones para el uso indebido de la información obtenida. Bajo dichos estándares, es que esta Ley y su articulado, buscan dar forma a las dimensiones aludidas.

De igual manera la experiencia europea,[[6]](#footnote-6) reconoce que el uso de sistemas de reconocimiento facial, soporta el ejercicio del denominado “test de proporcionalidad”; herramienta metodológica adoptada en los diversos sistemas de protección de derechos humanos, con fin de ponderar casos de conflictos entre derechos fundamentales, siendo el particular, el relativo a la Privacidad y la Seguridad Pública.

En ese orden de ideas, podemos afirmar que, a la luz del instrumento anteriormente referido, el sistema de video vigilancia y la tecnología de reconocimiento facial, persiguen un objeto lógico (la seguridad pública), el cual es lo suficientemente relevante para limitar el ejercicio de un derecho fundamental (privacidad) y su uso tiene conexión lógica y racional con el objeto.

Abundando en lo anterior, es pertinente precisar, que el sistema de video vigilancia y la tecnología de reconocimiento facial, no se utilizan para recopilar datos al azar; el procedimiento de reconocimiento facial, opera de la siguiente manera: los equipos con capacidades de reconocimiento facial, obtienen una imagen digital del rostro de las personas, con fin de extraer y procesar sus datos biométricos; esta imagen, es luego comparada con la información contenida en listas de excepción, cuyos rubros comprenden, desde órdenes de aprehensión, vehículos robados, mandamientos judiciales y ministeriales, así como personas ausentes y/o no localizadas, Alerta AMBER o Protocolo Alba, por referir algunas. Las personas que no se encuentren dentro de los archivos correspondientes a las listas de excepción referidas, o no actualicen alguno de los supuestos constitucionales previstos sobre flagrancia, no serán objeto del sistema de reconocimiento facial, asegurando con ello que la operación del mismo no ocurra de manera arbitraria.

Finalmente, y con propósito de cumplir con las garantías debidas para la óptima operación del sistema y con estricto apego a derechos humanos, hemos creado un comprehensivo capítulo sobre el régimen disciplinario, delitos y sanciones que permitan castigar cualquier uso ilegítimo o incorrecto que pretenda darse a los equipos y/o a la información contenida en sus archivos.

Por ello, creemos firmemente, que el uso de los sistemas de video vigilancia y reconocimiento facial es compatible con el Estado de Derecho y los principios de la sociedad democrática, en tanto existan mecanismos que regulen su uso y aplicación dentro de los estándares de la legalidad. Esta Ley es el primer paso para lograr esta meta.

En virtud de lo anterior, es que ponemos a consideración de esta Honorable Legislatura para su revisión, análisis y en su caso aprobación, la siguiente iniciativa con proyecto de:

**D E C R E T O**

**ARTÍCULO ÚNICO.** Se creala Ley que Regula el Uso de las Cámaras de Video Vigilancia y Video Inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza,para quedar como sigue:

**LEY QUE REGULA EL USO DE LAS CÁMARAS DE VIDEO VIGILANCIA Y VIDEO INTELIGENCIA PARA LA SEGURIDAD PÚBLICA DEL ESTADO DE COAHUILA DE ZARAGOZA**

**CAPÍTULO I**

**DISPOSICIONES GENERALES**

**Artículo 1**. La presente Ley es de orden público e interés social y de observancia general en todo elterritorio del Estado de Coahuila de Zaragoza.

**Artículo 2.** El presente ordenamiento tiene por objeto regular:

1. La ubicación, instalación y operación de equipos y sistemas tecnológicos de video vigilancia y video inteligencia a cargo de la Secretaría de Seguridad Pública;
2. La obtención, tratamiento y resguardo de la información obtenida, a través de equipos y sistemas tecnológicos de video vigilancia y video inteligencia.

Las autoridades encargadas de la aplicación de esta Ley, deberán actuar con pleno respeto a los derechos humanos, cumpliendo además con los principios de estricta legalidad, legitimidad, idoneidad, utilidad, necesidad y proporcionalidad.

**Artículo 3.** Para los efectos de esta Ley, se entenderá por:

1. Alerta AMBER: Herramienta de difusión para la pronta localización y recuperación de niñas, niños y adolescentes, que se encuentren en riesgo inminente de sufrir daño grave por motivo de no localización o cualquier circunstancia donde se presuma la comisión de algún delito ocurrido en territorio nacional;
2. Archivo:Colección de datos de un mismo tipo;
3. Biometría:Método de reconocimiento de personas basado en sus datos biométricos;
4. Centro de Comunicaciones, Cómputo, Control y Comando: Unidad administrativa adscrita a la Secretaría, encargada de implementar, administrar y desarrollar las herramientas tecnológicas aplicadas a la seguridad pública, promover su uso en favor de las instituciones y corporaciones autorizadas, además de comprender el registro, atención y despacho de las llamadas al sistema de emergencias y denuncia anónima;
5. Comité: Comité de Video Vigilancia y Video Inteligencia;
6. Datos Biométricos: Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles;
7. Datos Personales: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, 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;
8. Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;
9. Equipos y Sistemas Tecnológicos de Video Vigilancia y Video Inteligencia: Conjunto de aparatos y dispositivos dentro de la categoría detecnologías de la información y comunicación para la seguridad pública, adecuados para el tratamiento de datos biométricos;
10. Fiscalía: Fiscalía General del Estado de Coahuila de Zaragoza;
11. Información Confidencial:La información en posesión de los sujetos obligados, que refiera a la vida privada y/o los datos personales, por lo que no puede ser difundida, publicada o dada a conocer, excepto en aquellos casos en que así lo contemple la ley de acceso a la información pública, ley general de transparencia y/o la Ley General de Protección de Datos Personales;
12. Información Reservada: La información pública que por razones de interés público sea excepcionalmente restringido el acceso de manera temporal;
13. Instituciones de Seguridad Pública: Secretaría de Seguridad Pública, Fiscalía, Procuraduría para Niños, Niñas y la Familia, Secretariado Ejecutivo y dependencias encargadas de la seguridad pública en los municipios; sus unidades administrativas internas, delegaciones y/o coordinaciones;
14. Ley: Ley que Regula el Uso de las Cámaras de Video Vigilancia y Video Inteligencia para la SeguridadPública del Estado de Coahuila de Zaragoza;
15. Lista de Excepción: Archivo que contiene los datos necesarios para que el sistema de reconocimiento facial realice la búsqueda de una persona o una placa;
16. Medidas de Seguridad:Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;
17. Medidas de Seguridad Administrativas:Políticas, acciones y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;
18. Medidas de Seguridad Físicas:Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De maneraenunciativa más no limitativa, se deben considerar las siguientes actividades:
	1. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
	2. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
	3. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización;
	4. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;
19. Medidas de Seguridad Técnicas: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
	1. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea solamente por usuarios identificados y autorizados;
	2. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
	3. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;
	4. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;
20. Protocolo Alba: Documento que contiene lineamientos generales y los principios básicos para implementar un mecanismo de búsqueda y localización de mujeres y niñas desaparecidas en México;
21. Reconocimiento Facial: Sistema de recopilación e identificación biométrica, a través de una imagen digital del rostro, mediante la comparación de determinadas características de la cara con la información de esa persona en una base de datos;
22. Registro: Registro de Equipos y Sistemas Tecnológicos de Video vigilancia y Video inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza;
23. Reglamento: Reglamento de la Ley que Regula el Uso de las Cámaras de Video Vigilancia y Video Inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza;
24. Secretaría: Secretaría de Seguridad Pública del Estado de Coahuila de Zaragoza;
25. Secretariado Ejecutivo: Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública;
26. Tecnología: Conjunto de recursos, procedimientos y técnicas usados para el procesamiento, almacenamiento y transmisión de la información, utilizados para apoyar tareas de seguridad pública;
27. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, mismas que son relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;
28. Video de Evidencia: Se consideran a todos aquellos vídeos que se vean involucrados en una Solicitud de Grabación;
29. Video de Flujo Diario: Hace referencia al video que es recibido en tiempo real por las videocámaras del Sistema de Video vigilancia;
30. Video de Incidencia: Son los videos que se derivan del flujo diario donde el operador de video vigilancia detecte algún incidente, o cuando originado de algún reporte de incidente proveniente de una llamada de emergencia, uno o varios operadores de video vigilancia puedan dar seguimiento con alguna de las videocámaras;
31. Video Vigilancia: Herramienta tecnológica que, a través de cámaras de video localizadas estratégicamente e interconectadas entre sí, permiten apoyar la operación y despliegue policial, la atención de emergencias, la prevención del delito y la procuración de justicia;
32. Video Inteligencia: Instrumentos y herramientas de aplicación práctica, que refuerzan la operación de las instituciones de seguridad pública, aportando información estratégica para la ejecución de acciones, la elaboración de estrategias y el diseño de políticas públicas, que permitan prevenir, disuadir, contener y neutralizar, riesgos y amenazas a la seguridad. Son el resultado de la sistematización y análisis de la información cuantitativa y cualitativa recabada por el Sistema de Video Vigilancia.

**Artículo 4.** Se crea el Registro, mismo que estará a cargo de la Secretaría, que integrará aquellosequipos y sistemas tecnológicos de video vigilancia y video inteligencia de las instituciones de seguridad pública.

La organización del Registro y demás aspectos relacionados, estarán previstos en el Reglamento.

**CAPÍTULO II**

**DE LOS PRINCIPIOS**

**Artículo 5.** La captación o grabación de imágenes con o sin sonido en términos de esta Ley, se regirá por los principios de: Proporcionalidad; Riesgo Razonable; Peligro Concreto; Certeza y Seguridad Jurídica; Finalidad; Confidencialidad; Legalidad; Libertad y No Discriminación.

 **CAPÍTULO III**

**DEL COMITÉ DE VIDEO VIGILANCIA Y VIDEO INTELIGENCIA**

**Artículo 6.** El Comité de Video Vigilancia y Video Inteligencia, es un órgano colegiado de la Secretaría, encargado de conocer y vigilar lo relacionado con la obtención, tratamiento y resguardo de la información obtenida mediante los equipos y sistemas tecnológicos de video vigilancia y video inteligencia.

**Artículo 7**. El Comité estará integrado por los titulares de:

1. La Secretaría de Seguridad Pública del Estado, quien será su Presidente;
2. El Centro de Comunicaciones, Cómputo, Control y Comando;
3. La Dirección General Jurídica de la Secretaría;
4. La Unidad de Transparencia de la Secretaría;
5. La Dirección General de Derechos Humanos de la Secretaría;
6. La Fiscalía General del Estado;
7. La Comisión de los Derechos Humanos del Estado de Coahuila de Zaragoza;
8. El Instituto Coahuilense de Acceso a la Información.

El Comité contará con un Secretario Técnico, que será el representante del Centro de Comunicaciones, Cómputo, Control y Comando, mismo que se encargará de dar seguimiento a las sesiones, llevar actas y registros, documentar los trabajos, certificar documentos y archivos, así como de las demás funciones que señale el Reglamento.

Todos los integrantes del Comité, salvo quienes concurran como invitados, tendrán derecho a voz y voto. En caso de empate, el Presidente contará con voto de calidad.

En caso de que los titulares previstos en la integración del presente Comité no puedan concurrir a las sesiones, el Reglamento preverá lo conducente para la designación de los representantes correspondientes.

**Artículo 8.** El Comité deberá contar con invitados permanentes:

1. Un representante de la sociedad civil con experiencia en la materia;
2. Un representante del sector académico con experiencia en la materia.

Los invitados al Comité, tendrán carácter honorífico y solamente tendrán derecho a voz y no a voto.

**Artículo 9.** Serán facultades del Comité:

1. Vigilar el correcto tratamiento de la información obtenida por los equipos y sistemas tecnológicos de video vigilancia y video inteligencia;
2. Conocer del incumplimiento a lo establecido en la presente Ley, para su remisión a las autoridades competentes en la materia;
3. Certificar la información que se genera por la operación del sistema de video vigilancia y video inteligencia;
4. Dar aviso al superior jerárquico que corresponda, del uso indebido que se esté dando a un sistema de video vigilancia y video inteligencia;
5. Realizar inspecciones y visitas de supervisión a los sistemas de video vigilancia y video inteligencia;
6. Las demás que señale la Ley.

**Artículo 10**. El Comité deberá sesionar por lo menos una vez cada treinta días; para sesionar válidamente, se necesitará la presencia de más de la mitad de sus miembros; podrá sesionar de manera extraordinaria a petición de cualquiera de sus miembros o a solicitud de cualquier autoridad de seguridad pública que lo requiera, las veces que sea necesario.

Los acuerdos y/o resoluciones que emita, deberán ser aprobados por la mayoría de los presentes en la sesión.

**Artículo 11.** El Comité deberá rendir un informe de manera trimestral ante el Consejo Estatal de Seguridad Pública, en el que detalle de manera integral los trabajos desarrollados en la entidad en materia de Vídeo Vigilancia y Video Inteligencia.

**CAPÍTULO IV**

**DE LA SECRETARÍA**

**Artículo 12.** La Secretaría, para la operación de los equipos y sistemas tecnológicos del sistema de video vigilancia y video inteligencia tendrá las siguientes atribuciones:

1. Operar a través del Centro de Comunicaciones, Cómputo, Control y Comando el sistema de video vigilancia y video inteligencia;
2. Proponer, coordinar y ejecutar la implementación de las acciones derivadas de las disposicionesque en materia de uso de tecnologías de la información y comunicación para la seguridad pública, determinen la presente Ley y el Reglamento;
3. Operar, administrar y actualizar el Registro a través del Centro de Comunicaciones, Cómputo, Control y Comando; la organización y funcionamiento del Registro y demás aspectos relacionados, estarán previstos en el Reglamento;
4. Clasificar, resguardar y registrar la información captada por los equipos y sistemas tecnológicos enlos términos establecidos por la presente Ley, la Ley del Sistema de Seguridad Pública del Estado de Coahuila de Zaragoza, 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 Coahuila de Zaragoza, la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables;
5. Garantizar la inviolabilidad e inalterabilidad de la información recabada con equipos o sistemastecnológicos;
6. Promover y celebrar convenios con autoridades de los tres órdenes de gobierno, a fin de lograr una efectiva coordinación y funcionamiento del sistema de video vigilancia y video inteligencia;
7. Las demás que establezca esta Ley, su Reglamento y demás disposiciones aplicables.

**CAPÍTULO V**

**DEL CENTRO DE COMUNICACIONES, CÓMPUTO, CONTROL Y COMANDO**

**Artículo 13.** La Secretaría, operará y regulará el Centro deComunicaciones, Cómputo, Control y Comando, para el correcto uso, manejo, tratamiento y almacenamiento de la información obtenida con equipos y sistemas tecnológicos de video vigilancia y video inteligencia, de conformidad con lo establecido en la presente Ley, su Reglamento, la Ley del Sistema de Seguridad Pública del Estado de Coahuila de Zaragoza y demás ordenamientos aplicables.

**Artículo 14.** Los equipos y sistemas tecnológicos de video vigilancia y video inteligencia utilizados por dependencias y entidades de la administraciónpública estatal, por los municipios y por las instituciones de seguridad privada, deberán ser inscritos en el Registro.

La video vigilancia en vías públicas, será función exclusiva de las instituciones de seguridad pública.

**Artículo 15.** El Centro de Comunicaciones, Cómputo, Control y Comando deberá establecer medidas de seguridad de alto nivel, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

**CAPÍTULO VI**

**DE LOS LINEAMIENTOS A QUE SE SUJETARÁ**

**LA COLOCACIÓN DE EQUIPOS Y SISTEMAS TECNOLÓGICOS**

**Artículo 16.** La instalación de los equipos y sistemas tecnológicos del sistema de video vigilancia y video inteligencia estará a cargo de la Secretaría y se realizará acorde a los criterios establecidos en la presente Ley.

**Artículo 17.** La instalación se realizará en lugares en los cuales sea posible prevenir, inhibir y combatir conductas ilícitas, se refuerce la operación y despliegue policial, se brinde mejor atención y despacho de situaciones de emergencia y se fortalezca el estado de derecho para garantizar el orden y la tranquilidad de los habitantes del Estado de Coahuila de Zaragoza.

**Artículo 18.** Los equipos y sistemas tecnológicos instalados conforme a lo establecido en la presente Ley, sólo podrán ser retirados por la Secretaría cuando:

1. No contribuyan al objeto y fines de la presente Ley;
2. Se advierta un deterioro físico que imposibilite el adecuado cumplimiento de sus funciones, debiendo, en su caso, repararse o sustituirse conforme a la disponibilidad presupuestal en la materia;
3. Cuando así lo determine el Comité.

**Artículo 19.** Queda prohibido a cualquier ente público la colocación de equipos y sistemastecnológicos al interior de los domicilios particulares.

Queda prohibida la instalación en cualquier lugar, de equipos y sistemas tecnológicos, con el objeto de obtener información privada sin fines de seguridad pública y procuración de justicia.

La Secretaría podrá instalar los equipos tecnológicos fijos en bienes del dominio público del Estado o los municipios. Para la instalación en cualquier otro lugar, se requerirá autorización por escrito del propietario o poseedor del lugar en el que se pretendan ubicar los equipos y sistemas tecnológicos.

Dicha autorización será confidencial y deberá resguardarse junto con la información obtenida por los sistemas tecnológicos, de conformidad con lo dispuesto en la presente Ley y demás disposiciones aplicables.

Queda prohibida la colocación de propaganda, mantas, lonas, carteles, espectaculares, estructuras, señalizaciones y en general, cualquier objeto que impida, distorsione, obstruya o limite el cumplimiento de las funciones de los equipos y sistemas tecnológicos.

**Artículo 20.** Son criterios para la instalación y operación de equipos y sistemas tecnológicos de video vigilancia y video inteligencia lossiguientes:

1. Zonas escolares, recreativas y lugares de mayor afluencia de público, turismo o comercio;
2. Las áreas públicas de zonas, colonias y demás lugares de concentración o afluencia de personas o tránsito de las mismas, registradas con mayor incidencia delictiva en la estadística criminal de las instituciones de seguridad pública, de los municipios o de los sistemas de emergencia 911 y de denuncia anónima 089;
3. Las colonias, manzanas, avenidas, calles y demás lugares que registren los delitos de mayor impacto para la sociedad;
4. Las intersecciones viales más conflictivas clasificadas por la Secretaría o por los municipios;
5. Las zonas con mayor índice de percepción de inseguridad;
6. Las zonas con mayor vulnerabilidad a fenómenos de origen natural o humano identificados en losatlas de riesgo;
7. Cualquier instrumento de análisis diferente a la prevención, que permita la toma de decisionesen materia de seguridad pública, así como aquella información que posibilite su adecuada colocación, para el cumplimiento de sus fines;
8. Las zonas registradas con mayor incidencia de infracciones administrativas.

**CAPÍTULO VII**

**DEL RECONOCIMIENTO FACIAL**

**Artículo 21.** La tecnología de Reconocimiento Facial, es un sistema de recopilación e identificación biométrica, a través de una imagen digital del rostro, mediante la comparación de determinadas características de la cara con la información de esa persona en los archivos correspondientes a las listas de excepción.

**Artículo 22.** Para realizar el procedimiento de reconocimiento facial, los equipos y sistemas tecnológicos de video vigilancia y video inteligencia de la Secretaría, tomarán una fotografía digital del rostro, a efecto de extraer y procesar los datos biométricos correspondientes y compararlos con los archivos correspondientes a las listas de excepción.

**Artículo 23.** Los archivos y/o listas de excepción en las que se realizará la consulta de comparación, serán de manera enunciativa más no limitativa las siguientes:

1. Órdenes de Aprehensión y/o Reaprehensión;
2. Personas ausentes y/o desaparecidas;
3. Alerta AMBER;
4. Protocolo Alba;
5. Vehículos Robados;
6. Mandamientos Ministeriales y/o Judiciales.

Cualquier persona que no se encuentre en ningún archivo y/o lista de excepción o actualice los supuestos constitucionales correspondientes a la flagrancia, no será objeto del sistema de reconocimiento facial.

**Artículo 24.** Si derivado del procedimiento de reconocimiento facial, el sistema no encuentra coincidencias entre la imagen capturada y los registros comprendidos en los archivos y/o listas de excepción, la imagen y sus datos biométricos serán eliminados de inmediato.

**Artículo 25.** En caso que del procedimiento de reconocimiento facial, el sistema encuentre una coincidencia, con los archivos y/o listas de excepción preexistentes, los datos de alerta serán enviados a las corporaciones a través del Sistema Estatal de Emergencias del Centro de Comunicaciones, Cómputo, Control y Comando, para su atención.

**CAPÍTULO VIII**

**DE LA UTILIZACIÓN, TRATAMIENTO, CONTROL Y RESERVA DE LA INFORMACIÓN OBTENIDA CON LOS EQUIPOS O SISTEMAS DE VIDEO VIGILANCIA Y VIDEO INTELIGENCIA**

**Artículo 26.** Las imágenes y sonidos captados a través de equipos o sistemas tecnológicos de video vigilancia y video inteligencia, así como la información que se obtenga de aquellos, se podrá utilizar en:

1. La prevención de los delitos e infracciones administrativas;
2. El combate a la delincuencia;
3. La investigación de los delitos;
4. La localización de aquellas personas con mandamientos judiciales y/o ministeriales pendientes de cumplimiento;
5. La imposición de sanciones por infracciones administrativas;
6. La búsqueda y localización de personas ausentes y/o desaparecidas;
7. La identificación de vehículos robados;
8. Reacción inmediata, en los casos en que, a través de la información obtenida con equipos ysistemas tecnológicos, se aprecie la comisión de un hecho delictuoso o infracción administrativa y se esté en posibilidad jurídica y material de asegurar al presunto responsable, así como la identificación de vehículos con reporte de robo o como instrumentos de delito de conformidad con las leyes aplicables.

**Artículo 27.** Toda información obtenida por las instituciones de seguridad pública, con el uso deequipos y sistemas tecnológicos, deberá ser resguardada por el Centro de Comunicaciones, Cómputo, Control y Comando, de conformidad con lo establecido en la presente Ley y demás disposiciones aplicables.

**Artículo 28.** La información recabada, deberá ser resguardada en los siguientes términos:

1. Las grabaciones clasificadas como flujo diario, por un mínimo de quince días naturales;
2. Las grabaciones clasificadas como Incidente, un mínimo de seis meses;
3. Las grabaciones clasificadas como Evidencia, un mínimo de dos años, o el tiempo que sea necesario si así lo solicita la autoridad jurisdiccional.

**Artículo 29.** Toda información recabada por las instituciones de seguridad pública con el uso deequipos y sistemas tecnológicos, deberá ser remitida a petición de cualquier autoridad judicial o ministerial que la requiera para el cumplimiento de sus atribuciones.

**Artículo 30.** Se prohíbe proporcionar a los particulares y/o autoridades que no cuenten con atribuciones para ello, la información recabada por las instituciones de seguridad pública mediante el uso de equipos y sistemas tecnológicos.

**Artículo 31.** Las instituciones de seguridad pública deberán garantizar la inviolabilidad einalterabilidad de la información recabada con equipos y sistemas tecnológicos, mediante la Cadena de Custodia correspondiente.

Los servidores públicos que tengan bajo su custodia la información a que hace referencia este artículo, serán responsables directamente de su guarda, inviolabilidad e inalterabilidad, conforme a lo dispuesto por el Código Nacional de Procedimientos Penales.

**Artículo 32**. Al realizarse cualquier grabación cumpliendo los requisitos establecidos en esta Ley y si en ella existen elementos útiles para la investigación de un hecho punible, será certificada por el Comité y se pondrá a disposición del Ministerio Público o la autoridad jurisdiccional que lo solicite; cuando sean hechos punibles que se persigan de oficio, se enviará a la Fiscalía, o bien, a la Delegación de la Fiscalía General de la República, según corresponda.

La certificación del Comité se realizará sobre la forma, términos y fecha en que fue obtenida la grabación, así como del manejo y administración que se ha dado a la misma. La validación de los contenidos o respecto de la alteración o no de las grabaciones, en su caso corresponderá a los Servicios Periciales de la Fiscalía.

Tratándose de captación o manejo de las imágenes, el personal autorizado, en caso de advertir la posible comisión de un hecho punible, deberá dar aviso inmediato a su superior jerárquico, así como al Ministerio Público.

Cuando se trate de hechos que pudieran ser constitutivos de faltas administrativas relacionadas con la seguridad pública, se informará al órgano sancionador competente. En ambos casos, se deberá remitir un informe pormenorizado al Comité.

**Artículo 33.** Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones, deberá observar el debido sigilo en su tratamiento y garantizar su confidencialidad, siendo de aplicación, en caso contrario, lo dispuesto en la presente Ley en materia de sanciones.

**Artículo 34.** La Secretaría, no estará obligada a recabar el consentimiento del titular para el tratamiento de sus datos personales, cuando estos sean utilizados para el cumplimiento del objeto de esta Ley y cuando se actualicen los supuestos previstos por el artículo 16 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza.

**Artículo 35.** La información recabada con los equipos y sistemas tecnológicos, será considerada como reservada o confidencial, en los términos que establezcan las disposiciones vigentes en la materia.

**CAPÍTULO IX**

**DE LAS RESPONSABILIDADES ADMINISTRATIVAS Y LOS DELITOS**

**Artículo 36.** El incumplimiento a lo dispuesto por la presente Ley, será sancionado administrativamente por el Órgano Interno de Control de la Secretaría o la Comisión del Servicio Profesional de Carrera, Honor y Justicia, según corresponda y de conformidad con las disposiciones aplicables, sin perjuicio de las responsabilidades civiles y/o penales que resulten.

**Artículo 37.** A quien sin autorización conozca, obtenga, copie, utilice, modifique, destruya o provoque pérdida de información contenida en cualquier equipo o sistema tecnológico de video vigilancia y video inteligencia del Estado, se le impondrá pena de cuatro a diez años de prisión y de quinientos a mil días multa. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se aumentará hasta en dos terceras partes el máximo de las penas previstas y se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

**Artículo 38.** A quien estando autorizado para acceder u operar equipos o sistemas tecnológicos de video vigilancia y video inteligencia del Estado, indebidamente conozca, obtenga, copie, utilice, modifique, destruya o provoque pérdida de información contenida en cualquier equipo o sistema tecnológico de video vigilancia y video inteligencia, se le impondrá pena de cuatro a diez años de prisión y de quinientos a mil días multa. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se aumentará hasta en dos terceras partes el máximo de las penas previstas y se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

**Artículo 39.** Las resoluciones administrativas que en aplicación de la presente Ley dicten las autoridades, y que los interesados estimen ilegales, podrán ser recurridas mediante el recurso de revisión previsto en la Ley de Procedimiento Administrativo para el Estado de Coahuila de Zaragoza.

**T R A N S I T O R I O S**

**PRIMERO.** La presente Ley, entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado.

**SEGUNDO.** El Centro de Comunicaciones, Cómputo, Control y Comando deberá integrar el Registro de Equipos y Sistemas Tecnológicos de Video Vigilancia y Video Inteligencia para la Seguridad Pública, dentro de los noventa días naturales siguientes a la entrada en vigor de la presente Ley.

**TERCERO.** El Reglamento de la Ley que se expide deberá emitirse en un término de noventa díasnaturales contados a partir del inicio de la vigencia de la presente Ley.

**CUARTO.** Los ayuntamientos de los municipios del Estado tendrán la obligación de inscribir en elRegistro, sus tecnologías en materia de seguridad, ante la Secretaría, dentro de los noventa días naturales posteriores a la vigencia de la presente Ley.

**QUINTO.** Dentro de los ciento ochenta días naturales siguientes a la entrada en vigor de la presente Ley, el Congreso del Estado deberá realizar las adecuaciones a las leyes que resulten necesarias.

**SEXTO.** En un plazo no mayor a noventa días naturales posteriores a la entrada en vigor de esta Ley, deberán de expedirse las adecuaciones a las disposiciones reglamentarias y administrativas que resulten necesarias para la aplicación de la presente Ley.

**SÉPTIMO.** Se derogan todas las disposiciones de igual o menor jerarquía que se opongan a la presente Ley.

**DADO.** En la Residencia Oficial del Poder Ejecutivo del Estado, en la ciudad de Saltillo, Coahuila de Zaragoza, a los catorce días del mes de diciembre del año dos mil veinte.

**“SUFRAGIO EFECTIVO, NO REELECCIÓN”**

**EL GOBERNADOR CONSTITUCIONAL DEL ESTADO**

**ING. MIGUEL ÁNGEL RIQUELME SOLÍS**

|  |  |
| --- | --- |
| **EL SECRETARIO DE GOBIERNO****ING. JOSÉ MARÍA FRAUSTRO SILLER** | **LA SECRETARIA DE SEGURIDAD PÚBLICA****LIC. SONIA VILLARREAL PÉREZ** |

1. Ana Ponce. (2019). AMLO da espaldarazo a modelo de seguridad en Coahuila. Junio, 2020, de Milenio Sitio web: https://www.milenio.com/estados/amlo-da-espaldarazo-a-modelo-de-seguridad-en-coahuila [↑](#footnote-ref-1)
2. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2016). Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública. p.1. Junio, 2020, de SESNSP Sitio web: http://www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma\_tecnica\_sistemas\_video\_vigilancia.pdf [↑](#footnote-ref-2)
3. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2016). Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública. p.4. Junio, 2020, de SESNSP Sitio web: http://www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma\_tecnica\_sistemas\_video\_vigilancia.pdf [↑](#footnote-ref-3)
4. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2016). Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video Vigilancias para la Seguridad Pública. pp. 4-5. Junio, 2020, de SESNSP Sitio web: http://www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma\_tecnica\_sistemas\_video\_vigilancia.pdf [↑](#footnote-ref-4)
5. EUROPEAN COURT OF HUMAN RIGHTS. (2008). CASE OF S. AND MARPER v. THE UNITED KINGDOM. JUNIO, 2020., de ECHR Sitio web: http://hudoc.echr.coe.int/eng?i=001-90051 [↑](#footnote-ref-5)
6. Royal Courts of Justice. (2018). R (Bridges) v CCSWP and SSHD (Case No: CO/4085/2018). Junio, 2020, de High Court of Justice Sitio web: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf [↑](#footnote-ref-6)