

Claudia Rivera Hernández
Petra Armenta Ramírez
Carla Irene Rios Calleja
(coordinadoras)

Uso de dispositivos de vigilancia electrónica EN MATERIA DE SEGURIDAD PÚBLICA Y SEGURIDAD CIUDADANA: Retos y perspectivas

BUAP

BUAP

Instituto de
Ciencias de Gobierno
y Desarrollo Estratégico

Montiel & Soriano
EDITORES



Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana

Retos y perspectivas

Claudia Rivera Hernández

Petra Armenta Ramírez

Carla Irene Ríos Calleja

(coordinadoras)

Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana

Retos y perspectivas

Claudia Rivera Hernández

Petra Armenta Ramírez

Carla Irene Ríos Calleja

(coordinadoras)



BUAP

Instituto de Ciencias de Gobierno
y Desarrollo Estratégico



Montiel & Soriano
EDITORES



CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES
CIENCIAS Y TECNOLOGÍAS



CLACSO
Consejo Latinoamericano de Ciencias Sociales
Conselho Latino-americano de Ciências Sociais



COMECOSO



Universidad Veracruzana



UNIVERSIDAD VERACRUZANA

Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana. Retos y perspectivas

Claudia Rivera Hernández
Petra Armenta Ramírez
Carla Irene Ríos Calleja
(coordinadoras)

Primera Edición: Julio, 2024

ISBN versión impresa: 978-607-8975-17-4

ISBN versión digital: 978-607-8975-18-1

Montiel & Soriano Editores S.A. de C.V.

15 sur 1103-6 Col. Santiago
Puebla, Pue

Diseño de Portada: Mario Luna Cholula

Instituto de Ciencias de Gobierno y Desarrollo Estratégico

Av. Cúmulo de Virgo s/n. Acceso 4, CCU. Puebla, Pue. C.P. 72810
www.icgde.buap.mx

Instituto de Investigaciones Jurídicas de la Universidad Veracruzana

Calle Hermenegildo Galeana esquina 7 de noviembre s/n, Colonia Centro, 91000 Xalapa-Enríquez, Ver., México.
<https://www.uv.mx/ijj/>

Benemérita Universidad Autónoma de Puebla

4 Sur #104; Col. Centro C.P. 72000

Dra. Ma. Lilia Cedillo Ramírez
Rectora

Mtro. José Manuel Alonso Orozco
Secretario General

Dr. Ygnacio Martínez Laguna
Vicerrector de Investigación y Estudios de Posgrado

Dr. Jorge Luis Castillo Durán
Director del ICGDE



ESTA OBRA HA SIDO DICTAMINADA FAVORABLEMENTE POR PARES ACADÉMICOS MEDIANTE UN SISTEMA DOBLE CIEGO Y FORMA PARTE DE LA “COLECCIÓN DESARROLLO” DEL INSTITUTO DE CIENCIAS DE GOBIERNO Y DESARROLLO ESTRATÉGICO.

Este es un producto del proyecto: Diagnóstico y Modelo de Índice de Percepción de los dispositivos de vigilancia electrónica en materia de seguridad pública en México con enfoque de Derechos Humanos con número FORDECYT-PRONACES/3265530/2020, aprobado para implementarse en el período del 2020-2023 de acuerdo a la Convocatoria de Ciencia de Frontera 2019 de CONACYT. En este se reúne el trabajo colaborativo entre miembros y colaboradores del Cuerpo Académico: Gestión y Desarrollo (PRODEP BUAP-CA-293) vigente para el periodo 2020-2023, con el grado “consolidado” del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la Benemérita Universidad Autónoma de Puebla en colaboración con el Cuerpo Académico: Derecho, Gobierno y Multidisciplinariedad (PRODEP UV-CA-523) vigente para el periodo 2020-2023, con el grado “en consolidación” del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana.

Esta publicación no puede ser reproducida ni en todo ni en parte, ni registrada en, o transmitida por un sistema de recuperación de información, en ninguna forma ni por ningún medio, sea este mecánico, fotoquímico, electrónico, magnético, electro-óptico, por fotocopia o cualquier otro sin el permiso previo por escrito de la editorial.

Impreso y Hecho en México / *Printed and bound in México*

Índice

Introducción: Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana <i>Claudia Rivera Hernández</i> <i>Petra Armenta Ramírez</i> <i>Carla Irene Ríos Calleja</i>	6
Capítulo 1. Percepción de inseguridad en lugares donde existe presencia de DVE's en México <i>Claudia Rivera Hernández</i>	13
Capítulo 2. Dispositivos de vigilancia electrónica. Una mirada desde el ámbito jurídico <i>Arturo Miguel Chipulli Castillo</i> <i>Michel Marie Lago Cruz</i>	40
Capítulo 3. Normatividad de la video vigilancia en México. Una mirada desde el derecho a la privacidad y la protección de datos personales. <i>Karina Nohemí Martínez Meza</i> <i>Vanessa Rodríguez Medina</i> <i>Joaquina Aidé Viveros Montero</i>	64
Capítulo 4. Video vigilancia y derechos humanos <i>Jorge Martínez Martínez</i>	91
Capítulo 5. Videovigilancia: Las atribuciones de seguridad pública, retos y desafíos para la protección de derechos humanos <i>Maribel Luna Martínez</i>	115
Capítulo 6. Videovigilancia como política pública de seguridad ciudadana y su vinculación con los derechos humanos <i>Petra Armenta Ramírez</i> <i>Alejandra Cuevas Ramírez</i>	132

Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana. Retos y perspectivas

Capítulo 7. La video vigilancia en México, ¿protege o vulnera los derechos humanos de las personas en condición de niñez?

María Elisa Matilde Ceballos Díaz 152

Capítulo 8. Seguridad biométrica en el testamento digital: avances, retos y perspectivas

Armando Adriano Fabre

Modesta Lorena Hernández Sánchez 169

Capítulo 9. Influencia de los sistemas de videovigilancia en la formación de discursos mediáticos en materia de seguridad pública: Análisis del caso de Debanhi Escobar en Nuevo León, México

Araceli Espinosa Márquez

Carla Irene Ríos Calleja

Rubith Esther Gutiérrez Mejía 191

Capítulo 10. Videovigilancia e inteligencia artificial: Implicaciones para México

Eleazar Guerrero Barrera 211

Capítulo 11. La videovigilancia en el Estado de Veracruz: anomia jurídica e inexistencia de política pública

Alejandro de la Fuente Alonso

Karol Karim Mar Alonso 233

Capítulo 12. Diseño de un sistema prototipo de prospección inteligente con doble propósito: vigilancia para seguridad ciudadana, Control de GEI, PVs Y COVs. para monitoreo de cambio climático en ciudades inteligentes de los municipios conurbados de la Cd. de Puebla, Amozoc, Cuautlancingo, San Andrés Cholula, San Pedro Cholula, San Martin Texmelucan, Huejotzingo, Coronango y San Miguel Xoxtla, por los efectos toxicológicos del Rio Atoyac, GEI y Volcán Popocatepetl.

Cuitláhuac Alfonso Roviroza Madrazo

Armando Guadarrama Luyando

Pablo Saldívar Martínez 250

Capítulo 13. El aviso de privacidad de datos personales en la era digital de la videovigilancia

Dennisse de los Angeles Uribe Obregón 286

Introducción

Uso de dispositivos de vigilancia electrónica en materia de seguridad pública y seguridad ciudadana

*Claudia Rivera Hernández**

*Petra Armenta Ramírez***

*Carla Irene Rios Calleja****

En la actualidad, el uso de los dispositivos de vigilancia electrónica forma parte de la vida cotidiana de las personas y se ha convertido en un fenómeno social y complejo por sus características y naturaleza técnica. Los gobiernos los implementan como una solución tecnológica para los problemas públicos de seguridad, en cualquier contexto y latitud, incluyendo México.

El libro que usted tiene en sus manos, es resultado del segundo año de trabajo del Proyecto de Ciencia de Frontera FORDECYT- PRONACES 3265530 “Diagnóstico y Modelo de Índice de Percepción de los Dispositivos de Vigilancia Electrónica en materia de Seguridad Pública en México con Enfoque de Derechos Humanos”, el cual parte de la idea de que el uso de los dispositivos de vigilancia electrónica, en las estrategias de seguridad, requiere de un análisis multi e interdisciplinario, de nuevos métodos, modelos teóricos y empíricos, así como de nuevos estudios de caso, a fin de que los derechos humanos de privacidad y protección de datos personales, con base en

* Postdoctora en Educación Superior y Política Pública, Universidad de Nuevo México, USA; Doctora en Administración Pública. Profesora investigadora de la Benemérita Universidad Autónoma de Puebla (México). Miembro del Sistema Nacional de Investigadores Nivel II del CONACYT. [claudia.rivera@correo.buap.mx]; [https://orcid.org/0000-0002-3927-9366].

** Doctora en Derecho Público por la Universidad Veracruzana (UV), Licenciada en derecho (UV), Profesora – investigadora de tiempo completo del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana, es miembro del Sistema Nacional de Investigadoras e Investigadores (SNI) Nivel I por el CONACYT. Email: parmenta@uv.mx

*** Profesora-investigadora del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la BUAP. ORCID: https://orcid.org/0000-0001-9656-4238. Email: carla.rioscallega@correo.buap.mx.

los principios de legalidad, necesidad, proporcionalidad, transparencia, responsabilidad, supervisión independiente y participación ciudadana, sean protegidos.

Con este producto se consolida el trabajo colegiado entre la Universidad Veracruzana, a través del Instituto de Investigaciones Jurídicas (UV), el Centro de Estudios de Opinión y Análisis (UV), el Observatorio de Políticas Públicas con Enfoque de Derechos Humanos (UV) y la Benemérita Universidad Autónoma de Puebla, a través del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la BUAP. Con ello, se fortalece el trabajo interdisciplinario de la Red de Vigilancia Electrónica, que se aprobó en el año 2022, producto de esta colaboración donde se afirma el trabajo colegiado entre los Cuerpos Académicos: PROFEP UV-CA-523: Derecho, Gobierno y Multidisciplinariedad del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana y PROMEP BUAP-CA 295: Gestión y Desarrollo del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la Benemérita Universidad Autónoma de Puebla, relación que se cultiva desde el año 2020 y que ha dado diversos frutos entre los que destacan:

- a) La realización de un diagnóstico situacional a nivel internacional, nacional y local;
- b) La creación y desarrollo de 2 bases de datos (cualitativa y cuantitativa) sobre la percepción de los dispositivos de vigilancia electrónica en México en materia de seguridad pública;
- c) La realización de una estrategia metodológica para el monitoreo de los dispositivos de vigilancia electrónica en materia de seguridad pública en México;
- d) La realización de coloquios para la validación, difusión y comunicación de los resultados, diagnóstico y modelo;
- e) La creación de una página web: <https://icgde.buap.mx/content/frontera>;
- f) La creación de una red de investigación;
- g) La vinculación con observatorios gubernamentales, de la sociedad civil y de las universidades que realicen actividades sobre seguridad pública y derechos humanos;
- h) La implementación de una gran encuesta replicada en 21 estados de la República Mexicana, la cual contempla el diagnóstico situacional de los dispositivos de vigilancia electrónica en materia de seguridad pública con Enfoque de Derechos Humanos en México y su percepción;
- i) La publicación de diversos productos, por ejemplo, durante el primer año de trabajo se caracterizó la inversión, adquisición y uso de equipos de vigilancia electrónica en México y se rescataron entrevistas a los actores clave de la política de seguridad pública, los hallazgos pueden consultarse en el libro titulado “Vigilancia, dispositivos electrónicos y derechos humanos en México: Retos y oportunidades a enfrentar en el siglo XXI”, coordinado por Araceli Espinosa

Márquez, Karina Nohemí Martínez Meza y Arturo Miguel Chípuli Castillo, Publicado por la Editorial Montiel & Soriano Editores S.A. de C.V. en noviembre de 2021, el cual es de acceso abierto y se encuentra en la página web del ICGDE.

Tras concluir el primer año, el equipo de investigación procedió al análisis y recuento de información, lo que permitió, durante el segundo año de trabajo, orientar la línea de investigación hacia el análisis del marco legal sobre el uso de los dispositivos de videovigilancia como un elemento primordial para la prevención, investigación y sanción de actos delictivos. También se delimitó el marco contextual y se completó la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, realizada por la Universidad Veracruzana y la Benemérita Universidad Autónoma de Puebla entre los meses de febrero- agosto del año 2023, la cual cuestionó a 1,050 ciudadanos provenientes de las 21 principales ciudades del país.

El libro que tiene usted en sus manos se desarrolla con el objetivo de presentar un diagnóstico situacional del uso de los dispositivos de vigilancia electrónica en México y se construye bajo el cuestionamiento del respeto a los derechos humanos en un contexto donde la inseguridad, la corrupción y el crimen organizado son palabras que se asocian frecuentemente en México, pues el uso creciente de la tecnología en las estrategias de seguridad pública aún es debatible debido a diversas razones: primero, la capacidad técnica de los funcionarios relacionados con esta área, se encuentra en formación respecto al avance en otros países; segundo, pareciera que el crimen organizado va un paso adelante en la profesionalización de sus agentes; y tercero, en México, pese a las inversiones realizadas durante la última década, aun no se cuenta con la infraestructura y conectividad adecuada para que la seguridad pública a través de dispositivos de videovigilancia sea una realidad.

Por estas razones, nuestra investigación apunta a los efectos de inhibición y de disuasión que los dispositivos de videovigilancia producen en los ciudadanos debido a la sensación de seguridad que generan sobre la población. Este libro está integrado por trece capítulos que brindan al lector una caracterización clara sobre el uso y los efectos de los dispositivos de vigilancia electrónica en el país y su efecto en los derechos humanos. Este obra abona a las líneas de investigación relacionadas con las políticas públicas en materia de seguridad, los estudios de percepción y el enfoque de los derechos humanos.

El capítulo uno, titulado “Percepción de inseguridad en lugares donde existe presencia de DVE's en México”, escrito por Claudia Rivera Hernández, explica que, en México, los gobiernos estatales han implementado diversas estrategias para combatir el crimen y la inseguridad. La autora se centra en el uso de dispositivos de videovigilancia como prácticas para disuadir y prevenir los delitos, y mediante una encuesta nacional llevada a cabo por el equipo de investigación UV-BUAP, llega a la conclusión

de que en México la violencia e inseguridad han sido normalizadas. La autora afirma que los dispositivos de videovigilancia tienen un efecto positivo en la percepción de inseguridad, arrojando cifras aproximadas de 10 puntos porcentuales de diferencia frente a los lugares donde no se utilizan estos dispositivos.

El capítulo dos, titulado “Dispositivos de vigilancia electrónica. Una mirada desde el ámbito jurídico”, escrito por Arturo Miguel Chípulli Castillo y Michel Marie Lago Cruz, hace un recorrido por la normatividad relativa a los dispositivos de vigilancia electrónica, en particular, drones, cámaras de videovigilancia e inteligencia artificial en México. Los autores caracterizan la realidad jurídica de su implementación a través del método documental y análisis de la legislación a nivel internacional, nacional y estatal. Concluyen que existen áreas de oportunidad en el marco jurídico actual y enfatizan la importancia del Estado y su deber de garantizar el bienestar de la ciudadanía y sus derechos humanos.

En el capítulo tres, titulado “Normatividad de la video vigilancia en México. Una mirada desde el derecho a la privacidad y la protección de datos personales”, escrito por Karina Nohemí Martínez Meza, Vanessa Rodríguez Medina y Joaquina Aidé Viveros Montero, se analiza la normatividad de la video vigilancia en México con base en los derechos humanos, en particular los derechos a la privacidad y la protección de datos personales. En su análisis destacan los actores, procesos y elementos más importantes. Las autoras concluyen que, si bien existe una reglamentación que regula la video vigilancia, no es homogénea a nivel subnacional, y los hallazgos respecto al derecho a la privacidad y protección de datos personales no son concluyentes, lo cual podría provocar la violación de derechos humanos en México.

El capítulo cuatro, titulado “Video vigilancia y derechos humanos”, escrito por Jorge Martínez Martínez, enfrenta los pros y los contras en el uso de los dispositivos de videovigilancia y el respeto a los derechos humanos como son la intimidad, la vida privada y, de manera general, la protección de datos personales. El autor concluye que es necesaria una normativa especial en la materia que permita la implementación de políticas públicas acordes con el paradigma constitucional vigente para evitar vulnerar las libertades fundamentales del individuo, lo cual es contrario a la democracia y evolución del Estado constitucional de derecho.

En el capítulo cinco, titulado “Videovigilancia: Las atribuciones de seguridad pública, retos y desafíos para la protección de derechos humanos”, escrito por Maribel Luna Martínez, se documenta el uso incierto y el tratamiento que se le da a las grabaciones, cintas y demás información, producto de las políticas públicas de videovigilancia. La autora concluye que existe incertidumbre jurídica, evidenciando la necesidad de legislar adecuadamente el uso y tratamiento de los dispositivos utilizados por las autoridades para realizar la videovigilancia.

El capítulo seis, titulado “Videovigilancia como política pública de seguridad ciudadana y su vinculación con los derechos humanos”, escrito por Petra Armenta Ramírez y Alejandra Cuevas Ramírez, se explica el fenómeno de la videovigilancia como política pública de seguridad ciudadana y su relación directa con los derechos humanos a la privacidad, protección de datos personales y la seguridad ciudadana. Las autoras utilizan el método cualitativo documental, basándose en el análisis y recolección de datos a partir de revistas, libros y artículos académicos. Los hallazgos de su investigación permiten determinar cuáles son los estados de la República Mexicana que han adoptado, dentro de sus reglamentos o legislación, conceptos sobre videovigilancia y su aplicación.

En el capítulo siete, titulado “La video vigilancia en México ¿protege o vulnera los derechos humanos de las personas en condición de niñez?”, escrito por María Elisa Matilde Ceballos Díaz, se realiza una revisión y análisis de la normas vigentes a nivel internacional, nacional, y estatal, así como de libros, artículos, estadísticas y notas periodísticas, para contestar si la video vigilancia en México ¿protege o vulnera los derechos humanos de las personas en condición de niñez?, precisando que ante las deficiencias de las leyes y de las autoridades, se conciben trasgresiones a los derechos de los niños, niñas y adolescentes.

El capítulo ocho, titulado “Seguridad biométrica en el testamento digital: avances, retos y perspectivas”, los autores Armando Adriano Fabre y Modesta Lorena Hernández Sánchez utilizan el método de exploración cualitativa, sustentándose en argumentos doctrinarios, fundamentos de la legislación mexicana, y análisis de derecho comparado, en la que se basa la pertinencia del testamento digital, con la intervención de datos biométricos, como resultado de la modernidad de un país. Sus principales hallazgos advierten que el uso de la inteligencia artificial para recabar datos biométricos de los individuos, y el empleo de éstos, de manera correcta, son una herramienta indispensable para un sistema de manifestación y otorgamiento de la voluntad de manera virtual, pues aseguran la veracidad de estos documentos, a través de la identificación y autenticación de la persona que desee otorgar su testamento por medios electrónicos.

El capítulo nueve, titulado “Influencia de los sistemas de videovigilancia en la formación de discursos mediáticos en materia de seguridad pública: Análisis del caso de Debanhi Escobar en Nuevo León, México”, las autoras Araceli Espinosa Márquez, Carla Irene Rios Calleja y Rubith Esther Gutiérrez Mejía analizan los sistemas de videovigilancia que influyeron en los discursos utilizados sobre seguridad pública en la prensa digital local y nacional, en particular sobre el caso de “Debanhi Escobar” en Nuevo León, México, y que ocupó los titulares del país y en la prensa internacional por las discrepancias existentes entre la información otorgada por el gobierno estatal y el discurso mediático debido a las imágenes presentadas por la Fiscalía del Estado. Las autoras concluyen que la influencia de las grabaciones del sistema de video-

vigilancia tiene un fuerte impacto en las decisiones sobre seguridad pública y, en particular, para la resolución de casos.

En el capítulo, diez titulado “Videovigilancia e inteligencia artificial: Implicaciones para México”, escrito por Eleazar Guerrero Barrera, se explican los efectos que tienen los Sistemas Inteligentes de Videovigilancia (SIV) que usan macro datos. El autor concluye que, debido a la falta de un marco legal específico, los SIV, tienen el potencial de vulnerar los derechos humanos a la libertad, la intimidad, la privacidad y protección de datos personales, y usarse con fines diversos a los de la seguridad pública y nacional.

El capítulo once, titulado “La videovigilancia en el Estado de Veracruz: anomia jurídica e inexistencia de política pública”, los autores Alejandro de la Fuente Alonso y Karol Karim Mar Alonso explican que, aunque la video vigilancia coadyuve a disminuir la inseguridad, confronta con las libertades del individuo y su esfera más privada: la intimidad. A través del análisis del contexto del estado de Veracruz, los autores dan cuenta de la necesidad no solo de la creación de una política pública de videovigilancia en la entidad federativa, sino también la legislación en la materia por parte del Congreso Local.

El capítulo doce, “Diseño de un sistema prototipo de prospección inteligente con doble propósito: vigilancia para seguridad ciudadana y Control de GEI, PVs Y COVs para monitoreo de cambio climático en ciudades inteligentes de los municipios conurbados de la Cd. de Puebla; Puebla, Amozoc, Cuautlancingo, San Andrés Cholula, San Pedro Cholula, San Martin Texmelucan, Huejotzingo, Coronango y San Miguel Xoxtla, por los efectos toxicológicos del Rio Atoyac, GEI y Volcán Popocatepetl”, los autores Cuitláhuac Alfonso Roviroso Madrazo, Armando Guadarrama Luyando y Pablo Saldivar Martinez, muestran una investigación aplicada llevada a cabo entre el 13 y el 15 de mayo del 2019 en el estado de Puebla en material vegetativo impactado por fenómeno atmosférico conjugado. Con ayuda del sistema de informacion geográfica con imágenes de la NASA y ESA en combinación con técnicas Raman, encontraron azufre (S) volcánico, COVs como Benzyl disulfide, CAS: 150-6-7 y PVs PM 0.5 a 2.5 μm incrustadas en tejido forestal. De este estudio, se derivó en la necesidad de la inteligencia artificial para la prospección y control con sistemas de alerta de futuros fenómenos similares en Puebla.

Finalmente el capítulo trece, titulado “El aviso de privacidad de datos personales, en la era digital de la videovigilancia”, escrito por Dennisse de los Ángeles Uribe Obregón, identifica que los sistemas de videovigilancia son una herramienta tecnológica útil e indispensable que permiten reforzar la seguridad a través de los avisos de privacidad.

Tras la revisión de trece capítulos, se concluye que el carácter altamente intrusivo de los sistemas de vigilancia electrónica puede suponer serios riesgos para los derechos humanos, sobre todo en contextos como el de México, en donde la falta de una

normatividad clara y precisa, hace evidentes las deficiencias en las instituciones democráticas y la vigencia del Estado de derecho.

Deseamos que este libro sea de utilidad para ciudadanos y tomadores de decisiones, pues la política de seguridad no puede ser “ciega” a los derechos humanos; debe mantener un enfoque centrado en las personas y sus derechos, lo que permitirá dar cabal cumplimiento a las obligaciones adquiridas por el Estado en el marco del Derecho Internacional de los Derechos Humanos.

Vale la pena informar al lector que para el tercer año de trabajo de este colectivo de investigación se dará a conocer el diagnóstico situacional de los dispositivos de vigilancia electrónica en materia de seguridad pública con Enfoque de Derechos Humanos en México y su percepción, así como la presentación de un modelo de índice de percepción de los dispositivos de vigilancia electrónica en materia de seguridad pública con base en los derechos humanos.

Capítulo 1

Percepción de inseguridad en lugares donde existe presencia de DVE's en México

Perception of insecurity in places where DVE's are present in Mexico

*Claudia Rivera Hernández**

Resumen

En México, el 47% de los homicidios dolosos se concentran en tan solo seis ciudades. (SEDENA, 2023). Como respuesta, los gobiernos estatales han implementado diversas estrategias para combatir el crimen y la inseguridad. En particular nos interesan las relacionadas con el uso de dispositivos de video vigilancia como prácticas para disuadir y prevenir los delitos, por lo que en este análisis cuestionamos cómo se percibe la inseguridad en México y cual ha sido el efecto de la videovigilancia en la ciudadanía. Tras llevar a cabo la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos en la cual se cuestionó a 1050 ciudadanos provenientes de las 21 principales ciudades de México, se presenta el análisis del módulo 17: Percepción de inseguridad en lugares donde existe presencia de dispositivos de vigilancia electrónica en México. Los hallazgos de la investigación arrojan que pese a que en México la violencia e inseguridad ha sido normalizada, los dispositivos de videovigilancia tienen un efecto positivo en la percepción de inseguridad arrojando cifras aproximadas de 10 puntos porcentuales de diferencia frente a los lugares donde no se utilizan estos dispositivos.

Palabras clave: Sistemas de vigilancia electrónica, Políticas Pública de Seguridad; Inseguridad.

Abstract

In Mexico, 47% of intentional homicides are concentrated in just six cities (SEDENA, 2023). In response, state governments have implemented different strategies to combat crime and insecurity. We are particularly interested in those related to the use of video surveillance devices

* Postdoctora en Educación Superior y Política Pública, Universidad de Nuevo México, USA; Doctora en Administración Pública. Profesora investigadora de la Benemérita Universidad Autónoma de Puebla (México). Miembro del Sistema Nacional de Investigadores Nivel II del CONACYT. [claudia.rivera@correo.buap.mx]; [<https://orcid.org/0000-0002-3927-9366>].

as practices to deter and prevent crime, so in this analysis we question how insecurity is perceived in Mexico and what has been the effect of video surveillance on citizens. After conducting the National Survey on Perception of Electronic Surveillance Devices with a Human Rights Perspective, in which 1050 citizens from the 21 main cities of Mexico were questioned, we present the analysis of module 17: Perception of insecurity. The research findings show that even though violence and insecurity have been normalized in Mexico, video surveillance devices have a positive effect on the perception of insecurity, with a difference of approximately 10 percentage points compared to places where these devices are not used.

Keywords: Electronic surveillance systems, Public Security Policies; Insecurity.

Introducción

Las estrategias implementadas por el gobierno no se ocupan exclusivamente de la prevención del crimen real, sino que deben atender la criminalidad percibida, pues la idea de vivir en un lugar inseguro suprime la libertad y, por ende, limita el desarrollo de las capacidades de los habitantes de un país (SEN, 2000).

Las últimas mediciones sobre inseguridad en América Latina y el Caribe ponen en evidencia que los altos índices de incidencia delictiva no solo producen costos económicos significativos y deterioro de la confianza ciudadana hacia sus gobernantes e instituciones, sino que la sensación de inseguridad, consecuencia de esto, daña gravemente la forma de vida de los ciudadanos y limita el desarrollo de un país.

El 7 de marzo de 2024, el Banco Interamericano de Desarrollo (BID) publicó una hoja informativa con datos del UNODC, 2023, donde se detalla que la región de América Latina y el Caribe tiene una tasa de homicidios tres veces superior al promedio mundial (18 vs. 5.6 por 100,000 habitantes, según UNODC, 26/06/2023). Del total de homicidios reportados, el 50% se registra en las calles de las grandes ciudades y el otro 50% es atribuido al crimen organizado. Respecto a este último dato, el BID (2024) confirma que estamos presenciando un fenómeno de “gobernanza criminal”, pues el 54% de los hogares en la región reporta la presencia de grupos criminales con creciente proporción de regulación de seguridad y solicitud de derecho de piso (Latinobarómetro, 2020). Frente a estos datos es evidente que la percepción de inseguridad en la región está en crecimiento.

Lo anterior se demuestra con los hallazgos de la encuesta Gallup, llevada a cabo en enero del 2023. El informe generado confirma que en la región se mantiene una alta percepción de inseguridad y son los ciudadanos de Ecuador y Perú quienes perciben un aumento mayor en el crimen organizado y la delincuencia en los últimos cuatro meses, pues aquellos con ingresos más bajos declaran haber sido víctimas de algún robo en su hogar. El informe también demuestra que México, Nicaragua y Honduras se encuentran entre los países con mayores porcentajes de hogares víctimas de robo;

sin embargo, la población no percibe un aumento tan alto de la criminalidad, por lo que argumenta que se ha normalizado la violencia. El Salvador es el único país de la región donde la mayoría de la población percibe que la criminalidad ha disminuido en los últimos cuatro meses. (Gallup, 2023).

Por su parte, en México, el 13 de diciembre de 2023 se publicó el Informe de Seguridad, presentado por la Secretaría de la Defensa Nacional, SEDENA. Dicho informe establece que, en el país, seis de 32 entidades concentran el 47% de los homicidios dolosos, siendo éstas Guanajuato (2,875), Estado de México (2,426), Baja California (2,232), Chihuahua (1,913), Jalisco, (1,807) y Michoacán (1,610) (SEDENA, 2023).

Como respuesta a estas cifras, los gobiernos estatales, en coordinación con la Secretaría de la Defensa Nacional, han implementado diversas estrategias entre las que destacan la seguridad en carreteras, el decomiso de armas de fuego, cargadores, granadas, cartuchos, vehículos, sustancias ilícitas, dinero, aseguramiento de laboratorios clandestinos, estrategias para el fortalecimiento de aduanas y puertos, operaciones de combate al mercado ilícito de combustibles, operaciones de búsqueda y rescate, entre otras que se encuentran exclusivamente en manos de la policía local.

En particular nos interesan, para este análisis, las relacionadas con el uso de dispositivos de video vigilancia como prácticas para disuadir y prevenir los delitos, ya sean perpetrados por el crimen organizado o por la ciudadanía, al cometer infracciones que ameriten multas o sanciones administrativas. De ahí que nos cuestionemos cómo se percibe la inseguridad en México y cuál ha sido el efecto de la videovigilancia en los estados.

Por lo anterior, se realizó la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, llevada a cabo por la Universidad Veracruzana y la Benemérita Universidad Autónoma de Puebla entre los meses de febrero-agosto del año 2023, en la cual se cuestionó a 1,050 ciudadanos provenientes de las 21 principales ciudades de México. En este documento, se presenta el análisis del módulo 17: Percepción de inseguridad en lugares donde existe presencia de DVE's en México.

I. Definición conceptual

En relación con la revisión documental sobre el uso de la tecnología para prevenir la inseguridad, se encontró que es en el espacio de lo local donde, en la actualidad, se están modernizando los procesos y sistemas operativos de la política pública en cuestión, pues la tecnología es un medio para el desarrollo de estrategias innovadoras que la combaten, reduciendo el delito y previniendo el crimen. (Bermúdez et, al. 2022, Delgado, 2022; Morales y Monzón, 2022; Savall, 2022; Vivas, 2022).

En México, los sistemas de videovigilancia son un mecanismo utilizado sobre todo en ambientes urbanos; pueden ser considerados como una herramienta muy relevante que utilizan los cuerpos de seguridad cuyos efectos dependen de una minuciosa selección de la tecnología, capacitación adecuada e implementación estricta y se han convertido en una parte importante de las políticas de Estado para prevenir y castigar los delitos. El 30 de agosto de 2016 se aprobó la Norma Técnica para estandarizar las características técnicas y de interoperatividad de los sistemas de video vigilancia para la seguridad pública, la cual integró aspectos relacionados con la infraestructura, la coordinación con las corporaciones e instancias responsables de la seguridad ciudadana y los procesos de organización operativa que incluyeron tres fases: organización, operación y evaluación (SEGOB, S/Ra). Con ello, se fortalecieron los sistemas de video vigilancia en el país.

Un Sistema de Video Vigilancia (SVV) 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 (SEGOB, S/Ra, p. 1).

A través de los sistemas de videovigilancia se puede mejorar la seguridad de la ciudadanía mediante el monitoreo de ambientes abiertos y cerrados; por ello, sus principales críticas se encuentran relacionadas con la invasión del espacio público¹ y la pérdida de los derechos humanos. Pese a ello, su efecto es innegable en la capacidad de reacción de las fuerzas policiales.

Desde el año 2011 y de manera anual, en México se cuenta con información sobre los sistemas de videovigilancia a través del Censo Nacional de Gobierno, Seguridad Pública y Sistemas Penitenciarios Estatales, realizado por el Instituto Nacional de Estadística y Geografía, INEGI. El último censo realizado en el año 2020 arroja que la Ciudad de México es el lugar que cuenta con un mayor número de cámaras de videovigilancia en los espacios públicos, seguido por el Estado de México, Jalisco y Michoacán (ver Figura 1).

¹ Vale la pena aclarar que se considera “espacio público” a: “todo aquel lugar físico que no es de carácter privado y que está abierto a todas las personas. Éste tiene dos dimensiones: una material y una política”. (Narváez, Chorny, 29/01/2020). La dimensión material implica aquellos elementos físicos de un lugar público, es decir, lo tangible, mientras que la dimensión política implica la acción humana donde las personas se encuentran para realizar deliberación pública. En ella, los ciudadanos se convierten en agentes morales con derechos y obligaciones.

Figura 1. Infraestructura de la institución encargada de la función
de seguridad pública, por entidad federativa según tipo (2019)

Clave	Entidad federativa	Centros de control y confianza C3	Centros de Control, Comando, Cómputo y Comunicaciones C4	Centros de Control, Comando, Cómputo, Comunicaciones y Coordinación C5	Cámaras de vigilancia en la vía pública	Botones de pánico
	Estados Unidos Mexicanos	32	85	41	99,912	93,308
1	Aguascalientes	1	1	0	76	NA
2	Baja California	3	5	0	110	2,614
3	Baja California Sur*	1	3	0	115	325
4	Campeche	1	1	1	620	NA
5	Coahuila de Zaragoza	0	4	0	NA	NA
6	Colima	1	1	1	795	525
7	Chiapas	0	1	0	505	NA
8	Chihuahua	1	2	0	440	50
9	Ciudad de México	1	0	1	45,000	24,697
10	Durango	1	3	1	256	NA
11	Guanajuato	0	0	1	2,192	20,000
12	Guerrero	1	3	0	723	20
13	Hidalgo	1	3	1	5,077	1,255
14	Jalisco	1	0	1	5,943	1,438
15	México	2	0	2	15,740	7,899
16	Michoacán de Ocampo	1	0	11	5,316	17,900
17	Morelos	0	0	2	908	NA
18	Nayarit	1	4	0	160	NA
19	Nuevo León	0	11	1	762	NA
20	Oaxaca	1	1	0	456	560
21	Puebla	3	8	2	224	1,338
22	Querétaro	1	0	1	2,619	NA
23	Quintana Roo	1	4	0	1,240	402
24	San Luis Potosí	1	4	1	93	1,100
25	Sinaloa	1	3	0	867	106
26	Sonora	1	0	12	2,055	12,541
27	Tabasco	1	1	0	918	NA

Clave	Entidad federativa	Centros de control y confianza C3	Centros de Control, Comando, Cómputo y Comunicaciones C4	Centros de Control, Comando, Cómputo, Comunicaciones y Coordinación C5	Cámaras de vigilancia en la vía pública	Botones de pánico
28	Tamaulipas	1	6	0	1,513	NA
29	Tlaxcala	1	1	0	1,150	NA
30	Veracruz de Ignacio de la Llave	1	8	1	1,586	538
31	Yucatán	1	1	0	2,248	NA
32	Zacatecas	1	6	1	205	NA

Nota: la información se refiere a la infraestructura en funcionamiento de las instituciones encargadas de la función de seguridad pública de las administraciones públicas de las entidades federativas, al 31 de diciembre.

* La institución encargada de seguridad pública de la entidad federativa reportó no contar con estaciones, comandancias, módulos o casetas de policía, ya que en los despliegues de seguridad se utilizan instalaciones propiedad de otras instituciones del ámbito estatal o federal.

NA: no aplica, debido a que se reportó no contar con el tipo de infraestructura.

Fuente: INEGI Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2020. SNIEG Información de Interés Nacional.

Pese a la existencia de videocámaras y del incremento del crimen y los delitos en México, se prevé que la gobernanza criminal vaya en aumento y se normalice la violencia. Por lo anterior, cuestionamos a 1,050 mexicanos sobre su percepción de inseguridad en el país a fin de contrastar si existe una percepción diferenciada entre los espacios públicos que son parte del SVV y los que no.

II. Definición operativa

De acuerdo con la Encuesta Nacional de Victimización y Percepción Sobre Inseguridad Pública ENVIPE 2023, se estima que, a nivel nacional, 22.1 millones de personas de 18 años y más han sido víctimas de cualquier delito. lo cual equivale a 24,207 víctimas por cada 100,000 habitantes durante el año 2021.

Los delitos más cometidos son: el robo o asalto en calle o transporte público, 21.4%; fraude, 19.2%; extorsión, 17.5%, robo total o parcial del vehículo, 10.8%, amenazas verbales, 9.2%, otros delitos, 7.9%, robo a casa habitación, 6.0%, otros robos, 4.5%, lesiones, 3.6% (ENVIPE, 2023). La encuesta también identifica que el lugar de ocurrencia de dichos delitos es en los cajeros automáticos, en la calle, en la casa y en el transporte público.

Por ello, se realizó la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, realizada por la Universidad Veracruzana y la Benemérita Universidad Autónoma de Puebla, entre los meses de febrero-agosto del año 2023, en la cual se cuestionó a 1,050 ciudadanos provenientes de las 21 principales ciudades del país.

El instrumento incluyó 19 módulos, con una duración aproximada de 20 minutos de duración para responder completamente. Se aplicó una muestra estratificada en las ciudades de Acapulco, Guerrero; Benito Juárez, Quintana Roo; Ciudad de México; Cuernavaca, Morelos; Guadalajara, Jalisco; Guanajuato, Gto.; Hermosillo, Sonora; Mazatlán, Sinaloa; Mérida, Yucatán; Monterrey, Nuevo León; Oaxaca, Oax.; Pachuca, Hidalgo; Puebla, Pue.; Querétaro, Qro.; Saltillo, Coahuila; San José del Cabo, Los Cabos; Tijuana, Baja California; Tlaxcala, Tlax.; Toluca, Estado de México; Veracruz, Ver. y Xalapa, Ver.

Las principales razones para elegir estas ciudades se deben sobre todo a las redes de colaboración que se crearon específicamente para este proyecto. Se descartaron las capitales donde existe violencia evidente para garantizar la seguridad de los encuestadores. Tras el ejercicio, se obtuvieron 1,050 encuestas válidas.

Figura 2. Módulo de Percepción de inseguridad/ seguridad

Percepción de inseguridad/ seguridad	Lugar	Existen comúnmente dispositivos de vigilancia electrónica
	En su casa	Si
	En su trabajo	No
	En la calle	No
	En la escuela o espacios escolares	Si
	En el mercado	No
	En el centro comercial	Si
	En el banco	Si
	En el cajero automático localizado en vía pública	Si
	En el transporte público	No
	En su automóvil	No
	En la Carretera	No
	En el parque o centro recreativo	No

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Se presenta para este análisis el módulo 17, el cual verifica la Percepción de inseguridad en México. Para operacionalizar se incluyó la pregunta: ¿Qué tan seguro se siente en las siguientes ubicaciones? Las respuestas fueron emitidas en una escala del 1 al 5, donde 5 es muy seguro y 1 muy inseguro. En total, se contabilizan 12 ítems asociados a los espacios públicos donde los ciudadanos realizan su vida cotidiana.

Para el análisis, se ha integrado la última columna de la Figura 2, en la cual se identifica si el espacio público comúnmente cuenta con cámaras de videovigilancia o no.

El instrumento se analiza a partir de los criterios de la escala de likert:

Las escalas de valor y de estimación tipo Likert son aquellas que se utilizan para determinar la percepción de alguna variable cualitativa que por su naturaleza denota algún orden. Ha sido ampliamente utilizada en estudios sociales donde se recogen las percepciones no cuantitativas sobre algún tópico en específico. Esta naturaleza cualitativa y la necesidad de crear indicadores estadísticos que denoten confiabilidad sobre los resultados obtenidos han hecho que la estadística no paramétrica desarrolle metodologías para garantizar la confiabilidad de sus estimaciones (Canto de Gante, et. al. 2020, p. 34).

Por lo tanto, lo que esta escala determina es la conformidad de las personas y resulta útil cuando se requiere una opinión detallada sobre un tema cualitativo en particular como la percepción de inseguridad que se vive en un país.

III. Análisis

Figura 3. Conformación de la muestra por género

Escolaridad	Hombre		Mujer	
	Abs	%	Abs	%
Preescolar	4	0.4%	9	0.9%
Primaria Completa	37	3.5%	41	3.9%
Secundaria Completa	89	8.5%	81	7.7%
Preparatoria Completa	182	17.3%	182	17.3%
Carrera Técnica Completa	35	3.3%	37	3.5%
Licenciatura Completa	148	14.1%	132	12.6%
Posgrado	33	3.1%	35	3.3%

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

III.1. Descripción de la muestra

Los datos generales arrojan que la muestra estuvo compuesta por 50% de hombres y 50% de mujeres, cuya escolaridad se concentra sobre todo en preparatoria terminada y carrera universitaria completa (ver Figura 3).

Respecto a la edad de los encuestados, el 27.24% de la muestra se concentró en el grupo de edad entre los 21-30 años, seguido por el 18.96% en edad de 31-40 años (ver Figura 4).

Figura 4. Conformación de la muestra por rangos de edad

Rango	Encuestados por rango de Edad						
	18-20	21-30	31-40	41-50	51-60	61-70	70+
Numero de Encuestados	145	286	199	163	119	104	33
%	13.81%	27.24%	18.95%	15.52%	11.33%	9.90%	3.14%

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

III.2 Hallazgos generales según la percepción de la ciudad como “segura”, “insegura” y “muy insegura”

Para analizar este módulo y presentar los principales hallazgos, se operacionaliza la información a partir de la sumatoria general, del 0 al 5, por cada uno de los 12 ítems evaluados, siendo 60 la puntuación mayor y 5 la puntuación menor.

Con estos datos, se obtuvo una escala del 0 al 60, la cual se dividió en terciles. El primer tercil incluye el rango de 0 a 20 puntos y se catalogó como: “Me siento muy inseguro”; el segundo tercil incluye el rango de 21 a 40 puntos e indica “Me siento Inseguro” y el tercer tercil incluye el rango de 41 a 60 puntos y fue catalogado como “Me siento seguro”.

La Figura 5 muestra la estratificación de la encuesta y los resultados de frecuencia absoluta en cada capital del país. Los resultados arrojan que el 10% de los encuestados se sienten “muy inseguros”, el 59% se sienten “inseguros” y el 31% se sienten “seguros”.

Los hallazgos de la investigación demuestran que más del 10% de los ciudadanos mexicanos que se sienten “muy inseguros” habitan sobre todo en las ciudades de Mazatlán, Sinaloa; Cuernavaca, Morelos y Veracruz, Ver.

Figura 5. Percepción de inseguridad en México

Total encuestados Datos Absolutos		Muy inseguro	Inseguro	Seguro	Total
Acapulco	Guerrero	6	33	9	48
Benito Juárez	Quintana Roo	3	30	15	48
CDMX	Ciudad de México	4	27	7	38
Cuernavaca	Morelos	9	23	10	42
Guadalajara	Jalisco	9	35	18	62
Guanajuato	Guanajuato	9	33	19	61
Hermosillo	Sonora	4	22	13	39
Mazatlan	Sinaloa	10	22	14	46
Mérida	Yucatán	0	5	29	34
Monterrey	Nuevo León	6	27	12	45
Oaxaca	Oaxaca	1	25	10	36
Pachuca	Hidalgo	5	24	14	43
Puebla	Puebla	6	59	21	86
Querétaro	Querétaro	2	29	26	57
Saltillo	Coahuila	1	33	14	48
San José del Cabo	Baja California Sur.	5	23	41	69
Tijuana	Baja California Norte.	6	37	11	54
Tlaxcala	Tlaxcala	0	38	10	48
Toluca	Estado de México	2	20	6	28
Veracruz	Veracruz	9	30	6	45
Xalapa	Veracruz	5	39	23	67
No especificado	No especificado	3	2	1	6
Total		105	616	329	1050

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

En la ciudad de Mazatlán, Sinaloa, el 21.7% de los encuestados dijo percibir que su ciudad es muy insegura, el 21.4% del total de encuestados en Cuernavaca Morelos y el 20% del total de encuestados en Veracruz, Ver., indicaron la misma percepción (ver Figura 6).

Figura 6. Percepción de inseguridad en México “Me siento muy Inseguro” (%)



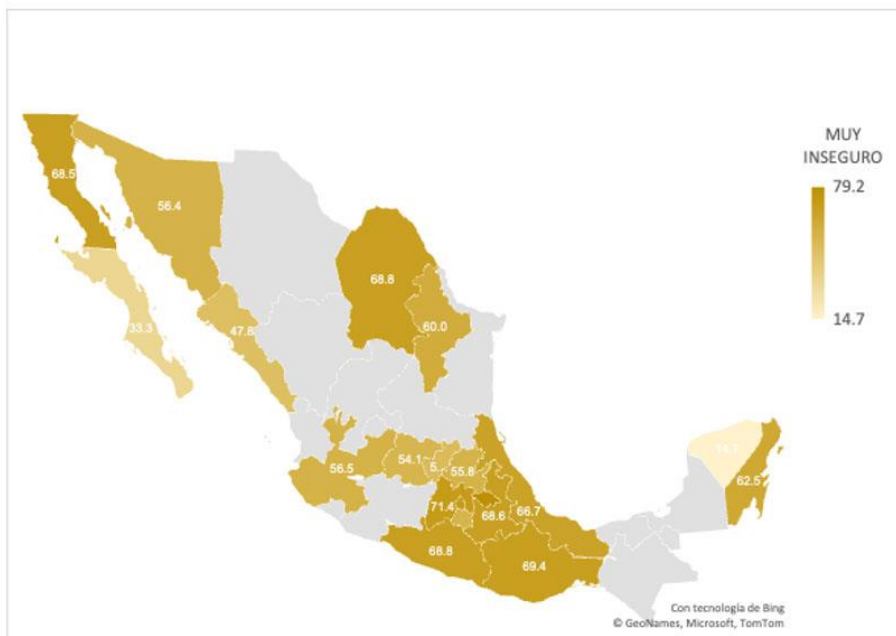
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Notas: 1) La intensidad del tono representa el porcentaje de habitantes que se sienten “muy inseguros”; 2) El tono gris representa las entidades donde no se aplicó la encuesta.

Por otra parte, como ya se ha mencionado, el 50% de los mexicanos encuestados se sienten inseguros. Esto implica que la calificación máxima para cada uno de los 12 ítems indagados emitidos por esta proporción de la muestra fue de 2 a 3 puntos.

Llama la atención la escala, la cual indica que la proporción de los habitantes en las ciudades encuestadas que respondieron percibir su ciudad como “insegura” oscila entre el 79% y 14% del total de la muestra por capital (ver Figura 7).

Figura 7. Percepción de inseguridad en México “Me siento inseguro” (%)



Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Notas: 1) La intensidad del tono representa el porcentaje de habitantes que se sienten “inseguros”; 2) El tono gris representa las entidades donde no se aplicó la encuesta.

Las ciudades donde habita una mayor proporción de población que percibe inseguridad son las siguientes: el 79.2% de los encuestados de Tlaxcala, Tlax.; el 71.4% de los encuestados que viven en Toluca, Edomex., el 71.4% de los habitantes de la Ciudad de México; el 69.4% de los habitantes de Oaxaca, Oax. Todas estas ciudades se caracterizan por contar con índices de inseguridad altos. (INEGI, 2020).

Finalmente, la descripción de los ciudadanos que perciben que viven en una ciudad segura se pueden distinguir en la Figura 8. Llama la atención que la proporción más alta de ciudadanos que perciben que su ciudad es segura se concentran en las ciudades de Mérida, Yucatán, donde el 85.3% de su población indica que habita en una ciudad segura, seguido de la ciudad de San José del Cabo, Los Cabos, donde el 59.4% de sus encuestados percibe que su ciudad es “segura” (ver Figura 8).

Figura 8. Percepción de inseguridad en México “Me siento seguro” (%)



Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Notas: 1) La intensidad del tono representa el porcentaje de habitantes que se sienten “seguros”. 2) El tono gris representa las entidades donde no se aplicó la encuesta.

Tras el análisis se puede inferir que:

- El 50% de los mexicanos encuestados se sienten inseguros;
- La ciudad de Mazatlán, Sinaloa, es la que se percibe como más insegura, seguida de las ciudades de Cuernavaca y Veracruz;
- La ciudad de Mérida, Yucatán, es la que se percibe como más segura.

III.3. Hallazgos de la investigación según género

Se presenta el siguiente análisis comparativo según género, a fin de identificar cuales son las ciudades más amigables según las opciones de respuesta para las mujeres y hombres.

Al analizar los datos, se observa que para la respuesta “Me siento seguro” los hallazgos son los siguientes:

- a) El lugar donde coinciden que se vive de manera segura tanto hombres como mujeres es la capital del estado de Yucatán, la ciudad de Mérida, en la cual los

hombres tienen mayor probabilidad de sentirse seguros (93.8%) frente a un 77.8% de las mujeres que perciben la misma cualidad de dicha ciudad;

- b) Para el caso de la ciudad de San José del Cabo, ubicada en el estado de Baja California Sur, el 77.8% de mujeres encuestadas se sienten seguras viviendo ahí, mientras que los hombres indicaron el 50% en ambas categorías: “seguro” e “inseguro”, debido, posiblemente, a los frecuentes levantamientos de personas que realiza el crimen organizado en el norte del país, por lo que podría inferirse que San José del Cabo en Baja California Sur es una ciudad segura para las mujeres pero no para los hombres;
- c) Llama la atención que los hombres que habitan en las ciudades de Querétaro, Qro. (53.1%), y Pachuca, Hidalgo (45.5%), tienen mayor probabilidad de sentirse seguros frente a la percepción de las mujeres (36% y 20% respectivamente), lo que representa veinte puntos porcentuales de diferencia entre la percepción de hombre y mujeres en ambas ciudades, por lo que se infiere que ambas ciudades son más seguras para los hombres que para las mujeres.

Respecto a la respuesta “me siento inseguro” los hallazgos se describen a continuación:

- a) Si se comparan las Figura 9 y 10 se puede observar que las ciudades de Acapulco, Guerrero, Benito Juárez, Quintana Roo, Guadalajara, Jalisco, Mazatlán, Sinaloa, Monterrey, Nuevo León, Oaxaca, Oaxaca, Puebla, Pue., Saltillo, Coahuila, Tlaxcala, Tlaxcala, Toluca, Edo. de Mex., Veracruz, Veracruz y Xalapa, Veracruz, presentan una proporción más alta de mujeres que se sienten inseguras; las cifras oscilan entre 8 y 24 puntos porcentuales de diferencia, siendo las ciudades de Toluca, Oaxaca, Tlaxcala, Monterrey y Guadalajara aquellas donde las mujeres perciben mayor inseguridad (ver Figura 9 y contrastar con Figura 10);
- b) Por su parte, los lugares donde existe mayor probabilidad de que los hombres perciban que la ciudad donde viven es “insegura” son las ciudades de Cuernavaca, Morelos, Tijuana, Baja California y la Ciudad de México;
- c) La diferencia más grande entre las respuestas emitidas por los hombres y mujeres encuestados, se encontró en la ciudad de Cuernavaca, donde existen casi 12 puntos porcentuales de diferencia según género, siendo los hombres los que se sienten más inseguros;
- d) Llama la atención que, en las ciudades de Guanajuato, Gto., y Hermosillo, Sonora, el 66% de las mujeres percibe mayor inseguridad; sin embargo, los hombres emitieron el 50% de respuestas para la categoría “inseguro” y el 50% para la categoría “seguro”;

Figura 9. Porcentaje de mujeres por ciudad encuestada

Mujeres (%)	Muy inseguros	Inseguros	Seguros	Total Mujeres
Acapulco, Guerrero	14.3	75.0	10.7	100
Benito Juárez, Quintana Roo	13.6	59.1	27.3	100
Ciudad de México	21.1	68.4	10.5	100
Cuernavaca, Morelos	16.7	50.0	33.3	100
Guadalajara, Jalisco	15.6	65.6	18.8	100
Guanajuato, Guanajuato	18.2	66.7	15.2	100
Hermosillo, Sonora	16.7	66.7	16.7	100
Mazatlán, Sinaloa	26.1	52.2	21.7	100
Merida, Yucatan	0.0	22.2	77.8	100
Monterrey, Nuevo León	16.0	68.0	16.0	100
Oaxaca, Oaxaca	5.9	82.4	11.8	100
Pachuca, Hidalgo	0.0	80.0	20.0	100
Puebla, Pue.	4.4	73.3	22.2	100
Querétaro, Querétaro	8.0	56.0	36.0	100
Saltillo, Coahuila	3.8	73.1	23.1	100
San José del Cabo, Los Cabos, Baja California Sur	8.6	20.0	71.4	100
Tijuana, Baja California Norte	16.7	66.7	16.7	100
Tlaxcala, Tlaxcala	0.0	90.9	9.1	100
Toluca, Edo. de Mex.	15.4	84.6	0.0	100
Veracruz, Veracruz	10.0	75.0	15.0	100
Xalapa, Veracruz	11.4	62.9	25.7	100
No especificado	0.0	50.0	50.0	100
Total	11.3	63.8	24.8	100

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Figura 10. Porcentaje de hombres por ciudad encuestada

Hombres (%)	Muy inseguros	Inseguros	Seguros	Total hombres
Acapulco, Guerrero	10.0	60.0	30.0	100
Benito Juárez, Quintana Roo	18.8	53.1	28.1	100
Ciudad de México	0.0	73.7	26.3	100
Cuernavaca, Morelos	19.0	61.9	19.0	100
Guadalajara, Jalisco	10.3	48.3	41.4	100
Guanajuato, Guanajuato	0.0	50.0	50.0	100
Hermosillo, Sonora	4.8	47.6	47.6	100
Mazatlán, Sinaloa	17.4	43.5	39.1	100
Merida, Yucatan	0.0	6.3	93.8	100
Monterrey, Nuevo León	10.0	50.0	40.0	100
Oaxaca, Oaxaca	0.0	57.9	42.1	100
Pachuca, Hidalgo	22.7	31.8	45.5	100
Puebla, Pue.	10.0	65.0	25.0	100
Querétaro, Querétaro	0.0	46.9	53.1	100
Saltillo, Coahuila	0.0	61.9	38.1	100
San José del Cabo, Los Cabos, Baja California Sur	5.9	47.1	47.1	100
Tijuana, Baja California Norte	3.4	72.4	24.1	100
Tlaxcala, Tlaxcala	0.0	69.2	30.8	100
Toluca, Edo. de Mex.	0.0	60.0	40.0	100
Veracruz, Veracruz	28.0	60.0	12.0	100
Xalapa, Veracruz	3.2	54.8	41.9	100
No especificado	0.0	100.0	0.0	100
Total	8.0	54.2	37.8	100

Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

- e) Finalmente, las ciudades más inseguras para las mujeres son Pachuca, Hidalgo (80%), y Querétaro, Qro. (56%); los hombres emitieron en ambas ciudades una mayor proporción para la categoría “Seguros” (45% y 53% respectivamente).

III.4. Hallazgos de la investigación según el lugar donde se sienten más inseguros

La integración de este módulo respecto a la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos realizada por la Universidad Veracruzana y la Benemérita Universidad Autónoma de Puebla entre los meses de febrero-agosto del año 2023, tuvo como objetivo identificar si en los lugares donde sabemos que existen dispositivos de vigilancia electrónica los pobladores perciben menor o mayor inseguridad.

De los 12 lugares cuestionados se detalla a continuación la clasificación según la existencia de dispositivos de vigilancia electrónica (ver Figura 11).

Figura 11. Clasificación de Lugares donde existen o no, dispositivos de vigilancia electrónica

Lugar	Existen comúnmente dispositivos de vigilancia electrónica	Lugar	Existen comúnmente dispositivos de vigilancia electrónica
En el mercado	No	En el banco	Si
En el parque o centro recreativo	No	En el cajero automático localizado en vía pública	Si
En el transporte público	No	En el centro comercial	Si
En la calle	No	En la escuela o espacios escolares	Si
En la Carretera	No	En su casa	Si
En su automóvil	No		
En su trabajo	No		

Fuente: Elaboración propia para la Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

a) Lugares donde no existen comúnmente dispositivos de vigilancia electrónica

Se enlistan en este grupo: trabajo, mercado, calle, transporte público, automóvil, carretera y parque o centro recreativo. Estos lugares se caracterizan por ser espacios públicos donde la existencia de dispositivos de vigilancia electrónica no era común hasta hace algunos años. Usualmente, se consideran espacios de tránsito de los habitantes de una ciudad; sin embargo, debido al incremento de la inseguridad, algunas ciudades han optado en la actualidad por incluir cámaras de video vigilancia en el transporte público, por ejemplo, para evitar el robo a mano armada.

Incluso, existen países como Rusia, en los cuales su normatividad obliga a los privados a portar una cámara de video dentro del automóvil, el cual es el un espacio privado que coadyuva a mantener el orden civil, pues todo lo que sucede en las calles queda registrado para uso de la justicia.

Los hallazgos de la investigación arrojan para esta categoría de análisis que:

- 1) El lugar donde se sienten más seguros es en el trabajo (40.5%);
- 2) Los encuestados informan que el lugar donde no se preocupan por la inseguridad es el parque o centro recreativo (34.8%);
- 3) El lugar donde se sienten más inseguros es el transporte público (35.8%). (Ver figuras 12-23).

b) Lugares donde comúnmente si existen dispositivos de vigilancia electrónica

Para esta categoría de análisis se integra la casa, la escuela o los espacios escolares, centro comercial, banco y cajero automático ubicado en vía pública.

Estos espacios se caracterizan porque, al ser espacios privados, con financiamiento privado, usualmente se invierte en seguridad para garantizar y prevenir conductas adversas que perjudiquen a los miembros de su comunidad. En ellos, usualmente existe la notificación explícita y pública dirigida a los usuarios sobre la existencia de video-grabaciones o seguimiento por parte de algún dispositivo electrónico y existe un común acuerdo sobre el tratamiento de los datos recabados.

Los hallazgos de la investigación arrojan para esta categoría de análisis que:

- 1) El lugar donde se sienten más seguros es en su casa (59.8%);
- 2) Los encuestados informan que los lugares donde no se preocupan por la inseguridad son la escuela y el centro comercial (26%);
- 3) El lugar donde se sienten más inseguros es el cajero automático ubicado en la vía pública (35.8%) seguido del banco (23.4%);

Tras estos hallazgos, se puede inferir que los lugares donde comúnmente sí existen dispositivos de vigilancia electrónica se perciben como más seguros. Obsérvese que la percepción de inseguridad también es más baja en los lugares donde existen dichos dispositivos (ver Anexo 1: Figuras 12-23).

Conclusiones

Los hallazgos de esta investigación dan cuenta de la existencia de sistemas de vigilancia electrónica en México. Éstos son necesarios para prevenir el crimen y la inseguridad.

ridad; sin embargo, se comprueba que los ciudadanos mexicanos hemos normalizado la inseguridad y la violencia, pues el análisis arroja que habitamos ciudades que nos hacen sentir “inseguros” naturalmente, es decir, el 50% de los participantes en esta encuesta, perciben un sentimiento de inseguridad constante.

Tras el análisis se concluye que las ciudades que se perciben como más inseguras no cuentan con un alto número de cámaras de video vigilancia, según cifras aportadas por el INEGI, 2020.

Respecto al género, se comprueba una vez más que, en México, son las mujeres quienes se sienten más inseguras, salvo los casos de las ciudades de Cuernavaca, Morelos; Tijuana, Baja California y la Ciudad de México, donde son los hombres quienes indican que se sienten más inseguros.

Finalmente, se pudo comprobar que los espacios públicos donde existen cámaras de vigilancia electrónica son 10 puntos porcentuales más seguros que los que no las tienen, siendo la casa y el trabajo los lugares donde los mexicanos se sienten más seguros, pese a que el INEGI ha comprobado que los hogares son los lugares donde se comenten con mayor frecuencia los delitos.

Por el contrario, el transporte público y los cajeros automáticos ubicados en vía pública son los lugares donde los mexicanos se sienten más inseguros. Esta idea se confirma con los datos presentados por el INEGI 2023.

Este ejercicio permite identificar los pros y los contras de la existencia de videocámaras, pues es un hecho que cuando la población conoce que existen sistemas de videovigilancia en su ciudad, se fortalece el sentimiento de seguridad. Sin embargo, los ciudadanos no son conscientes de los riesgos que se producirían en caso de que la información personal de cada ciudadano caiga en manos del crimen organizado.

Por otra parte, podemos asegurar que los sistemas de videovigilancia son necesarios, pero deben ir acompañados de normatividad adecuada para garantizar los derechos humanos, así como de procesos confiables de selección de personal, capacitación de punta para los operadores de los sistemas de videovigilancia e inversión constante en tecnología de punta a fin de que la información que contiene datos personales sensibles no caiga en manos del crimen organizado o sea utilizada con fines de control político.

Referencias

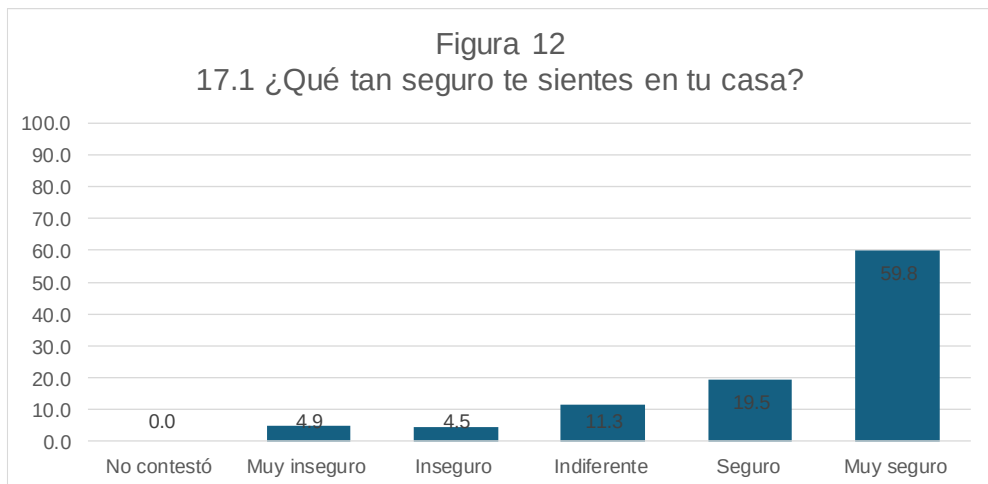
Bermúdez, C. A., y Ramírez, L. P., Herrera, M. Y., y Olaya, R. W. (2022). Propuesta de mejoramiento de la seguridad mediante drones en la ciudad de Bogotá (Project Selantrophus). *Revista Ingeniería, Matemáticas y Ciencias de la Información*, 105-115. <http://dx.doi.org/10.21017/rimci.2022.v9.n17.a115>

- BID. (07/03/2024). Seguridad Ciudadana en América Latina y el Caribe. Recuperado de: <https://www.iadb.org/es/noticias/seguridad-ciudadana-en-america-latina-y-el-caribe#:~:text=La%20región%20tiene%20una%20tasa,mundial%2C%20UNODC%2C%202023>).
- Canto de Gante, Á. G.; Sosa González, W. E.; Bautista Ortega, J.; Escobar Castillo J.; Santillán Fernández, A. (2020). Escala de Likert: Una alternativa para elaborar e interpretar un instrumento de percepción social. En: Revista de la Alta Tecnología y Sociedad 38 Vol. 12, No. 1, 2020. ISSN 1940-2171 pp. 38-45. Recuperado de: https://www.researchgate.net/profile/Alberto-Fernandez-45/publication/361533522_Escala_de_Likert_Una_alternativa_para_elaborar_e_interpretar_un_instrumento_de_percepcion_social/links/62b736d0d49f803365b96810/Escala-de-Likert-Una-alternativa-para-elaborar-e-interpretar-un-instrumento-de-percepcion-social.pdf
- Delgado, T. V. (2022). Modernización de la gestión pública y su influencia en la atención de la ciudadanía desde los gobiernos locales. *Ciencia Latina Revista Científica Multidisciplinar*. https://doi.org/https://doi.org/10.37811/cl_rcm.v6i2.2034
- Gallup. (2023). Ecuador y Perú, los países con mayor percepción de inseguridad en la región. CID Gallup. Encuestas de Opinión Pública. Recuperado de: https://www.cidgallup.com/uploads/publication/publication_files/publication_1677889138000.pdf
- INEGI. (2023). Encuesta Nacional de Victimización y Percepción Sobre Inseguridad Pública. ENVIPE. INEGI. Actualización 11 de septiembre de 2023. Recuperado de: <https://www.inegi.org.mx/programas/envipe/2023/#tabulados>
- INEGI. (2015). Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales (/programas/cngspspe/2016/).
- Latinobarómetro. (21/07/2023). Informe 2023. La recesión económica en América Latina. Corporación Latinobarómetro. AECID, BID. Recuperado de: <https://www.latinobarometro.org/lat.jsp>
- Morales, J., Monzón, H. (2022). *Sistemas de video vigilancia aplicado a la seguridad pública para la prevención y control del delito en la ciudad de San Rafael* [Tesis de título profesional, Universidad Nacional de Cuyo]. https://repositorio.utdt.edu/bitstream/handle/20.500.13098/12079/MPP_Vivas_2022.pdf?sequence=1&isAllowed=y.
- Narváez S., Chorny V. (29/01/2020). Videovigilancia en el espacio público: un obstáculo para las libertades civiles En: Red de defensa de los derechos digitales. Recuperado de: <https://r3d.mx/2020/01/29/videovigilancia-en-el-espacio-publico-un-obstaculo-para-las-libertades-civiles/>
- Prado Canchari, A.; Carrión Barco, G.; Alarcon Nuñez, C.; Agreda Cerna, H.W. (2024). Efectividad de las políticas públicas en los servicios de seguridad pública por video digital. En: VISUAL REVIEW. Vol. 16, No. 1, 2024. ISSN 2695-9631. International Visual Culture Review. Revista Internacional de Cultura Visual. Pp. 15.29 <https://doi.org/10.37467/revvisual.v15i136>
- Savall, V. (2022). *Ciber-tecnologías de la vigilancia: Un estudio comparativo a escala nacional sobre la aplicación de las nuevas técnicas de control en la seguridad pública y privada* [Tesis de Maestría, Universidad Miguel Hernández]. http://dspace.umh.es/bitstream/11000/28458/1/SEPP_TFG_SAVALL_IBIZA_VICTOR.pdf.

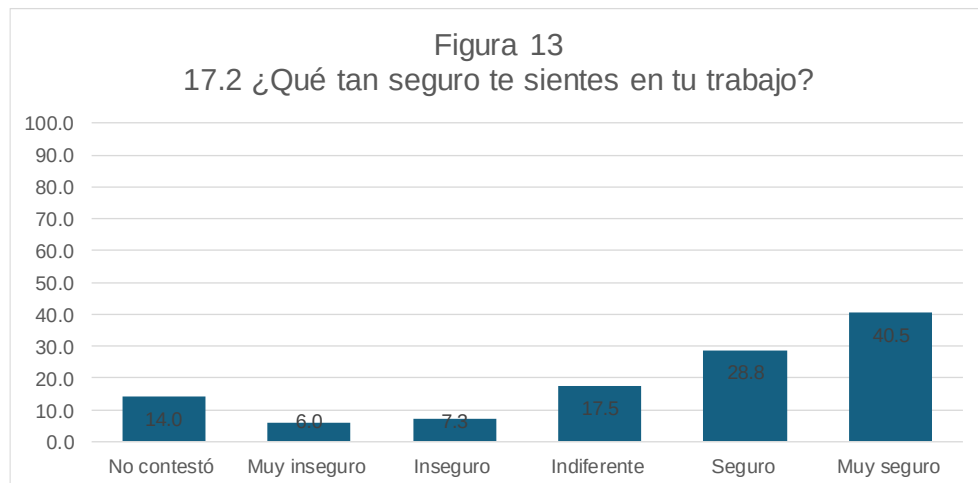
- SEDENA. (12/12/2023). Informe de seguridad. Gobierno de México, Secretaría de Seguridad y Protección Ciudadana. Secretaría de Marina. Guardia Nacional. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/876092/CPM_Informe_de_Seguridad__13dic23.pdf
- SEGOB. (2023). Fortalecimiento de los Sistemas de Videovigilancia y Geolocalización. SEGOB. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/798891/17_FortalecimientoSistemasVideoVigilancia.pdf
- SEGOB. (S/Ra) Norma Técnica para estandarizar las características técnicas y de interoperatividad de los sistemas de video vigilancia para la seguridad pública. SEGOB, Centro Nacional de Información. Secretariado Ejecutivo del Sistema nacional de Seguridad Pública. Recuperado de: https://secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf
- SEGOB. (S/Rb). Capítulo 3. Programa con prioridad nacional de Tecnologías, Infraestructura y Equipamiento de apoyo a la Operación Policial. Subprograma con prioridad nacional de: Sistemas de Videovigilancia. SEGOB. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. Recuperado de: <https://www.gob.mx/sesnsp/acciones-y-programas/programa-de-fortalecimiento-para-la-seguridad-fortaseg?idiom=es>
- Sen, A. (2000). Desarrollo y Libertad. Ed. Planeta. México.
- Rivera Hernández, C. (2021). Percepción de los estudiantes de nivel medio superior sobre el uso de cámaras de video en el aula virtual y cámaras de video vigilancia en los espacios educativos como instrumento para prevenir la violencia y el acoso escolar en Puebla, México durante la pandemia por COVID-19 En: Espinosa, Martínez y Chipulli (2021). Vigilancia, dispositivos electrónicos y derechos humanos en México: Retos y oportunidades a enfrentar en el siglo XXI. Ed. Universidad Veracruzana BUAP, CONHACYT, CLACSO, COMECOSO, Montiel y Soriano Editores S.A. de C.V. ISBN versión impresa: 978-607-8728-69-5 pp. 145-158.
- UNODC. (26/06/2023). El Informe Mundial sobre las Drogas 2023 de UNODC advierte sobre crisis convergentes a medida que los mercados de drogas ilícitas siguen expandiéndose. Oficina de las Naciones Unidas contra la droga y el delito en México. Recuperado de: <https://www.unodc.org/lpomex/es/noticias/junio-2023/el-informe-mundial-sobre-las-drogas-2023-de-unodc-advierte-sobre-crisis-convergentes-a-medida-que-los-mercados-de-drogas-ilicitas-siguen-expandindose.html>
- Vivas, E. (2022). *Utilización de herramientas tecnológicas para el desarrollo de una política pública de seguridad pública – El caso de la Ciudad Autónoma de Buenos Aires*, [Tesis de maestría. Universidad Torcuato Di Tella]. <https://repositorio.utdt.edu/handle/20.500.13098/12079>.

Anexo 1

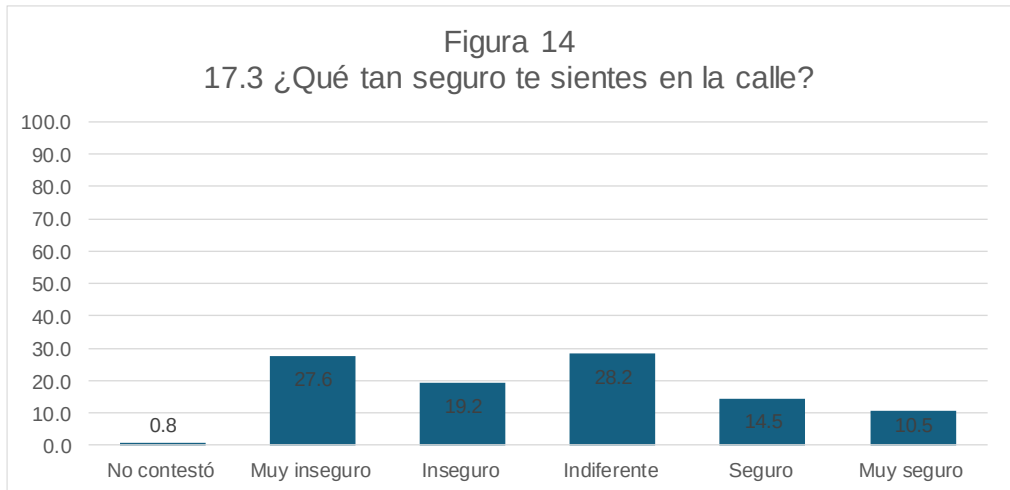
Lugares que se incluyeron en la evaluación de espacios públicos videovigilados



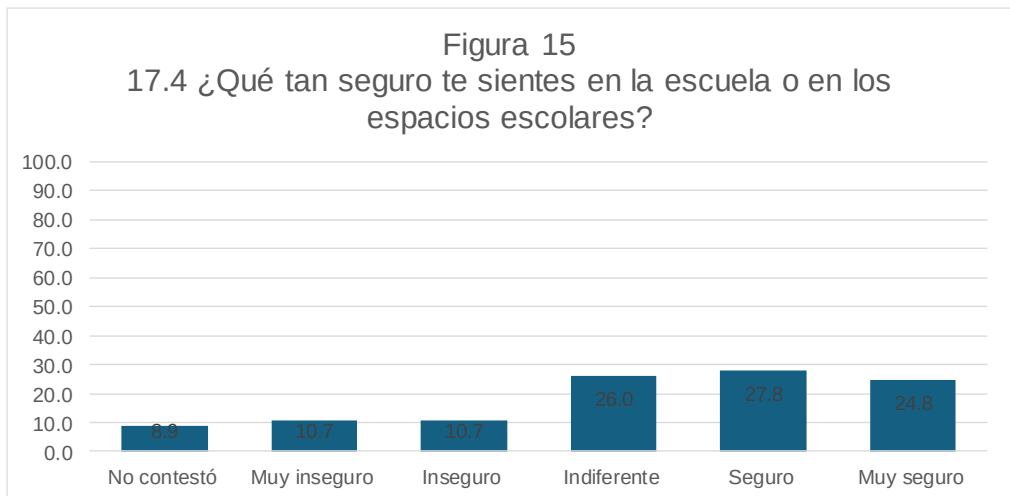
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



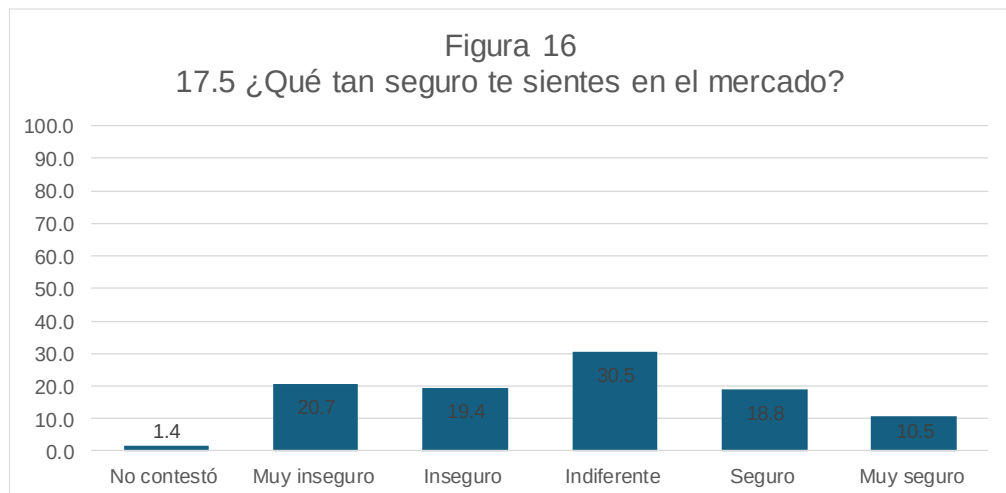
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



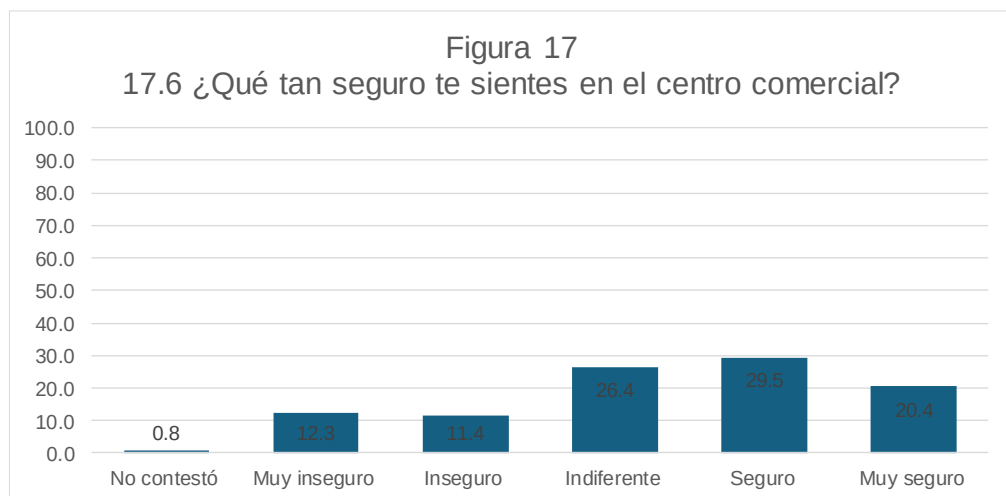
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



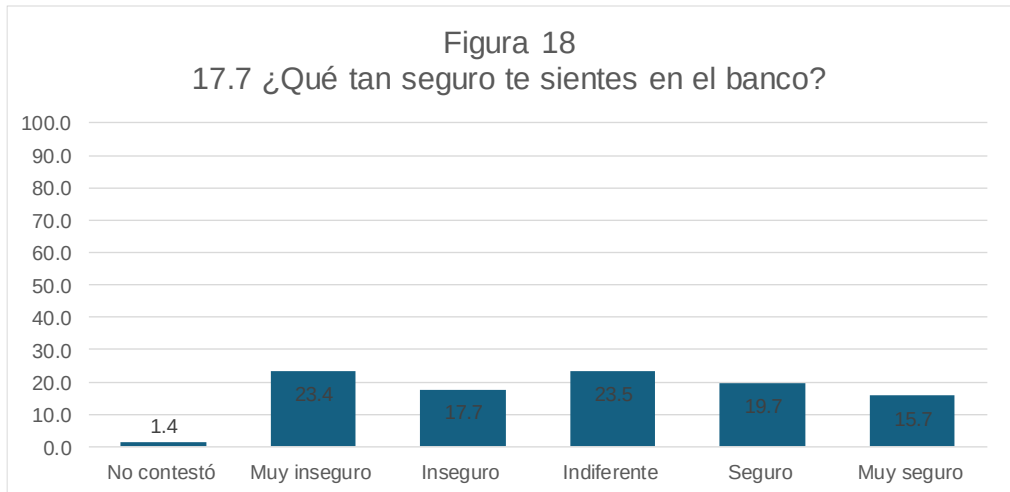
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



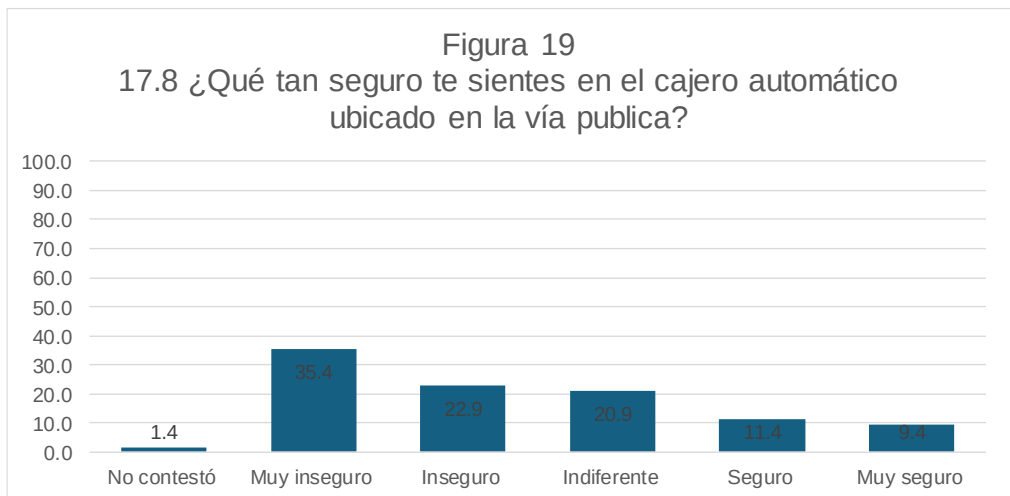
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



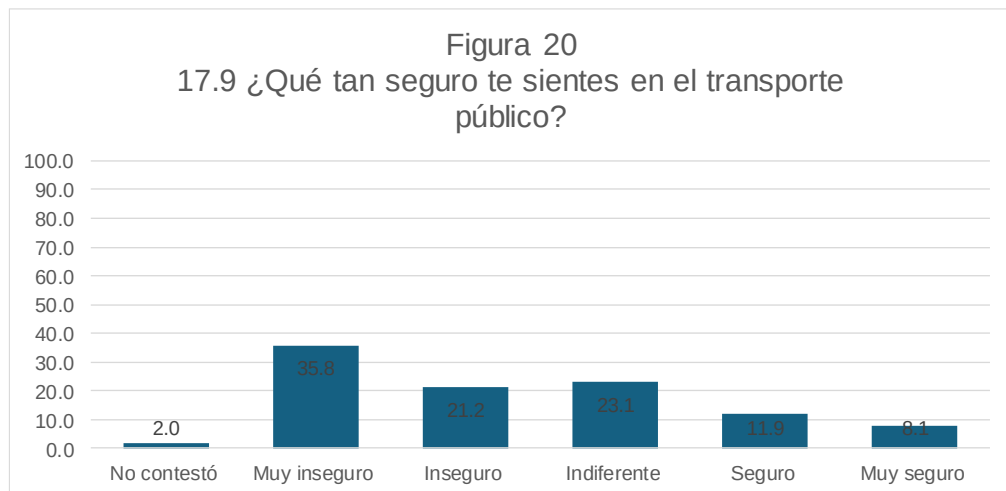
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



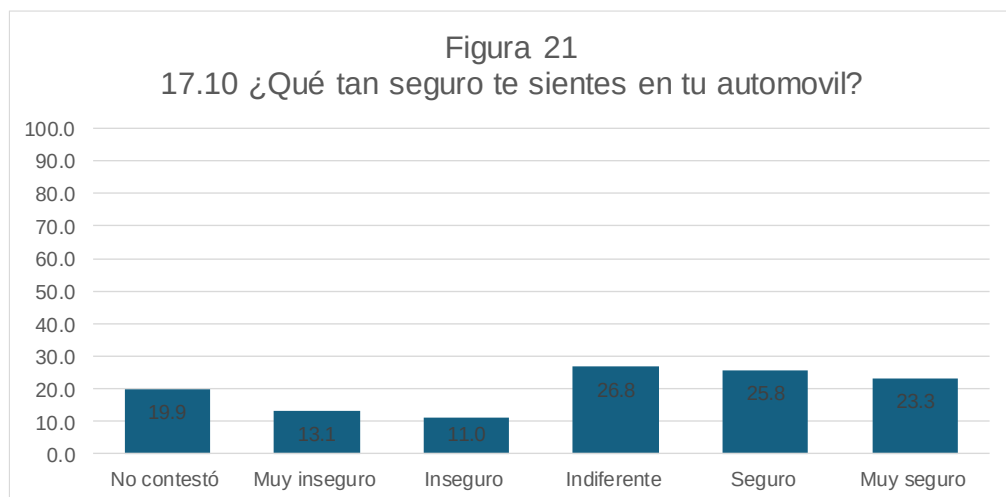
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



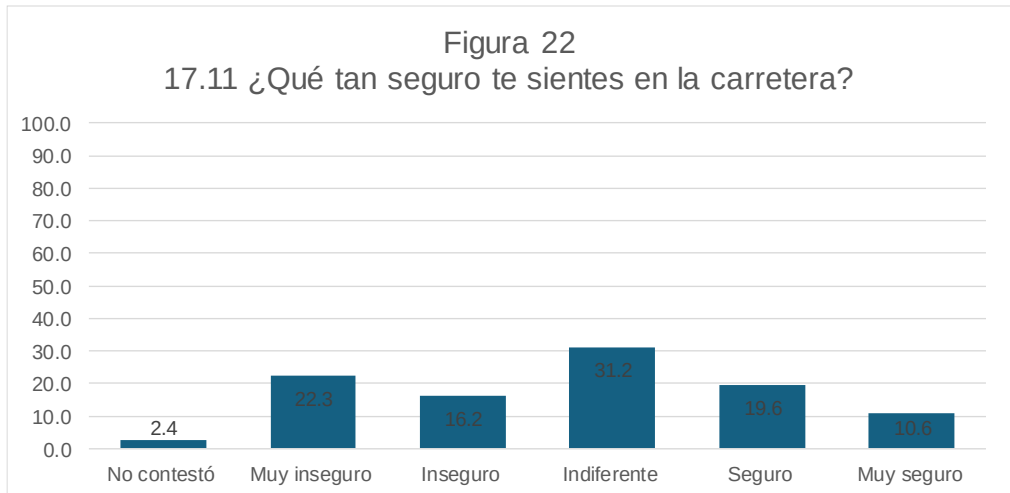
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



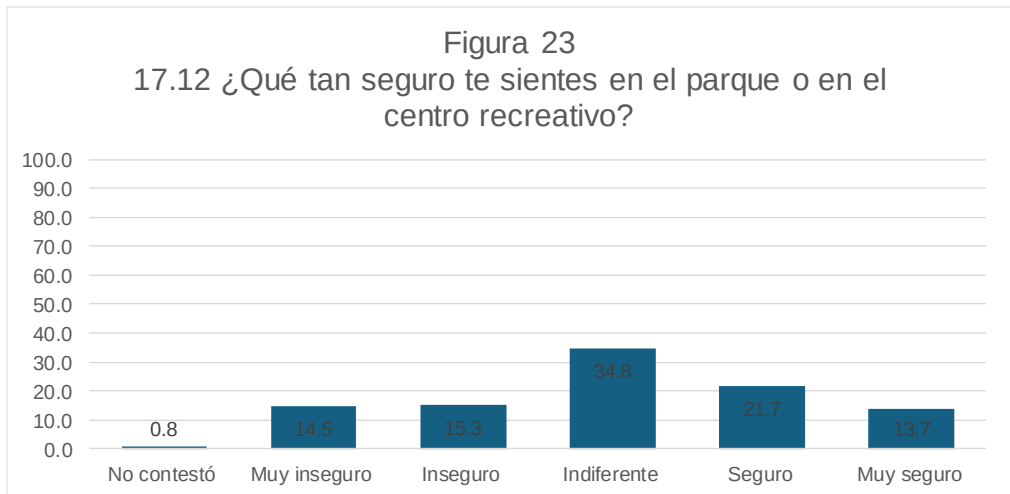
Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.



Fuente: Encuesta Nacional de Percepción de Dispositivos de Vigilancia Electrónica con Perspectiva de Derechos Humanos, UV-BUAP, 2023.

Capítulo 2

Dispositivos de vigilancia electrónica. Una mirada desde el ámbito jurídico

Electronic surveillance devices. A look from the legal field

*Arturo Miguel Chípulli Castillo**
*Michel Marie Lago Cruz***

Resumen

Este trabajo tiene como finalidad conocer la normatividad de los dispositivos de vigilancia electrónica, en particular, drones, cámaras de videovigilancia e inteligencia artificial en México, así como identificar la realidad jurídica de su implementación. Lo anterior, a través del método documental y análisis de la legislación a nivel internacional, nacional y estatal. Se concluye que existen deficiencias en el marco jurídico existente, enfatizando la importancia del Estado y su deber de garantizar el bienestar de la ciudadanía y sus derechos humanos. Igualmente, existe la necesidad de crear normas claras y precisas que regulen la adopción e implementación de estos dispositivos.

Palabras clave: Dispositivos de Vigilancia Electrónica; Drones; Cámaras de videovigilancia; Inteligencia Artificial; Política Pública de Seguridad.

* Licenciado en Derecho (Universidad de Xalapa). Maestro en Derecho Constitucional y Juicio de Amparo (Universidad de Xalapa). Maestro en Derechos Humanos y Democracia (Facultad Latinoamericana de Ciencias Sociales, FLACSO Sede México). Profesor-Investigador de tiempo completo en el Instituto de Investigaciones Jurídicas (IIJ) de la Universidad Veracruzana (UV). Miembro del Sistema Nacional de Investigadoras e Investigadores (SNII) Nivel 1 por el CONAHCYT achipuli@uv.mx <https://orcid.org/0000-0001-8808-3311>m

** Licenciada en Derecho de la Universidad Veracruzana. Maestranda en Política Pública y Gestión Educativa Estratégica. Becaria del Diagnóstico y Modelo de Índice de Percepción de los Dispositivos de Vigilancia Electrónica en materia de Seguridad Pública en México con Enfoque de Derechos Humanos, propuesta 3265530 del Consejo Nacional de Historia Ciencia y Tecnología (CONAHCYT), marielagocruz@gmail.com

Abstract

The purpose of this work is to understand the regulations of electronic surveillance devices, in particular, drones, video surveillance cameras and artificial intelligence in Mexico, as well as to identify the legal reality of the implementation of surveillance technology. The above, through the documentary method and analysis of legislation at the international, national, and state level. It is concluded that there are deficiencies in the existing legal framework, emphasizing the importance of the State and its duty to guarantee the well-being of citizens and their human rights. Likewise, there is a need to create clear and precise standards that regulate the adoption and implementation of these devices.

Keywords:

Electronic Surveillance Devices; Drones; Video Surveillance Cameras; Artificial Intelligence; Public Security Policy.

Introducción

Hoy en día, la vigilancia incluye todo un conjunto de tecnologías e información, cada vez más sofisticados, los cuales están integrados por diversos sistemas y dispositivos que permiten y facilitan captar imágenes ya sea fijas o en movimiento, inalámbricas o de conexión a internet, y que permiten el almacenamiento, consulta y tratamiento de datos de la vida cotidiana de las personas.

Gracias a los avances tecnológicos y de comunicación de los últimos años se ha podido lograr que las actualizaciones y mejoras de los dispositivos de vigilancia sean más eficaces en cuanto al procesamiento de grandes cantidades de datos, a partir de la inteligencia artificial, y en la optimización de los procesos de tomas de decisión, recolección y análisis de la información sobre las rutinas de las personas, ya sea en un ámbito laboral o académico; tendencia que identifica Nelson Arteaga Botello, quien advierte que “en la modernidad la forma aplicada de la vigilancia en poblaciones, grupos e individuos, es un elemento central de vida moderna” (Arteaga Botello, 2009).

En una definición más concreta, Lyon (2007) considera que la vigilancia es un elemento esencial de la vida moderna, ya que “permite tener un control sobre las distintas esferas de la sociedad que forman parte del desarrollo sistemático de las ciudades, su origen se remonta a la etapa intermedia entre los siglos VIII y IX en los cuales la organización militar y la necesidad de planificar la organización de las sociedades se logró a través de la vigilancia” (Lyon, 2007).

La evolución de las sociedades humanas siempre traerá consigo una nueva tanda de necesidades, problemas públicos y derechos que, aunque se traten en esencia de lo mismo, sus características y contextos a través de la historia podrían desarrollarse de manera diferente. Es decir que, si bien la seguridad, la protección y la paz, son derechos humanos que deben ser garantizados por el Estado y los gobiernos, actualmente requie-

ren de una vinculación directa con el uso de las nuevas tecnologías de información y comunicación, lo cual implica nuevas reflexiones teóricas y estudios empíricos, nuevas metodologías, así como nuevos procesos de implementación y de evaluación.

Las autoridades de protección de datos juegan un papel fundamental en la regulación de la videovigilancia a nivel internacional. Estas autoridades, principalmente en países europeos, trabajan para garantizar la correcta aplicación de las disposiciones generales sobre protección de datos en el contexto de la videovigilancia. Su labor incluye emitir dictámenes, directrices y códigos de conducta que orientan el uso de sistemas de videovigilancia, asegurando el respeto a los derechos fundamentales de las personas, como la privacidad y la protección de datos personales.

Estas autoridades supervisan que el tratamiento de datos personales, en el contexto de la videovigilancia, cumpla con las normativas vigentes, como la Directiva 95/46/CE de la Unión Europea, y que se respeten los principios de proporcionalidad, transparencia y seguridad en el manejo de la información captada por cámaras de vigilancia. Además, se encargan de evaluar las notificaciones de ficheros de imágenes de videovigilancia y de inscribirlos en los registros correspondientes, como en el caso de la Agencia Española de Protección de Datos.

En resumen, las autoridades de protección de datos desempeñan un rol crucial en garantizar que la videovigilancia se realice de manera legal, ética y respetuosa de los derechos individuales, contribuyendo a equilibrar la seguridad pública con la protección de la privacidad de las personas involucradas.

En este Siglo XXI, es importante hacer mención que estas herramientas tecnológicas se implementan en las esferas pública y privada con diversas finalidades, como son la seguridad preventiva de los delitos y el control social, tal y como lo señala la empresa española de tecnología Tradeseur (1995):

Los sistemas de seguridad son cada vez más demandados por nuestra sociedad ya que contribuyen al bienestar comunitario tanto en entornos privados como públicos. En la era digital contar con imágenes, vídeos o audios no solamente sirve para detectar y prevenir todo tipo de acción intrusiva, ataque o amenaza, sino que además resulta una prueba fehaciente de los hechos acontecidos que puede utilizarse como testimonio ante la justicia (Short & Ditton, 1995).

Con lo anterior, se señala que los dispositivos de vigilancia electrónica “han podido tomar terreno en diversos ámbitos de seguridad y prevención de delitos y han mostrado mejoras que funcionan como herramientas para tener de primera mano sucesos delictivos. Aunque, los resultados de su eficacia no son concluyentes ni definitivos” (Galdon, 2015).

El grado de operatividad que tengan depende de la profesionalización y capacitación en la materia; asimismo, las políticas criminales vigentes definen los mecanismos

de vigilancia que se pretenden implementar para un determinado espacio urbano. En efecto, el propósito de la vigilancia, precisamente, es obtener información comprobable respecto a la situación delincuenciales a partir de las estadísticas que son producto de las denuncias interpuestas y la tensión social que se vive en ciertos sectores.

Podría observarse que la evolución de las tecnologías y dispositivos de vigilancia ha llevado a que se conviertan constantemente en herramientas efectivas para salvaguardar tanto la seguridad privada como pública. Esto implica un respaldo sólido en casos que puedan ser objeto de litigio en el sistema judicial penal, al proporcionar pruebas concretas y fiables relacionadas con eventos específicos.

Por lo anterior, es que los avances y sistemas de videovigilancia aplicados a fortalecer la seguridad requieren la visualización pertinente de cada una de las áreas en las que se presenta, logrando así que los datos obtenidos logren prevenir, desalentar y enfrentar comportamientos ilegales, así como asegurar la paz y el bienestar de los ciudadanos.

Respecto al propósito primordial de los dispositivos de vigilancia electrónica, es crear las condiciones de control que prevengan la concurrencia de hechos delictivos. Esto implica una labor compleja de reconocimiento de conductas sospechosas, amenazas y patrones delictivos relacionados con el modus operandi de estructuras criminales que operan en sectores específicos. Por ello, en áreas urbanas, la supervisión desempeña un papel crucial en la formulación de políticas de seguridad que se ajusten a las necesidades específicas de cada región, centrándose especialmente en los patrones demográficos donde se busca implementar la vigilancia.

Es por esto por lo que el Estado debe trabajar arduamente en crear la normativa necesaria para garantizar el uso correcto de los dispositivos de vigilancia electrónica, ya que, debido a los rápidos avances y mejoras que muestran cada uno de estos dispositivos, se consideran como una de las primeras opciones entre la población para garantizar la seguridad, puesto que, al ser dispositivos de vigilancia, pueden tener un mejor control de lo que ocurre dentro de sus casas y espacios públicos.

Derivado de lo anterior, el objetivo de este trabajo es conocer la normatividad que existe actualmente de los dispositivos de vigilancia electrónica, en particular, drones, cámaras de videovigilancia e inteligencia artificial, en México. Se aplica el método documental, a partir del análisis del marco jurídico nacional, estatal e internacional.

I. Dispositivos de vigilancia electrónica. Concepto y características

A través de la literatura se ha podido identificar que el concepto de dispositivo de vigilancia electrónica se entiende como:

El conjunto de tecnologías, herramientas y dispositivos electrónicos, que permiten obtener, monitorear, administrar información de una población determinada, de manera sistemática y permanente, para el procesamiento de datos personales, que sirvan como calculador, clasificador y perfilador de riesgos cotidianos, que dependen de la tecnología de información y comunicación (Giddens, 1987; Gandy, 1993; Lyon, 1996; 2007).

En lo anterior, los autores señalan e identifican que el principal objetivo o sujeto de la vigilancia será una población determinada. Estos dispositivos se encargarán de recopilar y procesar toda imagen física o huella digital que desprenda una población, para así identificar y perfilar posibles riesgos, cumpliendo con la premisa con que son implementados: generar la percepción de seguridad y disminuir los índices delictivos.

En la actualidad, los dispositivos de videovigilancia electrónica son uno de los temas con mayor relevancia en términos de seguridad y de protección en México; esto derivado de los altos índices de inseguridad reportados día con día, así como la creencia –quizá errónea– de que son una medida que contrarresta directamente la violencia generalizada.

Los dispositivos de vigilancia han sido catalogados como mecanismos que sintetizan simultáneamente las fuerzas morales del bien y el mal en una sociedad. En ellos se puede ver un objeto sagrado o puro que garantiza la protección de las personas y colectivos, que permite monitorear peligros latentes, así como transmitir el sentido de obligatoriedad a los ciudadanos para respetar las reglas y, de la misma forma, castigar a quienes las rompen. Al mismo tiempo, hacen posible que los individuos se comporten adecuadamente en los espacios tanto públicos como privados, al tiempo que genera un historial de comportamientos.

Según ha señalado Arteaga Botello (2021), estos dispositivos no han tenido la aceptación esperada en algunos casos, pues se les ha concebido como “artefactos impuros que tienden a vulnerar a las personas en su intimidad y privacidad” (Arteaga Botello, 2021), denotándolos como un ataque a las libertades, ya que obligan a cumplir con leyes posiblemente injustas, que permiten la delación de actividades políticas y sociales. Lo anterior, toda vez que alteran los límites de lo público y lo privado, permitiendo que el pasado de las personas sea utilizado mediante poderes que lo escudriñan.

I.1 Drones

Los denominados *drones* tienen origen en las experimentaciones militares de inicios del siglo XX. Su denominación formal y más generalizada es UAV (Unnamed Aerial Vehicle) o RPA (Remotely Piloted Aircraft); en castellano, generalmente se les cataloga como VANT (Vehículo Aéreo No Tripulado). Un vehículo aéreo no tripulado es un avión sin piloto. En el sentido en el que lo contempla el artículo 8 del Convenio sobre Aviación Civil Internacional, su definición sería la siguiente: “operado sin piloto a

bordo, de forma remota y totalmente controlado desde otro lugar (tierra, otra aeronave, espacio) o programado y totalmente autónomo” (Convenio Sobre Aviación Civil Internacional, 1944). De esta manera, Nairí Guler (2022) afirma que:

El término dron tiene su aparición en 1935, cuando en un acto de la Marina Real británica una aeronave pilotada a control remoto hizo su demostración. Originalmente designado Fairey Queen, más tarde fue apodado Queen Bee debido al sonido que emitía, similar al del zumbido de las abejas. Por la misma razón, luego se lo bautizaría drone, que en inglés significa tanto ‘zumbido’ como ‘zángano’.

Actualmente, su denominación formal está tendiendo a mutar a UAS (Unmanned Aircraft System) y RPAS (Remotely Piloted Aircraft System), que en castellano se traducen como “sistema de aeronaves no tripuladas” y “sistema de aeronave pilotada remotamente” respectivamente. (p.6)

En este sentido, es de importancia recurrir a la legislación aplicable en México, la cual se circunscribe a las disposiciones del Derecho Internacional a través de la fracción IV del Artículo 42 de la Constitución Política de los Estados Unidos Mexicanos, que prevé que: “los drones con un peso mayor a los 2 kilogramos, deben de contar con un permiso especial para su manejo, mientras que los que tienen un peso menor al señalado por la SCT, solo deben respetar las disposiciones establecidas para su uso recreativo o comercial” (CPEUM Art. 42, fracción IV).

De la misma manera, en la Norma Oficial Mexicana (NOM 107 SCT3 2019), publicada por la Agencia Federal de Aviación Civil, en noviembre del 2019, se establecen “los requisitos para registrar y volar un dron para fines recreativos, comerciales o sin fines de lucro, en el espacio aéreo mexicano”. De acuerdo con la AFAC y la SCT, existen zonas en las que está prohibido operar un dron, esto debido a que se reconocen como zonas peligrosas y restringidas. Norma Oficial Mexicana (NOM-011-SCT3-2001).

I.2 Cámaras de Vigilancia

El término “sistema de videovigilancia” se refiere a un sistema de seguridad compuesto por cámaras de vigilancia y un software de grabación que registra, en tiempo real, imágenes y videos de lo que ocurre en ubicaciones locales o remotas. Su propósito principal es garantizar la seguridad y prevenir robos.

En general, lo que constatan estas evaluaciones internacionales es que “los sistemas de videovigilancia en el espacio público pueden contribuir a la reducción de la delincuencia en dicho ámbito, pero de manera desigual: más en lugares de poca actividad social y poco control informal, como los aparcamientos aislados, por ejemplo, que, en centros urbanos y zonas residenciales, sobre todo en el caso de los Estados Unidos”

(Short & Ditton, 1995; Tilley, 1993). El impacto de las cámaras de vigilancia, además, “parece ser mayor cuando hay carteles indicativos que pueden generar un efecto disuasorio y cuando la zona vigilada es un espacio de acceso limitado” (Díez-Ripollés & Cerezo, 2009).

El objetivo de los dispositivos de videovigilancia “comenzó por buscar detectar carteristas, pequeños defraudadores, comerciantes ilegales, así como disuadir comportamientos que alteran el orden social” (Hempel y Töpfer, 2009). Con el paso del tiempo, ha surgido la percepción de que las videocámaras contribuyen a la intervención del gobierno en diversas áreas de la vida social, extendiéndose más allá de la lucha contra el crimen y el terrorismo. En la Tabla 1 es posible advertir algunos tipos de cámaras de vigilancia.

Tabla 1. La variabilidad de cámaras de vigilancia

Tipos de cámaras	Características
Cámaras Wifi o inalámbricas	Se conectan a la red Wi-Fi para transmitir imágenes y videos sin cables.
Cámaras IP	Utilizan Internet Protocol (IP) para enviar y recibir datos a través de una red.
Cámaras exteriores	Diseñadas para resistir condiciones climáticas adversas y proteger áreas al aire libre.
Cámaras interiores	Diseñadas para monitorear y grabar actividades dentro de edificios o espacios cerrados.
Cámaras de visión nocturna e infrarrojos	Permiten capturar imágenes en condiciones de poca luz o en la oscuridad utilizando luz infrarroja.
Cámaras con movimiento y zoom	Pueden moverse horizontal y verticalmente, y algunas ofrecen capacidad de zoom.
CCTV o circuitos cerrados	Sistema de videovigilancia que utiliza cámaras conectadas a un sistema de monitoreo centralizado.

Fuente: Adaptado de Castillo Agurto, C. A. (2018) Propuesta de implementación de un sistema de cámaras de vigilancia para el Instituto Superior Tecnológico Privado Abaco–Piura.

Por otro lado, Botello (2009) plantea que la industria de las cámaras de vigilancia percibió un aumento en sus ventas de manera significativa en el periodo 2011-2012 en un 60%, manteniendo un crecimiento moderado hasta el año 2014, “cuando se detuvo sensiblemente por la introducción de las cámaras de vigilancia digital, lo anterior implicó un nuevo ajuste en las finanzas de las empresas y los distintos ámbitos del Gobierno”, quienes no presumían de solvencia presupuestal para adquirir estos equipos de última generación.

Es menester indicar que, aun con la presencia de los dispositivos de vigilancia electrónica, el hecho de que no se implemente a la par una evaluación constante sobre su efectividad frente a la inseguridad, evidencia los límites y alcances de dichos dispositivos en la disminución, prevención, y reedificación de hechos delictivos.

I.3 Inteligencia Artificial

Aunque no existe una definición definitiva sobre el término de Inteligencia Artificial, de acuerdo con la literatura esta se refiere “al grupo de tecnologías digitales que permiten a las máquinas llevar a cabo tareas complejas que normalmente requieren inteligencia humana; y en lo general puede dividirse en dos grandes campos: Inteligencia Artificial General e Inteligencia Artificial específica” (Hall & Pesenti, 2017). El primer campo implica la capacidad de las máquinas para replicar completamente las habilidades intelectuales humanas e incluso mostrar signos de conciencia.

Algunos autores coinciden en la afirmación de que la Inteligencia Artificial podría estar disponible en un periodo de 30 hasta 100 años. El segundo campo de inteligencia Artificial se define como el lugar “en donde tecnologías y técnicas como la minería de datos, aprendizaje profundo, aprendizaje de máquinas o redes neuronales artificiales son utilizadas para realizar acciones específicas, y que ya están disponibles para su uso en etapas iniciales” (Zapata, 2018).

La inteligencia artificial (IA) se define como el campo científico y técnico dedicado a crear máquinas capaces de realizar tareas de forma inteligente, centrándose en el desarrollo de programas informáticos avanzados; según la *Enciclopedia Britannica*, los proyectos de IA son sistemas dotados de procesos intelectuales característicos de los humanos, como la capacidad de razonar, descubrir significados, generalizar o aprender de experiencias pasadas. El término “IA” fue acuñado por John McCarthy, un informático estadounidense, en 1956, durante la Conferencia de Dartmouth, donde nació la disciplina. La IA acelera en segundos el procesamiento de millones de datos biométricos, convirtiéndose en la base de empresas líderes a nivel mundial, como Google, Amazon, Alibaba, Facebook, entre otras.

Los datos, especialmente los biométricos, se consideran útiles para comprender la conducta humana y las respuestas biológicas ante emociones, enfermedades, perspectivas o creencias. De tal modo, Harari subraya que el individuo no se conoce a sí

mismo, mientras que la IA es capaz de adelantarse a los resultados de esa conducta en ese mismo individuo, con un 98.9% de rapidez y precisión. Es precisamente que “gracias a la sistematización de la información el software es capaz de reconocer patrones con los que aproxima un resultado sustentado en estadística y probabilidad que termina siendo más acertado en ocasiones” (Harari, 2018). En la Tabla 2 es posible advertir algunos de los datos comúnmente guardados en la red.

Tabla 2. Datos guardados en la red

Datos que permanecen guardados en la red	
Consultas	Clics publicitarios
Hora	Visitas a páginas webs
Fecha	Redes sociales
Historial del navegador	Motores de búsqueda
Direcciones de correo electrónico	Emails
Direcciones IP	Teléfonos
Ubicación	Historial de números de teléfono
Sistema operativo	Búsquedas
Información de perfil.	

Fuente: Adaptado de Jiménez, J. W. I. (2017). Cuestiones jurídicas en torno a la cadena de bloques («blockchain») y a los contratos inteligentes («smart contracts»).

La importancia de identificar los datos que se guardan en la cadena de bloques radica en garantizar la integridad, autenticidad y trazabilidad de la información almacenada. Al identificar claramente los datos y asociarlos con sellos de tiempo, se asegura que no hay manipulación, alteración o borrado de la información registrada. Esto es crucial para mantener la confianza en la cadena de bloques como un medio seguro y fiable para documentar transacciones y registros legales. Además, la identificación precisa de los datos permite su verificación y validación por parte de los nodos de la red, asegurando que la información compartida sea coherente y confiable.

Según Meléndez Juarbe (2008), solo se adelantó “el interés de seguridad reduciendo la probabilidad de muerte o daño físico. Por tanto, para lograr los objetivos de esta concepción pura de seguridad (mediante, por ejemplo, la identificación de amenazas a la integridad física con el uso de mecanismos de vigilancia), podría ser legítimo y hasta necesario sacrificar otros valores aparentemente opuestos como la intimidad (mediante la exposición de información personal a agencias del gobierno)” (Meléndez Juarbe, 2008).

La identificación precisa de los datos almacenados en la red es fundamental para asegurar la integridad, autenticidad y trazabilidad de la información. Esta identifica-

ción facilita la prevención de manipulaciones o alteraciones de los datos, lo que es crucial para mantener la confianza en la cadena de bloques como un medio seguro y confiable para registrar todo tipo de actividad. Sin embargo, es importante plantear la reflexión adicional sobre el equilibrio entre la seguridad y la privacidad, donde es presumible que en algunos casos se puede considerar necesario sacrificar ciertos aspectos de la privacidad en aras de garantizar el derecho a la seguridad.

Actualmente, América Latina se encuentra en un proceso de análisis y crítica social sobre el uso de la tecnología, además del desarrollo de las primeras intervenciones del Estado a nivel normativo, ya que tanto los gobiernos como la ciudadanía adoptan e implementan, cada vez más, los dispositivos de vigilancia electrónica; así, por ejemplo, Colombia, quien ha destacado como uno de los países pioneros en la región al establecer un marco ético para la Inteligencia Artificial. Esto se logró al adoptar rápidamente las recomendaciones de ética para el sector público y privado en el ámbito de la IA, presentadas por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) durante un evento en Bogotá (MINTIC, 2022).

Estas recomendaciones proporcionan directrices para las entidades públicas sobre cómo abordar la formulación y gestión de proyectos que involucren el uso de IA, incorporando prácticas internacionales relevantes. “Éste sugiere la aplicación de principios éticos como: transparencia, explicación, privacidad, control humano de las decisiones, seguridad, responsabilidad, no discriminación, inclusión, prevalencia de los derechos de niños, niñas y adolescentes y beneficio social” (Ministerio de Tecnologías de la Información y las Comunicaciones, 2022).

En Argentina, más allá de ciertas disposiciones que apuntan al estudio y desarrollo de propuestas de marcos regulatorios o a la promoción de buenas prácticas en términos de IA, la materia no ha sido específicamente regulada, razón por la cual se presentan dos caminos:

Por un lado, encontramos a quienes sostienen la necesidad de regular jurídicamente la inteligencia artificial de manera específica y que la falta de regulación podría entorpecer su desarrollo; por otro lado encontramos la postura que sostiene que puede resultar más conveniente, si es posible, encuadrar las situaciones que surjan con motivo del uso de la IA en las normas jurídicas ya existentes aplicando los principios generales vigentes del derecho contractual, de las normas sobre propiedad intelectual, responsabilidad y privacidad vigentes como las de nuestro Código Civil y Comercial, la Ley de Protección de los Datos Personales, entre otras (Repond, 2020).

Es decir que, aunque existen disposiciones que abordan el estudio y desarrollo de marcos regulatorios para la inteligencia artificial (IA) y promueven buenas prácticas en este ámbito, la materia aún no ha sido específicamente regulada. Esta situación

plantea dos enfoques: por un lado, algunos abogan por la necesidad de una regulación específica para la IA, argumentando que la falta de regulación podría obstaculizar su progreso; por otro lado, se encuentra la postura que sugiere que sería más conveniente, si es posible, abordar las situaciones relacionadas con el uso de la IA dentro del marco de las normas jurídicas existentes, aplicando los principios generales del derecho contractual, normas sobre propiedad intelectual, responsabilidad y privacidad ya vigentes en el país, como las establecidas en el Código Civil y Comercial y la Ley de Protección de los Datos Personales, entre otras. La elección entre estos enfoques depende de consideraciones tanto prácticas como filosóficas sobre el equilibrio entre la innovación tecnológica y la protección legal de los individuos y la sociedad.

II. Normatividad internacional de los dispositivos de vigilancia electrónica

II.1 Cámaras de videovigilancia

Los dispositivos de vigilancia electrónica cuentan con diferentes perspectivas dentro de la normativa internacional; así mismo, tienen desarrollo y orígenes diferentes, puesto que diferentes países han tomado cartas en el asunto, tal es el caso del Gobierno británico, que prohibió el uso de cámaras de videovigilancia de origen chino (E. F. E., 24 de noviembre 2022).

Esta decisión, sin embargo, no fue ninguna sorpresa. Según Big Brother Watch, una organización británica que lucha por las libertades civiles y la privacidad, en los espacios públicos británicos se utilizan cámaras con origen de fabricación de dos grandes empresas: Hikvision o Dahua, lo que dio pie a que un grupo de 67 parlamentarios y diputados lograran prohibir la venta y el uso de equipos de vigilancia fabricados por ambas empresas, toda vez que se detectaron las siguientes deficiencias: a) La ausencia absoluta de autorización y supervisión independientes (entendida como las “medidas de protección de extremo a extremo”); b) Las categorías de los selectores de búsqueda no se incluían en las solicitudes de órdenes judiciales; c) No constaba una autorización previa de los términos utilizados para identificar individuos; y d) El Estado no examinó otras medidas menos intrusivas antes de activar e implementar programas electrónicos de vigilancia masiva, entre otros. (STEDH [N°2] Big Brother Watch v. Reino Unido, 25 de mayo 2021).

Por otro lado, en China se han creado programas como “Xue Liang”; sin embargo, no ha sido consagrado en las políticas nacionales, por lo que el presidente Xi Jinping expresaba, que: “se debe acelerar la construcción del sistema de prevención y control en lo referente al orden público, y combatir y castigar según la ley las infracciones y los delitos [...] con miras a proteger el derecho del pueblo a preservar su integridad física, poseer bienes y mantener la dignidad personal” (<http://ar.china-embassy.gov.cn>). Lo anterior, para evidenciar la importancia de tener una mejor regulación de los

sistemas de prevención y control del orden público, así como de lograr crear políticas públicas que regulen los dispositivos de videovigilancia.

Por su parte, en la Unión Europea existe el Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y que es conocido como el Reglamento General de Protección de Datos.

Varios países han establecido disposiciones normativas específicas sobre videovigilancia para regular su uso y proteger los derechos fundamentales de las personas. Algunos de los países que han implementado regulaciones en este ámbito se mencionan a continuación.

España

La videovigilancia en España está regulada por la Ley Orgánica 4/97, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, así como por la Ley 23/1992 de Seguridad Privada y sus reglamentos de desarrollo.

Alemania

La Ley Federal de Datos de 2001 regula el uso de la videovigilancia por entidades privadas y autoridades federales, como la policía y los servicios de inteligencia. Además, cada uno de los 16 estados federados de Alemania tiene disposiciones específicas sobre videovigilancia.

Bélgica

La autoridad de protección de datos emite dictámenes relacionados con el tratamiento de imágenes a través de sistemas de vigilancia por videocámara, garantizando el cumplimiento de las normativas de protección de datos.

Holanda

La autoridad de protección de datos ha publicado directrices para la vigilancia por videocámara, especialmente en lugares públicos, con el objetivo de proteger la privacidad y la propiedad de las personas. Cada país puede tener sus propias leyes y regulaciones en este ámbito, adaptadas a su marco legal y cultural particular (Téllez, Valdés, J., 2024).

Chile

En el año 2020 se aprobó el decreto legislativo N°1218, que regula el uso de las cámaras de video vigilancia y de la Ley No. 30120, Ley de apoyo a la seguridad ciudadana con cámaras de video vigilancia públicas y privadas.

II.2 Drones

Al hablar de la regulación de los drones en el sistema anglosajón, podemos encontrar a la Autoridad de Aviación Civil (CAA), que es un organismo regulador en el Reino Unido que establece las normas y regulaciones para los drones recreativos.

Se ha regulado que, para poder ser propietario de un dron, hay que tener 18 años o más y pagar una cuota anual de 10 libras para registrarse como propietario para tener derecho a una identificación de operador.

El gobierno de China ha implementado nuevas regulaciones para controlar el uso de drones en el país. La normativa, que entró en vigor el 1 de junio de 2019, tiene como objetivo garantizar el funcionamiento seguro de los drones, así como proteger la privacidad de los ciudadanos, por lo que estos tienen que estar registrados con el gobierno, incluidos los drones utilizados con fines comerciales. Y al igual que en Reino Unido y Londres, requieren que los operadores de drones obtengan licencias, que serán emitidas por La Administración de Aviación Civil de China (CAAC). En este país podemos agregar que los operadores de drones también deben completar una capacitación en seguridad y aprobar un examen escrito para obtener la licencia. El gobierno nacional prohibirá a los extranjeros utilizar drones no chinos para recopilar y difundir información geográfica sobre el país, un delito punible con la deportación sin los permisos necesarios (Bormioli, R. 2023).

En países como España, Francia y Brasil se habla de un reglamento en el que los drones deben mantener una altura mínima de 30 metros al sobrevolar áreas donde haya aglomeraciones de personas que no hayan autorizado ser filmadas o vigiladas por estos dispositivos, así como de regulaciones en el tamaño, pues contempla que los drones entre los 250 gramos y los 25 kilogramos deben ser apropiadamente registrados en la dependencia gubernamental correspondiente. (E.F.E., 3 de mayo de 2017).

Las regulaciones también imponen restricciones en las áreas donde se pueden volar los drones. Los operadores de drones deben obtener permiso de las autoridades locales antes de volar en ciertas áreas, como aeropuertos, bases militares y ciertas áreas urbanas. Además, los drones no pueden volar a más de 120 metros y deben permanecer dentro de la línea de visión del operador.

II.3 Inteligencia Artificial

La Inteligencia Artificial se intenta regular desde un reglamento de mejoras, cambios y prevención, por lo que, debido a sus riesgos y oportunidades futuras, los legisladores, señalaron que es necesario que tanto los desarrolladores como los usuarios tengan acceso a inteligencia artificial que sea segura, que funcione de acuerdo con su diseño, que sea transparente y que se pueda identificar una entidad legal responsable detrás de ella.

Por su parte la Administración del Ciberespacio de China (CAC) publicó recientemente las Medidas Administrativas para los Servicios de Inteligencia Artificial Generativa, donde señalan que las empresas:

[...] deben garantizar que sus productos defienden los valores socialistas chinos y evitar la emisión de contenidos discriminatorios, información falsa y contenidos que dañen la privacidad personal o la propiedad intelectual. Además, las normas prohíben los contenidos que contengan violencia, obscenidad, pornografía, promoción del terrorismo, extremismo y odio étnico” (CAC, sf).

En el caso de India, ésta se ha convertido en el primer país en tomar una postura en contra de regular la inteligencia artificial. Mientras que la Unión Europea, Estados Unidos y otras naciones trabajan contrarreloj para implementar una legislación que proteja a sus usuarios, el país asiático considera que esta tecnología es un área estratégica.

Las opiniones son variadas debido al uso que le quieran dar a este novedoso instrumento, pues, como hace mención el Ministerio, la IA es un facilitador de la economía digital y el ecosistema de innovación.

III. Normatividad en México

III.1 Cámaras de videovigilancia

En México existen escasas leyes referentes *per se* en materia de videovigilancia o tecnologías y específicamente para las cámaras de videovigilancia. Generalmente se encuentran contenidas estas tecnologías, en su vertiente aplicada a seguridad, en las leyes precisamente de seguridad y éstas, incluso, se tratan de leyes relativamente nuevas en comparación con la edad de dichas tecnologías. De igual manera ocurre con reglamentos internos que regulen estos dispositivos de vigilancia; razón por la cual no es sorpresa que se identifiquen las siguientes leyes que se presentan en las Tablas 3 y 4.

Para un aproximamiento certero a la regulación de las cámaras de videovigilancia, analizamos la Ley de Videovigilancia de Yucatán (2018) y La Ley de Video Vigilancia de Aguascalientes, (2019), ambas recientes y con un objeto de estudio delimitado, señalan lo siguiente:

La Ley de Video Vigilancia de Aguascalientes, promulgada en 2019, tiene como objetivo regular el uso de sistemas de video vigilancia en el estado de Aguascalientes, México. Esta legislación establece los lineamientos para la instalación, operación y manejo de cámaras de videovigilancia tanto por parte de autoridades gubernamentales como por entidades

Tabla 3. Leyes de videovigilancia en México

Entidad federativa	Nombre	Fecha de publicación	¿Concepto de cámaras de video vigilancia?
H. Congreso del Estado de Aguascalientes	La Ley de Video Vigilancia de Aguascalientes: Ley publicada en la Primera Sección del Periódico Oficial del Estado de Aguascalientes por el Decreto Número 252.	(2019, 22 junio)	Sí
H. Congreso del Estado de Baja California Sur	Ley de Video Vigilancia del Estado de Baja California Sur, publicada en el Boletín Oficial del Gobierno del Estado de Baja California Sur por el Decreto 2688.	(2020, 20 enero).	Sí
H. Congreso del Estado de Colima	Ley que Regula la Video Vigilancia en el Estado de Colima. Ley Publicada en el Suplemento del Periódico Oficial del Estado de Colima Por el Decreto No. 618.	(2009, 22 agosto).	Sí
H. Congreso del Estado de Durango	Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango: publicada en el Periódico Oficial No. 2 por el Decreto 291.	(2012, 2 julio).	Sí
H. Congreso del Estado de Morelos	Ley de Videovigilancia para el Estado de Morelos; Periódico Oficial 5853 “Tierra y Libertad”.	(2020, 15 julio).	Sí
H. Congreso del Estado de Yucatán	Ley de Videovigilancia del Estado de Yucatán; Decreto 634/2018.	(2018, 25 julio).	Sí
H. Congreso del Estado de Zacatecas	Ley de Videovigilancia para el Estado de Zacatecas; Decreto No. 407.	(2018, 22 agosto).	Sí

Tabla 4. Leyes en materia de seguridad pública

Entidad federativa	Nombre	Fecha de publicación	¿Concepto de cámaras de video vigilancia?
H. Congreso del Estado de Baja California	Ley del Sistema Estatal de Seguridad Ciudadana de Baja California. Publicada en el Periódico Oficial No. 84, Tomo CXXVII, Sección XI.	(2020, 28 diciembre).	No
H. Congreso del Estado de México	Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México. Decreto No 224.	(2014, 14 mayo).	No, sin embargo, aborda el tema del desarrollo de proyectos, programas, entre otros, relacionados a la aplicación de tecnologías para la vigilancia.
H. Congreso del Estado de Nuevo León	Ley de Seguridad Pública para el Estado de Nuevo León. Decreto No. 279.	(2018, 22 septiembre).	No
H. Congreso del Estado de Sinaloa	Ley de Seguridad Pública del Estado de Sinaloa. Decreto No. 392.	(2019, 14 octubre).	No
H. Congreso del Estado de Sonora	Ley de Seguridad Pública del Estado de Sonora. Ley No 161.	(2011, 14 julio).	No
H. Congreso del Estado de Tabasco	Ley de Seguridad Pública del Estado de Tabasco. Decreto No. 027.	(2016, 13 septiembre).	No
H. Congreso del Estado del Estado de Chihuahua	Ley del Sistema Estatal de Seguridad Pública del Estado de Chihuahua. Decreto 1390-2013 XIV P.E.	(2013, 12 octubre).	No
H. Congreso del Estado Libre y Soberano de Hidalgo	Ley de Seguridad Pública para el Estado de Hidalgo. Decreto No 230.	(2014, 10 noviembre).	No
H. Congreso del Estado de Querétaro	Ley de Seguridad para el Estado de Querétaro.	(2016, 30 mayo).	No

Fuente: Elaboración propia a partir de la legislación estatal vigente.

privadas. Entre los aspectos que aborda la ley se encuentran: los requisitos para la instalación de sistemas de videovigilancia; normativas sobre la protección de datos personales y la privacidad de los ciudadanos; obligaciones de las autoridades y empresas en relación con el uso y almacenamiento de las imágenes captadas por las cámaras; mecanismos de supervisión y control para garantizar el cumplimiento de la ley; protocolos de actuación en caso de vulneración de la seguridad o de violaciones a los derechos de las personas. La Ley de Video Vigilancia de Aguascalientes busca regular el uso de la tecnología de videovigilancia para garantizar la seguridad ciudadana y proteger los derechos individuales de los habitantes del estado.

La Ley de Videovigilancia del Estado de Yucatán, establecida mediante el Decreto 634/2018, regula el uso de sistemas de videovigilancia en el estado de Yucatán, México. Esta legislación tiene como objetivo principal garantizar la seguridad pública y ciudadana, así como salvaguardar los derechos individuales y la privacidad de los ciudadanos. Algunos de los aspectos principales que aborda la ley son: el establecimiento de lineamientos para la instalación, operación y manejo de sistemas de videovigilancia; la definición de los requisitos que deben cumplir las autoridades y entidades públicas o privadas para implementar sistemas de videovigilancia; la protección de datos personales y privacidad de los ciudadanos, asegurando que la recolección y tratamiento de imágenes se realice de manera ética y respetuosa; designación de autoridades encargadas de supervisar el cumplimiento de la ley y de investigar posibles irregularidades en el uso de los sistemas de videovigilancia; el establecimiento de sanciones en caso de incumplimiento de las disposiciones establecidas en la ley. La Ley de Videovigilancia del Estado de Yucatán busca regular el uso de la tecnología de videovigilancia con el fin de mejorar la seguridad pública, al tiempo que garantiza el respeto de los derechos fundamentales de los ciudadanos.

En términos generales, centran su objetivo en dos aspectos: “a) garantizar que la información que recogen sirva como elemento de prueba para castigar faltas administrativas y penales; y b) evitar las posibles violaciones al derecho de privacidad” (Arteaga, 2016).

Asimismo, afirma Arteaga Botello (2016) que:

En cada una de las reglamentaciones que se analizan se subraya, por un lado, la necesidad de expandir la videovigilancia para respaldar la investigación y prosecución de hechos criminales, la sanción de faltas administrativas, y agilizar la intervención en tiempo real de la policía y la recolección de información para el diseño de políticas públicas.

Por otro lado, sin embargo, se resalta la obligación de cuidar que la videovigilancia no vulnere ciertas garantías individuales y derechos ciudadanos. En este sentido, se le define, aunque solo sea de manera implícita, como una actividad que no es exclusivamente de orden administrativo, sino que pone en juego la relación entre el aparato gubernamental y el ejercicio de la ciudadanía. (p. 66)

La idea central es que en todas las regulaciones examinadas se enfatiza la importancia de ampliar el uso de la videovigilancia para apoyar la investigación y enjuiciamiento de delitos, así como para aplicar sanciones a infracciones administrativas. Además, se destaca su utilidad para facilitar la intervención policial en tiempo real y recopilar datos para la elaboración de políticas públicas. Además, se hace hincapié en la necesidad de garantizar que la videovigilancia no menoscabe ciertas garantías individuales y derechos de los ciudadanos. De manera implícita, se reconoce que esta actividad va más allá de lo administrativo y que implica la relación entre el gobierno y la ciudadanía. La manera en que se aborda esta dualidad en la regulación de la videovigilancia difiere en cada documento aplicable en el país.

III.2 Drones

En octubre de 2019 se publicó y aprobó la Norma Oficial Mexicana 107-SCT3-2019, y entrando en vigor para noviembre del mismo año. Su objetivo se centró en establecer un marco normativo mediante disposiciones legales aplicables, a efecto de que se regularice la operación de los RPAS (aeronave pilotada a distancia), que se refiere a Vehículo aéreo no tripulado, en una forma segura, armonizada y fluida equiparable con las operaciones de las aeronaves tripuladas.

En este sentido, la Norma Oficial Mexicana NOM-107-SCT3-2019 estableció ciertos requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano. Los puntos más importantes serían los siguientes: aplica a toda persona física/moral, operadores de estado, fabricantes, armadores, importadores y comercializadores de RPAS; no aplica a los RPAS de Estado que efectúen operaciones militares destinadas o en posesión del Ejército, Armada y Fuerza Aérea Nacionales, ni a aeronaves no tripuladas clasificadas como autónomas, ni a los globos libres no tripulados; indica referencias a otras normativas como la NOM-064-SCT3-2012, que establece las especificaciones del Sistema de Gestión de Seguridad Operacional (SMS: Safety Management System) o la que la sustituya; define el objetivo de la norma como establecer el marco normativo mediante disposiciones legales aplicables para realizar la operación de los RPAS de manera segura, armonizada y fluida equiparable con las operaciones de las aeronaves tripuladas (Norma Oficial Mexicana NOM-107-SCT3-2019, 2019).

Por otra parte, también se establecen las características físicas de los RPAS, ya sea para fines recreativos, cartografía, seguridad, investigación, publicidad, o casos de emergencia. Los drones han sido clasificados en micro (2 kg o menos), pequeño (de 2.1 kg hasta 25 kg), y grande (25 kg o más) y su uso está sujeto a una serie de reglas que el propietario debe cumplir.

Se ha determinado que los drones deben operarse exclusivamente durante las horas oficiales, desde la salida hasta la puesta del sol. Durante el vuelo, la aeronave debe ser

visible en todo momento para poder monitorear su ubicación, actitud, altitud y dirección. Además, todos los drones deben ser registrados ante el gobierno, independientemente de si se utilizan para fines personales, recreativos, laborales o de investigación. Los operadores deben tener al menos 18 años y ser ciudadanos mexicanos.

Esta norma impacta las regulaciones existentes para la aviación civil en México al introducir requisitos específicos para la operación de RPAS, lo cual incluye aspectos como la autorización, registro, operación, y mantenimiento de estas aeronaves no tripuladas. La norma también establece lineamientos para garantizar la seguridad de las operaciones de RPAS y su integración segura en el espacio aéreo mexicano, lo que impacta directamente en las regulaciones y procedimientos existentes para la aviación civil en el país.

III.3 Inteligencia Artificial

A lo largo de la historia, el ser humano ha buscado imitar los elementos que observa en la naturaleza mediante creaciones artificiales, conocidas como dispositivos mecánicos. Estos dispositivos están diseñados para llevar a cabo un conjunto específico de tareas de acuerdo con una instrucción o un diseño predefinido.

En México no hay una ley general que regule el uso de inteligencia artificial; no obstante, existen iniciativas de ley como la del diputado Ignacio Loyola Vera, del Partido de Acción Nacional (PAN), quien presentó el 30 de marzo de 2023 el proyecto de “Ley para la regulación ética de la Inteligencia Artificial para los Estados Unidos Mexicanos”, la cual a la IA como “la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o razonamiento lógico” (Iniciativa de Ley para la Regulación Ética de la Inteligencia Artificial para los Estados Unidos Mexicanos, 2023). Esta propuesta de ley busca crear estructuras y apuntar hacia estándares éticos de creación, investigación y uso de la IA en el país.

Según la exposición de motivos del documento, se busca regular aspectos éticos en el uso de la inteligencia artificial como:

- 1) Establecer normas éticas para el buen uso de la inteligencia artificial y la robótica en beneficio de la sociedad mexicana, respetando los derechos humanos y la paridad entre los géneros;
- 2) Prohibir explícitamente el uso de sistemas de inteligencia artificial para la calificación social y la vigilancia masiva, garantizando el acceso de los individuos a sus registros de datos personales y su derecho a borrarlos;

- 3) Guiar la construcción de una infraestructura jurídica que garantice un desarrollo saludable de la inteligencia artificial, abordando retos como el aumento de prejuicios de género y étnicos, amenazas a la privacidad y peligros de la vigilancia masiva.

El objetivo principal de la Ley para la Regulación Ética de la Inteligencia Artificial en México es establecer los lineamientos de políticas públicas para regular éticamente el uso de la inteligencia artificial y la robótica en el territorio nacional. Además, busca fomentar la creación de normas oficiales mexicanas basadas en principios éticos para el beneficio de la sociedad mexicana, siempre respetando los derechos humanos, la paridad entre los géneros y evitando cualquier forma de discriminación por raza, origen étnico, religión, clase social o posición económica.

La implementación de esta legislación representa un paso significativo hacia la regulación ética del uso de la inteligencia artificial y la robótica en el país. Esta iniciativa busca establecer principios éticos que guíen el desarrollo de la inteligencia artificial, protegiendo los derechos humanos, fomentando la igualdad de género y evitando cualquier forma de discriminación. Además, se pretende crear un marco legal que promueva un uso responsable de esta tecnología, protegiendo la privacidad de los individuos y garantizando su acceso a la información sobre el uso de la inteligencia artificial. En un contexto donde la inteligencia artificial está cada vez más presente en nuestra vida cotidiana, es fundamental contar con regulaciones que aseguren su aplicación ética y beneficiosa para la sociedad en su conjunto.

CConclusiones

Encontrar el equilibrio entre el uso adecuado y el abuso de los recursos es una tarea sumamente desafiante. En el contexto de la seguridad, surge la pregunta sobre cuál es el límite prudente en la instalación de cámaras de vigilancia. Existe una tendencia hacia un modelo social en el que el control se ejerce de manera sutil pero profunda.

La solución jurídica se articula a través de la protección de datos, independientemente de si identifiquemos a ese “dato” como personal o no, ya que, al considerar la imagen identificable como un *dato personal*, podrían ser evitados algunos excesos, pero el problema se está transformando en una cuestión cultural. Vivimos en una sociedad de las águilas, no porque volemos alto, sino porque se persigue el dominio total del entorno, ignorando cómodamente las transgresiones que nuestros actos cometen en contra de los derechos de un tercero, derechos como el derecho a la privacidad, a la protección de datos personales, a una vida pacífica y libre de todos los tipos de violencia.

Aun cuando, en aras de que esos datos personales se empleen para poner en marcha un sistema que intenta proteger al individuo de una inseguridad mayor causada por factores que nuevamente se escapan del control del individuo.

Y es que, de cierta forma, ¿no se estaría obligando a la población a enfrentar las consecuencias de malos gobiernos, cuyas políticas en materia de seguridad pública no contribuyen a la disminución de los crímenes y violencia, como los son los estados latinos?

En la actualidad, se promueve la seguridad mediante la instalación extendida de millones de cámaras, incluso en lugares de trabajo y templos. Sin embargo, la ciudadanía a menudo no reconoce haber consentido esta generalización del control social, lo que podría conducir a una deshumanización camuflada. Es importante reconocer que el uso de cámaras debe estar regulado por normas que equilibren la disuasión del delito con la protección de los derechos individuales.

Es crucial distinguir entre “ser observado” y “ser grabado”. La grabación de imágenes puede dar lugar a la manipulación, individualización, difusión, análisis y extracción de contexto de los datos capturados. Además, el exceso de cámaras puede generar dificultades en la visualización y procesamiento de datos, y los delincuentes pueden adaptar su comportamiento para eludirlas.

Por otro lado, el avance tecnológico de las cámaras puede aumentar su capacidad para afectar negativamente los derechos individuales. Es necesario tener en cuenta estos factores al regular el uso de cámaras de vigilancia para garantizar un equilibrio adecuado entre la seguridad y la protección de la privacidad y los derechos civiles.

De igual manera, es prudente puntualizar la importancia de la educación a las autoridades competentes en prevención del delito por medio de sistemas de videovigilancia orientados a espacios públicos, con un profundo enfoque de Derechos Humanos, para evitar y erradicar el atropello de estos, al que nos sometemos voluntariamente en aras de la seguridad.

Referencias

- Arteaga Botello, N., (2009) Sociedad de la vigilancia en el sur - global. México.
- Arteaga Botello, N., (2016) Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. Espiral (Guadalajara), 23(66), 193-238. Recuperado en 08 de agosto de 2023, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193&lng=es&tlng=es.
- Agamben, G. (2007), *Qu'est-ce qu'un dispositif?* París: Éditions Payot & Rivages.
- Bormioli, R. (2023, 29 junio) China toma medidas energéticas contra el uso de drones, exige registros y prohíbe volar sobre sitios sensibles. Nova agencia. <https://www.agenzianova.com/es/news/giro-di-vite-sulluso-dei-droni-in-cina-registrazioni-obbligatorie-e-divieto-di-sorvolo-nei-siti-sensibili/>
- Castillo Agurto, C. A. (2018). Propuesta de implementación de un sistema de cámaras de vigilancia para el Instituto Superior Tecnológico Privado Abaco–Piura, 2018.

- CONVENIO SOBRE AVIACION CIVIL INTERNACIONAL (CONVENIO DE CHICAGO)
Firmado en Chicago, el 7 de diciembre de 1944. http://portales.segob.gob.mx/work/models/PoliticaMigratoria/CEM/UPM/MJ/II_30.pdf
- Díez Ripollés, J. L. & Cerezo Domínguez, A. I. (2009). La prevención de la delincuencia callejera mediante videocámaras: Regulación jurídica y eficacia. *Política criminal*, 4(7), 171-196. En <http://www.scielo.cl/pdf/politcrim/v4n7/art06.pdf>
- E.F.E. (2017, 03 mayo) Brasil prohíbe el uso de drones comerciales para sobrevolar aglomeraciones. *La Vanguardia*. <https://www.lavanguardia.com/vida/20170503/422235544232/brasil-prohibe-el-uso-de-drones-comerciales-para-sobrevolar-aglomeraciones.html>
- E, F. E. (2022, 24 noviembre) El Gobierno británico veta las cámaras de seguridad fabricadas en China. *RTVE.es Noticias*. <https://www.rtve.es/noticias/20221124/gobierno-britanico-veta-cameras-seguridad-china/2410018.shtml#:~:text=El%20Gobierno%20de%20Reino%20Unido,con%20sus%20servicios%20de%20Inteligencia>
- Espinosa Márquez A. & Martínez Meza K. & Chípuli Castillo A. & *et al.* (2021) *Vigilancia, dispositivos electrónicos y derechos humanos en México: Retos y oportunidades a enfrentar en el siglo XXI*. <https://icgde.buap.mx/pdf/vigilancia-dispositivos-electr%C3%B3nicos-y-derechos-humanos-en-m%C3%A9xico-retos-y-oportunidades>
- Galdón, Gemma (2015). Si la videovigilancia es la respuesta, ¿Cuál era la pregunta? Cámaras, seguridad y políticas urbanas. *EURE Revista Latinoamericana de Estudios Urbanos y Territoriales*, https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0250-71612015000300004
- Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*, Boulder: Westview Press.
- Giddens, A. (1985). *The Nation State and Violence*, Cambridge: Polity Press.
- H. Congreso del Estado de Aguascalientes. (2019, 22 junio). La Ley de Video Vigilancia de Aguascalientes: Ley publicada en la Primera Sección del Periódico Oficial del Estado de Aguascalientes por el Decreto Número 252.
- H. Congreso del Estado de Baja California Sur. (2020, 20 enero). Ley de Video Vigilancia del Estado de Baja California Sur. publicada en el Boletín Oficial del Gobierno del Estado de Baja California Sur por el Decreto 2688.
- H. Congreso del Estado de Baja California. (2020, 28 diciembre). Ley del Sistema Estatal de Seguridad Ciudadana de Baja California. Publicada En el Periódico Oficial No. 84, Tomo CXXVII, Sección XI.
- H. Congreso del Estado de Colima. (2009, 22 agosto). Ley que Regula la Video Vigilancia en el Estado de Colima. Ley Publicada En el Suplemento del Periódico Oficial del Estado de Colima Por el Decreto No. 618.
- H. Congreso del Estado de Durango. (2012, 2 julio). Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango: Publicado en el Periódico Oficial No. 2 por el Decreto 291.
- H. Congreso del Estado de México. (2014, 14 mayo). Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México. Decreto No 224.

- H. Congreso del Estado de Morelos. (2020, 15 julio). Ley de Videovigilancia para el Estado de Morelos: Periódico Oficial 5853 "Tierra y Libertad".
- H. Congreso del Estado de Nuevo León. (2018, 22 septiembre). Ley de Seguridad Pública para el Estado de Nuevo León. Decreto No. 279.
- H. Congreso del Estado de Sinaloa. (2019, 14 octubre). Ley de Seguridad Pública del Estado de Sinaloa: Decreto No. 392.
- H. Congreso del Estado de Sonora. (2011, 14 julio). Ley de Seguridad Pública del Estado de Sonora: Ley No 161.
- H. Congreso del Estado de Tabasco. (2016, 13 septiembre). Ley de Seguridad Pública del Estado de Tabasco: Decreto No. 027.
- H. Congreso del Estado de Yucatán. (2018, 25 julio). Ley de Videovigilancia del Estado de Yucatán: Decreto 634/2018.
- H. Congreso del Estado de Zacatecas. (2018, 22 agosto). Ley de Videovigilancia para el Estado de Zacatecas: Decreto No. 407.
- H. Congreso del Estado del Estado de Chihuahua. (2013, 12 octubre). Ley del Sistema Estatal de Seguridad Pública del Estado de Chihuahua: Decreto 1390-2013 XIV P.E.
- H. Congreso del Estado Libre y Soberano de Hidalgo. (2014, 10 noviembre). Ley de Seguridad Pública para el Estado de Hidalgo: Decreto No 230.
- H. Congreso del Estado de Querétaro. (2016, 30 mayo). Ley de Seguridad para el Estado de Querétaro.
- Hall, W. & Pesenti, J., (2017) GROWING THE ARTIFICIAL INTELLIGENCE INDUSTRY IN THE UK. <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>
- Harari, Y. N. (2018). 471 pp. 21 lecciones para el siglo XXI. Debate. [versión en español], Penguin Random House. ISBN: 978-84-9992-877-7.
- Hempel, L., & Töpfer, E. (2009). "The Surveillance Consensus: Reviewing the Politics of CCTV in Three European Countries". *European Journal of Criminology* (2), 157-177.
- Iniciativa de Ley para la Regulación Ética de la Inteligencia Artificial para los Estados Unidos Mexicanos (2023). Grupo Parlamentario del Partido Acción Nacional en la LXV Legislatura (México).
- Jiménez, J. W. I. (2017). Cuestiones jurídicas en torno a la cadena de bloques («blockchain») ya los contratos inteligentes («smart contracts»). ICADE. *Revista de la Facultad de Derecho*, (101).
- Lyon, D. (2007). *Surveillance Studies: An Overview*, UK: Polity Press.
- Lyon, D. & Zureik, E. (Eds). (1996). *Computers, surveillance and privacy*, London: University of Minnesota Press Minneapolis.
- Meléndez Juarbe (2008) p.16 El Derecho a la Intimidad, Nuevas Tecnologías y La Jurisprudencia de Hernández Denton: Lo público de lo público. Artículo. Hiram Meléndez Juarbe. <https://derecho.uprrp.edu/revistajuridica/wp-content/uploads/sites/4/2016/11/83-REV-JUR-1035.pdf>

- Ministerio de Tecnologías de la Información y las Comunicaciones. (2022, 09 marzo). Colombia adopta de forma temprana recomendaciones de ética en Inteligencia Artificial de la Unesco para la región. MINTIC.gov.co <https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208109:Colombia-adopta-de-forma-temprana-recomendaciones-de-etica-en-Inteligencia-Artificial-de-la-Unesco-para-la-region>
- Nairí Guler, T., (2022). La industria de los drones en Argentina Oportunidades para su desarrollo. Ministerio de Desarrollo Productivo, Argentina. https://www.argentina.gob.ar/sites/default/files/2021/03/33_-_drones_-_arg._productiva.pdf
- Norma Oficial Mexicana NOM-107-SCT3-2019, (2019) Que establece los requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano. https://www.dof.gob.mx/normasOficiales/8006/sct11_C/sct11_C.html
- Norma Oficial Mexicana NOM-011-SCT3-2001, (2001). Que establece las especificaciones para las publicaciones técnicas aeronáuticas. Secretaría de Comunicaciones y Transportes.
- Repond, P., (2020). Inteligencia Artificial y su marco normativo. <https://abogados.com.ar/inteligencia-artificial-y-su-marco-normativo/25187>
- Sentencia del Tribunal Europeo de Derechos Humanos (Nº2) Big Brother Watch v. Reino Unido (2021, 25 mayo). <https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-reino-unido/?lang=es>
- Short, E. & Ditton, J. (1995). Does cctv affect crime? cctv Today, 2(2), 10-12. Tecnología de Seguridad. Vigilancia electrónica. España. TRADESEGUR. 2016. Disponibilidad y acceso: <http://www.tradesegur.com/productos/vigilancia-electronica/>
- Téllez, Valdés, J. (pendiente publicación) La regulación jurídica de la videovigilancia bajo una perspectiva de derecho comparado. La Regulación Jurídica de la Videovigilancia. Jurídicas UNAM. <https://biblioteca.tec.mx/APA-7a-ed/libro>
- Tilley, N. (1993). Understanding car parks, crime and cctv: Evaluation lessons from safer cities. Crime Prevention Unit Paper 42. Londres: Home Office. En <http://goo.gl/SBGVkl>
- Zapata, E., (2018) Inteligencia Artificial en México. <https://www.gob.mx/epn/es/articulos/inteligencia-artificial-en-mexico>

Capítulo 3

Normatividad de la video vigilancia en México. Una mirada desde el derecho a la privacidad y la protección de datos personales

Regulations of video surveillance in Mexico. A perspective from the right to privacy and protection of personal data

*Karina Nohemí Martínez Meza**

*Vanessa Rodríguez Medina***

*Joaquina Aidé Viveros Montero****

Resumen

Este trabajo tiene como finalidad analizar la normatividad de la video vigilancia en México con base en los derechos humanos, en particular los derechos a la privacidad y la protección de datos personales. Lo anterior, a partir de los actores, procesos y elementos más importantes. Es

* Doctora en Ciencias de Gobierno y Política por la Benemérita Universidad Autónoma de Puebla (BUAP), Maestra en Derecho con terminal en Ciencias Penales (BUAP), Catedrática del programa de Investigadores e Investigadoras por México del Consejo Nacional de Ciencia y Tecnología (CONAHCYT) comisionada en el Instituto de Investigaciones Jurídicas de la Universidad Veracruzana. Es miembro del Sistema Nacional de Investigadoras e Investigadores (SNII) Nivel 1 por el CONAHCYT, México. kmartinez@uv.mx <https://orcid.org/0000-0003-2257-1480>.

** Licenciada en Derecho por la Universidad Veracruzana. Maestrante en Gobierno por El Colegio de Veracruz. Becaria del Diagnóstico y Modelo de Índice de Percepción de los Dispositivos de Vigilancia Electrónica en materia de Seguridad Pública en México con Enfoque de Derechos Humanos, propuesta 3265530 del Fondo Institucional para el Desarrollo Científico, Tecnológico y de Innovación, por el Consejo Nacional de Historia Ciencia y Tecnología (CONAHCYT), v78anessa@outlook.es.

*** Licenciatura en Gestión de Educación y Capacitación por la UV. Maestra en Política Pública y Gestión Educativa Estratégica por el Instituto Consorcio Clavijero, A2100067@alumno.clavijero.edu.mx. Becaria del Diagnóstico y Modelo de Índice de Percepción de los Dispositivos de Vigilancia Electrónica en materia de Seguridad Pública en México con Enfoque de Derechos Humanos, propuesta 3265530.

una investigación cualitativa que aplica el método documental a través de la normatividad que regula la implementación de la video vigilancia. Se concluye que, si bien existe una reglamentación que regula la video vigilancia, no es homogénea a nivel subnacional ni concluyente, aún menos con base en el derecho a la privacidad y protección de datos personales, lo cual podría ser motivo de una violación de derechos humanos.

Palabras clave: Video vigilancia; Seguridad; Derecho a la privacidad; Protección de datos personales.

Abstract

The purpose of this work is to analyze the regulations that regulate the implementation of video surveillance in Mexico based on human rights, in particular the rights to privacy and the protection of personal data. The above, based on the most important actors, processes and elements. It is a qualitative investigation that applies the documentary method through the regulations that regulate the implementation of video surveillance. It is concluded that although there is a regulation that regulates video surveillance, it is not homogeneous at the subnational level, nor conclusive, even less so based on the right to privacy and protection of personal data, which could be a reason for a violation of human rights.

Keywords: Video surveillance; Security; Human right to privacy; Personal data protection.

Introducción

La video vigilancia forma parte del conjunto de tecnologías, sistemas, métodos, herramientas y dispositivos electrónicos cuyas capacidades técnicas permiten la captación, obtención, monitoreo, administración, gestión y acumulación de información y datos de una población y de su vida cotidiana de manera sistemática en tiempo real (Giddens, 1987; Gandy, 1993; Lyon, 1996; 2007, 2012; Lindblom, 2002). Lo anterior, para calcular riesgos o predecir oportunidades, clasificando y perfilando sus registros de manera rutinaria (Lyon, 2001).

Igualmente, se entiende como el “conjunto de tecnologías, herramientas y dispositivos electrónicos que permiten captar imágenes fijas o en movimiento con mayor alcance, visión, resolución, que posibilitan el almacenamiento, consulta y tratamiento de los datos” (Ibarra, 2010, pp. 253-254). Los gobiernos la adoptan e implementan para fortalecer las políticas y acciones gubernamentales de seguridad; para el manejo de riesgos y emergencias; para la reducción y prevención de inseguridad y percepción del delito; y para el orden y el control social.

La implementación de la video vigilancia y su regulación están vinculadas con el derecho a la privacidad. El derecho a la vida privada es un derecho humano fundamental reconocido en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1976, así como en el art. 12 de la Declaración Universal de Derechos Humanos, que establece: “Nadie será objeto de injerencias arbitrarias en su vida

privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” (ONU, 1948).

De acuerdo con el Informe sobre el Derecho a la Intimidad en la era digital, publicado por la Organización de las Naciones Unidas, en el número 5 se reconoce que la privacidad en el ámbito digital “abarca la información que existe o puede obtenerse acerca de una persona y de su vida y de las decisiones basadas en esa información” (El Derecho a la Privacidad en la Era Digital, 3d. C., p. 3), además de que se puede ver afectada cuando la recolección y el análisis es realizado por un ser humano o un algoritmo. Igualmente, en los numerales 9 y 10 se reconoce el deber de los Estados de garantizar y respetar los derechos humanos en los casos en que ejerza su control y poder efectivo sobre la infraestructura de las comunicaciones digitales y cuyas injerencias solo podrán ser admisibles conforme a los principios generales de legalidad, necesidad y proporcionalidad (El Derecho a la Privacidad en la Era Digital, 3d. C., p. 3).

En cuanto al principio de legalidad, se deberá garantizar en la implementación de la video vigilancia el cumplimiento de la ley y la norma en vigor. El principio de necesidad remite a la adecuación entre las circunstancias, la necesidad y la respuesta. El principio de proporcionalidad exige que la video vigilancia no sea la única solución para enfrentar la inseguridad y prevenir la delincuencia; también, que exista una adecuación entre los objetivos que se deben lograr y las medidas que se deben implementar (Carta para el Uso Democrático de la Vigilancia por Vídeo, 2017).

La video vigilancia puede regularse “de modo independiente al ordenamiento que implica el tratamiento de datos personales, es decir, a través de una normatividad especial o específica –así, por ejemplo, Francia, Suecia, España– o mediante una autorización previa por una autoridad administrativa que puede estar representada por la autoridad nacional y local de protección de datos personales –como Gran Bretaña, Italia, Bélgica, Luxemburgo y Alemania–” (Téllez, 2008, p. 768).

En América Latina, la normatividad no es clara ni concluyente, ya que “prevalece el rezago en materia de regulación de la videovigilancia en comparación con otras regiones del mundo que, desde hace décadas, cuentan con un marco jurídico. Destacan Estados Unidos, Alemania, Bélgica, Dinamarca, España, Francia, Holanda, Nueva Zelanda, Reino Unido y Suecia” (Jasso, 2020, p. 20).

México no es la excepción; si bien el marco jurídico de la video vigilancia tiene como base el reconocimiento y respeto al derecho a la privacidad y la protección de datos personales, no existe claridad en la regulación de su implementación, tampoco en sus efectos sociales, “lo cual mina en ciertos aspectos la capacidad de las personas y grupos para hacerse de espacios de autonomía y control frente a procesos de clasificación y discriminación social” (Arteaga, 2016, p. 198).

Por todo lo anterior, se puede advertir que, si bien a nivel internacional existen diversas disposiciones que reglamentan la implementación y operacionalización de los dispositivos de vigilancia, así como el reconocimiento y protección del derecho a la privacidad, en México son pocos los estudios que se han realizado al respecto, además de que no existe claridad sobre su normatividad, por lo que podría existir una regulación de implementación de video vigilancia aparentemente ciega a los derechos humanos.

De ahí que, el objetivo de este trabajo es analizar el marco jurídico que regula la implementación de la video vigilancia en México con base en los derechos humanos. Lo anterior, a partir de sus actores, procesos, elementos, principios y características técnicas. Es una investigación cualitativa que aplica el método documental a través del análisis de instrumentos internacionales, leyes y reglamentos.

I. Normatividad de la video vigilancia y derechos humanos

A nivel internacional, la video vigilancia puede regularse a través de un ordenamiento que implica el tratamiento de datos personales o por medio de una ley especial o específica. De igual forma, existen principios interdependientes que deben aplicarse en el uso de estos dispositivos, así, por ejemplo el principio de legalidad, necesidad, proporcionalidad, transparencia, responsabilidad, supervisión independiente y de participación de los ciudadanos (Carta para el uso democrático de la vigilancia por video, 2017), que resultan imperantes para la video vigilancia, la cual se ha presentado como una herramienta de control social, prevención y detección de hechos delictivos y riesgo en las ciudades.

En cuanto al derecho a la privacidad, se encuentra reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, que establece: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” (Declaración Universal de Derechos Humanos, 1948). De igual manera, se reconoce en el artículo 17 del Pacto Internacional de Derechos, Civiles y Políticos de 1976. El derecho a la privacidad se ve comprometido cuando la información acerca de una persona es identificada, analizada, procesada o utilizada por un ser humano o un algoritmo.

En relación con la protección de datos personales, podemos mencionar el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter personal en Estrasburgo, 1981; los Principios actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones correspondiente al 98o período ordinario de sesiones OEA/SER. q 5 – 9 abril de 2021 cji/doc. 638/21 sesión virtual; las Recomendaciones 01/2020 sobre Medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del Nivel de Protección de los Datos Personales de la UE versión 2.0 adoptado

el 18 de junio de 2021; el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos y por el que se deroga la directiva 95/46/ce (Reglamento General de Protección de Datos); el Informe Anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: el derecho a la privacidad en la era digital a/hrc/39/29; y el Convenio para la Protección de las Personas con respecto al Tratamiento de Datos personales 108 +, 2016, entre otros.

En el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos y por el que se deroga la directiva 95/46/ce, podemos observar diversos conceptos o definiciones de datos personales; elementos, componentes y principios del tratamiento de los datos; su licitud; además de subderechos como son: a) La transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado; b) El derecho a la información y acceso a los datos personales; c) El derecho de acceso del interesado; d) El derecho de rectificación y supresión (el derecho al olvido); e) El derecho a la limitación del tratamiento; f) El derecho a la portabilidad de los datos; g) El derecho de oposición y de decisiones individuales automatizadas, incluida la elaboración de perfiles; h) El derecho a presentar una reclamación ante una autoridad de control; i) El derecho a la tutela judicial efectiva contra una autoridad de control; j) El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento; k) Representación de los interesados; y l) El derecho a indemnización y responsabilidad (Parlamento Europeo, 2016).

Igualmente, en dicho Reglamento encontramos las obligaciones del encargado del tratamiento; el registro de las actividades del tratamiento, la seguridad de los datos personales; la evaluación de impacto relativa a la protección de datos y consulta previa; la figura jurídica del delegado de protección de datos; los códigos de conducta y supervisión; la certificación; la regulación sobre las transferencias de datos personales a terceros países u organizaciones internacionales; y las autoridades de control independientes (Parlamento Europeo, 2016).

En México, la privacidad se reconoce en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), que regula la inviolabilidad de las comunicaciones privadas, de la correspondencia por escrito y de las comunicaciones realizadas por las Tecnologías de la Información, vinculada principalmente con los actos de molestia. Del mismo modo, en el artículo 6, apartado A, fracción II de la CPEUM se reconoce el derecho a la vida privada y la protección de datos personales.

En cuanto a la legislación nacional, se encuentra la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la

Federación el 05 de julio de 2020, y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 21 de diciembre de 2011.

II. Marco jurídico de la video vigilancia en México. Norma Técnica para Estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia

La video vigilancia en México en espacios públicos se enfoca principalmente en las funciones de seguridad pública y ciudadana, que tienen como finalidad salvaguardar la integridad de las personas y preservar las libertades, el orden y paz pública. Si bien no hay una ley general que regule esta materia, sí existen algunas leyes a nivel subnacional, pero de manera heterogénea.

En este sentido, Jasso (2020) señala: “A pesar de que México es uno de los países pioneros en América Latina en la implementación de la video vigilancia, no cuenta con una ley nacional, lo que sí, son marcos normativos a nivel local de video vigilancia o leyes que regulan el uso de tecnología para la seguridad pública, que no siempre abordan elementos de la video vigilancia” (Jasso, 2020).

Por otra parte, se encuentra la Norma Técnica para Estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública, aprobada por el Consejo Nacional de Seguridad Pública el 30 de agosto de 2016, la cual tiene como objetivo: “Presentar los criterios normativos y técnicos que dicten a las Entidades Federativas las características técnicas y la forma de operación de los Sistemas de Video vigilancia” (SESNSP, 2016) en 5 rubros: infraestructura; coordinación en los 3 niveles de gobierno federal, estatal y municipal; organización; operación; y evaluación (por medio de la realización de diagnósticos e implementación de evaluaciones periódicas). Se resalta la formación y capacitación de los operadores y la participación de una autoridad de control que verifique todos los principios reconocidos en esta Norma (SESNSP, 2016).

Igualmente, define al sistema de video vigilancia 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, el seguimiento a vehículos en vialidades y vigilar cruceros, entradas y salidas de las ciudades; la vigilancia en sitios de potencialidad delictiva, zonas de concurrencia turística y pasos fronterizos; la vigilancia y protección de instituciones de educación básica, nivel medio y superior; la integración de sistema privados de video vigilancia externa, entre otros” (SESNSP, 2016, pp. 4 y 135).

La Norma Técnica presenta los diversos tipos de cámaras que pueden instalarse: cámaras día/noche, cámaras de alta definición, cámaras PTZ (Pan-Tilt-Zoom), cámaras

IP y cámaras para el reconocimiento de matrículas (LPR), además de los tipos de videos, por ejemplo: video de flujo diario (recibido en tiempo real); video de incidentes (cuando el operador detecta algún incidente de acuerdo con el catálogo de incidentes de emergencia); video de evidencia (aquellos videos que se vean involucrados en una solicitud de grabación); y video de reserva en sitio (grabaciones almacenadas en la misma cámara) (SESNSP, p. 136).

Sobre la solicitud de grabaciones, señala que “debe existir un procedimiento en el cual cada solicitud se encuentre debidamente identificada y se describa detalladamente cuál es la información que se está entregando, los formatos, duraciones, llaves de encriptación entregadas y validez” (SESNSP, p. 138).

Por otro lado, la Norma Técnica reconoce el respeto a los derechos humanos y los principios de equilibrio democrático, racionalidad, evaluación, proporcionalidad, integridad y transparencia acordes a los estándares jurídicos reconocidos por el derecho internacional de derechos humanos. Sin embargo, no establece cuáles son los mecanismos de garantía y protección en su implementación.

III. Marco jurídico a nivel subnacional en México.

Leyes de video vigilancia y Leyes de seguridad pública

A nivel subnacional, se pueden encontrar legislaciones y reglamentos que regulan la video vigilancia de manera independiente y específica, además de leyes en materia de Seguridad Pública que regulan su implementación en diversos apartados, ya que el sujeto activo calificado para el uso y operación de los dispositivos de videovigilancia son los elementos de seguridad pública estatales y municipales.

En el primer caso, se encuentran las leyes de video vigilancia de las entidades federativas de Aguascalientes, Baja California Sur, Colima, Durango, Morelos, Yucatán y Zacatecas; en el segundo caso, se encuentran las leyes que regulan el uso de tecnologías de la información y comunicación en materia de seguridad pública de la Ciudad de México y el Estado de México.

Del mismo modo, las leyes de Seguridad Pública de Baja California, Coahuila, Campeche, Chiapas, Chihuahua, Ciudad de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Oaxaca, Puebla, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Sonora, Tlaxcala, Tabasco, Tamaulipas, Veracruz, donde solo hacen mención de estos dispositivos y de los centros de control, pero no son concluyentes sobre los procedimientos y medios de impugnación, aún menos en materia de derechos humanos.

También se pueden encontrar Reglamentos de Video vigilancia a nivel municipal, como el caso de Guadalajara, cuya naturaleza es similar a las leyes de otras entidades

federativas que regulan el objeto de estudio, aunque en el estado de Jalisco no existe una ley de video vigilancia.

En los siguientes apartados se describirán los diversos procesos, actores, elementos de la normatividad que regula la video vigilancia a través de las siguientes categorías: concepto de video vigilancia; principios; grabaciones y almacenamiento; instalación e infraestructura; participación ciudadana; Comité de Video vigilancia; medios de defensa; derecho a la privacidad y protección de datos personales.

III.1 Concepto

En las legislaciones se puede encontrar una definición clara y precisa de la video vigilancia, además de otros conceptos vinculados con su implementación: sistema de videovigilancia; Circuitos Cerrados de Televisión (CCTV); videocámara; sistemas de video vigilancia urbana; sistemas y equipos tecnológicos complementarios; sistema tecnológico de video vigilancia; sistema único de monitoreo y operación de equipos tecnológicos de vigilancia.¹

Igualmente, establecen los sujetos o autoridades que pueden implementarla, así, por ejemplo, en la Ley de Video Vigilancia de Aguascalientes, en el artículo 3 Fracción XXII, se establece que “la captación de imágenes con o sin sonido la puede realizar no solo la seguridad pública del estado o municipio (por conducto del Centro de Control, Comando, Comunicación y Cómputo C4), sino, también, por concesión, la seguridad privada” (H. Congreso del Estado de Aguascalientes, 2009), que incluye a las “personas físicas o morales, las empresas de seguridad privada y los establecimientos mercantiles” (H. Congreso del Estado de Baja California Sur, 2020).

Por otro lado, se puede identificar que en el concepto se incorporan las finalidades del uso de la video vigilancia, como son la investigación de delitos, la documentación de faltas administrativas relacionadas con la seguridad pública, la prevención de los delitos, la solución de conflictos y el fortalecimiento de la responsabilidad cívica y la solidaridad comunitaria.

Se resalta el Estado de México, puesto que no cuenta con una definición de video vigilancia, pero establece que “tiene por objeto regular el uso, localización y operación de videocámaras para grabar o captar imágenes con o sin sonido, en lugares públicos

¹ El sistema de videovigilancia forma parte de un conjunto de dispositivos y sistemas tecnológicos (sistema de gestión de la seguridad de información, sistema de administración de base de datos y sistema de despacho o atención asistido por un sistema de cómputo) que se implementan en los Centros de Control, Comando, Cómputo y Comunicaciones (C4), donde se proporcionan servicios de seguridad pública, atención y despacho de emergencias, y las autoridades, incluyendo la policía, pueden tomar decisiones y ejecutar diversas acciones ante situaciones de riesgo.

o en lugares privados con acceso al público, en materia de seguridad pública”, según el artículo 20 en la Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública (H. Congreso del Estado de México, 2014).

Tabla 1. Concepto de Video Vigilancia en las Entidades Federativas

Entidad Federativa	Concepto de Video Vigilancia
Aguascalientes	“La captación de imágenes con o sin sonido en lugares públicos o privados con acceso al público, por los cuerpos de seguridad pública estatal o municipales o de seguridad privada, para la investigación de delitos y la documentación de faltas administrativas relacionadas con la seguridad pública, que realicen en términos de la presente Ley” (Ley de Video Vigilancia de Aguascalientes, 2009).
Baja California Sur	“Captación o grabación de imágenes con o sin sonido por las instituciones policiales, de procuración de justicia, prestadores de servicios de seguridad privada, establecimientos mercantiles y cualquier persona física o moral que se realicen en términos de la presente ley” (Ley de Video Vigilancia del Estado de Baja California Sur, 2020).
Colima	Sistema de video vigilancia constituido por cámaras digitales y análogas, y de un sistema de grabación y visualización (Ley que Regula la Video Vigilancia en el Estado de Colima, 2009).
Durango	“Captación de imágenes con o sin sonido por la seguridad pública estatal o municipal, por la seguridad privada y de particulares” (Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango, 2012).
Estado de México	“Captación y grabación por medio de cámaras, en espacios públicos cuya atribución es exclusiva de la seguridad pública estatal y municipal y en espacios privado con acceso al público” (Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México, 2014);
Ciudad de México	No aplica.
Morelos	“Captación o grabación de imágenes con o sin sonido por instituciones de seguridad pública, privada o por persona física y moral” (Ley de Videovigilancia para el Estado de Morelos, 2020).
Yucatán	“Captación o grabación de imágenes y, en su caso, de sonidos en espacios públicos o en lugares privados con acceso al público, por medio de cámaras, fijas o móviles, y los sistemas y equipos tecnológicos complementarios, que tiene por objeto contribuir al desempeño de la función de seguridad pública, prevenir la

	comisión de hechos posiblemente delictivos o de infracciones administrativas, y facilitar su investigación, así como la reacción oportuna ante estos o ante emergencias o desastres de origen natural o humano” (Ley de Videovigilancia del Estado de Yucatán, 2018).
Zacatecas	“Captación, grabación, de imágenes con o sin sonido realizado por la seguridad pública y privada” (Ley de Videovigilancia para el Estado de Zacatecas, 2018).

Fuente: Elaboración propia con base en: la Ley de Video Vigilancia de Aguascalientes (2009); Ley de Video Vigilancia del Estado de Baja California Sur (2020); Ley que Regula la Video Vigilancia en el Estado de Colima (2009); Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango (2012); Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México (2014); Ley que Regula el Uso de Tecnología para la Seguridad Pública en el Distrito Federal (2008); Ley de Videovigilancia para el Estado de Morelos (2020); Ley de Videovigilancia del Estado de Yucatán (2018); Ley de Videovigilancia para el Estado de Zacatecas (2018).

III.2 Principios

La implementación de la video vigilancia debe obligatoriamente apegarse a principios que permitan garantizar la privacidad y la protección de los datos personales, como son la proporcionalidad, idoneidad, intervención mínima, riesgo razonable, peligro concreto, no afectación a la intimidad personal y legalidad.

- 1) La *proporcionalidad*, que se refiere a la “necesidad de utilizar las cámaras de manera adecuada y equilibrada en relación con una situación dada. Esto incluye dos aspectos principales: la idoneidad al propósito, donde el registro debe ser relevante para la seguridad pública, y la intervención mínima, cuyo objetivo es lograr un equilibrio entre el propósito del registro y el respeto por la privacidad y otros derechos fundamentales” (H. Congreso del Estado de Aguascalientes, 2019).
- 2) El *riesgo razonable*, que se refiere al “uso de cámaras fijas, relacionado con la capacidad de prever y evitar daños o impactos en la seguridad pública. Esto significa que la instalación de cámaras debe basarse en una evaluación objetiva de los riesgos razonables de su uso” (H. Congreso del Estado de Aguascalientes, 2019).
- 3) El *Peligro concreto*, “se aplica a cámaras en movimiento y se refiere a un evento inminente, cierto o imprevisto que puede causar daño o afectar la seguridad pública” (H. Congreso del Estado de Aguascalientes, 2019).
- 4) La *No afectación a la intimidad personal* establece que “las autoridades no podrán utilizar videocámaras para grabar o captar imágenes y sonidos al interior de viviendas u otros bienes inmuebles privados, salvo consentimiento del propietario o de quien tenga la posesión, u orden judicial para ello, ni en cualquier otro sitio,

cuando tengan como propósito obtener información personal o familiar o cuando se afecte de forma directa y grave la intimidad de las personas” (H. Congreso del Estado de Baja California Sur, 2020).

- 5) Legalidad, “por virtud del cual la actuación de las Instituciones de Seguridad Pública se hará conforme a las facultades que las leyes, reglamentos y demás disposiciones jurídicas atribuyen a su respectivo empleo, cargo o comisión, respetándose los derechos humanos en todo momento” (H. Congreso del Estado de Baja California Sur, 2020).

Estos principios enfatizan la importancia del uso adecuado y proporcionado de la cámara de video en cada situación, teniendo en cuenta la facilidad de uso y la mínima interferencia; asimismo, destacan la necesidad de evaluar adecuadamente los riesgos antes de instalar cámaras fijas y utilizar cámaras móviles en situaciones especiales donde el peligro es inminente. En la Tabla 2 se presentan los principios que regulan cada legislación de video vigilancia en México.

Tabla 2. Principios aplicables a la video vigilancia de las entidades federativas

Entidad Federativa	Principios de la Video Vigilancia
Aguascalientes	Proporcionalidad, idoneidad, intervención mínima, riesgo razonable y peligro concreto.
Baja California Sur	Proporcionalidad, idoneidad, intervención mínima, riesgo razonable, peligro concreto, no afectación a la intimidad personal y legalidad.
Colima	Proporcionalidad, idoneidad, intervención mínima.
Durango	Proporcionalidad, idoneidad, intervención mínima y riesgo razonable.
Estado de México	No aplica.
Ciudad de México	No aplica.
Morelos	Legalidad, proporcionalidad, idoneidad, intervención mínima, riesgo razonable y peligro concreto, no afectación a la intimidad.
Yucatán	Proporcionalidad, idoneidad, intervención mínima, riesgo razonable y no afectación de la intimidad personal.
Zacatecas	Proporcionalidad, idoneidad, intervención mínima.

Fuente: Elaboración propia con base en la legislación de video vigilancia en México vigente.

III.3 Grabaciones y almacenamiento

Se pueden encontrar diversos actores o autoridades que tienen las atribuciones y competencias para realizar la grabación y el almacenamiento:

- a) La Secretaría de Seguridad Pública, a través de la subsecretaría en materia policial, quien “podrá monitorear a la video vigilancia y prestar servicios de estudio y análisis de riesgo y protección de bienes a entidades públicas, de personas físicas y morales que generen empleos y recursos económicos para el Estado” (H. Congreso del Estado del Estado de Chihuahua, 2013);
- b) La Comisión Técnica de Video Vigilancia, que será la encargada de recabar y resguardar las grabaciones realizadas por las instituciones públicas estatales y municipales, y de empresas privadas o de particulares (H. Congreso del Estado de Baja California Sur, 2014);
- c) Los Centros de Control, Comando, Comunicaciones, Cómputo, Coordinación C5, que serán los encargados de resguardar la información por mecanismos de video vigilancia (H. Congreso del Estado Libre y Soberano de Hidalgo, 2014);
- d) El Centro de Información y Análisis para la Seguridad, que realizará funciones de comando operación, monitoreo, control y almacenamiento (H. Congreso del Estado de Querétaro, 2016).

En las legislaciones de video vigilancia y las de seguridad pública, también se puede encontrar el procedimiento de grabación y almacenamiento, el cual se describe a continuación:

- a) “Cualquier autoridad o prestador de servicio de seguridad pública que capte o grabe y que haya detectado posibles delitos o faltas administrativas, deberá realizar un informe diario sobre las cámaras y sistemas. Igualmente, un informe semanal sobre los eventos detectados, así como del tratamiento y custodia de las grabaciones; y un informe mensual sobre la destrucción de grabaciones” (H. Congreso del Estado de Aguascalientes, 2019);
- b) “En cuanto a las grabaciones que no hayan captado hechos delictivos, o de riesgo, deberán almacenarse en los respaldos a cargo del responsable del sistema” (H. Congreso del Estado de Aguascalientes, 2019);
- c) “El manejo de grabaciones deberá seguir una secuencia de resguardo en un lugar seguro y protegido, que evite su contaminación para garantizar su autenticidad” (H. Congreso del Estado de Aguascalientes, 2019),
- d) “Las grabaciones serán almacenadas por instituciones públicas en sus tres niveles de organización, de empresas de seguridad privada y particulares hasta considerarse viable su destrucción” (H. Congreso del Estado de Colima, 2009),
- e) “La información que se obtiene por videocámaras deberá integrarse al Sistema de Información Estatal de Seguridad Pública y deberá mantenerse actualizada y

sistematizada a través de los registros² y bases de datos en materia de seguridad pública” (H. Congreso del Estado de Tabasco, 2016),

- f) “La conservación de la información deberá ser por estandarización y homologación de instituciones de seguridad pública y empresas de seguridad privada”. (H. Congreso del Estado de Yucatán, 2018),
- g) “La duración de almacenamiento será de 30 días y cuando se hayan captado información sujeta a proceso se enviarán a la autoridad competente” (H. Congreso del Estado de Durango, 2020).

En la Tabla 3 se señalan los elementos más importantes de las grabaciones y sus almacenamientos.

Tabla 3. Autoridades encargadas de realizar la grabación y almacenamiento de información captada por video vigilancia en las entidades federativas

Entidad Federativa	Grabaciones y Almacenamiento
Aguascalientes	“La seguridad pública y privada deben resguardar las grabaciones para evitar su contaminación, deberán presentar al Comité informes diarios de posibles hechos delictivos, faltas administrativas; informe mensual de eventos y tratamiento; informe mensual de destrucción de grabaciones” (Ley de Video Vigilancia de Aguascalientes, 2009).
Baja California	“El C4, es la institución facultada para establecer las bases sobre el funcionamiento de la videovigilancia y la información obtenida por videograbaciones” (Ley del Sistema Estatal de Seguridad Ciudadana de Baja California, 2020).
Baja California Sur	La Secretaria de Seguridad Pública del Estado será la encargada de desempeñar la función pública de videovigilancia” (Ley de Video Vigilancia del Estado de Baja California Sur, 2020).
Chihuahua	“La Secretaría de Seguridad Pública, a través de la subsecretaría y del despliegue de la función policial monitorea la video vigilancia” (Ley del Sistema Estatal de Seguridad Pública del Estado de Chihuahua, 2013).

² En relación con los registros, la Ley de Video Vigilancia del Estado de Baja California Sur presenta la figura jurídica del Registro Estatal de Video Vigilancia, que tiene por objeto “integrar información sobre las cámaras fijas y móviles de videovigilancia, así como los sistemas y equipos tecnológicos complementarios que, para el adecuado ejercicio de sus funciones, utilicen las instituciones de seguridad pública, las empresas de seguridad privada, los establecimientos mercantiles en el Estado; así como personas físicas o morales que celebren convenio de colaboración respectivo” (H. Congreso del Estado de Baja California Sur, 2020).

Entidad Federativa	Grabaciones y Almacenamiento
Colima	“Las grabaciones serán guardadas y destruidas hasta que se considere pertinente por las instituciones públicas de los tres órdenes de gobierno, empresas privadas y particulares, a menos que hayan captado faltas administrativas graves o hechos delictivos” (Ley que Regula la Video Vigilancia en el Estado de Colima, 2009).
Durango	“Las grabaciones que se realicen por instituciones públicas Estatal y Municipal, así como por empresas privadas y particulares, almacenará por 30 días la información” (Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango, 2012).
Hidalgo	“El C5, resguardará los Registros de información de los mecanismos de videovigilancia” (Ley de Seguridad Pública para el Estado de Hidalgo, 2014).
Estado de México	“El C5, resguardará y manejará la información obtenida con equipos y sistemas tecnológico” (Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México, 2014).
Morelos	“Las grabaciones realizadas por instituciones públicas Estatal y Municipal, empresas privadas o personas físicas y morales, serán recabadas por la Comisión Estatal de Seguridad Pública” (Ley de Videovigilancia para el Estado de Morelos, 2020).
Nuevo León	“Coordinación entre instituciones privadas que brinden servicios de video vigilancia y la administración de la información es facultad exclusiva de los cuerpos policiales” (Ley de Seguridad Pública para el Estado de Nuevo León, 2018).
Querétaro	“El Centro de Información y Análisis para la Seguridad de Querétaro se encargará de controlar el sistema estatal de video vigilancia” (Ley de Seguridad para el Estado de Querétaro, 2016).
Sinaloa	“Corresponde a la institución policial para la operación de seguridad pública la administración de información” (Ley de Seguridad Pública del Estado de Sinaloa, 2019).
Sonora	“El C4, prestará el servicio del Sistema Único de Monitoreo y Operación de Equipos Tecnológicos de Vigilancia. Y deberá existir una coordinación entre las dependencias y entidades federales, estatales y municipales competentes” (Ley de Seguridad Pública del Estado de Sonora, 2011).
Tabasco	“La información obtenida por video cámaras por instituciones policiales y servicios de seguridad privada se integrarán al Sistema de Información Estatal de Seguridad Pública” (Ley de Seguridad Pública del Estado de Tabasco, 2016).

Entidad Federativa	Grabaciones y Almacenamiento
Yucatán	“La información integrada, sistematizada y resguardada por una base de datos, se debe dar por la homologación de instituciones de seguridad pública y empresas de seguridad privada” (Ley de Videovigilancia del Estado de Yucatán, 2018).
Zacatecas	“Las grabaciones captadas por instituciones públicas y empresas de seguridad privada o particulares serán almacenadas por la Secretaría de Seguridad Pública de del Gobierno del Estado” (Ley de Videovigilancia para el Estado de Zacatecas, 2018).

Fuente: Elaboración propia con base en la legislación de Video Vigilancia y la legislación en materia de Seguridad Pública vigente.

III.4 Instalación e infraestructura

En la legislación, se puede encontrar un procedimiento para la instalación e infraestructura de la video vigilancia que se describe a continuación:

- a) La adquisición de tecnología de video vigilancia deberá hacerse por medio de un dictamen técnico, previo diagnóstico de factibilidad;
- b) Se realizarán propuestas sobre la instalación, operación y retiro de cámaras fijas y móviles de videovigilancia, por ejemplo, a través de la Secretaría General de Gobierno;
- c) La instalación de videocámaras que realice la autoridad Estatal o Municipal, Organismo Descentralizado, Desconcentrado, Autónomo, deberá ser comunicada al Comité de Video Vigilancia o a la Comisión de Video Vigilancia;
- d) El Comité o la Comisión de la Video Vigilancia llevará un registro de las videocámaras instaladas y supervisará el uso adecuado de las grabaciones obtenidas;
- e) Se deberá realizar una supervisión y validación de los sistemas de video vigilancia;
- f) La instalación, administración y vigilancia del funcionamiento de las cámaras de videovigilancia y otros equipos tecnológicos complementarios estarán cargo de la Secretaría de Seguridad Pública;
- g) Los equipos de videovigilancia instalados por la Secretaría 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 han dejado de cumplir sus objetivos o se determine el deterioro físico.

En la Tabla 4, se señalan los aspectos más apremiantes de la instalación e infraestructura.

Tabla 4. Instalación de Videocámaras por la Autoridad en las Entidades Federativas con base en las legislaciones de video vigilancia

Entidad Federativa	Instalación de Videocámaras por la Autoridad	Registro y Supervisión	Cámaras en Espacios Públicos
Aguascalientes	Comunicación con el Comité de Video Vigilancia.	Sí	Sí
Baja California	Comunicación con la Red Estatal de Comunicaciones de Seguridad	Sí	Sí (instaladas por autoridades estatales y municipales)
Baja California Sur	Registro por la Comisión de Video Vigilancia.	No	Sí
Colima	Autorización de la Comisión Técnica	Sí	Sí
Durango	Registro en la Comisión Estatal de Seguridad	Sí	Sí
Morelos	Realización de dictámenes de la Comisión Estatal de Seguridad.	Sí	Sí
Yucatán	Propuestas de la secretaria general de Seguridad.	Sí	Sí
Zacatecas	Registro ante la Secretaría de Seguridad Pública.	No especificado	No especificado

Fuente: Elaboración propia con base en las leyes de videovigilancia en México vigentes.

Las autoridades deberán garantizar el adecuado registro, procesamiento, almacenamiento y destino de las imágenes y sonidos que obtengan en el empleo de tales sistemas. Además, deberán operar, procesar, analizar, reservar, controlar, custodiar y manipular los equipos tecnológicos con un amplio sentido ético y de responsabilidad, ya que, por tratarse de datos sensibles, son protegidos por las leyes de transparencia y de protección de datos personales en posesión de sujetos obligados, en especial aquella información que es clasificada como reservada o confidencial; las sanciones administrativas y penales forman parte de la reglamentación de los sistemas de videovigilancia.

III.5 Participación ciudadana

En el caso de la participación ciudadana, se puede observar que el marco jurídico no es claro ni concluyente, ya que son pocas las legislaciones que regulan los mecanismos de participación como política pública. Algunas de ellas son las legislaciones de Video Vigilancia de Baja California Sur, Colima y Yucatán, donde se establece que la ciudadanía puede presentar propuestas y sugerencias sobre la implementación de video vigilancia, con voz, pero sin voto.

Tabla 5. Participación ciudadana en aspectos relacionados con la video vigilancia en las entidades federativas

Entidad Federativa	Participación de la Comunidad y Propuesta Ciudadana
Baja California Sur	“Las instituciones públicas, las asociaciones civiles, los particulares o la comunidad en general podrán proponer a la Secretaría de Seguridad Pública, la instalación de cámaras fijas y móviles de videovigilancia, para reforzar las condiciones de seguridad de determinado espacio público de su competencia” (Ley de Video Vigilancia del Estado de Baja California Sur, 2020).
Colima	“La comunidad y la ciudadanía pueden participar a través del Presidente del Comité Estatal de Consulta y Participación, presentando inquietudes, sugerencias y propuestas relacionadas con la video vigilancia, con voz, pero sin voto, en el Consejo Estatal de Seguridad Pública” (Ley que Regula la Video Vigilancia en el Estado de Colima, 2009).
Yucatán	“Las instituciones públicas, asociaciones civiles, particulares y la comunidad en general tienen la posibilidad de proponer al Gobierno del estado o a los ayuntamientos la instalación de cámaras fijas y móviles de videovigilancia, para reforzar la seguridad de determinados espacios públicos. Estas propuestas deben ser presentadas por escrito, justificando plenamente los motivos y considerando la disponibilidad presupuestal, la capacidad técnica y lo establecido en la ley” (Artículo 7 de la Ley de Videovigilancia del Estado de Yucatán, 2018).

Fuente: Elaboración propia con base en la Ley de Videovigilancia del Estado de Yucatán y Ley que Regula la Video Vigilancia en el Estado de Colima.

La ciudadanía se debe involucrar en el diseño de este tipo de políticas públicas y estrategias de seguridad pública, ya que son los que, de primera mano, pueden beneficiarse del éxito de las mismas o salir perjudicados ante el fracaso en su implementación. La participación ciudadana empieza desde las quejas, denuncias y sugerencias hasta la integración en comités consultivos de seguridad y protección civil.

III.6 Comité de video vigilancia

De acuerdo con el artículo 7, Fracciones de I, II, III, IV y V de la ley de Video Vigilancia del Estado de Aguascalientes, el Comité de Video Vigilancia es “un órgano autónomo de la Secretaría de Seguridad Pública, y lo conforman un representante del Secretario de Seguridad Pública; del Poder Legislativo, el Procurador de Justicia, de la Comisión Estatal de Derechos Humanos, de la Secretaría de seguridad pública o de los ayuntamientos con el Centro de Control Comando Comunicaciones y Cómputo C4” (H. Congreso del Estado de Aguascalientes, 2009).

En cuanto a sus facultades, señala las siguientes: podrán “realizar la instalación de videocámaras fijas; implementar la conexión de éstas de prestadores de servicio de seguridad privada a cuerpos de seguridad pública; resolver las solicitudes vinculadas a la protección de datos personales; certificar el contenido de una videograbación, así como su destino y custodia temporal; informar de uso indebido al superior jerárquico; inspeccionar los cuerpos de seguridad pública y privada y la destrucción de las grabaciones” (H. Congreso del Estado de Aguascalientes, 2019).

Es importante señalar que solo las leyes de video vigilancia de Aguascalientes, Baja California Sur, Colima, Durango y Morelos contemplan al Comité y Comisión de video vigilancia o afines. En la Tabla 6 se muestran los aspectos más importantes.

Tabla 6. Comités de video vigilancia

Entidad Federativa	Comité/ Comisión	Integración	Facultades
Aguascalientes	Comité de Video Vigilancia	Con voz y voto: • Representante del Secretario de Seguridad Pública del Estado; • Poder Legislativo; • Procurador General de Justicia del Estado; • Comisión Estatal de Derechos Humanos. Con voz, pero sin voto: • Secretarías de Seguridad Pública o similares de ayuntamientos con C4.	• Registro y retiro de videocámaras. • Destrucción de grabaciones. • Autorización de conexiones de videocámaras. • Resolución sobre solicitudes de cancelación, oposición o rectificación de datos personales. • Conocimiento y remisión de infracciones. • Certificación de contenido de videograbaciones. • Custodia y destino temporal de videograbaciones. • Inspecciones y visitas de supervisión.
Baja California Sur	Comisión Técnica de Videovigilancia	• El Secretario de Seguridad Pública del Estado, quien será su Presidente Ejecutivo.	• Coadyuvar con la Secretaría en el registro de sistemas tecnológicos de video vigilancia. • Realizar el seguimiento y destino de las imágenes y audio que se

Entidad Federativa	Comité/ Comisión	Integración	Facultades
		• Un Secretario Técnico, que será nombrado por el Secretario de Seguridad Pública. • El Procurador General de Justicia en el Estado. • El Presidente y/o la Presidenta de la Comisión de Seguridad Pública en el H. Congreso del Estado. • El Director del C4 Estatal. • Un representante de la Asociación de Empresas de Seguridad Privada. • El Presidente y/o la Presidenta del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California Sur; • Un representante de la Sociedad Civil Organizada, que represente el interés de la mayoría de las Cámaras, Colegios y Asociaciones empresariales de cada municipio, que tenga probada dedicación y conocimiento sobre temas de tecnología e historial en la participación en temas de seguridad.	obtenga, así como de la supervisión del uso adecuado de ésta. • Coadyuvar con la Secretaría para la elaboración y expedición normas reglamentarias y manuales operativos. • Vigilar que la Secretaría realice su función con apego a la Ley. • Analizar, determinar y en su caso solicitar a la Secretaría el retiro de sistemas tecnológicos de video vigilancia cuando, a su juicio, se vulneren derechos fundamentales de las personas.
Colima	Comisión Técnica de Video Vigilancia	Con voz y voto: • Secretario Ejecutivo del Consejo Estatal de Seguridad Pública (Presidente); • Procurador General de Justicia del Estado; • Director General de la Policía Estatal Preventiva. Con voz, pero sin voto: • Presidente del Comité Estatal de Consulta y Participación de la Comunidad.	• Autorización de instalación de videocámaras. • Emisión de resoluciones sobre solicitudes de información. • Procesamiento de información. • Elaboración de normas reglamentarias. • Destrucción de grabaciones que vulneren derechos. • Recabar las grabaciones solicitadas por autoridad competente.
Durango	Comisión Estatal de Seguridad Pública CES	• Secretario de Seguridad Pública (Presidente). • Director Del NIT (Secretario Técnico).	• Registro de instalación de sistemas de video vigilancia. • Emisión de resoluciones. • Procesamiento de información.

Entidad Federativa	Comité/ Comisión	Integración	Facultades
		• Secretario General de Gobierno. • General Fiscal Del Estado. • Comisario General de la Policía Estatal. • Titular de la Comisión Estatal de Derechos Humanos. • Representante de municipios con sistema de video vigilancia. • Representante del sector empresarial (a invitación del Presidente). • Titular del Consejo Estatal Ciudadano.	• Elaboración de normas reglamentarias. • Destrucción de grabaciones que vulneren derechos. • Recabar las grabaciones solicitadas por autoridad competente.
Morelos	Comisión Estatal de Seguridad Pública CES	Integrantes no especificados.	• Control del sistema estatal de videovigilancia. • Dotación de recursos al C5. • Manejo de Información Obtenida de Sistemas de Videovigilancia.

Fuente: Elaboración propia con base en: la Ley de Video Vigilancia de Aguascalientes (2009); Ley de Video Vigilancia del Estado de Baja California Sur (2020); Ley que Regula la Video Vigilancia en el Estado de Colima (2009); Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango (2012); Ley de Videovigilancia para el Estado de Morelos (2020).

III.7 Medios de defensa

De acuerdo con el artículo 42 de la Ley de Video Vigilancia del Estado de Aguascalientes, existen diversos Medios de Defensa:

- a) El Juicio de Nulidad para la Impugnación de las resoluciones de la Ley de Video Vigilancia contemplado en la Ley del Procedimiento Contencioso Administrativo del Estado de Aguascalientes (H. Congreso del Estado de Aguascalientes, 2009);
- b) El recurso de inconformidad para el acceso, rectificación, cancelación y oposición de datos personales, que se puede presentar directamente o después de una revisión, de acuerdo con la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes (H. Congreso del Estado de Aguascalientes, 2009).

Por su parte, en los artículos 26, 27 y 28 de la Ley de Video Vigilancia del Estado de Colima se establece el recurso de revisión y de inconformidad según la Ley del Procedimiento Administrativo del Estado de Colima y sus Municipios para suspender

la ejecución de sanciones pecuniarias si se solicita y no causa perjuicio al interés general. Igualmente, establece que el Tribunal de lo Contencioso Administrativo será la instancia competente para resolver los recursos presentados contra las resoluciones que niegan las peticiones de los particulares (H. Congreso del Estado de Colima, 2009)

El artículo 17 de la Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango señala que se pueden utilizar los medios de defensa establecidos en la Ley de Justicia Fiscal y Administrativa del Estado para la defensa jurídica de los particulares, siguiendo los procedimientos contemplados en dicha ley (H. Congreso del Estado de Durango, 2012).

Mientras que, en Morelos, es posible impugnar las resoluciones de la Ley de Video Vigilancia mediante el juicio de nulidad previsto en la Ley de Justicia Administrativa del Estado. Y para ejercer los derechos de acceso, rectificación, cancelación y oposición en el manejo de datos personales se podrá recurrir al proceso de revisión según la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado, de acuerdo con el artículo 64 de la Ley de Video Vigilancia de Morelos (H. Congreso del Estado de Morelos, 2020).

Tabla 7. Medios de Defensa en la video vigilancia en las entidades federativas

Estado	Medios de Defensa
Aguascalientes	- Juicio de nulidad en la Ley del Procedimiento Contencioso Administrativo del Estado de Aguascalientes. - Recurso de inconformidad en la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes
Colima	- Recurso de revisión y de inconformidad en la Ley del Procedimiento Administrativo. - Tribunal de lo Contencioso Administrativo.
Durango	- Medios de defensa en la Ley de Justicia Fiscal y Administrativa del Estado de Durango.
Morelos	- Juicio de nulidad en la Ley de Justicia Administrativa del Estado de Morelos. - Recurso de revisión en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Morelos.
Zacatecas	- Juicio de nulidad en la Ley de Justicia Administrativa del Estado de Zacatecas. - Recurso de revisión en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Zacatecas.

Fuente: Elaboración propia con base en la Ley de Video Vigilancia de Aguascalientes (2009); Ley que Regula la Video Vigilancia en el Estado de Colima (2009); Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango (2012); Ley de Videovigilancia para el Estado de Morelos (2020); y la Ley de Videovigilancia para el Estado de Zacatecas (2028).

La Ley de Video Vigilancia del Estado de Zacatecas señala en el artículo 39 que “cabe la posibilidad de impugnar las resoluciones de la Ley de Video Vigilancia mediante el juicio de nulidad establecido en la Ley de Justicia Administrativa del Estado” (H. Congreso del Estado de Zacatecas, 2018). Se señalan los aspectos sustanciales de este apartado en la Tabla 7.

III.8 Derecho a la privacidad

En cuanto a esta categoría, solo se reconoce el derecho a la privacidad, pero no se establece la manera en que se garantizará, es decir, la materialización del mismo en cuanto a la aplicación de la videovigilancia. Se resalta el artículo 48 de la Ley de Video Vigilancia del Estado de Baja California Sur, que establece “lo relativo al tratamiento de las videograbaciones captadas mediante cámaras fijas o móviles de videovigilancia, correspondiente a niños, niñas y adolescentes, privilegiando su interés superior” (H. Congreso del Estado de Baja California Sur, 2020). En la Tabla 8 se señalan diversos aspectos vinculados con el derecho a la privacidad e intimidad.

Tabla 8. Aspectos vinculados al derecho a la privacidad en la video vigilancia en las entidades federativas

Leyes de Video Vigilancia	Artículos	Derecho a la privacidad
Aguascalientes	Art. 6 inciso b	“Principio de proporcionalidad en su carácter intervención mínima, de la que existe una ponderación entre la finalidad pretendida y la afectación al derecho a la intimidad, honor y propia imagen” (Ley de Video Vigilancia de Aguascalientes, 2009).
Baja California Sur	Art. 4	“Obligación de Estado de garantizar y velar por la integridad de las personas, respetando y salvaguardando sus derechos humanos en las fases de grabación, respaldo y uso de las imágenes y sonidos obtenidos, conjunta o separadamente, por las cámaras y sistemas de videovigilancia de las Instituciones de seguridad pública y seguridad privada” (Ley de Video Vigilancia del Estado de Baja California Sur, 2020).
Colima	Art. 9 inciso c	“Obligación del Estado de proteger el derecho a la intimidad personal y familiar, honor y propia imagen” (Ley que Regula la Video Vigilancia en el Estado de Colima, 2009).
Durango	Art. 12 fracción II	“Obligación del Estado de proteger el derecho a la intimidad personal y familiar, honor y propia imagen” (Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango, 2012).

Leyes de Video Vigilancia	Artículos	Derecho a la privacidad
Morelos	Art. 6 fracción II inciso b	“Principio de proporcionalidad en su carácter intervención mínima, de la que existe una ponderación entre la finalidad pretendida y la afectación al derecho a la intimidad, honor y propia imagen” (Ley de Videovigilancia para el Estado de Morelos, 2020).
Zacatecas	Art. 5 fracción II	“Principio de proporcionalidad en su carácter intervención mínima, de la que existe una ponderación entre la finalidad pretendida y la afectación al derecho a la intimidad, honor y propia imagen” (Ley de Videovigilancia para el Estado de Zacatecas, 2018).

Fuente: Elaboración propia con base en la Ley de Video Vigilancia de Aguascalientes (2009); Ley de Video Vigilancia del Estado de Baja California Sur (2020); Ley que Regula la Video Vigilancia en el Estado de Colima (2009); Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango (2012); Ley de Videovigilancia para el Estado de Morelos (2020); y la Ley de Videovigilancia para el Estado de Zacatecas (2018).

III.9 Protección de datos personales

En relación con esta categoría, se puede observar que las legislaciones de la Video Vigilancia reconocen diversos derechos vinculados con la protección de datos personales: a) el derecho a recibir información sobre los lugares donde se realiza la videovigilancia, incluyendo el nombre de la autoridad o prestador de servicios de seguridad privada; b) el derecho a conocer el término en que se destruirán las grabaciones y los derechos de acceso, rectificación y oposición; c) el derecho de acceso a la información en relación con las grabaciones.

Tabla 9. Protección de datos personales de los vigilados

Entidad Federativa	Elementos importantes de protección de datos personales
Aguascalientes	- “Derecho a ser informado sobre lugares de videovigilancia. - “Diferenciación entre datos personales y reservados” (Ley de Video Vigilancia de Aguascalientes, 2009).
Baja California Sur	- “Derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos personales. - Derechos de información sobre las grabaciones, excepto cuando se presuma la comisión de hechos punibles o faltas administrativas relacionadas con la seguridad pública” (Ley de Video Vigilancia del Estado de Baja California Sur, 2020).

Morelos	- “Restricción de suministro e intercambio de información. - Derechos de acceso y protección de datos personales” Ley de Video vigilancia para el Estado de Morelos, 2020).
Zacatecas	- “Derechos de transparencia y protección de datos” (Ley de Video Vigilancia para el Estado de Zacatecas, 2018).

Fuente: Elaboración propia con base en la Ley de Video Vigilancia de Aguascalientes (2009); Ley de Video Vigilancia del Estado de Baja California Sur (2020); Ley de Video vigilancia para el Estado de Morelos (2020); y la Ley de Video vigilancia para el Estado de Zacatecas (2018).

Conclusiones

Sin duda, la discusión principal de la normatividad de la video vigilancia en México es la falta de armonización a nivel nacional y subnacional, de los sujetos, actores, procesos y elementos más importantes de la implementación. Es necesario que la Norma Técnica para Estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia establezca y regule los mecanismos de garantía y protección de los derechos humanos en el uso de la video vigilancia.

Otro aspecto es la poca regulación de la participación ciudadana, que es fundamental al hablar de la garantía de los derechos humanos y la eficacia de las políticas públicas de seguridad. A lo anterior, se suma la disparidad de determinar los Comités o Comisiones de Video Vigilancia, a efecto de que en la mayor medida de lo posible se pueda eficientar la instalación, las labores concernientes a la video vigilancia y protección de los derechos de las personas vigiladas. Finalmente, la falta de armonización a nivel subnacional de los medios de impugnación y de la materialización del derecho a la privacidad y la protección de datos personales, podría ser un factor que limite el goce pleno de los derechos humanos.

Las leyes de video vigilancia a nivel subnacional en México presentan una diversidad de enfoques y regulaciones de figuras jurídicas, lo que puede generar la vulneración de los derechos en ciertas regiones.

Es fundamental que las leyes de video vigilancia y las de seguridad pública a nivel subnacional definan claramente el concepto de video vigilancia. Esta definición debe incluir aspectos como los objetivos de la videovigilancia, los sujetos involucrados, los lugares donde se puede aplicar, y los límites en cuanto a la recopilación, uso y almacenamiento de las imágenes y sonidos captados por los sistemas de videovigilancia.

La regulación del proceso de grabación y almacenamiento de datos es otro aspecto crucial que debe ser abordado en las leyes de video vigilancia a nivel subnacional. Se deben establecer protocolos claros sobre la duración de la conservación de las graba-

ciones, los mecanismos de acceso a dichas grabaciones, y las medidas de seguridad para proteger la integridad y confidencialidad de los datos recopilados.

La participación ciudadana, la creación de Comités de Video vigilancia, la definición de medios de defensa para los ciudadanos y la protección del derecho a la privacidad y de los datos personales son aspectos clave que deben ser abordados de manera integral en estas leyes. La inclusión de mecanismos que fomenten la participación activa de la sociedad en la toma de decisiones sobre la implementación y operación de los sistemas de videovigilancia es fundamental para garantizar el respeto a los derechos humanos y la legitimidad de dichos sistemas.

Se concluye que no existe claridad, homogenización, análisis profundo y consideración de los derechos humanos de privacidad, intimidad y protección de datos personales en la normatividad vinculados a la video vigilancia. Estas conclusiones resaltan la importancia de seguir trabajando en la regulación de la video vigilancia en México para garantizar el respeto a los derechos humanos y la protección de la privacidad de los ciudadanos en un contexto cada vez más tecnológico y digitalizado.

Referencias

- Arteaga, Botello. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. Espiral, 66, pp. 193-238.
- Cámara de Diputados del H. Congreso de la Unión. (1917, 5 febrero). *Constitución Política de los Estados Unidos Mexicanos: Constitución publicada en el Diario Oficial de la Federación*.
- Cámara de Diputados del H. Congreso de la Unión. (2010, 5 junio). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares: Nueva Ley publicada en el Diario Oficial de la Federación*.
- Carta para el uso democrático de la vigilancia por video*. (2017, 22 agosto). Issuu. https://issuu.com/efus/docs/cctv_charter_es_full
- El derecho a la privacidad en la era digital. (3d. C.). En *Informe del Alto Comisionado de las Naciones Unidas Para los Derechos Humanos* (A/HRC/39/29). Organización de las Naciones Unidas. <https://documents.un.org/doc/undoc/gen/g18/239/61/pdf/g1823961.pdf?token=GBfX5esw9d8HPABksS&fe=true>
- H. Congreso del Estado de Aguascalientes. (2009, 22 junio). *La Ley de Video Vigilancia de Aguascalientes: Ley publicada en la Primera Sección del Periódico Oficial del Estado de Aguascalientes por el Decreto Número 252*.
- H. Congreso del Estado de Baja California. (2020, 28 diciembre). *Ley del Sistema Estatal de Seguridad Ciudadana de Baja California*. Publicada En el Periódico Oficial No. 84, Tomo CXXVII, Sección XI.
- H. Congreso del Estado de Baja California Sur. (2020, 20 enero). *Ley de Video Vigilancia del Estado de Baja California Sur*.

Capítulo 3. Normatividad de la video vigilancia en México. Una mirada desde el derecho a la privacidad y la protección de datos personales

- H. Congreso del Estado del Estado de Chihuahua. (2013, 12 octubre). *Ley del Sistema Estatal de Seguridad Pública del Estado de Chihuahua: Decreto 1390-2013 XIV P.E.*
- H. Congreso del Estado de Colima. (2009, 22 agosto). *Ley que Regula la Video Vigilancia en el Estado de Colima*. Ley Publicada En el Suplemento del Periódico Oficial del Estado de Colima Por el Decreto No. 618.
- H. Congreso del Estado de Durango. (2012, 2 julio). *Ley que Establece las Bases para la Video Vigilancia en el Estado de Durango: Publicado en el Periódico Oficial No. 2 por el Decreto 291.*
- H. Congreso del Estado de Hidalgo. (2014, 10 noviembre). *Ley de Seguridad Pública para el Estado de Hidalgo: Decreto No 230.*
- H. Congreso del Estado de México. (2014, 14 mayo). *Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México.* Decreto No 224.
- H. Congreso del Estado de Morelos. (2020, 15 julio). *Ley de Videovigilancia para el Estado de Morelos: Periódico Oficial 5853 “Tierra y Libertad”.*
- H. Congreso del Estado de Nuevo León. (2018, 22 septiembre). *Ley de Seguridad Pública para el Estado de Nuevo León.* Decreto No. 279.
- H. Congreso del Estado de Querétaro. (2016, 30 mayo). *Ley de Seguridad para el Estado de Querétaro.*
- H. Congreso del Estado de Sinaloa. (2019, 14 octubre). *Ley de Seguridad Pública del Estado de Sinaloa: Decreto No. 392.*
- H. Congreso del Estado de Sonora. (2011, 14 julio). *Ley de Seguridad Pública del Estado de Sonora: Ley No 161.*
- H. Congreso del Estado de Tabasco. (2016, 13 septiembre). *Ley de Seguridad Pública del Estado de Tabasco: Decreto No. 027.*
- H. Congreso del Estado de Yucatán. (2018, 25 julio). *Ley de Videovigilancia del Estado de Yucatán: Decreto 634/2018.*
- H. Congreso del Estado de Zacatecas. (2018, 22 agosto). *Ley de Videovigilancia para el Estado de Zacatecas: Decreto No. 407.*
- Ibarra, S. E. (2010). Videovigilancia. Punto de colisión entre derechos fundamentales, seguridad y protección de datos personales en México. En Ibarra, S. E. y Romero, F.R., Jurisnómica. El derecho y las nuevas tecnologías. Estudios. México: UNAM.
- Jasso, López. (2020). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en Latinoamérica. Dike. Revista de investigación en Derecho, Criminología y Consultoría Jurídica 14 (27), pp. 5-27. <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/914/1803>
- Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.
- Norma Técnica para Estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública aprobado por el Consejo Nacional

de Seguridad Pública el 30 de agosto de 2016. https://www.gob.mx/cms/uploads/attachment/file/647035/Norma_tecnica_sistemas_video_vigilancia.pdf

Organización de las Naciones Unidas. (1948, 10 diciembre). *Declaración universal de Derechos Humanos*.

Organización de las Naciones Unidas. (1966, 16 diciembre). *Pacto Internacional de Derechos Civiles y Políticos: Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI)*.

Organización de los Estados Americanos. (1948, 2 mayo). *Declaración Americana de los Derechos y Deberes del Hombre: La IX Conferencia Internacional Americana*.

Organización de los Estados Americanos. (1969, 22 noviembre). *Convención Americana sobre Derechos Humanos*. Suscrita En la Conferencia Especializada Interamericana Sobre Derechos Humanos San José, Costa Rica.

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2016, 30 agosto). *Norma Técnica para Estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública: Aprobado por el Consejo Nacional de Seguridad Pública, en su XL Sesión c*.

Téllez, Valdés. (2008) La regulación jurídica de la videovigilancia bajo una perspectiva de derecho comparado. En Ferrer, Mac-Gregor y Zaldívar Lelo De Larrea (coords.), *La ciencia del derecho procesal constitucional. estudios en homenaje a Héctor Fix Zamudio en sus cincuenta años como investigador del derecho*. México, Instituto de Investigaciones Jurídicas UNAM, 2008, p. 768).

Capítulo 4

Video vigilancia y derechos humanos

Video surveillance and human rights

*Jorge Martínez Martínez**

Resumen

El avance y utilización de la tecnología en el contexto actual es indudable; por lo cual es imprescindible que el derecho evolucione conjuntamente con dichos cambios. Los dispositivos tecnológicos de video vigilancia tienen un valor instrumental incalculable en materia de seguridad pública y defensa nacional, pues permiten la ubicación e identificación de personas, lo cual se logra gracias al reconocimiento de sus datos biométricos. Estos avances se enfrentan, por otro lado, con la tutela de derechos humanos como son la intimidad, la vida privada y, de manera general, la protección de datos personales.

En virtud de lo anterior, se precisa de normativa especial en la materia que permita la implementación de políticas públicas acordes con el paradigma constitucional vigente. Ahí encuentra sustento la necesidad del planteamiento y estudio del presente tema, sobre todo ante el riesgo de vulnerar las libertades fundamentales del individuo, lo cual es contrario a la democracia y evolución del Estado constitucional de derecho.

Palabras clave: Video vigilancia; Derechos humanos; Protección de datos personales; Vida privada.

Abstract

Advance and use of technology in the current context is unquestionable, therefore, it is fundamental for law to evolve jointly with such changes. Video surveillance devices has an invaluable worth for public safety and national defense matters, thus allow the people localization and identification through biometric data recognition. These technological advances are faced with the Human Rights protection, such as privacy, private life and un general the per-

* Doctor en Derecho Público, Universidad Veracruzana. Profesor investigador de la Universidad Veracruzana (México). Miembro del Sistema Nacional de Investigadores nivel I del CONAHCYT. [jormartinez@uv.mx]; [<https://orcid.org/0000-0002-2707-382X>]

sonal data protection rights. By virtue of which special regulation are required on the matter, which allow the implementation of public policies in accordance with the current constitutional paradigm, there the need for the approach and study of this topic find support, especially given the risk of violating the fundamental freedoms of individual, which is contrary to democracy and evolution of Constitutional rule of Law.

Keywords: Video surveillance; Human rights; Data protection; Private life.

Introducción

Desde hace algunos años se han observado los avances de la tecnología, ello incluye la proliferación de dispositivos electrónicos para muy diversos usos, entre los que se encuentran los de video vigilancia en distintas ciudades del país, lo cual es consecuencia de la evolución tecnológica en la que se sitúa la humanidad hoy en día, mejor conocida como *Industria 4.0*, que surge después del último cuarto del siglo XX, o bien se señala el año 2000; en donde se aprecian cambios tecnológicos de manera frecuente, con avances como la internet, las redes inalámbricas, software, automatización, mecatrónica y robótica (Tepe & Mucan, 2021, p. 160).

Esto ha sido un hito histórico debido a la manera en que los servicios y los productos se elaboran en la actualidad, mediante la aplicación de integración de nuevas tecnologías, a las que se agrega la inteligencia artificial como parte funcional u operativa en cadenas de suministro, indudablemente dirigido a un eventual reemplazo del ser humano por las máquinas, en este caso las computadoras.

Una de las características de la actualidad es el manejo de grandes cantidades de información y la facilidad de comunicación de diversos tipos gracias a la tecnología. Por ello, se afirma que se vive en los tiempos del *Big Data*, que se define como:

El big data (datos masivos) es el término que describe un gran volumen de datos, el cual crece de manera exponencial con el paso del tiempo. En pocas palabras, es un conjunto de datos tan grande y complejo que ninguna de las herramientas tradicionales de datos es capaz de almacenarlos o procesarlos de manera eficiente (Universidad Católica de San Pablo, 2023).

Cuando esto se aplica por ejemplo a las cuestiones de seguridad tanto exterior (defensa nacional) como interior (seguridad pública), permite de algún modo a las autoridades tener un mayor control de la conducta de los ciudadanos, de manera que se convierte en un instrumento invaluable e irremplazable, por ejemplo, para la investigación de las conductas delictivas.

De manera que los avances referidos permiten monitorear permanentemente las actividades de la población, saber en qué lugar se encuentran, qué es lo que hacen,

identificar sus rostros, etc., lo que, aunado al registro, por ejemplo, de sus movimientos bancarios, uso de teléfonos móviles, computadoras y demás, posibilitarían, por lo menos en teoría, encontrar casi a cualquier persona, no solo en el país, sino en el mundo.

Sin embargo, este tipo de vigilancia puede ser violatoria de los derechos a la privacidad o a la intimidad, así como la protección de datos personales, ya que mediante este tipo de tecnologías puede llegarse al reconocimiento de datos biométricos, del mismo modo, esta información se aloja en registros que pueden ser vulnerados y utilizados con fines distintos a los que deberían tener por parte del Estado.

Asimismo, cobra relevancia el estudio del presente tema, ya que la evolución de la protección de datos personales ha sido relativamente reciente en el país y, a pesar de contar hoy en día con los denominados derechos ARCO, en muchas de las ocasiones la realidad se impone y hace difícil la tutela efectiva de estos derechos humanos.

I. Evolución tecnológica y video vigilancia

Hoy en día el progreso en áreas como la informática, robótica e inteligencia artificial, así como las telecomunicaciones, es indudable y se aplica a aspectos de la vida cotidiana tanto simples como avanzados; incluso, se habla de que la inteligencia artificial puede superar al ser humano, eventualmente sustituirlo y llegar a ser un problema a mediano y largo plazo.

La aplicación de la tecnología ha llegado para quedarse. Al respecto, las grandes empresas que han liderado el campo de la informática, como es el caso de IBM, han señalado que el internet de las cosas mejora notablemente los procesos productivos:

El uso de dispositivos del IoT de alta tecnología en fábricas inteligentes conduce a mayor productividad y mejor calidad. Reemplazar los modelos comerciales de inspección manual con insights visuales basados en IA reduce los errores de manufactura y ahorra tiempo y dinero. Con una inversión mínima, el personal de control de calidad puede configurar un smartphone conectado a la nube para supervisar los procesos de manufactura desde prácticamente cualquier lugar. Al aplicar algoritmos de machine learning, los fabricantes pueden detectar errores de inmediato, en lugar de hacerlo en etapas posteriores, cuando el trabajo de reparación resulta más costoso (IBM, 2023).

Lo citado con antelación tiene indudable valor para las cadenas de producción en las empresas y en la industria, aunado a la proliferación de la inteligencia artificial que permite el incremento de resultados y ganancias en el sector privado; no obstante, cuando las tecnologías mencionadas se aplican a la sociedad, recuerdan los planteamientos que hacía George Orwell en su libro 1984 (Orwell, 2021), pues ahí se vislumbra cómo la humanidad llegaría al punto de estar controlada por cámaras con las que se mantendría un control absoluto y, por ende, despótico del gobierno.

Con ello, el ser humano pierde su esencia y es controlado cual si fuera un robot programado para realizar determinadas conductas bajo una aparente libertad, coartada por la influencia de la tecnología. En consecuencia, la autonomía de la voluntad emanada de las libertades de pensamiento y conciencia, se hacen nugatorias.

El planteamiento cobra fundamental relevancia debido a que la tecnología en general, y particularmente la video vigilancia, debe ocuparse en beneficio de la sociedad, como un instrumento que permita la investigación de los delitos, o por lo menos se convierta en una herramienta disuasiva para la realización de conductas no solo antijurídicas, sino también las que llegasen a ser moralmente reprobables, para finalmente vivir en un Estado de Derecho, en una sociedad más justa y equitativa. En caso contrario, la tecnología mal aplicada se convertiría en un mecanismo de represión y control.

La necesidad de regular adecuadamente el tema tiene como sustento las ideas de Montesquieu, quien sostiene que: “El gobierno despótico tiene por principio el temor: para pueblos tímidos, ignorantes, rebajados, no hacen falta muchas leyes” (Montesquieu, 2018, p. 54.). De lo anterior, se desprende que, a menor regulación, habrá mayor margen de discrecionalidad para la utilización de dispositivos y, por ende, temor sobre el mal uso que se le pueda dar, en detrimento de los derechos a la privacidad y a la intimidad.

En los últimos tiempos, el uso de la tecnología se ha incrementado, lo que comprende, por ejemplo, la informática, la robótica e inteligencia artificial. Así, la utilización de los dispositivos móviles de comunicación, a lo cual contribuyó la pandemia de COVID-19, puesto que muchas personas, aún con conocimientos incipientes sobre estas cuestiones, se vieron en la necesidad de utilizar la tecnología para trabajar (en los casos en que la naturaleza de sus labores lo permitiera). En este sentido, destaca que, en los países más industrializados, la tecnología ha tenido un impacto siquiera imaginable en otro tipo de contextos:

Cuando el coronavirus comenzó a propagarse en Japón, el Gobierno declaró el estado de emergencia en las principales ciudades e instó a la población a reducir el contacto entre las personas por lo menos en un 70%. Por consiguiente, se exigió a los empleadores que pasaran al trabajo en línea. Uno de los principales grupos de telecomunicaciones es partidario del teletrabajo hace varios años y, desde febrero de 2020, ha instado a los empleados a evitar los desplazamientos en las horas pico o que simplemente trabajen desde casa, para proteger a sus 200 000 empleados en todo Japón del creciente brote de coronavirus en el país. La empresa también comenzó a utilizar robots avatar en abril de 2016 como parte de sus esfuerzos para promover el teletrabajo, una política destinada a permitir que los empleados sigan trabajando mientras crían a sus hijos o cuidan de sus padres ancianos. Usando los robots avatares, los trabajadores remotos pueden ver su oficina y comunicarse con sus colegas. Los robots miden aproximadamente 20 cm de altura con cámara, micrófono y

altavoces incorporados, junto con una aplicación de “teletrabajo” instalada en un teléfono o un iPad, son operados a distancia por el teletrabajador y pueden ser llevados por el personal de la oficina. Incluso, pueden asistir a reuniones en nombre de los empleados remotos. Además, es posible manejar las manos y la cabeza del robot, incluso utilizando la comunicación no verbal con diversos gestos, desde aplausos hasta saludos. “Puedo sentir el ambiente en la oficina y es como si estuviera allí”, dijo un teletrabajador de unos 40 años. (OIT, 2021).

Lo anterior, pone de manifiesto que el avance en materia tecnológica puede conducir a múltiples beneficios, si es que su aplicación se hace de manera correcta al dirigirse a la solución de problemas, aunque, por otro lado, requiere contar con el presupuesto para hacerlo, aunado a la capacitación para su operación y, como se verá más adelante, con la correspondiente protección de los datos personales.

De ahí se desprende la necesidad de estudiar el tema y reflexionar sobre los límites de la video vigilancia sobre la vida humana, bajo el riesgo de violar otros derechos humanos igualmente importantes para el desenvolvimiento del individuo.

II. El derecho a la vida privada y a la intimidad

Existe una relación indisoluble entre democracia y derechos humanos. Por ello es que cobra relevancia el estudio del derecho vida privada y a la intimidad, como parte de los derechos humanos que han experimentado cambios tanto en la realidad social, como en la norma jurídica, sobre todo debido a la colisión y, en su caso, ponderación del alcance y protección que debe darse a la tutela del derecho a la información y las posibles violaciones a la privacidad.

El derecho a la intimidad, de acuerdo con Antonio Muñozcano Eternod, es: “La intimidad es el poder que la persona tiene de excluir a los demás del conocimiento de sus actos y actividades personales, de aquellas que constituyen el círculo de su vida individual y familiar” (Muñozcano, 2010, p. 62).

Del mismo modo, conviene establecer que la intimidad, como derecho, se encuentra relacionada con la toma de conciencia que tiene una persona, ya que de ello depende su actuación al exterior y con la sociedad, por lo cual el referido autor señala lo siguiente:

Conviene que se establezcan algunos caracteres de la persona con respecto a la intimidad, desde una perspectiva filosófica. Esto se concreta en la auto propiedad, la autorresponsabilidad y la auto finalidad. La auto propiedad se entiende en el sentido de que la persona pertenece a sí misma. Ello implica que está cerrada en sí misma y en cierta medida es comunicable; por ello la persona es singular, independiente, frente a cualquier otro ser. Respecto a la autorresponsabilidad, se comprende que es la capacidad de actuar desde sí

misma: a esto es a lo que denominamos libertad. En los referidos a la auto finalidad, la persona actúa y piensa por sí misma, con ello pretende la perfección, con esta pretensión se configura asimismo, se utiliza a sí misma” (Muñozcano, 2010, p. 67).

Existen, desde luego, algunos antecedentes del derecho a la vida privada, en donde, de manera supranacional, es referencia obligada la Declaración Universal de Derechos Humanos, la cual, en su artículo 12, establece: “Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” (ONU, 2023).

Igualmente, se encuentra regulado en el Pacto Internacional de Derechos Civiles y Políticos; en su artículo 17; en la Convención sobre los Derechos del Niño, en su artículo 16; en la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares, en su artículo 14; en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, en su artículo 8; en la Convención Americana sobre Derechos Humanos, en su artículo 11; en el Convenio del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, en la Directiva de Protección de Datos de la Unión Europea (2016/680), sin menoscabo de la demás normatividad que pudiera existir en en diversas regiones del mundo.

Al tratarse de un derecho humano, encuentra relación con otros de su misma naturaleza, como es la igualdad, no discriminación, libertad de pensamiento, conciencia, expresión y, desde luego, el libre desarrollo de la personalidad.

De acuerdo con la Organización de las Naciones Unidas, el derecho a la privacidad se relaciona con los siguientes derechos:

La privacidad permite el ejercicio de otros derechos: el desarrollo de la expresión libre de la personalidad, la identidad y las creencias individuales, y la capacidad de participar en la vida política, económica, social y cultural. El relator especial tiene el mandato de promover y proteger el derecho a la privacidad [...] (ONU, 2023).

Por estas razones, debe tutelarse por el Estado, de manera que se impidan ataques a este derecho a la vida privada, que permita la autorrealización del ser humano, con las limitaciones relativas a la seguridad pública, seguridad nacional, etc.

Como antecedente relevante se encuentra la observación general número 16 sobre el derecho a la intimidad, reconocido en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, por parte de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, quien, en su 32º período de sesiones (1988), expresó que los Estados deberían adoptar medidas legislativas y de otra índole

para hacer efectiva la prohibición de las inferencias y ataques y la protección del derecho a la vida privada:

Incluso con respecto a las inferencias que sean conformes al Pacto, en la legislación pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas inferencias. La decisión correspondiente competará solo a la autoridad designada por la ley a ese efecto, que dará la autorización necesaria tras examinar cada caso en particular. El cumplimiento del artículo 17 exige que la integridad y el carácter confidencial de la correspondencia estén protegidos *de jure* y *de facto*. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones. Los registros en el domicilio de una persona deben limitarse a la búsqueda de pruebas necesarias y no debe permitirse que constituyan un hostigamiento. Por lo que respecta al registro personal y corporal, deben tomarse medidas eficaces para garantizar que esos registros se lleven a cabo de manera compatible con la dignidad de la persona registrada. Las personas sometidas a registro corporal por funcionarios del Estado o por personal médico que actúe a instancias del Estado serán examinadas solo por personas de su mismo sexo (ACNUDH, 2023).

En el mismo documento se expresa que los registros y recopilación de información personal en computadoras, bancos de datos y otros dispositivos, ya sea por parte de las autoridades públicas o particulares o entidades privadas, deben estar reglamentados por la ley, y que las medidas deben ser eficaces para tutelar el derecho a la vida privada, sobre todo para que dicha información no caiga en manos de personas no autorizadas.

De lo anterior se desprende que el contexto ha cambiado; que hoy en día, debido a la evolución de las instituciones jurídicas, como es el caso del derecho de acceso a la información y a la protección de datos personales, se cuenta con normatividad extensa para el manejo y tratamiento de dichos datos, pero que, en el caso de la video vigilancia, sigue siendo insuficiente, por lo que hay que tener cuidado de que, en la práctica, estos derechos sean debidamente salvaguardados, sobre todo porque en el Estado de Derecho debe cumplirse con las obligaciones que emanan de los referidos tratados internacionales.

Igualmente, se debe hacer notar que, debido a la utilización de la tecnología, la vida privada se ve vulnerada no solo con el uso de las cámaras de video vigilancia, sino con el uso de las cámaras de los dispositivos de comunicación, como es el caso de los teléfonos celulares, los cuales llegan a ocupar algoritmos (procesos) que tienen que ver con la reacción facial de las personas, así como la invasión a la vida privada en cuanto a la posibilidad de escuchar también conversaciones.

En el año 2015, el Consejo de Derechos Humanos de las Naciones Unidas emitió la resolución 28/16, con lo que se creó el primer mandato sobre la privacidad. La relatora especial de ello recabó información de los gobiernos, organizaciones gubernamentales y otros sujetos para el conocimiento de situaciones y casos relacionados con la privacidad, lo cual se hizo para que los gobiernos (entre otras finalidades) alcancen mejores prácticas en la materia.

En cuanto a las disposiciones internas, el derecho a la vida privada se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos en el artículo sexto apartado a fracción II:

Artículo 6º [...]

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

[...]

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 (CPEUM, 2023).

Igualmente, en la fracción tercera se reconoce el derecho de acceso a los datos personales, o a la rectificación de los mismos.

No obstante, hay que preguntarse, en el caso de las cámaras de video vigilancia, lo que sucede con este tipo de información, que tiene que ver con los rasgos biométricos del ser humano y que dicha información viaja a través de la Internet y es almacenada en algún dispositivo físico y/o nube, en donde puede ser accesible con muy diversos fines, de manera que está expuesta a su mal uso, y pone en tela de juicio el actuar del gobierno en relación con la tutela de este derecho.

III. Derechos de la personalidad

Una de las cuestiones medulares al abordar el presente tema es la importancia de proteger el derecho a la vida privada o a la intimidad, lo cual deriva desde el enfoque de los derechos humanos; sin embargo, desde el punto de vista del derecho civil, puede estudiarse desde la perspectiva de los derechos de la personalidad.

Ello conduce a que la justificación de la tutela de los citados derechos es que emanan de la persona, de la cual, a su vez, deriva su personalidad jurídica. Son numerosas las definiciones que se han dado al respecto de los derechos de la personalidad, incluso desde el punto de vista teórico y, en relación con las personas jurídicas colectivas, pueden adquirir otra dimensión y una mayor protección, ya que estas últimas carecen de sustantividad psicofísica y, a su vez, se han tenido que crear ficciones jurídicas para

tutelar los derechos humanos de las personas morales (como en caso de que sean quejas en el Juicio de Amparo), lo cual evidentemente parece un contrasentido.

Los derechos de la personalidad, de acuerdo con Ernesto Gutiérrez González, son:

[...] bienes constituidos por determinadas proyecciones físicas o psíquicas del ser humano, relativas a su integridad física y mental, que las atribuye para sí o para algunos sujetos de derecho y que son individualizados por el ordenamiento jurídico. (Gutiérrez y González, 2022, p. 765.)

De esto se desprende que, indudablemente, protegen la esencia de la persona, de acuerdo con su naturaleza humana, y le permiten al individuo su desenvolvimiento en sociedad.

Como características principales de los derechos de la personalidad se encuentran el estar indisolublemente ligados al ser humano, por lo tanto dependen de la vida; su reconocimiento por parte del derecho positivo y la exigibilidad que hay frente a los demás, su respeto, la oponibilidad frente a terceros, así como el ser inalienables, imprescriptibles irrenunciables; finalmente, puede destacarse que los derechos de la personalidad forman parte, de acuerdo con el autor citado, del patrimonio moral y, por lo tanto, ésta es la vía para reclamar el daño ocasionado a ellos aun cuando, en parte, se traduzca en una reparación de tipo pecuniario.

Excede los límites del presente análisis el hacer una enumeración de los derechos de la personalidad; sin embargo, debe decirse que el propio derecho a la imagen, a la reputación, el secreto, reserva, a la intimidad y al olvido, son los que interesa destacar para efectos de la temática que se aborda, y los cuales, en la opinión del autor referido, forman parte de lo que él ha clasificado como el sector social público de estos derechos.

IV. La protección de datos personales

La protección de datos personales guarda estrecha relación con el derecho a la intimidad, ya que este tipo de información, de acuerdo con la clasificación legal, se subdivide en datos sensibles o simplemente datos personales, y puede causar afectaciones a la persona hacia el interior y hacia el exterior, es decir su divulgación debe ser cuidadosamente ponderada de acuerdo no solo a la naturaleza de la misma, sino al impacto o repercusiones que pudieran generarse, porque, indudablemente, repercutirá en la violación de otros derechos humanos o derechos de la personalidad.

La protección de datos personales ha sufrido, igualmente, una evolución a través del tiempo en el mundo. Hoy en día, a pesar de la regulación, sigue siendo una tarea pendiente del Estado y que, además, se encuentra en constante transformación, con independencia de la variabilidad del contexto, pues se transforma de acuerdo con las

restricciones que se impongan jurídicamente a la tecnología, así como de su aplicación efectiva.

La tutela del derecho a la vida privada y protección de datos personales se realiza de manera conjunta con la tutela del derecho a la información, como rasgo de la evolución democrática del Estado, con las limitaciones establecidas por la norma y las ponderaciones correspondientes.

Sin embargo, el ejercicio de este derecho tiene algunas limitantes, al igual que todos los demás, pues no es absoluto, ya que frente al derecho a saber se opone el derecho a no saber, que en el caso se traduce en los derechos a la vida privada y a la intimidad, que son algunos de los llamados derechos de la personalidad.

La determinación de los datos que deben saberse y los que no, se halla sujeta, en México, a la regulación específica en materia de protección de datos personales. A nivel federal existen la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como la legislación que en la materia puedan expedir las entidades federativas.

El órgano garante federal y, en su caso, los locales son los encargados de la tutela de los datos personales, sin menoscabo de las responsabilidades que se pueden determinar tanto a los sujetos obligados, como a los particulares. La normativa actual es el resultado de la evolución en la protección de los derechos a la vida privada y a la intimidad.

Igualmente, conviene destacar que la protección de datos personales, así como la tutela de los derechos que se relacionan con la vida privada y la intimidad, forman parte hoy en día de lo que puede considerarse como un derecho emergente a la buena administración, ya que es responsabilidad del Estado el manejo de este tipo de información de manera adecuada para no vulnerar los derechos mencionados de los particulares, incluso de los servidores públicos que han renunciado a una buena parte de su vida privada en cuanto a su proceder público, aunque, de cualquier modo, queda una pequeña porción de vida privada que es objeto de protección.

De acuerdo con lo expuesto hasta aquí, la regulación sobre los datos personales es relativamente reciente, debido a que los avances tecnológicos han permitido el manejo de mayores volúmenes de información, así como la interferencia que puede producirse con la vida privada de las personas, que ha llegado a niveles nunca antes concebidos.

En América, la protección de datos personales inicia en el año de 1974 con la *Privacy Act*, en los EUA, en la que se estableció lo siguiente:

- 1) Todo individuo tiene derecho a acceder a la información personal que le afecte y, especialmente, a aquella que se encuentra en bancos de datos informatizados;

- 2) Todo individuo ha de tener la posibilidad y el derecho a controlar de forma razonable la transmisión de la información personal que le afecte;
- 3) La norma ha de regular necesariamente como garantía del derecho a la intimidad:
 - a) El tiempo durante el que se puedan conservar los datos personales;
 - b) La determinación de los fines a que obedece la creación del fichero o los ficheros;
 - c) Prohibición de la revelación de datos personales, garantizándose su veracidad, actualización e integridad (Gómez & Ornelas, 2006, pp. 12-13).

Otro antecedente es el Convenio 108 de Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, de fecha 28 de enero de 1981. Ahí se consagra el derecho a la vida privada:

Artículo 1. El fin del presente convenio es garantizar, en el territorio de cada Parte, a cualquier persona física, sea cuales fueren su nacionalidad o su residencia, el respeto de sus derechos o sus libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (AEPD, 2023).

Sin duda, las imágenes de las personas que se videograban son parte del tratamiento de los datos personales, pues son almacenados en medios tecnológicos del Estado, además de que debe evitarse su mal uso.

El referido convenio es de los primeros documentos que define al dato personal, que es la información relativa a una persona identificada o identificable, los que en la actualidad son manejados tanto por el Estado como por el sector privado.

En nuestro país, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, contiene la definición en su artículo 3°:

Artículo 3.- Para los efectos de la presente Ley, se entenderá por:

[...]

- III. 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;
- IV. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como

origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

[...] (LGPDPPO, 2023).

Cuando se trata de datos personales sensibles, su manejo debe ser con mayor cautela, pues, tal como lo refiere la norma, las consecuencias pueden generar riesgos graves para sus titulares e incluso discriminación.

Conviene señalar también que el inadecuado tratamiento de los datos personales, y con mayor razón si se trata de sensibles, puede permitirle a su titular el reclamarlo mediante el ejercicio de sus derechos ARCO, ante los sujetos obligados por las respectivas leyes de la materia, pero también es posible reclamar indemnizaciones por el daño moral que se ha generado, máxime que hoy en día es de explorado derecho la reparación de este tipo, tal como lo ha establecido la Corte Interamericana de Derechos Humanos en diversas resoluciones, en donde ha comprendido los conceptos de daño emergente y lucro cesante con motivo de las mencionadas reparaciones.

En nuestro país, es hasta el año 2002 que el tema se regula de manera incipiente por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; de modo que, a partir de ahí, se originaron las primeras dificultades para la tutela adecuada de los derechos a la vida privada y a la intimidad.

Es hasta el 5 de julio del año 2010 cuando fue promulgada la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y en fecha 26 de enero de 2017 la actual Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Asimismo, se debe hacer notar que, a pesar de la reciente regulación en la materia, su tutela desde otras ramas del derecho, como es el caso de los derechos de la personalidad en materia civil, surge desde los inicios del siglo XX, pues, además, hay que recordar que los derechos de la personalidad comprenden, entre otros, el de la vida privada, la imagen y el honor.

Con el manejo de las cámaras de video vigilancia, indudablemente puede dañarse la imagen y el honor de la persona, que pueden derivar por ejemplo (sin ánimo de exhaustividad) de las noticias que surgen desde el ámbito periodístico, del robo de imágenes con fines comerciales, así como la utilización en general para cuestiones diversas a los de seguridad pública y/o defensa nacional.

Ernesto Villanueva conceptualiza de la siguiente manera el derecho a la vida privada:

Es el derecho fundamental de los individuos que consiste en no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público (Villanueva, 2008, p. 133).

Y es que el conocimiento sobre hechos de la vida privada, sin duda, puede generar consecuencias en el honor del individuo, al darse a conocer aspectos que, por su propia naturaleza, pertenecen a su esfera íntima, excepción hecha y con las limitaciones cuando se trata de servidores públicos.

En cada caso, debe de realizarse una adecuada ponderación entre los derechos que se encuentran en colisión, como es el caso de la libertad de expresión frente al derecho a la vida privada. No obstante, en el caso del Estado, debe tenerse cuidado con la utilización y el valor que se le da a la pretendida justificación del interés colectivo o el interés público, debido a la subjetividad de este concepto y, sobre todo, a su aplicación dentro del paradigma constitucional de los derechos humanos, y es que no se trata de que el Estado no pueda actuar en su marco de atribuciones convencional y constitucionalmente establecidas, sino que hoy en día existen mayores limitaciones en virtud, precisamente, de la evolución y reconocimiento de los derechos humanos a nivel supranacional.

El autor Garzón Valdés plantea una distinción entre lo íntimo, lo privado y lo público, donde lo público y lo privado pueden sufrir algún daño, pero, de modo alguno, lo íntimo, aunque los datos personales se ubican entre las primeras dos categorías, y de ahí depende el grado de protección que la normatividad les otorga.

En otros países, como España, la Ley Orgánica 13/1999 de Protección de Datos de Carácter Personal, define a los datos personales como:

Artículo 3. Definiciones.

Para los efectos de la presente Ley Orgánica, se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas, identificadas o identificables (BOE, 2023).

La definición trasunta resulta muy amplia para los efectos de su protección y, del mismo modo, se debe destacar que, en el citado país, el órgano garante se encuentra separado y en el caso de México opera de manera fusionada.

Los datos personales sensibles, como ya se ha expresado, deben ser protegidos con mayor cuidado, por lo que la ley de la materia, en su artículo 8, dispone que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones señaladas en la ley, y que el titular manifiesta su consentimiento tácito al ponerse a su disposición el aviso de privacidad y no se haya opuesto; aunque los datos

financieros o patrimoniales requieren el consentimiento expreso, salvo las excepciones enumeradas en los artículos 10 y 37 de la ley de la materia.

También, es necesario referirse a los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, al regular la información reservada y confidencial respectivamente:

Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

- I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
- II. Pueda menoscabar la conducción de las negociaciones y relaciones internacionales;
- III. Se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional;
- IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;
- V. Pueda poner en riesgo la vida, seguridad o salud de una persona física;
- VI. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;
- VII. Obstruya la prevención o persecución de los delitos;
- VIII. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada;
- IX. Obstruya los procedimientos para fincar responsabilidad a los Servidores Públicos, en tanto no se haya dictado la resolución administrativa;
- X. Afecte los derechos del debido proceso;
- XI. Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;
- XII. Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público, y
- XIII. Las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en esta Ley y no la contravengan; así como las previstas en tratados internacionales (LGTAIP, 2023).

Hay que destacar que el tipo de información mencionada debe clasificarse de esta manera, a través de la prueba del daño y el correlativo interés público para el caso de las excepciones, en donde, conforme a la ley, puede ejemplificarse que se trate de información relacionada con actos de corrupción, en cuyo caso no se podrá invocar es el carácter de reservado, de conformidad con los artículos 114 y 115 de la Ley General de Transparencia y Acceso a la Información Pública:

Artículo 114. Las causales de reserva previstas en el artículo anterior se deberán fundar y motivar, a través de la aplicación de la prueba de daño a la que se hace referencia en el presente Título.

Artículo 115. No podrá invocarse el carácter de reservado cuando:

- I. Se trate de violaciones graves de derechos humanos o delitos de lesa humanidad, o
- II. Se trate de información relacionada con actos de corrupción de acuerdo con las leyes aplicables (LGTAIP, 2023).

De hecho, el artículo 113 fracción XIII, abre la posibilidad de clasificar bajo este tipo de información la que en realidad no tiene tal naturaleza, de manera que los órganos garantes deben ser cuidadosos en la tutela del derecho de acceso a la información y la protección de datos personales, acorde a la naturaleza de la información de que se trata y desde luego del principio de máxima publicidad.

Por otra parte, el artículo 116 señala la información confidencial:

Artículo 116. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.

La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales (LGTAIP, 2023).

La información confidencial no está a disposición de los particulares y, por ello, los sujetos obligados deben elaborar las correspondientes versiones públicas, con las excepciones señaladas expresamente por el diverso 120 de la ley en comento.

Artículo 120. Para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información.

No se requerirá el consentimiento del titular de la información confidencial cuando:

- I. La información se encuentre en registros públicos o fuentes de acceso público;
- II. Por ley tenga el carácter de pública;
- III. Exista una orden judicial;
- IV. Por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros, se requiera su publicación, o
- V. Cuando se transmita entre sujetos obligados y entre éstos y los sujetos de derecho internacional, en términos de los tratados y los acuerdos interinstitucionales, siempre y cuando la información se utilice para el ejercicio de facultades propias de los mismos.

Para efectos de la fracción IV del presente artículo, el organismo garante deberá aplicar la prueba de interés público. Además, se deberá corroborar una conexión patente entre la información confidencial y un tema de interés público y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información (LGTAIP, 2023).

No todos los datos personales deben ser catalogados o tratados como información confidencial, por ejemplo, aquellos que se contienen en registros públicos, ya que la esencia de este tipo de organismos es, precisamente, darle publicidad a la información que ahí se halla contenida y se desvirtúa su finalidad.

Es por ello que, en algunos casos, los datos personales se encuentran indisolublemente ligados a la demás información y, de hecho, la tutela de los derechos a la vida privada y a la intimidad encuentran algunas dificultades dependiendo del tipo de sujeto obligado de que se trate, pues habrá versiones públicas en algunos casos, aun cuando esa información testada pueda encontrarse en algún otro registro público.

La tutela de los datos personales también encuentra como una dificultad considerable el manejo que se tiene de los mismos mediante las tecnologías de información y comunicación, pues resulta difícil suprimirlos una vez que han entrado al ciberespacio, y esto puede acontecer tratándose de la video vigilancia.

Parte de lo que puede observarse, y en su caso puede ser perfectible, es que, de acuerdo con lo señalado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, quienes posean datos personales son denominados responsables, y tal normativa los obliga a la observancia, entre otros, de los principios de licitud, consentimiento y responsabilidad, pues de lo contrario pueden ser sancionados.

La obtención de los datos personales se encuentra sujeta a la elaboración de un aviso de privacidad, que se define como

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

I. Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.

[...] (LFPDPPP, 2023).

Igualmente, el responsable debe dar a conocer a su titular, la finalidad que persigue, a través del mismo documento:

Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (LFPDPPP, 2023).

Y cumplir con los requisitos señalados por el artículo 16 del mismo ordenamiento:

Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:

- I. La identidad y domicilio del responsable que los recaba;
- II. Las finalidades del tratamiento de datos;
- III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
- V. En su caso, las transferencias de datos que se efectúen, y
- VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos. (LFPDPPP, 2023.)

El ordenamiento legal en cita no tendría aplicación directa para la video vigilancia, a menos que se tratase del manejo de estos datos por parte de empresas privadas, las que, en un esquema de gobernanza, podrían involucrarse con el Estado en la instalación, mantenimiento u operación de este tipo de dispositivos electrónicos.

Hay que mencionar que la normativa en comento debe ser conocida y, desde luego, respetada en su correspondiente ámbito de aplicación, es decir, si se trata de sujetos

obligados o de particulares, pues, de lo contrario, puede sancionarse administrativa o penalmente.

En el caso, las sanciones que establece el artículo 64 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, (DOF 5/7/2010), que son de tipo pecuniario, van desde 100 a 320,000 días de UMA, con penas adicionales en caso de reiteración por otros 100 a 320,000 días y pueden aumentarse hasta por dos veces los montos cuando sean infracciones cometidas en el tratamiento de datos sensibles.

La ley en comento contempla los delitos en materia del tratamiento indebido de datos personales, lo que sin duda constituye un paso significativo y punto apenas de partida para el caso de la video vigilancia, pues, tal como se analizó, la regulación es aún muy general.

V. Normatividad en materia de video vigilancia

En México es necesario adecuar la legislación respecto a la video vigilancia, lo cual se sustenta en la necesidad de evitar trasgredir los derechos humanos a la vida privada y a la intimidad.

Igualmente, es indudable que existe una tendencia al aumento de los citados dispositivos sin que existan cifras del todo exactas; no obstante, para darse un idea, se tiene que, de acuerdo con el Gobierno de la Ciudad de México, tan solo en dicha entidad existen más de sesenta mil: “En 2018 se tenía registro de 18 mil 410 cámaras del C5, a la fecha, hemos instalado un total de 64 mil 807, con ellas podemos contar con vigilancia en tiempo real, además, contribuyen al soporte de las carpetas de investigación y seguimiento de diversos delitos en la capital; nuestra meta para 2022 es llegar a 80 mil cámaras” (Gobierno de la Ciudad de México, 2023.)

Existe cierta normatividad en el país, aun insuficiente, la cual es mencionada por la *Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública*, publicada por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, en donde se expresa que:

La regulación federal marca las directrices que deben ser respetadas por la Federación, los Estados y Municipios. Este apartado contiene la revisión de diez instrumentos jurídicos que norman la actuación de los SVV, permitiendo entender por un lado el sustento jurídico del uso de SVV en el espacio público y por otro, lo relativo a la protección de los datos personales obtenidos por los dispositivos de vigilancia, así como aquellos almacenados por las instituciones de seguridad pública. Enlistamos a continuación los instrumentos analizados:

- Ley de Seguridad Nacional (LSN)
- Programa Nacional de Seguridad Pública 2014-2018 (Programa)
- Ley General del Sistema Nacional de Seguridad Pública (LGSNSP)

- Reglamento de la Ley General del Sistema Nacional de Seguridad Pública (RLGSNSP)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (RLFPDPPP)
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG)
- Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal (Lineamientos) (SESNSP, 2023, p. 15).

En diversos países se ha regulado la operación de las cámaras de video vigilancia, como es el caso de Alemania, Bélgica, Dinamarca, España, Francia, Holanda, Nueva Zelanda, Reino Unido, Suecia y Estados Unidos. Por ejemplo, en el caso de España, la Ley Orgánica 4/1997 que Regula la utilización de video cámaras por las fuerzas y cuerpos de seguridad en lugares públicos. En ella destaca lo siguiente:

Artículo 6. Principios de utilización de las videocámaras

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. En 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 (BOE, 2023).

Destaca igualmente, en el artículo 8º, que las grabaciones deben ser destruidas en el plazo máximo de un mes, salvo que se relacionen con infracciones penales administrativas graves o muy graves en materia de seguridad pública, investigaciones policiales o procedimientos judiciales o administrativos, con lo cual, indudablemente se protege el derecho a la intimidad, pues, además, los servidores públicos deben de guardar confidencialidad en relación tanto con las imágenes como con la información que manejan.

En México, la *Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública* establece que:

Este documento sugiere la observancia de los derechos a la privacidad y la no discriminación, de modo que las tecnologías de grabación de audio, reconocimiento facial y reconocimiento biométrico, se hagan uso con apego a la ley. De igual manera, capacitar al personal que opere los SVV a evitar tomen decisiones bajo prejuicios de raza, género, origen, idioma, posición económica, entre otros; ni que el uso de las cámaras de seguridad pública sea efectuado al interior de domicilios y espacios privados. El uso de los SVV 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 Norma es el primer paso para lograr esta meta (SESNSP, 2023, p. 6).

Es pertinente examinar si de verdad los sistemas de video vigilancia son compatibles con el Estado de derecho y los principios de la sociedad democrática, pues en ésta deben maximizarse las libertades esenciales del ser humano que, como ya se ha mencionado, en el caso que nos ocupa, se trata del derecho a la intimidad o vida privada, la protección de datos personales y los derechos relacionados con estos, como son la libertad de tránsito, el derecho a la imagen, al honor, entre otros.

Con ello se pone de manifiesto parte de la problemática, que no es exclusiva de México, así como la necesidad de regular el tema lo más pronto posible, que debe dirigirse hacia la consecución de armonizar las cuestiones de seguridad nacional, seguridad pública en relación con la tutela efectiva del derecho a la vida privada y la intimidad, así como la protección de los datos personales.

VI. Consideraciones finales

Para poder establecer un régimen de excepción que permita la utilización de información en donde se contienen datos personales, como es el caso de los biométricos de las personas, así como una video vigilancia permanente que vulnera el derecho a la vida privada o a la intimidad, debe establecerse una adecuada valoración –por lo menos en torno a la prueba del interés público.

El planteamiento parte de la base de que la naturaleza de la información que se está manejando atañe a la vida privada del ser humano y en modo alguno es permanentemente información de naturaleza pública, excepción hecha la que corresponda a los servidores públicos, por ejemplo tanto al interior como al exterior de las oficinas gubernamentales en cualquiera de sus niveles de competencia, así como en cualquiera de los poderes del Estado. Pero, aun así, los servidores públicos tienen un espacio más reducido en el ámbito de su vida privada que debe igualmente respetarse, pues esto no significa que su ámbito íntimo y de vida privada no exista.

Esto encuentra sustento en la valoración que se hace para poder ponderar cuáles son los límites para el acceso a los datos personales y el manejo de ellos, por lo que se debe realizar el análisis bajo la denominada prueba del interés público y, en su caso,

como se hacía anteriormente, con la prueba del daño; es decir, establecer la preponderancia del beneficio hacia la colectividad respecto a la tutela del derecho a la intimidad o privacidad, así como determinar con la mayor precisión posible si se vulneran los principios de legalidad, así como el consentimiento del titular de los datos personales; de manera que hay colisión en el interés público de conocer dicha información que se enfrenta al interés privado de que permanezca oculta y o protegida.

De hecho, la prueba del interés público fue la que sustituyó a la denominada prueba de daño, en donde lo que había que ponderar es si se causaba un daño al revelar la información considerada como datos personales, aunque finalmente en ambos casos se realizaba un balance.

Sin embargo, el propio concepto de interés público (en realidad colectivo) es un concepto utilizado a conveniencia del Estado, que ha permitido, a través del tiempo, justificar innumerables decisiones bajo este argumento, en donde lo imperante es, generalmente la visión del utilitarismo jurídico, derivada a su vez del utilitarismo general; lo que da como resultado finalmente a violaciones a los derechos humanos ya mencionados.

En este punto también habría que reflexionar respecto a las video grabaciones y, en su caso, reconocimiento de datos biométricos que sean utilizados por los particulares con respeto a los límites legalmente determinados por la normatividad, porque, por ejemplo, se presentan los casos de colocación de cámaras de video vigilancia en el exterior de sus domicilios, o en los comercios, pues este tipo de dispositivos se apuntan en algunas ocasiones hacia la vía pública, en donde son grabadas las imágenes y datos de las personas sin su correspondiente consentimiento.

Actualmente, y debido al avance de la tecnología, pueden operarse conjuntamente con las video grabaciones del sector gubernamental. Con ello se extiende la cobertura de las áreas vigiladas y se justifica en un esquema de gobernanza o corresponsabilidad, en donde se debe involucrar al sector privado y social en las acciones de gobierno, sobre todo por la complejidad de la sociedad actual, así como de las limitaciones presupuestales que pueden tenerse desde el punto de vista estatal.

De hecho, tratándose de información reservada o confidencial, el artículo 149 de la Ley General de Transparencia y Acceso a la Información, retoma y desglosa de manera general el test de proporcionalidad de Robert Alexy, al mencionar que la prueba del interés público debe de satisfacer los criterios de idoneidad, necesidad y proporcionalidad:

Artículo 149. El organismo garante, al resolver el recurso de revisión, deberá aplicar una prueba de interés público con base en elementos de idoneidad, necesidad y proporcionalidad, cuando exista una colisión de derechos.

Para estos efectos, se entenderá por:

- I. Idoneidad: La legitimidad del derecho adoptado como preferente, que sea el adecuado para el logro de un fin constitucionalmente válido o apto para conseguir el fin pretendido;
- II. Necesidad: La falta de un medio alternativo menos lesivo a la apertura de la información, para satisfacer el interés público, y
- III. Proporcionalidad: El equilibrio entre perjuicio y beneficio a favor del interés público, a fin de que la decisión tomada represente un beneficio mayor al perjuicio que podría causar a la población (LGTAIP, 2023).

Esto debe considerarse al resolver los correspondientes recursos de revisión que le son planteados, en el caso debido a la clasificación de información como reservada o confidencial.

Ha habido algunos casos en que los dispositivos tecnológicos, más que buscar seguridad, buscan beneficios políticos para el gobierno. Para ello hay que mencionar la sentencia de la Suprema Corte de los Estados Unidos emitida en fecha 24 de julio de 1974 por los jueces Douglas, Brennan, White, Marshall, Blackmun, Stewart, y Powell, en donde se ordenó entregar grabaciones que vulneraban el derecho a la intimidad del presidente Nixon, quien se negaba a hacerlo bajo el argumento de que se trataba de asuntos internos del gobierno y hasta ahí debería extenderse la inmunidad presidencial; finalmente, en fecha 9 de agosto de 1974, el presidente renunció (IIJ - UNAM, 2023).

Puede establecerse que la protección de los datos personales, particularmente los que se obtienen con el manejo y operación de las videocámaras y sus videograbaciones, indudablemente pueden vulnerar derechos humanos, por lo que debe legislarse adecuadamente al respecto, con límites claros, o por lo menos con algunos elementos que permitan la ponderación de derechos humanos. En esta normatividad debe contemplarse el correcto uso de este tipo de dispositivos, ya que la tecnología puede ser perjudicial en torno a las actividades que realizan los ciudadanos dentro del Estado constitucional de derecho.

La tecnología ha impuesto nuevos retos a la ciencia del derecho y también a la convivencia social, debido, sobre todo, a la facilidad con la que pueden manejarse los datos personales, así como el desarrollo, por ejemplo, de software espía en donde indudablemente también se afectan el derecho a la vida privada y/o a la intimidad de las personas no solo en las calles, sino en sus propios hogares. De manera que en el contexto actual sigue siendo un tema pendiente.

Conclusiones

1. La tecnología ha dado grandes pasos en los últimos tiempos al punto que la vida cotidiana resulta difícil de concebir sin su auxilio, lo que ha generado consecuentemente tanto ventajas, como desventajas.

2. La tecnología utilizada para la video vigilancia es una de tantas aplicaciones que deben ser utilizadas en beneficio de la sociedad, ya que permite a los modelos y sistemas de seguridad pública y defensa nacional contar con información en tiempo real para la localización de las personas, entre otras finalidades.
3. En el tema se pueden trastocar derechos humanos, como es el caso de la vida privada y la intimidad, ya que es posible contar con tecnología de reconocimiento facial y, por ende, se emplean datos biométricos que de alguna manera deben estar protegidos por los sujetos que los manejan, ya sea en el ámbito público o privado.
4. En nuestro país, con independencia de que la ponderación de derechos humanos sea llevada a cabo en sede administrativa o jurisdiccional, de inicio se requiere legislación adecuada que regule la utilización de las cámaras de video vigilancia para evitar la violación a los derechos humanos.
5. Hoy en día y derivado del paradigma constitucional de los derechos humanos, se requiere que las políticas públicas y las normas jurídicas protejan los datos personales y reduzcan la posible vulneración de derechos como son la imagen, el honor, la intimidad y la vida privada, entre otros, ya que, de lo contrario las libertades fundamentales de individuo se hacen nugatorias.

Referencias

- Agencia Española de Protección de Datos [AEPD]. (20 de mayo de 2023). http://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.
- Constitución Política de los Estados Unidos Mexicanos. DOF. 5/2/1919.
- Gobierno de la Ciudad de México. (30 de mayo de 2023). <https://gobierno.cdmx.gob.mx/noticias/crece-el-numero-de-camaras-del-c5/#:~:text=En%202018%20se%20ten%C3%ADa%20registro,es%20llegar%20a%2080%20mil>.
- Gómez, A. & Ornelas, L. (2006). *Protección de datos personales en México: El caso del Poder Ejecutivo Federal*, Porrúa, México.
- Gutiérrez, E. (2022), *El Patrimonio*, 12ª ed. Porrúa.
- IBM. (24 de mayo de 2023). <https://www.ibm.com/mx-es/topics/industry-4-0>
- IIJ – UNAM. (26 de mayo de 2023). Sentencia United States vs. Nixon. <https://lecturasconstitucionalesua.juridicas.unam.mx/sentencias-tseu/united-states-vs-nixon/>
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF 5/7/2010..
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. DOF 5/7/2010.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, DOF 26/1/2027.

Ley General de Transparencia y Acceso a la Información Pública. DOF 4/5/2015.

Ley Orgánica 13/1999 de Protección de Datos de Carácter Personal. (2023) BOE (298) 14 de diciembre de 1999. http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1999/23750

Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, (2023). BOE. (186). <https://www.boe.es/buscar/act.php?id=BOE-A-1997-17574#:~:text=La%20presente%20Ley%20regula%20la,utilizaci%C3%B3n%20pac%C3%ADfica%20de%20las%20v%C3%ADas>.

Montesquieu. (2018). *Del espíritu de la leyes*, Porrúa.

Muñozcano, A. (2010). El derecho a la intimidad frente al derecho a la información, Porrúa.

OIT (2021). Guía Práctica. *El teletrabajo durante la pandemia de COVID-19 y después de ella* https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_758007.pdf

ONU, 2023. (22 de mayo de 2023). <https://www.ohchr.org/es/special-procedures/sr-privacy>.

ONU. ACNUDH. (23 de mayo de 2023). Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. <https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf>

ONU. DUDH. (23 de mayo de 2023). <https://www.un.org/es/about-us/universal-declaration-of-human-rights>

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (24 de mayo de 2023). *Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública*. https://secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf.

Tepe, G., & Mucan Özcan, B. (2021). Review and Bibliometric Analysis of Industry 4.0 in Social Sciences, *Dumlupınar University Journal of Social*, (67), 159 – 175. <https://doi.org/10.512901/dpusbe.789178>

Universidad Católica de San Pablo, Perú. (26 de mayo de 2023). *Que es big data*. <https://postgrado.ucsp.edu.pe/articulos/que-es-big-data/>

Villanueva, E. (2008). El derecho de la información frente a los derechos de la personalidad. *Derecho Comparado de la Información*. IIJ – UNAM. México. (11). 131-152.

Capítulo 5

Videovigilancia: Las atribuciones de seguridad pública, retos y desafíos para la protección de derechos humanos

Video surveillance: Public security powers, challenges and challenges for the protection of human rights

*Maribel Luna Martínez**

Resumen

En México, la vigilancia con uso de medios electrónicos es una de las innovaciones que se han implementado como parte de las políticas de seguridad pública, como medida para eficientar el resguardo de las personas que transitan en las calles de las ciudades. Sin embargo, es incierto el uso y tratamiento que se le da a las grabaciones, cintas y demás información, pues pone de manifiesto violaciones al derecho humano a la intimidad, la protección de datos personales, la seguridad jurídica y el libre tránsito. La ciudadanía ignora si es o no constantemente vigilada, si las autoridades u otras personas tienen acceso a su persona, sus desplazamientos cotidianos y, más allá, si dicha información recibe un tratamiento que garantice el respeto a la protección de su privacidad e intimidad. A partir de un análisis de las políticas públicas y disposiciones que permiten y regulan la videovigilancia con interconexión y el uso inteligencia artificial en materia de seguridad pública en México, con apoyo del método descriptivo, se comprobará que existen violaciones a derechos humanos, provocando incertidumbre jurídica, vislumbrando la necesidad de legislar adecuadamente el uso y tratamiento de los dispositivos utilizados por las autoridades para realizar la videovigilancia, que permita generar certeza jurídica sujeta a los principios establecidos en el marco constitucional mexicano.

Palabras clave: Estado de derecho; Seguridad pública; Videovigilancia; Derechos humanos.

Abstract

In Mexico, surveillance with the use of electronic means is one of the innovations that have been implemented as part of public security policies, as a measure to improve the protection of

* Dra. en Derecho Público por el Instituto de investigaciones jurídicas de la Universidad Veracruzana, Docente de la Facultad de derecho

people traveling on city streets; however, it is uncertain. the use and treatment given to recordings, tapes and other information, as it reveals violations of the human right to privacy, the protection of personal data, legal certainty and free transit. Citizens do not know whether or not they are constantly monitored, whether the authorities or other people have access to their person, their daily movements and beyond, whether said information receives treatment that guarantees respect for the protection of their privacy and intimacy. Based on an analysis of public policies and provisions that allow and regulate video surveillance with inter-connection and the use of artificial intelligence in matters of public security in Mexico, with the support of the descriptive method, it will be proven that there are violations of human rights, causing legal uncertainty. envisaging the need to adequately legislate the use and treatment of the devices used by the authorities to carry out video surveillance, which allows generating legal certainty subject to the principles established in the Mexican constitutional framework.

Keywords: Rule of law; Public security; Video surveillance; Human rights.

Introducción

Los avances de la tecnología a partir de la década del año 2000 han transformado la rutina diaria de todos los seres humanos. En cuestiones de inteligencia artificial, mejoró la utilidad de los asistentes virtuales, así como el internet de las cosas, con la creación de dispositivos interconectados, como sucede en la creación de hogares inteligentes, los sistemas de automatización industrial, sistemas de videovigilancia que cuentan con captaciones de tipo sensorial, procesamiento en tiempo real, detección de eventos o comportamientos específicos, reconocimiento facial, lo que permite una gestión integral automatizada de la seguridad.

Esta revolución tecnológica ha provocado un impacto a las cuestiones esenciales de la vida de las personas desde las formas de comunicación, trabajo, convivencia social, imagen personal y pública hasta formar parte de políticas públicas diseñadas por gobiernos abiertos, en cuyo caso la tecnología es un elemento esencial, pues a través de las plataformas y herramientas se permite la recopilación, el procesamiento y la captación de información personal de los ciudadanos.

En el presente trabajo se analiza, a través de la metodología descriptiva, la función esencial de la seguridad pública diseñada por el Estado, la estrategia para la identificación de la comisión de conductas antijurídicas por medio de los dispositivos de videovigilancia, sus implicaciones y los retos que representa. Comprende tres ejes temáticos, el primero de ellos refiere a la seguridad pública y videovigilancia, cuyo propósito es analizar la seguridad pública, fines de creación y el poder coactivo del Estado, la videovigilancia como parte de las estrategias de seguridad pública, en el que se demostrará sus ventajas, como la prevención, la investigación y resolución en materia de delitos, el control de la seguridad en tiempo real a través de monitoreos que lo-

gran detectar situaciones de peligro como robo, actos de vandalismo y, en general, identificación de conductas presuntamente delictuosas.

El segundo eje temático refiere a la implementación de la tecnología, la inteligencia artificial y el internet de las cosas como parte de las políticas públicas gubernamentales, lo que representa un desafío, pues si bien su propósito es la protección de la seguridad de las personas, pone de manifiesto el respeto al derecho humano a la privacidad y a la protección de datos personales, lo cual ha requerido que los países regulen adecuadamente la videovigilancia en la vía pública, pues, de lo contrario, representa un acto de arbitrariedad de las autoridades.

En el último tema se plantea una propuesta respecto a la necesidad de implementar una regulación para el sistema de videovigilancia utilizado por las autoridades de seguridad pública en México al amparo de un sistema de principios, la cual tendrá por objeto generar certeza en el actuar de la función policial, de seguridad material y jurídica de los individuos, generando relaciones de equilibrio para el Estado y los ciudadanos.

I. Seguridad pública y videovigilancia

Existen distintas vertientes para estudiar el Estado, ya sea desde su aspecto bajo la cualidad de soberanía, o bien desde un aspecto subsidiario. En un estudio más integral, el Estado es un concepto político-jurídico; se define como “la organización política soberana de una sociedad humana, establecida en un territorio determinado, bajo un régimen jurídico con independencia y autodeterminación, con órganos de gobierno y de administración que persigue determinados fines mediante acciones concretas” (Acosta Romero, 2001).

Como elemento del Estado, el concepto de gobierno, en un sentido amplio, es sinónimo de poder supremo en una nación, es decir, que es la legislación, ejecución incluyendo la administración de justicia (Garza Salinas, 2012, p. 101). Por otra parte, la seguridad jurídica es un derecho inalienable para las personas que el Estado debe garantizar; en su actuación, el Estado no debe invadir la esfera de la vida privada de los ciudadanos, lo que debe observarse con la inclusión de la tecnología empleada como medida de protección ante la inseguridad (Ibarra Sánchez, 2010, p. 363), pues la paradoja es, un ciudadano protegido por cámaras de videovigilancia utilizados como forma preventiva y persuasiva de prevenir el delito y por otra parte la arista de un ciudadano controlado en cada movimiento.

Como lo señala González Fernández, el Estado de derecho genera las condiciones que permiten al individuo realizar sus actividades con la confianza de que su vida, familia, su patrimonio, y otros bienes jurídicos tutelados están exentos de todo peligro, daño o riesgo (González Fernández, 2012). Los ciudadanos requieren el respaldo institucional para crear ese sentido de confianza, pertenencia y respeto.

Desde la teoría del Estado garantista de Luigi Ferrajoli, la protección de los derechos humanos representa el límite del actuar de quiénes ostentan el poder, esto es, la subordinación de las autoridades al marco de legalidad con sujeción al respeto de los derechos fundamentales (Ferrajoli, 2001). Por ende, las estrategias de videovigilancia deben dirigirse para resguardar la seguridad física de las personas, sin trastocar los derechos de los individuos, pues primero debe verificarse el nivel de fiabilidad de los resultados de la información y la responsabilidad de quien la resguarde.

Pues bien, existen dos posturas teóricas al respecto: las sociedades de control y las sociedades disciplinarias. Las primeras se caracterizan por una constante vigilancia en sus efectos y tienen la particularidad de poder ser discontinua en su acción (Agustín, 2013, p. 19). Esto sucede en cualquier ciudad que utiliza la videovigilancia como medio de control. ¿Qué es lo que sucede con la cámara? ¿Dónde se almacena la información generada? ¿Funciona la cámara adecuadamente? ¿Quién la observa? ¿Cuáles son los propósitos? Estos y otros son los cuestionamientos planteados por los ciudadanos al sentirse vigilados, los cuales no son respondidos por el Estado.

Por lo que respecta a las sociedades disciplinarias, éstas funcionan con reglas y eventuales castigos establecidos por la autoridad; parecieran adoptar la tecnología más eficaz para cada situación particular. Según Foucault, en este tipo de sociedades el poder no se concentra en un solo poder de autoridad; se diluye en distintas instituciones. El poder disciplinario busca producir sujetos obedientes y normalizados, pero con miras a transitar las distintas formas de control (Foucault, 2006, pp. 75-79). Esto sirve de apoyo para diferenciar la naturaleza de la seguridad pública en los regímenes democráticos, distinguiéndola de los regímenes autoritarios.

En la concepción del Estado Moderno, el fundamento del poder político se entiende como el uso de la fuerza o coacción física, cuyos pensamientos filosófico-políticos liberales se fundamentan en la idea de soberanía y poder público, con una división de funciones (Ibarra Sánchez, 2010, p. 361), cuentan con atribuciones y competencias específicas, además que el involucramiento de la ciudadanía en la implementación de las políticas públicas se ha convertido en un requisito esencial para su aprobación.

Con la justificación del Estado Constitucional y democrático de derecho, la seguridad pública se transforma en seguridad ciudadana, cuyo fin es preservar libertades, proteger a los ciudadanos y generar entre ellos los sentimientos de seguridad (Serafin, 2018). De acuerdo con el Programa de las Naciones Unidas, la seguridad ciudadana es el proceso de establecer el orden civil democrático, eliminando las amenazas de violencia en la población, permitiendo una coexistencia pacífica y ciudadana; propone una estrategia para mejorar la calidad de vida (Programa de las Naciones Unidas, 2013).

De acuerdo con la Organización de los Estados Americanos, el concepto de seguridad ciudadana surge como resultado del distintivo de los regímenes demócratas y los regímenes autoritarios (Americanos, 2009); esto es, no solo implica el control del

Estado como parte de sus atribuciones coactivas para hacer cumplir sus determinaciones, sino el involucramiento de los ciudadanos para sujetarse a los mecanismos de seguridad como deber para disfrutar de un lugar seguro y en paz.

El Estado, como ente regulador y protector de su población, cuenta con amplias atribuciones para brindar la seguridad pública como forma de garantizar la paz y la armonía entre sus ciudadanos. El Sistema Nacional de Seguridad Pública fue creado mediante decreto publicado en el Diario Oficial de la Federación el 31 de diciembre de 1994. En la misma fecha, se reformaron los artículos 21 y 73 fracción XXIII de nuestra Constitución Política de los Estados Unidos Mexicanos; así también, se reformó la entonces Ley Orgánica de la Administración Pública Federal en lo relativo a las funciones de la Secretaría de seguridad pública (Diario Oficial de la Federación, 1994). Posteriormente, se promulgó la ley reglamentaria de la materia denominada Ley General del Sistema Nacional de Seguridad Pública, publicada el dos de enero de 2009, misma que ha sufrido diversas reformas, siendo la última el veinticinco de abril del año dos mil veintitrés.

Históricamente, el país ha enfrentado diversos desafíos en este ámbito, como el crimen organizado, la violencia o la corrupción, lo que ha llevado a sus instituciones a implementar diversas estrategias para hacer frente a estos problemas. Una de las estrategias ha sido el plantear políticas públicas para fortalecer las capacidades de seguridad pública y promover la participación ciudadana en la prevención del delito.

Las políticas públicas en materia de seguridad pública implementadas por el gobierno federal de este sexenio son la guardia nacional como organismo al servicios de la sociedad civil, fortaleciendo la policía estatal y en algunos casos las municipales a la postre del modelo de justicia penal acusatorio, ajustados al Plan Nacional de Desarrollo 2018-2024, trazando dentro de sus objetivos, el erradicar la corrupción y reactivar la procuración de justicia; garantizar empleo, salud y bienestar; pleno respeto a los derechos humanos; regeneración ética de las instituciones y de la sociedad; reformular el combate a las drogas y articular la seguridad nacional, la seguridad pública y la paz (Plan Nacional de Desarrollo, 2018).

En su artículo 2, la Ley General del Sistema Nacional de Seguridad Pública (2009) establece que: “la seguridad pública es una función a cargo de la Federación, las entidades federativas y municipios, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos”. En el referido precepto se prevé que la seguridad pública de los individuos es responsabilidad del Estado, como forma de garantizar los derechos fundamentales en México.

La seguridad pública en su operatividad y nivel de eficacia es compleja, ya que involucra no solo a las instituciones de seguridad, sino a las causas que generan la conflictiva social, las cuales requieren atención, tales como el desarrollo social, la

educación, la salud y la generación de empleo. En México este tema guarda gran complejidad, ya que la inseguridad es un problema social grave y diverso, de acuerdo con las regiones del país.

El panorama de la seguridad pública en México resulta un desafío representativo del Estado de derecho, pues existe la percepción ciudadana de cierta incapacidad de resolver los problemas graves en la materia, resultando en una pérdida de confianza en las instituciones por no tener el control del índice de criminalidad y la prevención adecuada del delito por parte del Estado; además, desde la perspectiva jurídica, política, territorial y social existen obstáculos de índole estructural (Benítez Manaut, 2016, p. 116). De acuerdo con los índices reportados por la OCDE, en el año 2018 solo el 42% de las personas afirmó sentirse seguro al caminar por la noche, lo cual representa una de las tasas más bajas de los países miembro que integran dicho organismo, lo que significa una desventaja competitiva (Seguridad, 2018).

Jasso López refiere que en las ciudades existen dos temores que organizan los miedos que moldean la ciudad. El primero corresponde a la desigualdad económica, que ha servido para justificar la implementación de las nuevas tecnologías de exclusión urbana; y el segundo, se refiere al desconocimiento de los otros, esto es los sujetos alternos que producen desconfianza (Cortés, 2010, p. 7 citado por Jasso López, 2023, p. 24), motivos en los que se fundamenta la intensificación de las políticas de control ciudadana.

En la década de los años 2000, los avances de la tecnología, internet y redes de comunicación permitieron la implementación de las cámaras de videovigilancia IP, las cuales permiten transmitir en tiempo real a través de redes IP (protocolo de Internet), lo que facilita la visualización remota y el almacenamiento de servidores. Actualmente, las cámaras de videovigilancia han avanzado a pasos agigantados en cuanto a calidad, tamaño, facilidad de uso y capacidades. Algunas cuentan con detección de movimiento, sistemas de reconocimiento facial y el acceso remoto de aplicaciones móviles.

Tellez Valdés (2007, p. 2) señala que un sistema automático de videovigilancia incluye tareas de localización de objetos, seguimiento visual, clasificación de objetos y reconocimiento de actividades y acciones humanas, significando un control más preciso de las acciones realizadas por los ciudadanos en tránsito, lo que pone de manifiesto la invasión en el ejercicio de sus libertades.

En ese sentido, la instalación de cámaras de videovigilancia en las urbes surgió como medida de prevención para mitigar la comisión de delitos; representan un elemento disuasorio, pues buscan limitar las conductas delictivas al considerar que los individuos se inhiben al sentirse observados, además de que las captaciones que realizan se consideran un medio de prueba en los casos de investigación ministerial y jurisdiccional. No obstante, no es el único objetivo en esencia de la seguridad pública, al respecto señala Jasso (2023):

La vigilancia es característica de las sociedades disciplinarias en las que se trata de ejercer el mayor control social posible. En estas sociedades, la mirada permanente y el escudriñamiento de la sociedad a través de las tecnologías de la vigilancia, es la posibilidad de ejercer el poder. (p. 28)

Los trayectos de calles, avenidas, carreteras de tránsito nacional, aeropuertos, terminales de autobuses, parques, centros comerciales, fraccionamientos privados, por mencionar los más frecuentes, están cubiertos de cámaras que, en su mayoría, no pueden ser identificadas a simple vista por los transeúntes; sin embargo, la videovigilancia traspasa la identificación de personas. En esencia, busca hacer un seguimiento individual por medio de un GPS (sistemas de posicionamiento global, chips RFID (identificación por radiofrecuencia), un GIS (sistema de información geográfica) y tarjetas inteligentes de identificación o señales de radio emitidas por teléfonos móviles u ordenadores portátiles (Tellez Valdés, 2007, p. 3).

Los sistemas de videovigilancia se diseñaron para la prevención de crímenes; empero, en la medida en que la tecnología se ha ido perfeccionando, su uso comprende, además, la identificación de otro tipo de infracciones de naturaleza administrativa, como la captación de personas que arrojan basura, aparcamiento en lugares prohibidos y, en algunos de los casos, las infracciones a los reglamentos de tránsito en los ámbitos local y federal, las que también serán sancionadas por los ordenamientos correspondientes.

En el régimen jurídico español, los principios que prevalecen respecto a la captación de imágenes en orden a la vigilancia de personas y lugares en una investigación, son válidas siempre que se produzcan en un espacio público fuera del domicilio, respetando los derechos fundamentales de fundamentación y motivación, por delito grave, cuando no existen otros medios para conseguir el fin conseguido. Dichos medios de convicción ostentan valor probatorio siempre y cuando se hayan respetado las debidas garantías y formalidades (Navarro Miranda, 2012, p. 99).

En México existe una iniciativa de ley general de videovigilancia, cuya propuesta data del año 2015, la cual está pendiente de dictaminarse en la cámara de senadores. No obstante, las entidades federativas que cuentan con una regulación en materia de videovigilancia son la Ciudad de México con el pronunciamiento de la Ley que regula el Uso de Tecnología para la Seguridad Pública promulgada en el año 2008 (Ley que regula el uso de tecnología la seguridad pública del Distrito Federal, 2020), Aguascalientes, Baja California Sur, Colima, Durango, Nuevo León, mientras que para el estado de Morelos, en el año 2023, la Suprema Corte invalidó la Ley de videovigilancia del Estado por irregularidades en el proceso legislativo, consecuencia de una acción de inconstitucionalidad promovida por la Comisión Nacional de Derechos Humanos.

Se advierte que en el sistema jurídico mexicano existe una ausencia de regulación del sistema de videovigilancia general como forma de prevenir el delito e identificar los momentos de su comisión, que defina los criterios de cumplimiento, las medidas de observancia por parte de las autoridades, con apego irrestricto a los derechos humanos de los individuos, de conformidad alineadas a la política pública en la materia.

Al respecto, la Suprema Corte de Justicia de la Nación señala los requisitos para detectar la comisión de delitos por medio de videovigilancia, mediante la tesis “Detención en flagrancia. Requisitos para que se actualice cuando la policía advierte hechos delictivos por medio de cámaras de videovigilancia” (Semanario Judicial de la Federación y su Gaceta, 2022, p. 4652), los cuales son los siguientes:

- i. el agente perciba por dichas cámaras y en tiempo real los hechos;
- ii. aportar a otros elementos policiacos que se encuentren el lugar datos idóneos que les permitan identificar y detener en ese propio momento al sujeto activo, o bien perseguirlo inmediata e ininterrumpidamente.

En la referida tesis (Semanario Judicial de la Federación y su Gaceta, 2022) se señala que la flagrancia no es incompatible con el uso de la tecnología, no obstante, no debe constituirse como el único medio de convicción para la imputación de un delito, sino que debe ser utilizado como herramienta para corroborar la información aportada por los elementos policiacos que intervinieron en la detención respecto de la existencia del delito y la intervención del detenido en su comisión.

II. Derechos Humanos

Sanchez Barrilao señala que la sociedad enfrenta el conflicto entre la dignidad humana y las transformaciones que la sociedad tecnológica supone; el Estado atraviesa una crisis en su responsabilidad de garantizar los derechos fundamentales de su población (Sánchez Barrilao, 2023, p. 161) y, por otro lado, la vulnerabilidad que enfrenta respecto a los avances de la tecnología de la información y la comunicación, la inteligencia artificial, por lo que debe implementar políticas que preserven los derechos de los individuos en cuanto a su dignidad, privacidad, intimidad y sus datos personales.

El derecho a la vida privada es un derecho humano reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, la cual establece que: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Naciones Unidas, 1948).

Dentro del rubro del derecho a la intimidad de las personas, el Alto Comisionado de las Naciones Unidas define la privacidad como:

[...] la presunción de que el individuo debe tener una esfera de desarrollo autónomo, intervención y libertad; una esfera privada con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva de otros (Alto Comisionado de las, 2018, p. 3).

Asimismo, el Alto Comisionado de las Naciones unidas refiere que el derecho a la privacidad comprende la información sustantiva de comunicaciones, los metadatos, cuyo alcance integra información relativa a las preferencias privadas, la identidad de la persona. Este derecho no se limita a los espacios privados, como su domicilio, sino se extiende a los espacios públicos y a la información de acceso público (Alto Comisionado de las, 2018), lo que resulta cotidiano, tal es el caso de la vigilancia en una institución bancaria, en el supermercado o en alguna terminal de autobuses.

El derecho fundamental a la privacidad comprende los siguientes ejes:

- a) Derecho a la vida privada, comunicaciones personales, cuestiones de salud, relaciones, actividades en el hogar, entre otras;
- b) Confidencialidad y secrecía de las comunicaciones, implica el resguardo en correos electrónicos, mensajes de texto, llamadas telefónicas;
- c) Protección de datos personales, lo cual implica la reserva en el uso y divulgación de estos datos;
- d) Domicilio y espacio personal;
- e) Protección contra la vigilancia y el seguimiento; las personas tienen derecho a estar protegidas contra la vigilancia y el seguimiento no autorizado por parte de entidades gubernamentales.

Con los cambios vertiginosos que se suscitan en materia de tecnología de la información y la comunicación, la capacidad de análisis basada en datos continúa fortaleciéndose, pues la inteligencia artificial permite a los gobiernos y a las empresas obtener información cada vez más específica de las personas; ya que identificar y predecir perfiles detallados de la personalidad, clasifica, evalúa, al grado de tomar decisiones respecto de ellas (Alto Comisionado de las, 2018), lo que lleva a repensar los derechos de la privacidad y la ideología de los individuos.

En Europa la videovigilancia se ha implementado como parte de su política criminal, pues se asume como un instrumento eficaz para la prevención y la persecución de delito y para la protección de la seguridad ciudadana. A pesar de ello, se reconoce que existen abusos de derechos producidos por las técnicas aplicadas a la vigilancia por la reproducción ilícita de imágenes y sonidos (Cataoira, 2003, p. 23).

Proteger el derecho humano a la privacidad representa diversos desafíos, los cuales se suscitan al momento de que la información personal es analizada por otro ser humano o por la inteligencia artificial. Por tanto, el alcance de la videovigilancia es la captación de datos personales, así como la imagen personal definida como un medio para identificar a la persona; ambas comprenden el concepto de “datos personales” (Ibarra Sánchez, 2016, p. 235). Estos perfiles representan parte de la esencia de los individuos.

El derecho a la protección de datos personales tiene como principio que cada individuo cuenta con la libertad de decidir qué información personal desea compartir, el tratamiento que pretende darle y a quién le quiere proporcionar esta información. De ahí la justificación que debe otorgar su consentimiento para externar dicha información personal.

En la era de la información, la importancia de los datos personales radica en el valor económico en una sociedad globalizada, pues la mayoría de las operaciones están automatizadas y, más allá de esto, es posible el conocimiento completo y exacto sobre las cosas o las personas (Ibarra Sánchez, 2016, p. 245). La garantía de este derecho resalta su importancia en la era digital, pues el procesamiento de la información personal es casi obligatorio su transmisión para que las personas puedan realizar sus actividades cotidianas, tales como trámites de identidad, ante autoridades administrativas, operaciones bancarias, ingreso a recintos laborales, estadía en centros comerciales, entre otros.

En cuanto a un criterio interpretativo, la Suprema Corte de Justicia de la Nación, respecto al derecho a la protección de la vida privada protegida en la Convención Americana de Derechos Humanos y la Convención de los derechos de niños, se ha pronunciado que:

[...] su significado atañe a la esfera de la vida en la que las personas pueden expresar libremente su identidad, en sus relaciones con los demás o en lo individual, y destacan su vinculación con un amplio abanico de otros derechos, como la inviolabilidad de la correspondencia y de las comunicaciones en general, la inviolabilidad del domicilio, las garantías respecto de los registros personales y corporales (SCJN, 2009).

Al respecto, la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6º, apartado A, fracción II, establece que: “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” (Constitución Política de los Estados Unidos Mexicanos, 2023, p. 12), de manera que la información videograbada contiene información y datos personales de los individuos, los cuales están sujetos al régimen constitucional. Surge así un cuestionamiento inevitable: ¿cuál es el tratamiento que se provee para las grabaciones generadas por los dispositivos de videograbación?

Para ello, los derechos fundamentales reconocidos por el Estado Mexicano respetan la libertad del individuo respecto del tratamiento de sus datos personales, la decisión de con quien compartir, atributos que deben respetar las autoridades. En el artículo 16, párrafo segundo, de la Constitución Mexicana, se establece que:

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, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros (Constitución Política de los Estados Unidos Mexicanos, 2023, p. 17).

En el año 2002, con la expedición de la Ley Federal de Transparencia, se incorporó en México la protección de datos personales como contrapeso al derecho de acceso a la información, aceptando la relación del derecho a la privacidad, a la intimidad y a la protección de datos personales. En ese actuar, la Ley General de datos Personales en Posesión de sujetos obligados vigente en su artículo 3°, establece que:

Artículo 3° Para efectos de esta 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;

X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

El derecho a la imagen se ubica en la categoría de los comprendidos en el derecho a la intimidad y la personalidad; se considera un derecho subjetivo al tratarse de una facultad personalísima de captar, imprimir, difundir o distribuir la imagen, o bien cuando la imagen conlleva beneficios económicos, como el caso de artistas, deportistas, entre otros (Flores Avalos, 2006). Del mismo modo, también comprende el derecho a permitir o prohibir su difusión, su reproducción o bien su propagación; evidenciando la paradoja en relación con las videograbaciones realizadas por los dispositivos en la vía pública ante la protección al derecho humano a la personalidad.

En un análisis de derecho comparado, el sistema jurídico español, en su Constitución, reconoce el derecho a la imagen como parte del derecho humano a la intimidad e inviolabilidad del domicilio, el cual establece, en su artículo 18 “18: 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”. Al respecto, Moreno Flores define el propósito del derecho a la intimidad el delimitar, evitar o sancionar toda acción tendiente a la intromisión física, la publicación de material personal considerado perjudicial o embarazoso o la publicación de fotografías o grabaciones de un individuo que se hayan realizado sin su consentimiento (Moreno Flores).

El derecho a la imagen comprende el derecho de la personalidad, que faculta a la persona para impedir que su apariencia física y/o su voz sean reproducidos de cualquier manera si ella no otorga su consentimiento. Los derechos a la imagen y a la voz se extienden a la familia; se requiere fortalecer la cultura del respeto para la debida protección jurídica (Flores Avalos & Pérez García, Junio de 2019).

El consentimiento del individuo es toral en la protección y ejercicio de este derecho. La complejidad de la instalación de las cámaras de videovigilancia en la vía pública ha generado polémica entre los individuos, pues éstas captan a cualquier individuo sin un criterio posible establecido, ni circunstancias específicas de forma indiscriminada, como es el caso de los menores, pues son dispositivos productos de la inteligencia artificial y su algoritmo no logra tal precisión. Esto puede generar un cambio en la conducta del individuo en grupo de acuerdo con las normas y valores sociales, pues el estar observado modifica el comportamiento de los grupos.

La observación prolongada y detallada modifica la conducta. La respuesta de las personas al sentirse observadas no es la misma; hay un impacto psicológico que modifica el comportamiento, lo cual constituye una intromisión a la privacidad, como puede ser el hecho de que en una manifestación la videovigilancia en la vía pública constituirá una amenaza para el derecho a la libertad, de movimiento y expresión de las personas (Agustín, 2013, p. 15).

Al respecto, el Estado requiere establecer políticas públicas que comprendan el entramado funcional de las instituciones, un marco regulatorio estandarizado que apremie el respeto a los derechos a la intimidad, la personalidad y privacidad de las personas privilegiando el interés superior del menor, pues, como se señala en el presente, los dispositivos de videovigilancia no disciernen a detalle la información. No obstante, los gobiernos justifican su utilidad como medida para prevenir el delito.

III. Propuesta

El uso de dispositivos tecnológicos representa una medida de disuasión en las políticas de seguridad pública de los gobiernos; se han convertido en una práctica cotidiana para la vigilancia de las personas como parte de la actuación de las instituciones policiales especializadas. Los sistemas de videovigilancia instalados en las ciudades forman

parte de la estrategia para la prevención e investigación de los delitos; sin embargo, no existen parámetros estandarizados acerca de la instalación, tratamiento, almacenamiento e incluso funcionamiento del sistema de videovigilancia.

Atendiendo a la característica de progresividad de los derechos humanos y la estrecha relación con la revolución tecnológica, se deben marcar las pautas relativas a la captación con fotografías e imágenes de las personas, identificación de su movimiento y desplazamiento, pues tales acciones comprenden o trastocan derechos inherentes al ser humano, como a la identidad, a su personalidad, a la protección de datos personales y a la libertad de movimiento y de tránsito.

El Alto Comisionado de Naciones Unidas (2018) admite que existe una falta generalizada en el orden mundial en la regulación sobre el derecho a la privacidad, ante las carencias de una legislación especializada en los Estados que garanticen un nivel adecuado de la protección de datos personales. En nuestro país, los sistemas de videovigilancia forman parte de las estrategias de seguridad pública para prevenir e identificar las conductas constitutivas de delito o de infracciones; no obstante, aún presentan retos para su funcionamiento, utilidad y eficiencia, pues existen prácticas desvirtuadas en su manejo y resguardo.

En México, formalmente solo seis entidades federativas cuentan con un marco normativo para el uso, funcionamiento y mecánica de los sistemas de videovigilancia. La Ley General del Sistema Nacional de Seguridad Pública tiene como objeto salvaguardar la integridad y derechos de las personas, comprendiendo la prevención y persecución de los delitos; sin embargo, requiere de criterios precisos respecto a la protección al derecho de imagen, libertad y privacidad personal, así como los lineamientos en cuanto al funcionamiento, alcances y límites de los sistemas de videovigilancia, tales como las fallas en el suministro de energía eléctrica, fallas en las videocámaras por la pérdida parcial o total de las imágenes, y el que en algunos puntos de las ciudades las videocámaras no funcionan por completo.

Luego entonces, los sistemas de videovigilancia pueden tener repercusiones en su eficacia, la densidad (número de cámaras por zona), cobertura de la zona (área de cámaras que pueden ver) y el posicionamiento de las mismas. La iluminación de la zona influye para tener una mejor captación y evitar puntos ciegos (Nobili, 2023, p. 102), significando un reto para las cuestiones técnicas en el uso de la videovigilancia en México.

Por estas razones, es oportuno que el poder legislativo proponga una norma con efecto *erga omnes*, que regule la videovigilancia, cuyo fundamento debe considerar los siguientes aspectos:

- 1) Objeto, alcances y fines de los sistemas de videovigilancia como parte de las estrategias de prevención e investigación del delito;

- 2) Planteamiento de los principios y lineamientos del marco legal para garantizar la seguridad, protección de los ciudadanos, y de otros bienes jurídicos tutelados como la imagen, la privacidad y la intimidad;
- 3) Promoción de la colaboración del sector público, el sector empresarial y la comunidad para prevenir, investigar y combatir la delincuencia;
- 4) Implementación de las campañas de prevención y educación a la comunidad;
- 5) Definición del marco de distribución de competencias de las fuerzas policiales y de seguridad, comprendiendo la coordinación para la colaboración en los tres órdenes de gobierno;
- 6) Formalizar las áreas de supervisión y control, cuyo fin sea la transparencia y rendición de cuentas, además de crear un área autónoma para atender las denuncias de la ciudadanía, así como establecer los requerimientos de altos valores éticos del personal a cargo del manejo de dicha información;
- 7) Se torna imperante proponer lineamientos generales para la instalación de las cámaras, puntos de referencia, distancia entre una cámara y otra, características y tipos de dispositivos de videograbación, mantenimiento y supervisión; esto es, el monitoreo del funcionamiento técnico y de ingeniería de éstas, procedimiento de acceso, almacenamiento de la información, temporalidad de su resguardo y las generalidades de la big data.

En dichos criterios también se podrá contemplar un marco parametrizado de la asignación de recursos, criterios para el cálculo del presupuesto estándar en su implementación y mantenimiento del sistema.

No debe pasar inadvertido que en el orden internacional existen propuestas encaminadas a regular el intercambio de información interestatal, comprometiendo la posibilidad de que la información vertida en las videograbaciones se torne un medio de convicción relacionado con procedimientos que se instauren en otros Estados en la procuración de justicia, lo cual se deja como tema pendiente, ya que se tendrá que plantear la salvaguarda de los derechos humanos.

Otro aspecto por considerar es el procedimiento de petición de información entre autoridades sin transgredir la esfera jurídica de los ciudadanos y a los principios de legalidad, fundamentación y motivación, pues, si bien se consideran trámites de naturaleza administrativa, por la sensibilidad de la información es menester definir sus limitantes, así como prever las prohibiciones relativas a los requerimientos de información para el caso de particulares.

Asimismo, la función gubernamental debe disponer de mecanismos de reparación en caso de transgresiones a víctimas de vulneraciones a los derechos de privacidad, intimidad, entre otros cometidos por los Estados o por particulares, los cuales deben

comprender tipologías de reparación eficaces, según la naturaleza del caso y el contexto de los acontecimientos.

Conclusiones

Ante los cambios vertiginosos y acelerados, la tecnología y la inteligencia artificial, los cuales agilizan, automatizan y facilitan las actividades diarias de los individuos, se han convertido en artefactos ineludibles para su subsistencia, lo cual no es limitativo para los seres humanos, sino también para las instituciones gubernamentales, al incluirlos como herramientas para eficientar las políticas y estrategias planteadas en su rectoría gubernamental, como es el caso de estudio, las cámaras de videovigilancia como estrategia para la prevención, identificación e investigación de delitos u otros actos delictivos.

En nuestro país, la seguridad pública está organizada por competencias específicas distribuidas en los tres órdenes de gobierno; sin embargo, los índices de inseguridad concluyen que las personas que transitan en vía pública en México no se sienten seguras. Por ello, la política de seguridad pública ha intensificado las estrategias para vigilar el actuar de las personas que transitan las calles, parques, centros comerciales, entre otros. No obstante, a pesar de que las ciudades cuentan con un sistema tecnológico de videovigilancia, en nuestro país carecemos de una ley general que contemple el uso y tratamiento de datos contenidos en el referido sistema, pues, a la fecha, solo seis entidades federativas han legislado del tema.

Es necesario proponer un ordenamiento legal que equilibre las relaciones de Estado y sociedad. Para ello, se requiere establecer una regulación sólida que cumpla con los principios establecidos en nuestra Constitución Mexicana, esto es, garantizando los derechos humanos contenidos en ella, creando las condiciones necesarias para actuar con respeto a la legalidad, a la seguridad jurídica, al marco de una debida fundamentación y motivación, que generen fiabilidad de los ciudadanos en las instituciones de seguridad pública.

Se advierte, además, la consolidación de los sistemas de videovigilancia en cuanto al resguardo y protección de la información, grabaciones, generación de información, tiempo de resguardo y un mecanismo eficaz para rendir a las autoridades competentes la información idónea con motivo de los procedimientos en que represente un medio de convicción.

Referencias

- Acosta Romero, M. (2001). *Derecho Administrativo*. México: Porrúa.
- Agustín, F. (2013). Ingeniería y Sociedad de control: sobre diseño y videovigilancia pública. Tecnología y Sociedad. *Revista del Centro de Estudios sobre Ingeniería y Sociedad*. Obtenido de <http://bibliotecadigital.uca.edu.ar/repositorio/revistas/ingenieria-sociedad-control-diseño.pdf>
- Alto Comisionado de las Naciones Unidas (2018). *El derecho a la privacidad en la era digital*.
- Benítez Manaut, R. (2016). México: seguridad ciudadana, conflictos y orden público. *Atlas de la Seguridad y la defensa de México*.
- Cataoira, A. (2003). La videovigilancia y la Garantía de los Derechos individuales: su marco jurídico. (U. d. Coruña, Ed.) *Anuario de Facultad de Derecho da Universidade da Coruña*.
- Constitución Política de los Estados Unidos Mexicanos. (29 de mayo de 2023). *Diario Oficial de la Federación*. Obtenido de <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>
- Diario Oficial de la, F. (31 de diciembre de 1994). Reforma a artículos de la Constitución. *Diario Oficial de la Federación*.
- Flores Avalos, E. L., & Pérez García, X. (Junio de 2019). Protección al derecho a la imagen y a la voz ante las tecnologías. (U. N. México, Ed.) *Estudios de Derecho a la información*(7).
- Flores Ávalos Elvia Lucía, Derecho a la Imagen y a responsabilidad civil, en Adame Goddard Jorge, Derecho Civil y Derecho Romano, (p. 372) México. México. Instituto de Investigaciones Jurídicas. UNAM
- Foucault, M. (2006). *Seguridad, territorio y población*. (P. Horacio, Trad.) Argentina : Fondo de Cultura Económica Argentina .
- Garza Salinas, M. A. (2012). Políticas Públicas y Seguridad. En P. J. Peñaloza, & M. Garza Salinas, *Los desafíos de la seguridad pública en México* (pág. 101). México: Instituto de Investigaciones Jurídicas UNAM.
- González Fernández, J. (2012). La seguridad pública en México. En L. d. México, *La seguridad pública en México* (pág. 125). México, México: Instituto de Investigaciones Jurídicas. Recuperado el 15 de mayo de 2023, de <https://archivos.juridicas.unam.mx/www/bjv/libros/1/419/12.pdf>
- Ibarra Sánchez, E. (2010). Videovigilancia y Seguridad Pública. En T. V. A., *Memorias del XIV Congreso Iberoamericano de Derecho Informático*.
- Ibarra Sánchez, E. (2016). Videovigilancia Punto de colisión entre derechos fundamentales, seguridad y protección de datos personales en México. En E. Ibarra Sánchez, & R. Romero Flores, *Jurismática: El Derecho de las Nuevas Tecnologías*. Instituto de Investigaciones jurídicas UNAM.
- Jasso López, C. (2023). *La ciudad videovigilada entre la prevención del crimen y el control social*. México: Instituto de Investigaciones Jurídicas UNAM.
- Ley General del Sistema, N. (2 de enero de 2009). *Federación Diario Oficial de la*.
- Ley que regula el uso de tecnología para el uso de tecnología para la seguridad pública del Distrito Federal. (16 de Diciembre de 2020). *Gaceta Oficial de la Ciudad de México*.

Capítulo 5. Videovigilancia: Las atribuciones de seguridad pública, retos y desafíos para la protección de derechos humanos

- Moreno Flores, A. (s.f.). *Suprema Corte de Justicia de la Nación*. Obtenido de Derecho a la intimidad su significación y regulación en el derecho español y mexicano: https://www.scjn.gob.mx/Transparencia/Documents/Becarios/Becarios_003.pdf
- Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos*. Obtenido de <https://www.un.org/es/about-us/universal-declaration-of-human-rights>
- Navarro Miranda, J. R. (2012). La seguridad ciudadana y las videograbaciones en lugares públicos. En G. d. Canarias, *Seguridad Urbana, urbanismo y entornos urbanos*. Dykinson.
- Organización de Estados Americanos [OEA]. (31 de diciembre de 2009). *Informe sobre seguridad ciudadana y Derechos humanos*. Obtenido de <https://www.cidh.oas.org/countryrep/Seguridad/seguridadii.sp.htm>
- Programa de las Naciones Unidas. (febrero de 2013). Obtenido de Seguridad Ciudadana : [https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief%20\(spanish\).pdf](https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief%20(spanish).pdf)
- Sánchez Barrilao, J. F. (2023). Transformaciones en la protección pública de los derechos. En A. Uscanga Barradas, C. Reyes Díaz , & A. M. Peña Freire, *Los derechos como límites al poder*. Instituto de Investigaciones Jurídicas UNAM.
- Semanario Judicial de la Federación y su Gaceta, u. é. (14 de junio de 2022). Tesis (A): 1a. XV/2022. V(Reg.dígital 2024749). México.
- Serafin, O. O. (2018). Algunas Reflexiones sobre la Seguridad Pública y la Seguridad ciudadana. En *Derechos humanos, seguridad humana, igualdad y equidad de género* (pág. 314). México, México: Comisión Nacional de Derechos Humanos. Obtenido de <http://www.cndh.org.mx/>
- Suprema Corte de Justicia de la Nación [SCJN]. (2009). Derecho a la Vida Privada Su contenido general. *1a. Sala SCJ y su gaceta 9a. época*.
- Tellez Valdés, J. (2007). *Regulación jurídica de la videovigilancia*.

Capítulo 6

Videovigilancia como política pública de seguridad ciudadana y su vinculación con los derechos humanos

Video surveillance as a public policy for citizen security and its connection with human rights

*Petra Armenta Ramírez**
*Alejandra Cuevas Ramírez***

Resumen

El presente trabajo de investigación pretende explicar el fenómeno de la videovigilancia como política pública de seguridad ciudadana y su relación directa con los derechos humanos a la privacidad, protección de datos personales y la seguridad ciudadana. La metodología que se utilizó en el presente trabajo fue cualitativa documental, basándose en el análisis y recolección de datos a partir de revistas, libros y artículos académicos. De los datos recabados y del estudio de la normatividad vigente a nivel estatal y federal, pudimos determinar cuáles son los estados de la República que han adoptado dentro de sus reglamentos o legislación conceptos sobre videovigilancia y su aplicación.

Palabras clave: Videovigilancia; Seguridad ciudadana; Protección de datos personales; políticas públicas.

* Doctora en Derecho Público por la Universidad Veracruzana (UV), Licenciada en derecho (UV), Profesora – investigadora de tiempo completo del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana, es miembro del Sistema Nacional de Investigadoras e Investigadores (SNI) Nivel I por el CONACYT. Email: parmenta@uv.mx

** Licenciada en Derecho con mención honorífica por la Universidad Veracruzana. Ex Becaria del “Programa Semilla” del Centro de Estudios sobre la Enseñanza y el Aprendizaje del Derecho, A.C. Ha realizado movilidades académicas por estudios e investigación en León, España, Cartagena, Colombia y Buenos Aires, Argentina. Email: alecuevasr1@gmail.com.

Abstract

This research work aims to explain the phenomenon of video surveillance as a citizen security politic public and its direct relationship with the human rights to privacy, personal data protection and citizen security. The methodology used in this work was qualitative documentary, based on the analysis and collection of data from journals, books and academic articles. From the data collected and the study of the current regulations at state and federal level, we were able to determine which states of the republic have adopted within their regulations or legislation, concepts on video surveillance and its application.

Keywords: Videosurveillance; Public security; Personal data protection; Public policy.

Introducción

El concepto de seguridad se encuentra estrechamente relacionado y vinculado con el de vigilancia; contrario a éste, la inseguridad, entendida como un desorden social y económico que justificará la intervención de poderes gubernamentales dentro del espacio público para su contención.

La videovigilancia sirve como una herramienta que distintos países han utilizado o comienzan a utilizar como medida de seguridad en los espacios públicos y privados. Ejemplo de ellos podemos mencionar a España y Reino Unido, en el caso del occidente, y Argentina, Brasil, Bolivia, Colombia, Costa Rica, Ecuador, México, Nicaragua, Perú y el Salvador en América Latina.

Si queremos referirnos al término videovigilancia, podemos recurrir al Diccionario panhispánico del español jurídico, que la define como aquella captación de imágenes a partir de cualquier medio de grabación que tendrá como finalidad la “prevención y la persecución de los delitos” (Panhispánico, 2023).

La videovigilancia repercute en el actuar de la población, inhibiéndola de cometer un delito. Como ya se mencionó, es un método o herramienta que utilizan algunos países para regular la seguridad pública. La autora Carmina Jasso ha explicado que la videovigilancia puede ayudar a disminuir el problema público de la violencia y por lo tanto, “la incidencia delictiva desde su prevención, actuando como un agente disuasor” (Jasso López, 2023, p. 47). Además, explica que funciona como un complemento para los agentes policiales, pues permite vigilar diferentes lugares y circunstancias de forma remota que, en ocasiones, por el estado de fuerza que involucran, se convierten en riesgosas (Jasso López, 2023, p. 47).

Siguiendo a Jasso, la videovigilancia podemos entenderla como aquella herramienta que busca contribuir con el fomento de la seguridad ciudadana, involucrando el orden y control urbanos, de modo que las autoridades puedan identificar las problemáticas políticas, sociales, económicas o culturales sin la necesidad de encontrarse de

forma física en el lugar donde se desarrollan y, aun así, controlando lo que ocurre (Jasso López, 2023, p. 47).

Para que la videovigilancia pueda aplicarse y funcionar dentro de cada país, han tenido que adecuarse los marcos normativos internos, de modo que puedan garantizar la seguridad de los habitantes. (Moreno Pérez & Hernández Olascoaga, 2018, p. 10). A continuación, se mencionan algunos ejemplos.

En el caso de Reino Unido, Gran Bretaña se considera uno de los lugares con más videovigilancia del mundo, con un número de 4.2 millones de videocámaras por persona, garantizando que espacios como “centros urbanos, autopistas, hospitales, bancos, escuelas, centros comerciales, transporte público y ferrocarril” (Moreno Pérez & Hernández Olascoaga, 2018, p. 11) se encuentran vigilados.

España, por su parte, específicamente en Madrid, desde la década de los 80s cuenta con un marco normativo que protege los datos personales de sus habitantes. Mientras que, en los 90s, se consolida la regulación del uso de la videovigilancia a través de cuerpos de seguridad. Para el año 2006 se regula lo relativo al uso y tratamiento de aquellas imágenes que son captados por videos (Moreno Pérez & Hernández Olascoaga, 2018, p. 11).

En Latinoamérica, la videovigilancia surge a partir de una necesidad que buscaba atender y procurar la seguridad pública, contrario a ciudades de primer mundo como Londres o Nueva York, en las que la videovigilancia se originó como una estrategia de seguridad nacional y un mecanismo de prevención implementado posteriormente a las intervenciones terroristas (Jasso López, 2020).

En la provincia de Buenos Aires, Argentina, se observa un avance significativo en los sistemas de videovigilancia para prevenir actos delictivos. Su sistema funciona a través de una RED a nivel nacional con información compartida de agencias de seguridad denominada “SIBIOS”, implementada por su gobierno nacional. A través de este sistema, la ciudadanía argentina tiene la obligación de registrarse ante los organismos de seguridad pública y social de Argentina (Moreno Pérez & Hernández Olascoaga, 2018, p. 11).

Mientras que, en México, solo algunos estados como Aguascalientes, Baja California Sur, Colima y Durango, disponen de leyes en materia de videovigilancia (Moreno Pérez & Hernández Olascoaga, 2018, p. 12). En el caso de la Ciudad de México, se han encaminado esfuerzos a través de iniciativas de ley por consolidar una “Ley General en materia de videovigilancia”; sin embargo, aún falta mucho por avanzar.

La instalación y uso de dispositivos de videovigilancia, son un ejemplo de nuevas políticas en materia de seguridad pública y de renovación urbana. Como se ha mencionado previamente, el comportamiento de la sociedad está estrechamente vinculado con la seguridad que percibe y el grado de autonomía, de modo que, si estos se ven coludidos, pueden presentarse repercusiones negativas.

El catedrático Sergio García Ramírez explica que la “seguridad” consiste en la inexistencia de amenazas que disminuyan los bienes y derechos de las personas y que, por lo tanto, existen condiciones para un pleno desarrollo (García Ramírez, 2002, p. 81). Mientras que, la seguridad ciudadana va involucrar aquel proceso por medio del cual se establece, fortalece y protege el orden civil democrático y se eliminan las amenazas de violencia en la población, permitiendo una coexistencia segura y pacífica (PNUD, 2013, p. 1)

Por otro lado, es importante mencionar que el control social que ejerce el gobierno a partir del uso de estos mecanismos permite unificar a los individuos en lo que conocemos como “sociedad”, sometiéndolos a normas sociales con la finalidad de garantizar una convivencia pacífica (Jasso López, 2023, p. 48). Solo a través de una relación clara y directa entre vigilancia y control es como puede ejercerse un verdadero control social e identificación de desviaciones o incumplimiento de normas.

Ahora, es importante precisar los dilemas y confusiones sobre el uso y falta de regulación de la videovigilancia en nuestro país, pues su estrecha vinculación con derechos a la privacidad, seguridad ciudadana y protección de datos personales pueden verse afectados. De ahí radica la importancia de reconocer la vinculación estrecha entre videovigilancia y derechos humanos involucrados, surgiendo la siguiente pregunta: ¿Cómo garantizar los derechos humanos a partir de la implementación de la videovigilancia en México?

Para tratar de resolverla tuvimos que detallar el objetivo central de este estudio, el cual consiste en abordar la importancia y aplicación de la videovigilancia en México vista como una política pública de seguridad ciudadana e identificando de qué manera el Estado mexicano debe actuar para resguardar los derechos a la privacidad, protección de datos personales y seguridad de la ciudadanía implicada.

I. Concepto y características de la videovigilancia y seguridad ciudadana

I.1 Videovigilancia

La videovigilancia es un sistema que se utiliza como medida de prevención de actos delictivos, de modo que influye en la garantía de la seguridad ciudadana. Se trata de un modelo que se dedica a “observar a través de un sistema de cámaras, monitores e interfaces de video una escena” o grupo de escenas simultáneas que buscan comportamientos específicos de carácter inadecuados, o que indiquen su aparición o existencia (ALGOTIVE, 2022).

Los sistemas de videovigilancia se componen de dispositivos como: red de cámaras, pantallas, VMS (software de gestión de video) y video analítica. Las cámaras que

se utilizan para los procesos de videovigilancia no son convencionales; las que más se utilizan son las siguientes:

- 1) Analógicas, las cuales cuentan con una resolución de menor calidad, utilizan “conexiones de cable coaxial al DVR para cada cámara y conexiones por cable separadas para la alimentación”; por lo tanto, su campo de visión es más estrecha y distorsionada;
- 2) IP-Digital, estas cámaras cuentan con mayor claridad y resolución, se alimentan a través de un conmutador por Ethernet para conectarse a un “network video recorder”; estas cámaras tienen un costo elevado a comparación de las analógicas y requieren mayor almacenamiento;
- 3) Cámaras especializadas, diseñadas para finalidades específicas, por ejemplo, las domo internas y externas, cámaras con movimiento horizontal, vertical o que pueden hacer un acercamiento específico, cámaras discretas, bala, de imagen térmica o infrarroja, y de alta definición (ALGOTIVE, 2022).

Sin duda, la presencia de estas tecnologías ha permitido que la sociedad y los gobiernos las utilicen como una herramienta de seguridad. En Perú, por ejemplo, la inseguridad y delincuencia representaban ya un retroceso económico y social. Esta región optó por la implementación de las tecnologías de la compañía “Axis Communications”, empresa que oferta cámaras de videovigilancia, logrando reducir los índices de violencia a partir de su implementación (AXIS, 2021).

Otro país que utilizó los servicios de la compañía AXIS fue Colombia, en donde el uso de estas tecnologías, como cámaras HD, ha permitido que, en zonas metropolitanas como Bucaramanga, se disminuyan problemas como el tráfico de drogas y, en consecuencia, se faciliten sus detenciones (AXIS, 2021).

Como podemos observar, la videovigilancia resulta efectiva para el combate de actividades delictivas, motivando la seguridad pública y ciudadana. Su estudio no solo se inserta en el campo jurídico, sino que abarca otras disciplinas, lo que la convierte en una tecnología multidisciplinar. De acuerdo con Carmina Jasso, en el ámbito sociológico, la representación social de la tecnología se debe a la interacción entre los individuos y estas (Jasso López, 2020).

Siguiendo a Javier Moreno, existen tres enfoques teóricos para estudiar la interacción de la videovigilancia con la sociología. Éstas se relacionan con su uso en la vida cotidiana, su utilidad en la manipulación y, finalmente, su uso rutinario en los ámbitos individuales y colectivos (Moreno Galvez, 2016).

Por otro lado, desde un enfoque criminológico, el delito tendrá múltiples factores, por lo que su prevención no tendrá una sola variable o política pública como la videovigilancia (Jasso López, 2023, p. 46).

En el ámbito tecnológico, los servicios de videovigilancia comprenden otra serie de “capacidades” como lo son la disuasión, entendida como la disminución del delito, el control como el monitoreo y detección de anomalías y la economía, pues se reduce el personal de seguridad y permite ejercer una seguridad más extensa (SIE, 2015).

Los sistemas de videovigilancia tienen un grado de eficacia que es importante señalar. Ésta varía de acuerdo con el tipo de delito que se trate, el lugar en el que se desarrolla, el protocolo que siguen los operadores al observar las imágenes y el servicio de la policía (Mucchielli, 2021, p. 178).

Para Gian Guido, la eficacia en los sistemas de videovigilancia resultará de la confluencia de elementos como la densidad, es decir el número suficiente de cámaras en zonas particulares, la cobertura de la cámara que permita que puedan verse todas las áreas requeridas y el posicionamiento. También menciona que es importante tomar en consideración la cantidad de iluminación, su visibilidad clara y ubicación. Además, ésta aumentará si el personal que las opera se encuentra debidamente motivado y entrenado (Guido Nobili, 2021, p. 105).

Sin embargo, como lo menciona Carmina Jasso en el libro *Ciudad videovigilada*, se debe considerar que, en la realidad, son pocas las evaluaciones que estudian la verdadera eficacia de las cámaras de videovigilancia y que permiten determinar su efectividad en la incidencia delictiva o percepción de la inseguridad (Jasso López C. , 2023, p. 46).

Esto motiva el fortalecimiento de las políticas públicas, corroborando la eficacia de las cámaras instaladas en el país y la gestión de su operación en las ciudades, de modo que se protejan paralelamente los derechos humanos que puedan verse vulnerados (Jasso López, 2023, p. 108)

De acuerdo con Jasso, las políticas públicas deben considerar aspectos inherentes a las tecnologías de vigilancia. El cambio e innovación es uno de ellos, ya que modifica la vida en sociedad de forma continua, como en el caso de la inteligencia artificial o el reconocimiento facial, que repercuten directamente en las personas, lo que hace necesaria una construcción social de videovigilancia que garantice decisiones pertinentes y anticipe posibles impactos sociales (Jasso López, 2023, p. 342).

I.2 Seguridad Ciudadana y Gobierno

El término seguridad ciudadana ha sido desarrollado por la propia *Comisión Interamericana de Derechos Humanos* (CIDH), que la diferencia del concepto de seguridad humana. De modo que la seguridad ciudadana debe entenderse como una

política pública que se rige bajo los lineamientos o cursos de acción que proponen las autoridades de los Estados y que buscan alcanzar un objetivo específico y, a su vez, permiten crear o transformar las condiciones en que se desarrollan las actividades de las personas y grupos que integran la sociedad (CIDH, s/a, p. 2).

En Latinoamérica, una de las preocupaciones que continuamente se externalizan, particularmente en el Estado mexicano, son los índices de violencia y criminalidad. La violencia y los delitos constituyen grandes barreras para el desarrollo humano pleno de los habitantes en América Latina. De este escenario se pueden rescatar tres ideas fundamentales que plantea la maestra en política criminal, Nereida Cervantes:

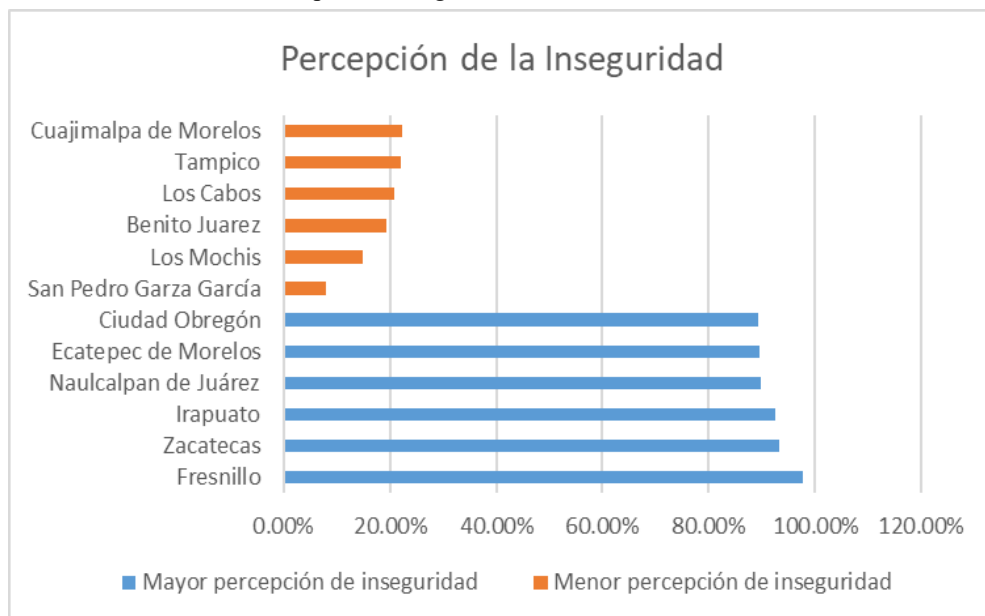
- La falta de seguridad ciudadana trae como consecuencia la dificultad de la sociedad de desarrollarse de forma plena y, por lo tanto, les inhibe de contribuir con todo su potencial a mejorar las condiciones en sus espacios de desarrollo, como lo son la familia, instituciones y sus comunidades;
- La delincuencia, que se traduce en un desafío para las zonas urbanas pobladas, produce temor para desarrollar las actividades de la vida cotidiana y genera niveles de ansiedad e intranquilidad, generando inseguridad;
- La diferencia entre seguridad ciudadana y seguridad humana, pues la primera de ellas consistirá en la idea de un ciudadano capaz de involucrarse como un agente de cambio y no solo como un individuo que le demanda seguridad al Estado (Cervantes Facundo, 2018, pp. 134, 135).

Para el autor Jesús Rojas, el impacto de las cámaras de seguridad en la ciudadanía es notable, pues, a partir de su incorporación en espacios públicos, la sociedad se siente controlada y, de alguna forma, tienen utilidad para constatar aquellas actividades delictivas que ocurren, como lo son robos, crímenes o infracciones de tráfico (Rojas, 2007, p. 35).

La videovigilancia, además de propiciar la seguridad ciudadana, disminuye los índices de criminalidad y la sensación latente de inseguridad. El fundamento esencial radica en que “aquellos espacios monitoreados por estos dispositivos serán más seguros que aquellos que no estén vigilados, siendo promotores de estos ideales los mismos líderes sociales, servidores públicos y organizaciones vecinales” (Jasso López, 2023, p. 42).

A continuación, presentamos una tabla con datos extraídos del comunicado de prensa 21/23 del *Instituto Nacional de Estadística y Geografía* (INEGI), a través de la cual se señala el índice de percepción de seguridad en los distintos estados de México de personas con 18 años y más durante el año 2020.

Tabla 1. Percepción de seguridad en distintos estados de México



Fuente: Elaboración propia a partir de base de datos del INEGI en 2023.

El mayor porcentaje de ciudades en las que se considera que vivir es inseguro, de acuerdo con las personas de 18 años y más encuestadas por el INEGI fueron: Fresnillo, con 97.7%; Zacatecas, con 93.3%; Irapuato, con 92.6%; Naucalpan de Juárez, con 89.7%; Ecatepec de Morelos, con 89.6% y Ciudad Obregón, con 89.2% (INEGI, 2023, p. 1).

En contraste, las ciudades donde la percepción de inseguridad es menor fueron: San Pedro Garza García, con 8.1%; Los Mochis, con 15.0%; Benito Juárez, con 19.4%; Los Cabos, con 20.9%; Tampico, con 22.1% y Cuajimalpa de Morelos, con 22.3% (INEGI, 2023, p. 2).

En el mismo comunicado se señalan algunos de los espacios físicos en donde la población manifestó sentir mayor índice de inseguridad, predominando los cajeros automáticos localizados en vía pública, el transporte público y las calles que usualmente transitan (INEGI, 2023, p. 5).

Promover la seguridad ciudadana y crear los mecanismos necesarios para hacerla efectiva es un deber de los Estados a través de sus gobiernos. En el plano internacional, existen países que han integrado estrategias, así como objetivos y acciones, en materia de videovigilancia dentro de sus programas nacionales, como el caso de “Bolivia,

Colombia, Costa Rica, Ecuador, Nicaragua, Perú y El Salvador, como parte de su planeación estatal” (Jasso López, 2023, p. 86).

Por otro lado está el caso de Bolivia y Costa Rica, que los incluyen como parte de sus planes de “Seguridad Ciudadana para una vida sin violencia” y como “Política Integral Sostenible y de Seguridad Ciudadana y de Promoción de la Paz Social”, respectivamente (Jasso López, 2023, p. 87).

Destaca Perú, que implementó un “Plan Nacional de Seguridad Ciudadana 2013-2018”, a través del cual propone la creación de un “Centro Nacional de Video Vigilancia y Radio Comunicación para la Seguridad Ciudadana”, que funcionará como una plataforma que opera la propia Policía Nacional del Perú, de modo que involucra elementos que propician la seguridad ciudadana (Jasso López, 2023, pp. 87,88).

Para Jasso, la planeación de la videovigilancia dentro de América Latina debe formar parte de los programas de seguridad, considerando que en ellos existe un uso cotidiano que sus resultados apuntan a un crecimiento que continua en incremento (Jasso López, 2023, p. 88). Una vía a través de la cual los gobiernos de cada estado adoptan medidas especiales para garantizar la seguridad de su ciudadanía es través de las políticas públicas.

Si bien los gobiernos y organizaciones privadas se centran en la adquisición e instalación de las cámaras como mecanismo para proteger a la ciudadanía de la inseguridad, como forma de prevención y control del crimen, de acuerdo con Nelson Arteaga, esto dependerá de los patrocinadores y gestores de los instrumentos de videovigilancia, de modo que su correcta implementación ha propiciado la “recuperación” de las ciudades en lo que al turismo, infraestructura y calidad de vida respectan. Por lo tanto, no solo funcionan como mecanismos que previenen delitos, sino que garantizan y gestionan el orden público y la convivencia ciudadana (Arteaga Botello, 2016, p. 203).

No obstante, entre algunas quejas e implicaciones que trae consigo, y retomando el factor de los intereses de quienes las gestionan, están la utilización de éstas por agentes policiales en colisión con el crimen organizado o como testigo de hechos atroces, por ejemplo: “el asesinato de una activista en Ciudad Juárez frente al Palacio de Gobierno”, o cuando han servido de cómplice en actos como el “secuestro de los estudiantes de la escuela normal de Ayotzinapa por parte de policías municipales y narcotraficantes” (Arteaga Botello, 2016, p. 204).

Como podemos observar, las tecnologías de videovigilancia funcionan como instrumentos que legitiman el poder y el orden social; su eficacia dependerá del uso que el gobierno le destine. Aunado a esto, se puede observar que quienes tienen un mayor avance normativo respecto al tema son aquellos países que han gestionado previamente sistemas de videovigilancia y, por lo tanto, tienen mayor demanda social por parte de la ciudadanía, que les exige la garantía de sus derechos humanos (Jasso López, 2023,

p. 69). Por lo tanto, la seguridad y su vinculación con la videovigilancia estarán motivadas por las decisiones del gobierno en la medida en que establezcan una protección integral a los derechos fundamentales de la ciudadanía vigilada.

En el caso de México, una de las problemáticas y retos que encontramos son la falta de leyes y reglamentos municipales que regulen la videovigilancia y, de acuerdo con Arteaga, aquellos que existen se enfocan en dos aspectos: “a) garantizar que la información que recogen sirva como elemento de prueba para castigar faltas administrativas y penales; y b) evitar las posibles violaciones al derecho de privacidad” (Arteaga Botello, 2016, p. 207).

Sin embargo, esto no es suficiente. Existen otras necesidades que deben ser cubiertas, como: “la expansión de la videovigilancia para el respaldo de la investigación y prosecución de hechos criminales, la sanción de faltas administrativas, la agilización de la intervención en tiempo real de policía y la recolección de información para el diseño de políticas públicas”, cuidando que no se vulneren derechos humanos de la ciudadanía. Para ello, y siguiendo a Arteaga, existen tres esferas de intervención en el uso de la videovigilancia: la relativa a las “áreas de responsabilidad y decisión, a la gestión y uso de las cámaras y al manejo de imágenes y sonidos que se recolectan y graban” (Arteaga Botello, 2016, p. 207).

I.3 Videovigilancia como política pública de seguridad ciudadana

En México y el mundo, la videovigilancia se ha expandido como una vía para promover la seguridad ciudadana, motivando a los gobiernos a establecer políticas públicas adecuadas e instituciones capacitadas para su correcta incorporación y funcionamiento.

Existen diversos programas que surgen a partir de política pública en materia de videovigilancia en México, como lo son “arcos de seguridad, programas de operación y mantenimiento a las videocámaras y Centros de Comando, Cómputo, Control y Comunicaciones (C5)” de diferentes entidades federativas en la República. De estas entidades, de acuerdo con Jasso, dependen la operación y gestión de cámaras públicas, a través de sus instalaciones se tiene acceso a las imágenes generadas y, en coordinación con otras instituciones públicas, se atienden las emergencias y delitos que se suscitan (Jasso López, 2023, p. 269).

Es común cuestionarnos qué ocurre con el presupuesto que se les destina a las iniciativas y políticas públicas en materia de videovigilancia. La videovigilancia toma mucha relevancia en zonas metropolitanas, como lo es el Estado de México. En el año 2017, por ejemplo, se destinó un presupuesto de \$1,502,054,004 pesos mexicanos para la “Operación y Mantenimiento del Programa de Seguridad y Monitoreo en el Estado de México”. (DOF, 2016, p. 61). Mientras que en el *Programa de Egresos de la Federación 2023* se destinó al rubro de “Seguridad y Protección Ciudadana”, encarga-

do de “implementar políticas, acciones y programas que garanticen la seguridad pública”, solo \$3,854,560.00 pesos mexicanos y a los “servicios de protección, custodia, vigilancia y seguridad de personas, bienes e instalaciones”, \$1,992,912,344 pesos mexicanos (DOF, 2022).

Habiendo explicado lo anterior, y para tener un orden y control sobre el número de videocámaras y centros de monitoreo, es necesaria la creación de otra política pública que logre realmente regular su uso, delimitar las zonas en donde deben ubicarse, establecer el límite de cámaras por zona y la infraestructura necesaria que deberán tener para poder operar de una manera efectiva y precisa, de modo que la seguridad ciudadana no corra riesgo alguno por errores en la operación de estas videocámaras.

En el año 2016, el *Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública*, en colaboración con el *Instituto Politécnico Nacional*, a través de un convenio de colaboración, se comprometieron a elaborar un estándar técnico sobre videovigilancia que mejore la atención de emergencias, seguridad pública y la prevención del delito, denominado “Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de videovigilancia para la seguridad pública” (GOBMX, 2016).

El objetivo de la norma mencionada es “generar criterios normativos y técnicos que dicten a las entidades federativas las características técnicas y la forma de operación de los Sistemas de Video Vigilancia” y, a su vez, establecer los parámetros de organización, infraestructura, tecnología y evaluación de los Sistemas de Video Vigilancia en concordancia con la *Ley General del Sistema Nacional de Seguridad Pública*. (SEGOB, s/a, p. 3). Además, en esta norma se establecen todos los requisitos, especificaciones, diseños y parámetros para el uso de todo dispositivo de videovigilancia para estandarizar, definir y establecer las condiciones óptimas de su correcto funcionamiento.

Es imperante que se conozcan y efectúen las políticas públicas que el Estado implementa a través de estos programas en materia videovigilancia, pues solo así se puede garantizar un uso óptimo y funcional. Por otro lado, no se debe perder de vista que el eje por el que deben ceñirse estas normas y políticas deberán ser siempre los derechos humanos involucrados, como lo son la privacidad, la protección de datos personales y la seguridad ciudadana.

II. Derechos humanos involucrados en la adopción de la videovigilancia en México: privacidad, protección de datos personales y seguridad ciudadana

Los derechos humanos deben analizarse en cualquier política pública de manera transversal. En el presente apartado se analizan los derechos humanos a la privacidad, la seguridad y la protección de datos personales que se desprenden del uso de dispositivos de videovigilancia.

II.1 Derecho a la privacidad

El derecho a la privacidad lo encontramos reconocido en la propia *Declaración Universal de los Derechos Humanos*, específicamente en su artículo 12, el cual establece que ninguna persona puede ser “objeto de injerencias” en ningún núcleo de su vida (privada, familiar, domicilio o correspondencia), incluyendo su honra y dignidad, y, en caso de ser perjudicadas, toda persona cuenta con una protección especial por parte de la ley (*Declaración Universal de Derechos Humanos*, 1948).

Ahora, de acuerdo con Jorge Carlos Estrada, los derechos a la intimidad, privacidad e identidad, pueden estudiarse desde dos perspectivas: una negativa o excluyente, en donde la persona no permitirá que se conozcan aspectos de su vida íntima o subjetiva; y, por otro lado, la positiva o “autodeterminación informativa”, donde la persona controla su información y, por lo tanto, puede exigir la rectificación, corrección, actualización o supresión de la información (Estrada Avilés, s/a, p. 3).

Para hablar del derecho a la privacidad, la doctora Ana Elizabeth Villalta explica que deben considerarse otros derechos fundamentales involucrados, como: “el honor, la dignidad, la intimidad, la propia imagen, así como en la libertad de expresión, pensamiento, opinión y asociación.” A su vez, estos derechos también están insertos en instrumentos internacionales como el *Pacto Internacional de Derechos Civiles y Políticos* y Legislación de los Estados miembros de la Organización de los Estados Americanos. (Villalta Vizcarra, 2017, p. 276).

De acuerdo con las Naciones Unidas, la privacidad es en sí misma un valor necesario para el desarrollo de la personalidad y la protección de la dignidad humana; además, se trata de un derecho que no es absoluto, pues en situaciones particulares puede verse limitado. No obstante, como lo ha desarrollado el propio Tribunal Europeo de los Derechos Humanos, las intrusiones o intromisiones a la privacidad deben ser en todo momento proporcionales al beneficio que aporten a la sociedad (ONU, 2018).

Para Joaquín Rueda, la privacidad se ha visto vulnerada con el avance de los dispositivos tecnológicos de tres formas: a través de la libertad de expresión, la cual, al externalarla en medios como redes sociales, es objeto de confrontación; la segunda, sobre la recolección ilegal de los datos personales de los usuarios de la red, los cuales se encuentran expuestos; y, finalmente, la que se genera a partir de la videovigilancia que está a cargo de las instituciones de seguridad de los Estados u corporaciones (Rueda Carrillo, 2019, p. 3).

II.2 Derecho a la protección de datos personales

El Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR) ha desarrollado el concepto de datos personales como aquellos datos vinculados a un individuo por medio de los cuales podrá identificarse o ser identificado. Estos datos

incluyen: biodatos, es decir información biográfica como el nombre, estado civil, sexo, lugar y fecha de nacimiento; país de asilo; país de nacimiento; ocupación; religión; y origen étnico. A su vez, se involucran datos biométricos que consisten en huellas dactilares, fotografías, imágenes de iris o rostro y manifestaciones de opinión (ACNUR, 2015, p. 11).

Una de las preocupaciones para cualquier ciudadano es que sus datos personales se filtren o sean utilizados para fines distintos a los establecidos. Siguiendo al ACNUR, esta filtración se traduce como “una violación de la seguridad de los datos” que puede consistir en la alteración, pérdida, divulgación no autorizada o acceso ilegal de la información (ACNUR, 2015, p. 11).

A través del Comité Jurídico Interamericano de la Organización de los Estados Americanos se han desarrollado una serie de principios que regulan la privacidad y la protección de los datos personales, destacando su finalidad, la cual debe ser legítima y a través de medios leales, la importancia de la transparencia y consentimiento, la pertinencia y necesidad, confidencialidad, el tratamiento y conservación que no debe exceder el tiempo necesario, la seguridad de los datos, su exactitud, el acceso efectivo para su rectificación, oposición o cancelación, la atención a aquellos datos sensibles en contextos particulares, la responsabilidad de los encargados en su tratamiento y su flujo (OEA, 2022, pp. 12-15). El principio trece guarda especial relevancia, ya que establece la necesidad de que los Estados Miembros establezcan “órganos de supervisión independientes, dotados de recursos suficientes”, acorde con las estructuras constitucionales, administrativas y organizacionales de los Estados para monitorear la protección de los datos (OEA, 2022, p. 16).

En Europa existe un “Reglamento General de Protección de Datos” (RGDP), a través del cual se protegen los datos personales de los usuarios en la Unión Europea. Dentro de sus disposiciones están la de respetar la privacidad individual de aquellos que son captados a través de imágenes en espacios públicos y la necesidad de señalarles. Por otro lado, a aquellas grandes empresas que manejan datos personales de distintos usuarios se les exige contar con un “Delegado de Protección de Datos” que garantice un tratamiento conforme a la ley (SCATI, 2024). Es importante tomar como parámetro aquellos países que muestran mayores avances en la materia para replicar lo conducente en América Latina.

II.3 Derecho a la seguridad ciudadana

El término “seguridad” podemos ubicarlo en el artículo tercero de la *Declaración de los Derechos Humanos*, en donde se menciona que todo individuo tendrá derecho a la seguridad de su persona. (Declaración Universal de Derechos Humanos, 1948).

Para Ilda Lilian Cartagena, los seres humanos tenemos la necesidad de sentir seguridad cuando estamos en un estado de vulnerabilidad. Las amenazas a los niveles de

seguridad de las personas pueden deberse a la economía, medioambiente y la ética de las personas. El Estado es el responsable de adoptar medidas de seguridad a través de su administración de justicia y órganos competentes, sin ser contrarias a los propios derechos humanos (Cartagena Santos, s/a, p. 5)

Ahora, siguiendo a Lilian Cartagena, la seguridad ciudadana surge derivado del crecimiento de las ciudades y de la necesidad de ampliar la seguridad. Derivado de la demanda social comienzan a implementarse nuevas políticas para afrontar la delincuencia, surgiendo el deber del Estado de garantizar la seguridad de la ciudadanía, el respeto entre las personas y la vigencia de su libertad (Cartagena Santos, s/a, pp. 7,8).

Por otra parte, en el ámbito institucional la seguridad ciudadana va suponer un dilema político y social, pues tendrán, en principio, garantizado el goce de sus derechos y libertades emanadas por el mismo Estado democrático. Por ello, la seguridad ciudadana es en sí un derecho fundamental que no debe marginar o criminalizar a un sector para proteger a otro, sino ser incluyente con pautas de convivencia democrática (Cartagena Santos, s/a, pp. 9,10).

La seguridad ciudadana, en comparación con la seguridad pública, tendrá fines distintos, pues la segunda buscará mantener el orden público, la protección integral de las personas y sus bienes, la prevención en la comisión de delitos o infracciones a reglamentos y la colaboración en la investigación y persecución de delitos fungiendo como auxiliar de la población (Moreno Luce, 2004, p. 4).

De lo antes expuesto podemos señalar que las personas tenemos una necesidad de protección y de sentirnos seguras; la obligación de garantizárnosla le corresponde al Estado, quien debe implementar medidas de seguridad y regular de forma oportuna y eficaz los sistemas de videovigilancia, en este caso, para garantizar nuestros derechos personalísimos a la privacidad, seguridad ciudadana y protección de datos personales.

Ahora, no debe perderse de vista que estas políticas públicas que el Estado decida implementar o poner en práctica deben siempre garantizar los derechos humanos de la ciudadanía. Existe, incluso, un “Manual y protocolo para la elaboración de políticas públicas de Derechos Humanos conforme a los nuevos Principios Constitucionales,” el cual establece que las políticas públicas deben estar en constante evolución y deben considerar elementos como la transversalidad, la perspectiva de género, la igualdad y no discriminación, participación ciudadana, progresividad, el principio pro persona y la transparencia y rendición de cuentas (SEGOB, 2014).

En México, la *Ley Federal de Protección de datos personales en posesión de los particulares*, en sus artículos 7 y 8, establece que, cuando se utilicen datos personales, estos en todo momento deben tratarse con expectativa de privacidad y ésta se traduce como la “confianza que deposita” la persona respecto de aquellos datos que proporciona, además de señalar la importancia del consentimiento del titular de los datos, el cual deberá ser expreso de forma verbal o escrita a través de medios ópticos o electró-

nicos (Ley Federal de Protección de datos personales en posesión de los particulares, 2010).

Una de las problemáticas en México en cuanto al uso de datos personales es que algunas instituciones no cuentan con la suficiente difusión respecto a su aviso de privacidad, de modo que la ciudadanía no conoce el uso y posesión de quien maneja y administra estos datos personales obtenidos a través de cámaras de videovigilancia, por ejemplo. Al respecto el *artículo 12* de la misma *Ley de Protección de Datos Personales* establece que el tratamiento de los datos personales “debe limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad”, pues si su uso derivará en un fin distinto al establecido, requerirá nuevamente del consentimiento de su titular (Ley Federal de Protección de datos personales en posesión de los particulares, 2010).

La autora Ana Aba Catoira explica que, al utilizar sistemas de videovigilancia y para garantizar la protección de los datos personales, es importante considerar que las imágenes se utilicen a partir de un sistema de circuito cerrado y no se vinculen con los datos personales del titular, el método que se utiliza para su tratamiento, la técnica, el tipo de equipo, las herramientas utilizadas y la legalidad del tratamiento (Aba Catoira, s/a).

Si bien en nuestra *Constitución Política de los Estados Unidos Mexicanos* no hay un apartado sobre seguridad ciudadana, el derecho a la seguridad pública si se menciona, estableciendo que ésta “es una función de Estado a cargo de la Federación” y las entidades federativas que buscan salvaguardar los derechos a la vida, integridad, libertades y patrimonio de los ciudadanos, además de propiciar el orden público y la paz social (Constitución Política de los Estados Unidos Mexicanos, 2024).

III. Normatividad que regula la videovigilancia en México con enfoque de Derechos Humanos

Una vez que se explicó el alcance e importancia de los derechos humanos a la privacidad, seguridad ciudadana y protección de datos personales en torno al tema de videovigilancia, consideramos pertinente realizar un análisis de la normativa y legislación de los 32 estados de la República para vislumbrar su aplicación. A continuación, enunciamos aquellos estados que en sus decretos, leyes o reglamentos internos se desarrolla el concepto de videovigilancia, así como los principios rectores y específicamente el derecho humano a la privacidad.

En primer lugar, mencionaremos aquellos estados que cuentan con decretos de ley en materia de videovigilancia y que dedican un capítulo específico a la “Videovigilancia su concepto y efectos”. Estos estados son: Aguascalientes, Baja California Sur, Colima, Durango, Jalisco, Morelos, San Luis Potosí y Yucatán.

En segundo lugar, mencionaremos aquellos estados que cuentan con decretos y leyes en materia de Seguridad Pública que involucra la actuación de las autoridades e instituciones en materia de seguridad de sus estados y municipios y que incluyen en su normativa los “principios de legalidad, eficiencia, profesionalismo y honradez”. Los estados que se encontraron son: Campeche, Chiapas, Chihuahua, Ciudad de México, Guanajuato, Guerrero, Hidalgo, Michoacán, Nayarit, Nuevo León, Oaxaca, Puebla, Querétaro, Quintana Roo, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz y Zacatecas.

De los estados previamente señalados, solo los que a continuación se señalan prevén dentro de sus decretos o leyes estatales sobre seguridad pública el término “videovigilancia”: Guanajuato, Hidalgo y Nuevo León.

Finalmente, consideramos oportuno señalar que existen estados que cuentan con reglamentos específicos en la materia, como lo es Baja California (Reglamento del Centro de control, comando, comunicación y computo del Estado de Baja California, 2011), en el que, se encuentra inserto un concepto de videovigilancia, sus facultades, así como los principios de confidencialidad, de reserva y sigilo.

En Coahuila, a través de la (Ley para el Control de Video Cámaras Urbanas para el Estado de Coahuila de Zaragoza, 2011) se menciona el concepto de videocámaras y los principios de “proporcionalidad, riesgo razonable y peligro concreto”.

Ahora, el Estado de México cuenta con una (Ley que regula el uso de tecnologías de la información y comunicación para la seguridad pública del Estado de México, 2014) en la que se menciona el concepto de videovigilancia, pero no los principios.

El derecho humano a la privacidad también fue objeto de análisis en este trabajo, por lo que se mencionan aquellos estados en los que, a partir de sus decretos, reglamentos o leyes sobre “Video Vigilancia o Seguridad Pública” internos, el derecho a la privacidad es tomado en cuenta. Estos estados son: Aguascalientes, Baja California, Baja California Sur, Coahuila, Colima, Durango, Guanajuato, Jalisco, Ciudad de México, Morelos, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Yucatán y Zacatecas.

IV. Hallazgos

A través del presente trabajo pudimos observar la percepción que tiene la población respecto de la inseguridad en su entorno cotidiano, el cual se detalla en la Tabla de “Percepción de la Inseguridad”, en la que se recabó información por estado y municipio de la República, siendo Fresnillo el percibido como más inseguro y San Pedro Garza como el menos inseguro.

Observamos que los sistemas de videovigilancia efectivamente funcionan como mecanismos que disminuyen los índices de delincuencia o crimen, ya que inhiben a la

sociedad a realizarlos. Sin embargo, constatamos que la sociedad presenta un grado de incertidumbre o preocupación respecto de los derechos humanos involucrados, como lo son la privacidad, la protección de sus datos personales y la seguridad ciudadana.

Enfatizamos en la importancia del Estado en contribuir con los principios que rigen la protección de datos personales y el consentimiento informado de la ciudadanía, pues ésta tiene el derecho de exigir en todo momento la actualización, rectificación, corrección o supresión de la información capturada a través de los dispositivos, ya que, de no ser así, su dignidad humana podría verse afectada injustificadamente.

Finalmente, queremos destacar que, a pesar de que existen algunos estados de la República que presentan un avance dentro de sus leyes y reglamentos en materia de videovigilancia y el derecho a la privacidad, aún falta mucho por hacer.

Es necesario que todas las entidades federativas avancen y cumplan con los parámetros establecidos, en atención al principio de progresividad. Tal es el caso de Campeche, Chiapas, Chihuahua, Guerrero, Michoacán, Nayarit, Oaxaca, Puebla, Sinaloa, Tabasco, Tamaulipas y Tlaxcala, pues es preocupante que la mayoría no cuenten con conceptos o desarrollo normativo respecto de la videovigilancia y el derecho a la privacidad de sus ciudadanos, siendo, como ya se advirtió, una situación que nos está rebasando a través de la implementación de las nuevas tecnologías.

Conclusiones

La videovigilancia es una estrategia que permite reducir los índices de criminalidad e inseguridad en los estados, por lo que es importante comprender su funcionamiento y aplicación para su correcto manejo y plena efectividad.

En cuanto a los derechos humanos involucrados, se comprendió que no puede hablarse de privacidad sin protección de datos personales, pues, en ambos casos, el consentimiento previo de los sujetos es indispensable, quienes estarán, además, en su derecho de rectificar en todo momento su información.

En cuanto a la función del gobierno de garantizar la seguridad ciudadana y las medidas especiales que utiliza a través de la implementación de políticas públicas, nosotros como sociedad, tenemos el derecho de exigir que nuestra privacidad e intimidad sean respetadas, solicitando transparencia y rendición de cuentas y el correcto uso de estas imágenes y videos.

Finalmente, consideramos necesaria la creación de una “Ley Nacional en materia de Videovigilancia”, que contemple un “Reglamento General de Protección de Datos”, como el caso de Europa, y un órgano encargado de vigilar el tratamiento y uso de estos, privilegiando el consentimiento previo de los titulares de los datos personales.

Referencias

- Aba Catoira, A. (s/a). La Videovigilancia y la garantía de los derechos individuales: su marco jurídico. (A. d. Dereito, Ed.) Recuperado el 03 de marzo de 2024, de <https://ruc.udc.es/dspace/bitstream/handle/2183/2251/AD-7-1.pdf?sequence=1&isAllowed=y>
- ACNUR. (2015). Política sobre la Protección de Datos personales de las personas del Interés del ACNUR. Recuperado el 03 de marzo de 2024, de <https://www.acnur.org/fileadmin/Documentos/Publicaciones/2016/10909.pdf>
- ALGOTIVE. (2022). ¿Qué es un sistema de videovigilancia y cómo funciona?. Recuperado el 02 de marzo de 2024, de: <https://www.algotive.ai/es-mx/blog/que-es-un-sistema-de-videovigilancia-y-como-funciona>
- Arteaga Botello, N. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. *Espiral, Estudios sobre Estado y Sociedad*, xxiii(66), 203. Recuperado el 03 de marzo de 2024, de <https://www.scielo.org.mx/pdf/espiral/v23n66/1665-0565-espiral-23-66-00193.pdf>
- AXIS. (2021). a videovigilancia en red y sus posibilidades en América Latina. Recuperado el 02 de marzo de 2024, de <https://newsroom.axis.com/es-mx/article/la-videovigilancia-en-red-y-sus-posibilidades-en-america-latina>
- Cartagena Santos, I. L. (s/a). Seguridad ciudadana un derecho humano. *Revista Regional de Derechos Humanos*, 13.
- Cervantes Facundo, N. (2018). La seguridad ciudadana ¿realidad o ficción en México? *Las ciencias sociales y la agenda nacional*, viii, 134-135. Recuperado el 03 de marzo de 2024, de <https://www.comesco.com/ciencias-sociales-agenda-nacional/cs/article/view/1484/655>
- CIDH. (s/a). Comisión Interamericana de Derechos Humanos. Informe sobre seguridad ciudadana y derechos humanos. Recuperado el 03 de marzo de 2024, de <https://www.corteidh.or.cr/tablas/r25279.pdf>
- Constitución Política de los Estados Unidos Mexicanos. (2024). México: Cámara de Diputados del H. Congreso de la Unión. Recuperado el 03 de marzo de 2024, de <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>
- Declaración Universal de Derechos Humanos. (1948). Recuperado el 03 de marzo de 2024
- DOF. (2016). *Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2017*. México. Recuperado el 03 de marzo de 2024, de https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2017/PEF_2017_orig_30nov16.pdf
- DOF. (2022). *Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2023*. Recuperado el 03 de marzo de 2024, de https://dof.gob.mx/nota_detalle.php?codigo=5672637&fecha=28/11/2022#gsc.tab=0
- Estrada Avilés, J. C. (s/a). El derecho a la intimidad y su necesaria inclusión como garantía individual. Recuperado el 03 de marzo de 2024, de <http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf>
- García Ramírez, S. (2002). En torno a la seguridad pública -desarrollo penal y evolución del delito-. En P. J. Peñaloza, *Los desafíos de la seguridad pública en México* (pág. 81). México: Instituto de Investigaciones Jurídicas de la UNAM. Recuperado el 02 de marzo de 2024, de http://biblioteca.juridicas.unam.mx:8991/F/?func=direct&doc_number=1874006

- GOBMX. (2016). Firman acuerdo para estandarizar sistemas de videovigilancia en el país. Recuperado el 03 de marzo de 2024, de <https://www.gob.mx/segob/prensa/firman-acuerdo-para-estandarizar-sistemas-de-videovigilancia-en-el-pais>
- Guido Nobili, G. (2021). Los sistemas de videovigilancia para prevenir la delincuencia: lecciones aprendidas. *Revista Constructos Criminológicos*, 1(1), 105, 106. Recuperado el 02 de marzo de 2024, de <https://constructoscriminologicos.uanl.mx/index.php/cc/article/view/7/6>
- INEGI. (2023). *Encuesta Nacional de seguridad pública urbana cuarto trimestre de 2022*. Comunicado de prensa núm. 21/23. Recuperado el 03 de marzo de 2024, de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ensu/ensu2023_01.pdf
- Jasso López, C. (2023). *La Ciudad Videovigilada. Entre la prevención del crimen y el control social* (Primera ed.). Ciudad de México: Universidad Nacional Autónoma de México. Recuperado el 02 de marzo de 2024
- Jasso López, L. C. (2020). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en Latinoamérica. *Revista en Investigación en derecho y criminología*(27). Recuperado el 02 de marzo de 2024, de <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/914/1803>
- Ley Federal de Protección de datos personales en posesión de los particulares. (2010). México: Cámara de Diputados del H. Congreso de la Unión. Recuperado el 03 de marzo de 2024, de <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Ley para el Control de Video Cámaras Urbanas para el Estado de Coahuila de Zaragoza. (2011). Congreso del Estado Independiente Libre y Soberano de Coahuila de Zaragoza. Recuperado el 03 de marzo de 2024, de <https://www.congresocoahuila.gob.mx/portal/wp-content/uploads/2014/11/20110412184.pdf>
- Ley que regula el uso de tecnologías de la información y comunicación para la seguridad pública del Estado de México. (2014). Gobierno del Estado de México. Recuperado el 03 de marzo de 2024, de <https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig209.pdf>
- Moreno Galvez, J. (2016). Representaciones sociales de la tecnología. El estudio de caso de la red Guadalinfo. *H-ermes, Journal of Communication*(7), 142. Recuperado el 02 de marzo de 2024, de <https://idus.us.es/handle/11441/132809>
- Moreno Luce, M. S. (2004). La seguridad pública, los derechos humanos y su protección en el ámbito internacional. *Universidad Veracruzana. Centro de Estudios sobre Derecho, Globalización y Seguridad.*, 9, 1-13. Recuperado el 03 de marzo de 2024, de <https://cdigital.uv.mx/handle/1944/50984>
- Moreno Pérez, S., & Hernández Olascoaga, S. M. (2018). *Vigilar sin castigar. Un panorama de la videovigilancia en México*. México: Centro de Estudios Sociales y de Opinión Pública. Recuperado el 02 de marzo de 2024, de CESOP-IL-72-14-VigilarSinCastigar-090718%20(3).pdf
- Mucchielli, L. (2021). ¿Cuál es el propósito de la videovigilancia? Lecciones de la experiencia francesa. *OBETS. Revista de Ciencias Sociales*, 16(1), 178. doi:<https://doi.org/10.14198/OBETS2021.16.1.11>

- OEA. (2022). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Washington, D.C. Recuperado el 03 de marzo de 2024, de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
- ONU. (2018). *Artículo 12: derecho a la intimidad*. Recuperado el 03 de marzo de 2024, de <https://news.un.org/es/story/2018/11/1446671>
- Panhispánico, D. (2023). *Diccionario panhispánico del español jurídico*. Recuperado el 02 de marzo de 2024, de <https://dpej.rae.es/lema/videovigilancia>
- PNUD. (2013). *Programa de las Naciones Unidas para el Desarrollo*. Recuperado el 02 de marzo de 2024, de Sinopsis: Seguridad Ciudadana: [https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief%20\(spanish\).pdf](https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief%20(spanish).pdf)
- Reglamento del Centro de control, comando, comunicación y computo del Estado de Baja California. (18 de marzo de 2011). Periódico Oficial del Estado de Baja California. Recuperado el 03 de marzo de 2024, de <http://www.ordenjuridico.gob.mx/Documentos/Estatal/Baja%20California/wo60232.pdf>
- Rojas, J. (2007). Mecanismos de videovigilancia en la sociedad de la información. *Revista sobre la sociedad del conocimiento*(5), 35. Recuperado el 03 de marzo de 2024, de <https://www.uoc.edu/uocpapers/5/dt/esp/rojas.pdf>
- Rueda Carrillo, J. (2019). Videovigilancia ¿Derecho del ciudadano o facultad del estado? El caso de la Ciudad de México. México: INFOTEC Centro de Investigación e Innovación en tecnologías de la información y comunicación. Recuperado el 03 de marzo de 2024, de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/386/1/INFOTEC_MDTIC_JRC_24032020.pdf
- SCATI. (31 de enero de 2024). *¿Cómo afectan las leyes de protección de datos a la videovigilancia?* Recuperado el 03 de marzo de 2024, de <https://www.scati.com/2024/01/31/como-afectan-las-leyes-de-proteccion-de-datos-a-la-videovigilancia/>
- SEGOB. (2014). *Manual y Protocolo para la elaboración de políticas públicas de Derechos Humanos conforme a los nuevos Principios Consistucionales*. México. Recuperado el 03 de marzo de 2024, de http://www.gobernacion.gob.mx/work/models/SEGOB/Resource/1093/8/images/Manual_politica_publica_dh.pdf
- SEGOB. (s/a). *Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video-vigilancia para la seguridad pública*. Recuperado el 03 de marzo de 2024, de https://secretariadodjejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf
- SIE. (2015). *Seguridad Integral Empresarial. Compañía de seguridad*. Recuperado el 02 de marzo de 2024, de El importante rol del sistema de CCTV en la Seguridad Privada: <https://siesa.com.ar/el-importante-rol-del-sistema-de-cctv-en-la-seguridad-privada/>
- Villalta Vizcarra, A. E. (2017). La privacidad y la protección de datos personales. En O. D. Americanos, *Curso de Derecho Internacional* (págs. 275-297). Brasil: Organización de los Estados Americanos. Recuperado el 03 de marzo de 2024, de <https://archivos.juridicas.unam.mx/www/bjv/libros/12/5718/13.pdf>

Capítulo 7

La video vigilancia en México, ¿protege o vulnera los derechos humanos de las personas en condición de niñez?

Does video surveillance in Mexico protect or violate human rights of people in childhood condition?

*Maria Elisa Matilde Ceballos Díaz**

Resumen

La inseguridad y la violencia es una problemática frecuente en México y para contrarrestarlas se utilizan en las ciudades cámaras de video vigilancia, las cuales, además, funcionan como instrumentos de apoyo para la impartición de justicia; por lo que todas las personas son observadas, sin saber cómo es que se manejan sus datos personales. Este trabajo se enfoca en la niñez, atendiendo al principio del interés superior que debe de prevalecer en las actuaciones de las autoridades. Para ello, es que se procedió a efectuar una revisión y análisis de las normas vigentes a nivel internacional, nacional, y estatal, así como de libros, artículos, estadísticas y notas periodísticas, para contestar si la video vigilancia en México protege o vulnera los derechos humanos de las personas en condición de niñez, precisando que, ante las deficiencias de las leyes y de las autoridades, se conciben trasgresiones a los derechos de los niños, niñas y adolescentes.

Palabras clave: Video vigilancia; Personas en situación de infancia; Niños, niñas y adolescentes; Derechos humanos; Seguridad pública.

Abstract

Insecurity and violence is a frequent problem in Mexico and to counteract them, video surveillance cameras are used in cities, which also function as support instruments for the adminis-

* Doctora en Derecho Instituto de Investigaciones Jurídicas Universidad Veracruzana; candidata al grado de Maestría en Sistema Penal Acusatorio y Adversarial, Universidad de Xalapa; Grado de Maestría en Derechos Humanos y Juicio de Amparo; Docente en la Universidad de Xalapa y Colegio de Veracruz; mariaelisaceballosdiaz@gmail.com; ORCID 0000-0002-4358-9869.

tration of justice; therefore, all persons are observed, without knowing how their personal data is handled; In this work, the focus is on children, taking into account the principle of the best interest that should prevail in the actions of the authorities. To this end, we proceeded to review and analyze the regulations in force at international, national and state level, as well as books, articles, statistics and journalistic notes, to answer whether video surveillance in Mexico protects or violates the human rights of children? specifying that in view of the deficiencies of the laws and the authorities, transgressions to the rights of children and adolescents are conceived.

Keywords: Video-surveillance; People in situations of infancy; Human rights; Public security.

Introducción

En México, las personas cotidianamente viven violencia e inseguridad, principalmente en las zonas urbanas. Como solución, se está recurriendo a la video vigilancia en las zonas públicas, como calles, parques, estadios, edificios gubernamentales, etc., para prevenir y proteger a los habitantes, al igual que como herramientas para investigar delitos. Con ello, el Estado demuestra que cumple con el deber constitucional de proporcionar seguridad pública y satisfacer los reclamos ciudadanos.

El uso actual de las cámaras de video vigilancia se ha vuelto más frecuente, tan es así que en año 2016 se contabilizan la existencia de 25,631 cámaras (INEGI, 2016), y en el año 2021 se incrementó su uso cuatro veces más, con 124,204, destacando a la Ciudad de México y el Estado de México como los estados en los que se concentra el mayor número de ellas (INEGI, 2021).

En ese sentido, el uso de estas tecnologías ha causado discusiones. Así, por un lado, están los autores que opinan que son herramientas de control social y de gestión de riesgos, como lo señalan el Doctor Nelson Arteaga Botello y la Doctora Carmina Jasso López, pero esta última, además, añade que la video vigilancia trasgrede derechos fundamentales, puesto que violenta el “derecho a no ser discriminado, a la protección de datos personales y desde luego a la privacidad” (Jasso López, 2023, p. 346). En el mismo sentido se posiciona el investigador Vladimir Elizalde, quien ha expresado que, “efectivamente, puede constituir una violación al derecho a la privacidad, o pueden recabarse datos o informaciones que tampoco sabemos cuál es el tratamiento que se les está dando” (Ramírez, 2023).

Contrario a lo antes expuesto, las empresas dedicadas a la venta de tecnologías digitales, como *Genetec*, así como los estados del país, pugnan por el uso de la video vigilancia, principalmente en los entornos escolares¹, opinión a la que se han unido

¹ Muestra de ello, la Ciudad de México, que cuenta con una Ley que regula el uso de tecnología para la seguridad pública, donde se considera la instalación de cámaras de video vigilancia en

grupos de la sociedad civil, padres de familia y maestros, expresando las bondades que generan su utilización, principalmente como una herramienta de prevención del delito y de seguridad pública, uso con el cual concuerda el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) y que fue plasmada en la Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública

Por esta razón, los habitantes del país, incluidos a los niños, niñas y adolescentes², son percibidos por las cámaras de video vigilancia instauradas en los espacios abiertos de sus ciudades, como calles, parques, edificios públicos etc., que, en su tránsito, logran obtener sus rasgos y características, incluso su identificación biométrica facial, toda vez que, en la actualidad, la tecnología ha evolucionado desmedidamente y ha pasado de “los primeros sistemas solo incluían cámaras en blanco y negro conectadas a monitores [...] hasta el reconocimiento facial” (Cadavid Parra, 2017).

Ahora bien, es importante reflexionar si es permitido que el Estado sobreponga la utilidad del uso de la tecnología en beneficio de una mayoría, a costa de limitar y vulnerar los derechos fundamentales de sectores minoritarios, como es la niñez³, surgiendo el cuestionamiento de si la video vigilancia en México protege o vulnera los derechos humanos de las personas en condición de niñez, por lo que esta discusión se desarrollará siguiendo el enfoque garantista de Luigi Ferrajoli, quien indica que deben de imponerse límites a la función estatal, pugnando por el cumplimiento, protección y efectividad de los derechos de todas las personas, y en el caso concreto de los niños, niñas y adolescentes, los cuales son reconocidos tanto a nivel constitucional e internacional.

Esta investigación es de tipo cuantitativo, utilizando documentos bibliográficos, así como los que se encuentran en internet, principalmente de índole normativo, de carácter internacional y nacional, que exponen la protección de las infancias, y la regulación de la video vigilancia en el país, así como estadísticas otorgadas por el Instituto Nacional de Geografía y Estadística (INEGI) sobre realidades de la niñez y de la instalación y funcionamiento de las cámaras de video vigilancia, así como la

las escuelas de cualquier nivel; incluso, el Gobierno de Querétaro, en este año, está evaluando su implementación, y en ambos casos es para la prevención y la seguridad pública.

² La Convención de los Derechos del Niño ha establecido que *niño* es todo ser humano menor de dieciocho años de edad, y en México, adoptando este criterio, se ve reflejado en su Constitución Política al considerar que es ciudadano la persona con dieciocho años de edad, replicando en los ordenamientos civiles, para el ejercicio de sus derechos.

³ En el año 2020, se contabilizó que en México había 38.3 millones de personas en condición de infancia, representando el 30.4% de la población nacional (INEGI, 2021).

revisión de notas periodísticas que evidencian casos concretos sobre el tratamiento de esta tecnología.

I. Marco jurídico de protección de las infancias en México

México, al formar parte del sistema universal de protección de los derechos humanos, debe de dar cumplimiento a lo contenido en la Declaración Universal de los Derechos Humanos, instrumento que no regula en forma especial los derechos de los infantes, pero si precisa que ellos deben de tener una atención especial en sus cuidados y en su asistencia (Declaración Universal de los Derechos Humanos, 2023, art. 25).

Es la Convención de los Derechos del Niño la que, a lo largo de sus 54 artículos, desarrolla los derechos de las infancias, así como mecanismos de supervisión para su cumplimiento y vigilancia. Para tal efecto ha instaurado al Comité de los Derechos del Niño (CDN). Cabe mencionar que este documento normativo fue ratificado por México en el año de 1990, y es a partir de ese momento en que su acatamiento es obligatorio, debiendo de ajustar sus legislaciones internas al contenido de la Declaración.

De esta manera es que el Comité de los Derechos del Niño, como órgano que supervisa el cumplimiento y vigilancia de la Convención, elabora observaciones a los países adheridos, cuya “finalidad de examinar los (sic) progresos realizados en el cumplimiento de las obligaciones contraídas” (UNICEF, 1989, art. 43.1), donde se tratan temas prioritarios que requieren atención inmediata para la preservación de los derechos de los infantes y que se traducen en refuerzos para su cumplimiento, interpretación y aplicación de la Convención,.

Para este trabajo, sirve de apoyo la *Observación General 25 sobre los derechos del niño en relación con el entorno digital*, elaborada en el año 2021, en el que se han establecido los parámetros en que los Estados deberán de asegurar la aplicación de los derechos ahí instituidos en el mundo de las tecnologías, en los que debe de destacarse los principios de: *no discriminación, supervivencia y desarrollo, el interés superior de las infancias y el respeto de las opiniones de las personas en condición de niñez* (Comité de los Derechos del Niño, 2021, apartado III).

En esta observación, se atribuye a los Estados el deber de efectuar periódicamente revisiones a sus legislaciones, en específico sobre la materia de privacidad y protección de datos, así como a las medidas preventivas, todo ello para que no se cometan, de forma intencional o accidentalmente, violaciones a la privacidad de los niños, niñas y adolescentes, tanto en “entornos públicos, como calles, escuelas, bibliotecas, lugares de deporte y esparcimiento y locales comerciales, como tiendas y cines, además del hogar” (Comité de los Derechos del Niño, 2021, párr. 70).

Además, esta observación es enfática, al establecer que, con respecto a las cámaras de video vigilancia, los Estados deben de asegurar que:

[...] las tecnologías digitales, los mecanismos de vigilancia, como los programas informáticos de reconocimiento facial, y la elaboración de perfiles de riesgo que se utilizan en la prevención, la investigación y el enjuiciamiento de delitos no se apliquen injustamente a los niños sospechosos o acusados de delitos y no se utilicen de manera que vulneren sus derechos, en particular su derecho a la privacidad, a la dignidad y a la libertad de asociación (Comité de los Derechos del Niño, 2021, párr. 119).

De lo anterior, resulta el deber utilizar prudentemente la video vigilancia como herramienta auxiliar en la impartición de justicia tratándose de niños, niñas y adolescentes, toda vez que se debe garantizar y proteger sus derechos ampliamente, con el fin de evitar trasgresiones en forma indiscriminada, en especial a los relativos a la privacidad, la dignidad y la libertad de asociación.

Ahora bien, esta observación no solo es dirigida a los Estados, si no que, tratándose de la protección de las personas en condición de infancia, involucra a la sociedad civil para que participen en la elaboración, aplicación y evaluación de las leyes, programas y políticas públicas respecto al uso de las tecnologías, pero que difundan los derechos que los infantes tienen en este ámbito (Comité de los Derechos del Niño, 2021, párr. 34); señalando, además, que las empresas que ofertan productos digitales sean éticos en su elaboración y diseño, máxime que se trata de la población infantil, exponiendo los riesgos y beneficios que acarrea su uso, para lograr la efectiva protección y de respeto de los derechos de los infantes (Comité de los Derechos del Niño, 2021, párr. 39).

Todos estos criterios son tomados por la Corte Interamericana de Derechos Humanos, apropiándose de los principios de la Convención de los Derechos del Niño, toda vez que, como se ha manifestado, es el marco legal especializado de protección de los niños, reconociéndolo en el *Caso de los Niños de la calle* [Villagrán Morales y otros] vs. Guatemala, en su párrafo 194, ya que, relativo a la niñez, la Convención Americana sobre Derechos Humanos solo establece que “todo niño tiene derecho a las medidas de protección que su condición de menor requiere por parte de su familia, de la sociedad y del Estado” (Convención Americana sobre Derechos humanos, 1978, art. 19).

Como puede observarse, la dogmática internacional referente a los infantes es abundante y México la ha trasladado a su normatividad interna, iniciando con reformas constitucionales en las que se reconoce a los niños, niñas y adolescentes como sujetos de derechos, insertando el principio de igualdad, y el *principio de interés superior de la niñez*, atribuyéndole al Estado su cumplimiento en las decisiones y actuaciones que realice para garantizar sus derechos (Constitución Política de los Estados Unidos Mexicanos, 2024, art. 4).

Por ello, es que se expide la Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA) aplicable a todo el país, cuyo objetivo es garantizar su protección y prevención, así como establecer las obligaciones por parte del Estado, de los padres

y/o de las personas que los tienen bajo su cuidado, incluso a la sociedad en general (Ley General de Niños, Niñas y Adolescentes, 2023).

Con esta ley se crean las Procuradurías de Protección de Niñas, Niños y Adolescentes y la Secretaría Ejecutiva del Sistema Nacional de Protección de Niñas, Niños y Adolescentes, como instituciones que tienen a su cargo garantizar el cumplimiento de estos derechos.

La Suprema Corte de Justicia de la Nación ha emitido diversas sentencias y jurisprudencias que ayudan a reforzar los derechos de las infancias, las cuales son abundantes y no se abordarán en esta investigación, pero todas ellas derivan de la reforma constitucional efectuada en el año 2011 en la materia de los derechos humanos, ordenando atender las normas de la ley fundamental del país y de los tratados internacionales.

II. Normatividad aplicable en materia de video vigilancia respecto a la protección de datos personales en México

Este apartado se plantea la forma en que deben de tratarse, a nivel Constitucional y legal, los datos personales; posteriormente, se abordarán los lineamientos existentes en la administración pública sobre la video vigilancia, en la que se justifica su instalación, ubicación y uso; y, por último, el reconocimiento que la Suprema Corte de Justicia ha otorgado a esta tecnología en la impartición de justicia.

En realidad, no existe a nivel federal una norma que regule especialmente la video vigilancia, pero si hay leyes y/o reglamentos en los treinta y dos estados del país cuyos preceptos, en lo general, legalizan la adquisición, ubicación, instalación y funcionamiento de las cámaras de video vigilancias; de igual manera, refieren el tratamiento de los datos personales obtenidos por ellas; ligeramente comentan sobre la protección de derechos humanos; incluso, mencionan sobre el almacenamiento y destrucción de las grabaciones, así como las infracciones y tipos penales que se aplican a los servidores públicos que hagan mal uso de ellas.

Así pues, la falta de un marco jurídico adecuado en la materia se debe principalmente a que la tecnología evoluciona demasiado rápido, contrario a la emisión de normas por parte del órgano legislativo, pero, también, a la forma desproporcionada en que se han implementado las cámaras de video vigilancia en el país, al existir estados con mayor número de cámaras que otros, por lo que el interés de regulación es diverso, dependiendo de la visualización de sus efectos, así como de la cuestión presupuestal.

Independientemente del número de cámaras existentes, la captación de imágenes a través de videocámaras facilita la exposición de datos personales, los cuales se deben de precisar como “cualquier información concerniente a una persona física identificada o

identificable” (Ley General de Protección de Datos Personales en Posesión de Sujetos obligados, 2017, art.3).

Además, la Constitución del país ha elevado la protección de los datos personales como un derecho humano, como bien se plasma en el artículo 16, segundo párrafo, al expresar que:

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, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros (Constitución Política de los Estados Unidos Mexicanos, 2024).

De modo que, para lograr esta protección, se ha dictado a nivel federal la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y, por lo que apunta al orden estatal, cada entidad federativa ha emitido una para tal efecto; también se ha regulado este tema para el ámbito privado, dictándose Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual solo se hace mención, sin profundizar en ella.

Derivada de esta protección normativa en cita, es que los sujetos obligados⁴ tienen el deber de proteger el derecho a la protección de datos personales, como por ejemplo la imagen, quedando implícitas las infancias, incluso accionar ante la Unidad de Transparencia del Sujeto Obligado los derechos de acceso, rectificación, cancelación y oposición de los mismos, también conocidos como derechos ARCO, precisando que son supuestos de excepción *a los principios vigentes* sobre datos personales.

Es oportuno precisar que, cuando se habla de supuestos de excepción, la constitución se refiere a los principios que deben regir en el tratamiento de datos personales, que son “licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad” (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, art.16).

En relación con el nivel internacional, la Convención sobre Derechos Humanos no incluye expresamente en su contenido el derecho a la propia imagen; sin embargo, el artículo 11 sí establece que “nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada” (Convención sobre Derechos Humanos, 1969), por lo que, al

⁴ Cuando se habla de sujetos obligados, los que se ubican “en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos” (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, art. 1).

concatenarse con lo establecido en el artículo 16 de la Constitución del país, se refuerza esta protección de datos personales, ya que, para que no se cumpla, es necesaria la existencia de una orden fundada y motivada que restrinja este derecho; en caso contrario, implicaría una trasgresión grave.

Ahora bien, tratándose del uso de esta tecnología para lograr seguridad pública y consolidar la paz, la administración gubernamental ha trabajado al respecto, dictando diversos documentos, los cuales implementan, a través de normas y conocimientos técnicos, la forma en que debe de usarse y la forma en que deben de colocarse, así como su ubicación; por ello, es que el Sistema Nacional de Seguridad Pública (SNSP), considerando la utilidad que la video vigilancia ofrece para lograr seguridad pública, pugna por el manejo de sistemas de video vigilancia 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” (Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la Seguridad Pública, 2016, p. 1).

Pero el Sistema Nacional de Seguridad Pública (SNSP) ha destacado que, ante el uso de este sistema de video vigilancia, no deben de olvidarse el respeto a los derechos humanos de las personas; por lo tanto, propone efectuar una capacitación a todo el personal que tenga a su cargo la operatividad de ellos.

Actualmente, el Gobierno Federal ha contemplado como un objetivo estratégico el “mejorar las capacidades tecnológicas de investigación científica en los ámbitos de seguridad pública” (Presidencia de la Republica, 2019), sin especificar a detalle la forma en cómo es que podría realizarse este fortalecimiento.

Por consiguiente, en el año 2023, con la “finalidad de disuadir la incidencia delictiva, las instituciones de seguridad pública de las 32 entidades federativas han implementado diversas tecnologías orientadas a la prevención, investigación, y persecución de los delitos” (Roldan, 2023), elaborándose como prioridad nacional el subprograma Fortalecimiento de los sistemas de video vigilancia y geolocalización, y es a través del Secretariado Ejecutivo del Sistema Nacional de Seguridad Publica, quien se encargara de dotar de recursos tecnológicos en materia de video vigilancia, con la participación de todos los niveles de gobierno, para un intercambio de información.

Con ello se constituye la justificación oficial para considerar a la video vigilancia como una solución de seguridad pública, plasmada en normatividad; asimismo, se considera un mecanismo de procuración de justicia, toda vez que la Suprema Corte de Justicia de la Nación ha considerado que es posible que estas tecnologías se puedan constituir como prueba para acreditar una detención en flagrancia, ya que se monitorea el lugar en donde se cometió el hecho delictuoso inmediatamente después de ejecutado, registrándose lo sucedido a detalle y siempre que el seguimiento del presunto infractor

se realice en tiempo real, sin existir interrupción del recorrido de la persona y que ésta sea detenida en un tiempo razonable al cometer la falta (Tesis: I.1o.P. J/3 (10a.), 2018). Cumplidas estas exigencias se garantiza la legalidad de la detención, logrando así un fortalecimiento a la seguridad jurídica, pero también proporcionando seguridad pública de forma inmediata.

III. La video vigilancia en México, ¿protege o vulnera los derechos humanos de las personas en condición de niñez?

Después de haber expuesto la normatividad aplicable a la protección de los infantes, la regulación existente en México respecto a las cámaras de video vigilancia, y su uso en la impartición de justicia, además de la legislación que protege los datos personales de los ciudadanos, en este apartado se procederá a efectuar el análisis respecto a si la video vigilancia en México protege o vulnera los derechos humanos de las personas en condición de niñez.

Por este motivo, se parte de los postulados del garantismo establecido por Luigi Ferrajoli, en el que, a través de los derechos fundamentales, que son aplicables a todas las personas, se limita el poder de las autoridades, maximizando su protección y restando la actuación arbitraria del Estado, los cuales, para proporcionar seguridad jurídica, se encuentran plasmados en cuerpos normativos, como es la Constitución y en los Tratados Internacionales y, en el caso de los niños, niñas y adolescentes, ya se ha determinado la normatividad específica que les aplica, así como en el ámbito de estas tecnologías.

Es por ello que cuando las autoridades del país o de los estados pretendan ejercitar acciones o legislar respecto al tema de la video vigilancia, inicialmente deben de considerar la existencia de la diversidad de grupos que conforman la sociedad, y que cada uno de ellos tienen sus características propias, como es el caso de la población infantil y adolescente, a quienes deben de proporcionar una protección especial.

Por consiguiente, los tres niveles de gobierno y todas las personas adultas, en atención a la perspectiva implícita en la legislación, deben de asimilar que la niñas, niños y adolescentes son sujetos de derechos, sin gozar de la autonomía que tienen los adultos; es por ello que, ante la toma de decisiones que afecten sus derechos, los infantes deben ser informados al respecto, pues así podrán externar sus opiniones (de acuerdo a su edad y madurez) sobre los temas que les perjudiquen, lo cual constituirá un “intercambio de pareceres entre niños y adultos sobre la elaboración de políticas, programas y medidas en todos los contextos pertinentes de la vida de los niños” (Comité de los Derechos del Niño, 2009).

Conviene destacar que el énfasis que se efectúa a los derechos del sector infantil y de adolescencias no se debe a mero capricho. Esto deriva de que son un grupo en riesgo, el cual es discriminado atendiendo sus condiciones de vida, como por ejemplo

la pobreza, el analfabetismo, las preferencias sexuales, la religión, discapacidad, emociones etc., pero principalmente por su condición natural de edad (desarrollo y madurez), que hace que los adultos los minimicen en sus derechos y se crean los únicos con el poder de decisión sobre ellos, poniendo a los niños, niñas y adolescentes en situación de desventaja. Por este motivo, también se ha impulsado y se debe de garantizar el derecho a la igualdad y la no discriminación; asimismo, la aplicación del interés superior de la niñez, que es un principio constitucional, además de un criterio orientador y de interpretación para todas las autoridades.

Así pues, este marco jurídico debe de ser entendido y respetado por todas las autoridades, mismo que debe de ser empleado en la elaboración de acciones y/o programas públicos, y de políticas públicas, en los que intervengan los derechos infantiles, principalmente atendiendo a los nuevos contextos que se presentan en la realidad, como lo es el uso de las tecnologías, porque, se repite, su omisión dificulta la aplicación de los derechos de la infancia y adolescencia.

Por lo tanto, el anteponer el interés superior de las infancias, en todas y cada una de las acciones estatales, hace que se constituya un límite a su actuar, toda vez que se constituye como “vínculos normativos idóneos para asegurar efectividad a los derechos subjetivos” (Ferrajoli, 1996, p. 28), por lo que la niñez puede defenderse de esos abusos o trasgresiones a sus derechos, ya que, a través de lo instituido en la ley, le impone a la autoridad un freno en su forma de actuar frente a determinados actos.

Con lo expresado anteriormente, no significa que los derechos de la infancia deban de verse desde un enfoque utilitarista, o sea pugnar sobre la existencia de un beneficio mayor para este sector y así disminuir los derechos del resto de la población, lo que obviamente acarrearía un panorama de desigualdad y trasgresión de derechos humanos. Por el contrario, lo que se expresa es que si estos derechos entran en conflicto con otros, se debe de considerar primordialmente los atribuidos a los niños, niñas y adolescentes, decidiendo siempre aplicar una medida lesiva lo mínimamente posible.

No debe pasarse por alto que la entidad gubernamental tiene deficiencias para garantizar en forma plena los derechos humanos a todas las personas, como en el caso concreto el de proporcionar seguridad pública. Por ello es que se recurre a diversas opciones, verbigracia los sistemas de vigilancia, cuyo avance tecnológico marcha a pasos agigantados.

Se debe de tener en consideración que no existen evidencias de efectividad, ni tampoco estadísticas, en las que se demuestre que por el uso de las cámaras de video vigilancia se disminuya o se erradique el cuantificado de los delitos y de los actos de violencia en el país; solo existen investigaciones cuyo objeto es por determinadas ciudades, tomando en consideración para su realización la densidad poblacional, el avance tecnológico, por tener un número mayoritario en la instalación de cámaras o porque presentan un alto índice delictivo, pero sin lograr una evidencia en su totalidad del

país, como lo han realizado en la Ciudad de México el Doctor Nelson Arteaga Botello y más recientemente la Doctora Carmina Jasso.

Ahora bien, tocante a las empresas dedicadas a la venta de esta tecnología, los gobiernos estatales, grupos de la sociedad civil, padres, madres y maestros, quienes están a favor de la puesta en funcionamiento de este mecanismo tecnológico, se avocan a exaltar solamente sus beneficios, las características de los equipos de vigilancia y, además, que con ellas posibilitan la ubicación de los trasgresores de la ley. Pero, del mismo modo, no presentan una evaluación que demuestre su efectividad.

Y respecto a la afirmación de que las cámaras de video vigilancia son un apoyo para la ubicación de los responsables de los delitos, la autora Carmina Jasso concuerda con ello, al expresar que si un “delito ocurre y es registrado por una cámara, éste pueda ser atendido debidamente, así el indicador promedio tiempo de respuesta es una forma de aproximarnos a la medición de esta efectividad” (Jasso, 2023, p. 279), es decir la video vigilancia es una herramienta útil, para el apoyo del esclarecimiento de hechos delictivos.

Esto se advierte de diversos casos que son expuestos mediante notas periodísticas. Por ejemplo, se expone el caso de una mujer asesinada en la alcaldía de Tlalpan, lográndose el esclarecimiento de los hechos a través del análisis de las cámaras de video vigilancia que realizó el personal de la Secretaría de Seguridad Ciudadana y el personal de la Fiscalía General de Justicia de la Ciudad de México, desplegando a los policías para la búsqueda de los presuntos responsables (Quintero, 2022), constituyendo así una evidencia que puede ser ofrecida para fincar presuntivamente responsabilidad del hecho delictivo a un individuo en el proceso penal. Incluso, este tema, como se ha indicado anteriormente, fue abordado por la Suprema Corte de Justicia de la Nación, la cual emitió una jurisprudencia en la que se valida el uso de esta tecnología en la detención en flagrancia de un individuo.

Pero como critica, se puede decir que como una forma de protección o prevención no es eficaz, ya que los cuerpos policiacos, al momento en que perciben el delito a través de las cámaras de video vigilancia, no actúan o no llegan rápidamente al lugar en que se está cometiendo el hecho delictuoso para evitarlo, y esto es por distintas causas, como las distancias, la congestión del tránsito vehicular, la falta de personal para atender el suceso, etc.

Y aquí también es importante especificar que el esclarecimiento de los hechos mediante la herramienta tecnológica de la video vigilancia puede verse obstruido por el interés humano, tanto de los policías, del personal encargado de tener a su resguardo los videos obtenidos, del personal de las Fiscalías, de los abogados, incluso de la víctima u ofendido y del investigado, lo que se traduce en el fenómeno denominado corrupción. Se debe de recordar, que México es considerado como uno de los países más corruptos del mundo (Índice de Percepción Global de la Corrupción, 2022), ocu-

pando el lugar 130 de 180, atribuyéndose como servidores públicos más corruptos a los policías y a órganos de impartición de justicia.

Lo anterior se refleja en el caso de la maestra de primaria Laura Ramírez, de 50 años, que fue atropellada por un automóvil en el centro de la Ciudad de México y el responsable se dio a la fuga. Verónica, hija de la finada, se dio cuenta de que había cámaras de seguridad en la intersección donde su madre fue atropellada y, con el fin de dar con el responsable, pidió a la Fiscalía solicitara los videos al Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano (C5), y en las afueras de las instalaciones del órgano investigador, una persona se le acercó a Verónica, identificándose como asistente legal de la oficina del fiscal y le pidió \$4,000.00 (cuatro mil pesos 00/100 M.N.) para que le proporcionara las grabaciones, indicándole que estas se borran pasada una semana. Verónica, junto con apoyo de amigos, logro reunir una cantidad menor a la solicitada, la entregó y, posteriormente, al regresar a la fiscalía, le informaron que las grabaciones no estaban disponibles. Por la insuficiencia de medios de pruebas el caso se cerró, por lo que Verónica lamenta que no se le pudo ayudar a encontrar al asesino de su madre, y que “esta tecnología, que se supone que es un instrumento de justicia, se convirtió en una ficha para la extorsión” (Wattenbarger, 2021).

De igual manera, “la tecnología de reconocimiento facial refuerza la práctica policial racista” (Amnistía Internacional España, 2022), ya que en la ciudad de Nueva York los policías, a través de la vigilancia por reconocimiento facial, realizan detenciones injustificadas a las personas que viven en barrios considerados peligrosos, considerando su color de piel y sus características faciales, pero, además, las personas que se sintieron más expuestas por esta tecnología de reconocimiento facial fueron las que participan en marchas y protestas, ya que, al efectuarse en parque y calles, que tienen cámaras de video vigilancia publica, es más posible que sean identificadas y amedrentadas con el fin de limitar sus derechos humanos (Amnistía Internacional España, 2022).

Por tanto, es de advertirse la existencia de diversas narrativas de personas que ejemplifican las diversas irregularidades que se pueden cometer en contra de sus derechos humanos por el uso de las cámaras de video vigilancia, entre ellos los infantes y adolescentes. Además, se deben de adicionar las anomalías que son atribuidas a la falla de los softwares que controlan los sistemas de video vigilancia, y que pueden dar lugar a la discriminación, trasgrediendo el derecho a la privacidad, a la igualdad, no discriminación, así como a la libertad de reunión.

Justamente, la Red en Defensa de los Derechos Digitales expone los peligros y debilidades que representan las cámaras de video vigilancia, ya que la Comisión Federal de Comunicaciones de Estados Unidos ha expresado que las cámaras de vigilancia *Dahua*, permiten a terceros (*hackers*) tomar el control de los equipos, con el fin de espiar, registrar video (Red en Defensa de los Derechos Digitales, 2022) y, por

consiguiente, obtener datos biométricos de las personas para realizar delitos, ya que en estos tiempos son formas de identificación personal para acceder a plataformas, como la banca en línea o realizar trámites, pudiendo hacer transferencias o pedir préstamos. Lo expuesto, causa alarma, toda vez que cámaras con reconocimiento facial de marca *Dahua* están instaladas en el país, específicamente en el estado de Coahuila, con el fin de proporcionar seguridad pública.

Cabe señalar, también, que la académica Carmina Jasso concluye que se vulneran derechos humanos, toda vez que la “videovigilancia impacta en las ciudades y desde luego en la sociedad, sobre todo aquella que se ha colocado de tal manera que permite la observación constante, permanente y sistemática del espacio público y de la vida de quienes en él habitan y transitan”(Jasso, 2023, p. 15), sin que la mayoría de las veces los individuos tengan conocimiento de que son observados e identificados por la captación de la imagen, por quienes están a cargo de estos sistemas de vigilancia y a través de sus rasgos físicos, vestimenta o accesorios, aplican prejuicios y, por lo tanto, asignan etiquetas a las personas, corriendo el riesgo de que se motive una detención ilegal por basarse en estos estereotipos o una agresión física por parte de la sociedad, conocidos como linchamientos.

Ahora bien, es cierto que los ejemplos presentados refieren a las personas adultas, pero no se debe de olvidar que los niños, niñas y adolescentes transitan en las calles, parques, y todo espacio público en donde se han instalado las cámaras de video vigilancia, y también están expuestos a esta clase de trasgresiones a sus derechos humanos, que son atribuibles al humano, a la propia tecnología y, además, a la influencia de la corrupción.

Derivado de ello, en estos momentos es posible responder el cuestionamiento de si la video vigilancia protege o vulnera los derechos humanos de las personas en situación de infancia en México, y en términos simples se contesta que sí, que vulneran los derechos humanos de las infancias y de todas las demás personas.

Y esto, no significa que la tecnología sea del todo incorrecta, por el contrario, también de los ejemplos brindados se alcanzan a visualizar sus bondades en su uso, incluso los fines que promueven tanto de las empresas tecnológicas y del Estado no son del todo desatinadas, ya que el desarrollo debe de tomarse siempre en beneficio de la humanidad. Pero el actuar debe de ser siempre apegado a la ley, sin visualizar beneficios individuales en materia económica; las buenas practicas deben de prevalecer.

Por ello, es fundamental que todas las autoridades se capaciten en materia de derechos humanos, para que, así, desde el ámbito de competencia, sus actuaciones, leyes, políticas públicas y normas administrativas que se elaboren en materia de seguridad, visualicen el marco normativo implementado para la protección de la infancia, en especial la Observación General 25 sobre los derechos del niño en relación con el entorno digital, pero siempre observando en ellos el interés superior de la

infancia. Porque las leyes y/o reglamentos que imperan a nivel estatal, en forma general, solo regulan la adquisición de las cámaras, su ubicación e instalación, incluyendo el funcionamiento de las mismas, someramente el tratamiento de los datos personales obtenidos por ellas, y el procedimiento administrativo que se aplicará a los servidores públicos que trasgreden su función; pero en la mayoría de estas normas no se observa inserto el principio del interés superior del infante.

Uno de los casos es la Ley de Video Vigilancia para el estado de Baja California Sur, en la que se hace solamente referencia al principio de interés superior, al tratarse de la captación de imágenes por las cámaras de video vigilancia de niños, niñas y adolescentes, sin explicar la forma en que se garantizará por parte de las autoridades involucradas (Ley de video vigilancia para el estado de Baja California Sur, 2022, art. 48).

Esto es porque la actuación del Estado, al emitir sus legislaciones y políticas públicas, debe de proteger la información de las personas en infancia, pero indicar la forma en que su principio rector deberá de manifestarse en su aplicación, ya que la protección de datos personales está estrechamente vinculada al principio del interés superior de niñas, niños y adolescentes, todo con el fin de garantizar, sus derechos de privacidad y seguridad.

Conclusiones

Todas las personas tienen derechos humanos y son protegidas por un marco normativo nacional e internacional. En el caso los infantes y adolescentes, se cuenta con normas especiales que puntualizan una atención específica, delineados por la igualdad, no discriminación e interés superior del niño, niña y adolescente.

La video vigilancia es una herramienta tecnológica favorable a los intereses de los seres humanos, en el que se ubican las infancias, siempre que se respeten el principio de legalidad, que las autoridades mexicanas deben de tener claro los límites legales que la propia norma le marque, proteja y respete la atención especial que se le marca en tratándose de infancias.

Debe de permear que los niños, niñas y adolescentes son sujetos de derechos y, por ello, los estos deben de ser respetados, evitando la discriminación por edad. Por lo tanto, deben de ser informados y escuchados en los temas que les atañe y, en su caso, les perjudique, para que, en conjunto, todos puedan tomar decisiones, elaborar programas, políticas públicas y leyes desde sus diferentes perspectivas.

Se resalta la importancia de que se tenga un marco regulatorio adecuado en las entidades federativas y a nivel federal, que permita la protección de los derechos humanos que potencialmente pueden vulnerarse con la video vigilancia en la ciudad de los infantes; pero, además, que las mismas sean revisadas de forma periódica e, incluso, se reformen atendiendo al avance tecnológico.

Como complemento, es necesario que las irregularidades humanas y tecnológicas mostradas como ejemplos a lo largo de este trabajo, sean subsanadas, sobresaliendo como solución una capacitación de todas las autoridades inmiscuidas.

Referencias

- Al sur. (2021). Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf
- Amnistía Internacional España. (2022). *Estados Unidos: La tecnología de reconocimiento facial refuerza la práctica policial racista en Nueva York*. Amnesty.org. <https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/estados-unidos-lla-tecnologia-de-reconocimiento-facial-refuerza-la-practica-policial-racista-en-nueva-york/>
- Cadavid Parra, J.C. (2017, 16 de noviembre). *Videovigilancia: Historia*. América comunicaciones. <https://www.americacomunicaciones.com/videovigilancia-historia/>
- Caso de los “Niños de la calle” (Villagrán Morales y otros) vs. Guatemala, Corte Interamericana. https://www.corteidh.or.cr/docs/casos/articulos/seriec_63_esp.pdf
- Comité de los Derechos del Niño. (2009). *Observación general número 12, relativa a el derecho del niño a ser escuchado*, <https://www.acnur.org/fileadmin/Documentos/BDL/2011/7532.pdf>
- Comité de los Derechos del Niño. (2021). Observación general número 25 relativa a los derechos de los niños en relación con el entorno digital <https://www.plataformadeinfancia.org/wp-content/uploads/2021/09/observacion-general-25-relativa-a-los-derechos-de-los-ninos-en-relacion-con-el-entorno-digital.pdf>
- Constitución Política de los Estados Unidos Mexicanos, que reforma a las del 5 de febrero de 1957. Cámara de Diputados del H. Congreso de la Unión. Última reforma 18 de noviembre de 2022. Diario Oficial de la Federación 5 de febrero de 1917, (México). Disponible en <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>
- Gallardo, M. (2024). *Analizan poner cámaras de vigilancia en escuelas queretanas*. Diario de Querétaro, <https://www.diariodequeretaro.com.mx/local/analizan-poner-cameras-de-vigilancia-en-escuelas-queretanas-11290444.html>
- Genetec. (s.f.). <https://www.genetec.com/products/unified-security/omnicast>
- https://www.corteidh.or.cr/docs/casos/articulos/seriec_63_esp.pdf
- Human Rights Watch. (2020). *Argentina publica en línea datos personales de niños y niñas acusados de cometer delitos*. <https://www.hrw.org/es/news/2020/10/09/argentina-publica-en-linea-datos-personales-de-ninos-y-ninas-acusados-de-cometer>
- INEGI, Censo nacional de gobierno, seguridad pública y sistema penitenciario 2016. México. <https://www.inegi.org.mx/programas/cngspspe/2016/#Documentacion>
- INEGI, Censo Nacional de seguridad pública estatal 2021. México. https://www.inegi.org.mx/contenidos/programas/cnspe/2021/doc/cnspe_2021_resultados.pdf

Capítulo 7. La video vigilancia en México, ¿protege o vulnera los derechos humanos de las personas en condición de niñez?

- Jasso López, C. (2023). *La ciudad videovigilada: entre la prevención del crimen y el control social* (1ª. ed.). Editorial: Universidad Nacional Autónoma de México <https://ru.iis.sociales.unam.mx/handle/IIS/6081>
- Ley de video vigilancia para el estado de Baja California Sur. (2022). H. Congreso del Estado. <https://www.cbcs.gob.mx/index.php/trabajos-legislativos/leyes>
- Ley que regula el uso de tecnología para la seguridad pública del Distrito Federal, Reformada, Gaceta Oficial de Ciudad de México, 16 de diciembre de 2020, <https://www.congresocdmx.gob.mx/media/documentos/8ea7523101a88c4d0c8c94c7eb166fb5833c5949.pdf>
- Ley General de los derechos de Niñas, Niños y Adolescentes [LGDNNA], Reformada, Diario Oficial de la Federación [D.O.F.], 11 diciembre 2023, (México) <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA.pdf>
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [LGPDPPO], 26 de enero 2017, (México), <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPO.pdf>
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP], 5 de julio de 2010, (México) <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Naciones Unidas (2023), Declaración Universal de Derechos Humanos <https://www.un.org/es/about-us/universal-declaration-of-human-rights>
- Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública. (2016). Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). https://secretariadoejecutivo.gob.mx//docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf
- Presidencia de la República (2019), *Plan Nacional de Desarrollo 2019-2024*, México, Gobierno Federal, en https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019#gsc.tab=0
- Protocolo para juzgar con perspectiva de infancia y adolescencia. (2021). Suprema Corte de Justicia de la Nación. (1a. ed.) <https://www.scjn.gob.mx/derechos-humanos/sites/default/files/protocolos/archivos/2021-11/Protocolo%20para%20juzgar%20con%20perspectiva%20de%20IA%2010nov21.pdf>
- Quintero M, J. (2022, 02 de diciembre). Asesinan a una mujer en Tlalpan; señalan a ex pareja como responsable. La Jornada. <https://www.jornada.com.mx/notas/2022/12/02/capital/asesinan-a-una-mujer-en-tlalpan-senalan-a-ex-pareja-como-presunto-responsable/>
- Ramírez, V.R (2023, 15 de mayo). ¿Sistema de seguridad o sobrevigilancia? El dilema de las videocámaras. IMER Instituto Mexicano de la Radio. <https://noticias.imer.mx/blog/sistema-de-seguridad-o-sobrevigilancia-el-dilema-de-las-videocamaras/>
- Red en defensa de los derechos digitales. (2022, 6 de diciembre). *Estados Unidos veta el uso de cámaras de videovigilancia de las empresas chinas Dahua y Hikvision*. <https://r3d.mx/2022/12/06/estados-unidos-veta-el-uso-de-camaras-de-videovigilancia-de-las-empresas-chinas-dahua-y-hikvision/>

- Roldan, Rodea, Miguel Angel (2023), *Fortalecimiento de los sistemas de video vigilancia y geolocalización*, Centro Nacional de Información (CNI). https://www.gob.mx/cms/uploads/attachment/file/798891/17_FortalecimientoSistemasVideoVigilancia.pdf
- Tesis: I.1o.P. J/3 (10a.). (2018). DETENCIÓN EN FLAGRANCIA. SE ACTUALIZA SI INMEDIATAMENTE DESPUÉS DE QUE EL SUJETO ACTIVO COMETIÓ EL HECHO DELICTIVO, SE LE PERSIGUIÓ MATERIALMENTE SIN INTERRUPCIÓN ALGUNA POR MEDIO DEL MONITOREO DE LAS CÁMARAS DE SEGURIDAD PÚBLICA INSTALADAS EN EL LUGAR DEL EVENTO (LEGISLACIÓN APLICABLE PARA LA CIUDAD DE MÉXICO). En *Semanario Judicial de la Federación*. Décima Época. <https://sjf2.scjn.gob.mx/detalle/tesis/2017234>
- Torres Zarate, F. y García Martínez, F. (2023). El interés superior del niño en la perspectiva del garantismo jurídico en México. *Alegatos*, 21(65), 97–112. <http://alegatos.azc.uam.mx/index.php/ra/article/view/483/471>
- UNICEF. (1989). Convención de los Derechos del Niño. Disponible en <https://www.unicef.org/es/convencion-derechos-nino/texto-convencion>
- Von Hirsch, A. (2007). *Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión*. Revista para el análisis del derecho. https://indret.com/wp-content/themes/indret/pdf/476_es.pdf
- Wattenbarger, M. (2021, 19 de enero 19). *Where surveillance cameras work, but the justice system doesn't*. <https://restofworld.org/2021/mexico-city-security-theater/>

Capítulo 8

Seguridad biométrica en el testamento digital: avances, retos y perspectivas

Biometric Security in the Digital Will: Advances, Challenges, and Perspectives

*Armando Adriano Fabre**

*Modesta Lorena Hernández Sánchez***

Resumen

El objetivo primordial de este trabajo es conocer qué es la biometría, el uso de información biométrica de los individuos en conjunto con la seguridad pública y jurídica que se aplica a trámites cotidianos que realiza la sociedad moderna, tales como el testamento otorgado por medios electrónicos. Se utilizó un método de exploración cualitativa, sustentándose en argumentos doctrinarios, fundamentos de la legislación mexicana, y análisis de derecho comparado, en la que se basa la pertinencia del testamento digital, con la intervención de datos biométricos, como resultado de la modernidad de un país. Esta investigación permite advertir que el uso de la inteligencia artificial para recabar datos biométricos de los individuos, y el empleo de éstos de manera correcta, son una herramienta indispensable para un sistema de manifestación y otorgamiento de la voluntad de manera virtual, pues aseguran la veracidad de estos documentos a través de la identificación y autenticación de la persona que desee otorgar su testamento por medios electrónicos. Se concluye que, más allá de estar a la vanguardia, esta modalidad del testamento reconoce las necesidades de sus habitantes a través de las reformas a las leyes mexicanas que consienten el uso de las nuevas tecnologías de la información y comunicación, combinado con el sistema biométrico, a fin de proporcionar seguridad a los actos jurídicos que realicen los ciudadanos.

Palabras clave: Biometría; Datos biométricos; Huella digital; Testamento; Testamento electrónico.

* Doctor en Ciencias Jurídicas, Administrativas y de la Educación por la Universidad de las Naciones.

** Doctora en Ciencias Jurídicas, Administrativas y de la Educación por la Universidad de las Naciones.

Abstract

The objective of this research is to know what biometrics is, the use of biometric information of individuals and the public and legal security applied to daily procedures carried out by modern society, such as the will granted by electronic means. A qualitative exploration method was used, based on doctrinal arguments, fundamentals of Mexican legislation, and comparative law analysis, in which the relevance of the digital will is based, with the intervention of biometric data, as a result of the modernity of a country. This research allows concluding that the use of artificial intelligence to collect biometric data of individuals, and the use of these data in a correct way, are an indispensable tool for a system of manifestation and granting of the will in a virtual way, because they ensure the veracity of these documents, through the identification and authentication of the person who wishes to grant his will by electronic means. Concluding that beyond being at the forefront, this modality of the will recognizes the needs of its inhabitants through the reforms to the Mexican laws that allow the use of new information and communication technologies combined with the biometric system, in order to provide security to the legal acts performed by the citizens.

Keywords: Biometrics; Biometric data; Fingerprint; Will; Electronic will.

Introducción

El contenido del presente capítulo reviste las características de una investigación exploratoria consistente en un tipo cualitativo, que se sustenta en doctrina especializada y estudio de fundamentos legales sobre el testamento digital y su vinculación con la biometría, la seguridad biométrica y el uso correcto de los datos biométricos que le brindan seguridad pública y jurídica a dicho acto jurídico.

Para alcanzar ese propósito se parte de lo general a lo particular, haciendo mención sobre la conceptualización de la biometría que, en palabras sencillas, es el estudio de los rasgos de un individuo para reconocerlo. Siguiendo esa línea, se abordan las generalidades de los datos biométricos, su definición y los tipos mayormente utilizados por las nuevas tecnologías. Conociendo la definición de la biometría y los datos biométricos, se presentan los usos de estos datos, tales como la identificación, autenticación y otorgamiento del consentimiento, que están estrechamente vinculados con la seguridad biométrica y abarca desde el uso de la nueva inteligencia artificial útil para la obtención de datos biométricos, el uso de datos biométricos como medio de seguridad, hasta el conocimiento de lo que prevé la legislación sobre el tema.

Para acotar las consideraciones en torno a esta investigación, se establece un análisis de las leyes mexicanas que contemplan el otorgamiento por medios electrónicos del testamento y leyes extranjeras que, de igual manera, establecen esta modalidad en sus normativas; tal es el caso de Perú y Brasil. Asimismo, se examina la relación que se vislumbra entre el testamento digital y su vinculación con los datos biométricos, como herramienta eficaz para reconocer y autenticar el consentimiento de la persona

que se identifique a través de patrones biométricos debidamente empleados, en virtud de que resulta un medio inequívoco para dar veracidad a un documento tan importante como lo es el testamento, que involucra el patrimonio y certeza jurídica de las personas que deciden otorgarlo de manera virtual.

El capítulo concluye con la exposición de los retos que enfrenta el testamento otorgado de forma electrónica y cómo el uso de las herramientas científicas, como lo es la firma electrónica avanzada verificada por datos biométricos, es la solución a la incertidumbre que, en un momento dado, puede generar la realización de un trámite digital.

1. Generalidades

1.1. La biometría

A pesar de considerarse una ciencia del futuro, es importante destacar que tiene antecedentes históricos que datan de la época de los egipcios, quienes, por medio de la antropometría, tenían fórmulas fijas para la representación del cuerpo humano, las cuales se estudiaban para identificar tanto la complexión, rasgos faciales o características destacables que ayudaban a clasificar e identificar a los obreros que participaban en la construcción de las pirámides (Russ, 2004). Asimismo, la civilización china también merece mención, pues, como señala Jeffery G. Barnes (2011), la cultura china es la primera conocida por haber manejado impresiones de crestas de fricción para identificar a las personas, dado que existen registros donde se observa que desde la antigüedad se hacía uso de la impresión de la huella dactilar como un instrumento de identificación y, desde luego, individualización.

Ahora bien, para comprender correctamente qué es la seguridad biométrica, primeramente se tiene que tener esclarecido el concepto de biometría. Sánchez Calle (2005, p. 10) sostiene que dicho término procede de dos vocablos griegos: *bios*, que significa vida y *metron* que significa medida. Es decir, se refiere al estudio de medidas utilizadas para el reconocimiento de la vida, particularmente del ser humano, basándose en los rasgos físicos y conductuales del ser. Los seres humanos, al ser seres únicos, se pueden individualizar estudiando los rasgos corporales únicos e inigualables.

En relación con la idea anterior, Martínez García (2007) brinda una perspectiva tecnológica donde pretende explicar qué es la biometría, a lo que responde que es la “práctica tecnológica de identificar a un individuo por sus rasgos biológicos y conductuales”. Asimismo, destaca que la combinación de la tecnología con la biometría se logra con el “uso de técnicas matemáticas auxiliadas por computadora, conocida como biometría informática”, dando por resultado la construcción de la identidad biométrica del individuo.

1.2. Datos biométricos

Tomemos en consideración el criterio de la Dra. Díaz (2013), quien dice que los datos biométricos “constituyen información referente a las medidas y características tanto fisiológicas como morfológicas de los seres vivos, a través de técnicas manuales o automatizadas”. Igualmente, la autora hace hincapié en que no todas las características físicas y morfológicas pueden y deben ser consideradas como datos biométricos, dado a que en diversas ocasiones se tienen que utilizar múltiples datos biométricos para elaborar un reconocimiento o autenticación.

En la guía de datos biométricos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI (2018, p. 5), los datos biométricos son definidos como “las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles”. Para esclarecer el término, se afirma que los datos biométricos son diversos y se complementan unos con otros para identificar a cada individuo; estos se obtienen a partir de mecanismos tecnológicos que estudian las características que hacen a una persona única. Tal situación abarca tanto a las tipologías físicas como a las conductuales y fisiológicas que dan como resultado la confirmación de la identidad de imágenes faciales, vocales o dactilares.

Cabe añadir que estos datos biométricos tienen la principal característica de ser universales, en virtud de que todos los individuos las poseen; son únicos, debido a que cada ser humano es diferente; son permanentes, en razón a que se mantienen con el paso del tiempo; y son medibles, en virtud de que son cuantificables. En adición a lo anterior, se mencionan los datos biométricos mayormente estudiados.

La huella dactilar es el dato biométrico con mayor popularidad. Como se mencionó en líneas anteriores, su uso se ha dado desde la antigüedad. La guía de datos biométricos supracitada (INAI, 2018) nos proporciona información sobre cómo podemos identificar a este dato biométrico; dice que depende de la manera de su estructura, pues las huellas dactilares “se forman a partir de la superficie desigual de la piel de los dedos de la mano, en donde se identifican diversas protuberancias y hendiduras conocidas como crestas y valles, las cuales se encuentran dispuestas de modo único”. Es importante destacar que recolectar la información de las huellas dactilares es muy común, porque implica un procedimiento sencillo. Entonces, para identificar la información que contienen y estar en condiciones de ser categorizada como un dato biométrico, se utiliza la técnica biométrica automatizada basada en minucias, que son un patrón único e individualizado de cada huella dactilar.

Otro dato biométrico que ha cobrado popularidad es el reconocimiento facial, sobre todo porque la mayoría de las personas lo conocen debido a su uso a través de dispositivos móviles como teléfonos inteligentes, computadoras, tabletas inteligentes, entre otros. Al respecto, Gimeno Hernández (2010, p. 8) argumenta que el reconocimiento

facial toma varias características que pueden ser físicas, por ejemplo las pupilas, estructura facial, iris, entre otras; y también características psicológicas, por ejemplo los gestos, en donde el registro de la información facial se da en tres pasos principales, que son detectar el rostro, capturar la información y traducir los rasgos, para finalmente comparar la información y verificarla. Por otra parte, la Organización Internacional de Policía Criminal (2020), INTERPOL por sus siglas en inglés, parte de una visión amplia, en la que da a conocer que, dentro de los factores de la identificación facial se encuentran elementos que son alterables, pues se pueden involucrar cambios por envejecimiento, cirugía estética, uso de cosméticos, efectos del consumo excesivo de sustancias nocivas, la pose de la persona e, incluso, la calidad de la imagen.

También conforme a lo dicho por el INAI, dentro de los datos biométricos que funcionan con rasgos físicos se encuentra el reconocimiento de iris, donde se reconocen patrones que están marcados desde el nacimiento y rara vez se modifican con el paso del tiempo; en un caso similar se encuentra el reconocimiento de retina, el cual está basado en el modelo de los vasos sanguíneos, que es único. Igualmente, la geometría de la mano, que para determinarla es necesario la captura de imágenes en tercera dimensión, a fin de poder estudiar las características de la mano, tales como: grosor, longitud y curva de los dedos, articulaciones y estructura ósea (INAI, 2018, p. 10)

Además de lo anterior, existen registros de datos biométricos que se basan en información, como el comportamiento y la personalidad de un individuo; los más utilizados son el reconocimiento de firma, que es determinada por el análisis del movimiento de la mano, forma, velocidad, presión al apoyar el lapicero, y el tiempo para realizar una firma; el reconocimiento de escritura, el cual está basado en rasgos de escritura como inclinación y precisión; el reconocimiento de voz, la cual es determinada por sistemas de inteligencia artificial que miden la semejanza de los ejemplares para devolver un resultado —cabe indicar que este dato biométrico es muy utilizado por las instituciones bancarias, a través de la vía telefónica—; el reconocimiento de escritura de teclado, midiendo la fuerza infringida de tecleo, la continuación de pulsación etc., así como el reconocimiento de la forma de andar (INAI, 2018, p. 11).

1.3 Uso de los datos biométricos

Su utilidad consiste en reconocer a los individuos que han sido registrados en una base de datos, pues el sistema biométrico implica realizar una comparación de forma manual o automatizada de las muestras biométricas previamente registradas.

La identificación de un individuo requiere comparar sus muestras biométricas contra una base completa de datos biométricos, sin que sean necesarios otros datos como nombre, nacionalidad, fecha de nacimiento; no obstante, si la base de datos cuenta con la relación completa del individuo, será más eficiente.

En función de lo planteado, una forma simple del uso cotidiano de datos biométricos es a través del lector de huellas digitales, ya sea para acceder a diferentes dispositivos electrónicos o aplicaciones móviles, registrar la asistencia en el lugar de trabajo, o para restringir o permitir el acceso a sitios exclusivos, como áreas restringidas de un hospital o instituciones bancarias, por mencionar algunos. Otro uso es para robustecer bases de datos, por ejemplo, como medio de control migratorio, donde al ingresar un dato biométrico, se puede obtener información de la persona de manera inmediata. En el ámbito penal se utiliza para identificar a un imputado, al hacer un reconocimiento pronto del individuo; en adición a lo anterior, también se usan con mayor frecuencia para registrar la identidad de las personas al momento de realizar transacciones financieras, con el objeto de protegerla de daños patrimoniales o jurídicos, de ahí la importancia de éstos como herramienta de seguridad.

Ahora bien, sobre los antecedentes del uso de los datos biométricos en México, López Vázquez (2017, p. 73) señala a Benjamín Martínez como introductor de la dactiloscopia en México, quien en el año 1920 escribió su *Manual de dactiloscopia mis lecciones*, en el que se enfocó en la identificación de los individuos en asuntos criminalísticos; sin embargo, es importante destacar la forma en la que se fueron introduciendo los conocimientos biométricos en México, dado a que el uso de éstos se ha visto reflejado en la evolución tecnológica y vanguardista que persigue el país.

El autor Leandro Ucciferri (2019, p. 26) afirma que en el año 1992 se publicó una reforma a la Ley de Población que obligaba a los mexicanos a registrar sus datos ante el Registro Nacional de Población e Identidad, incluyendo la huella dactilar, que sería ligada a la Clave Única del Registro de la Población, CURP por sus siglas en español, esto para obtener una cédula de identificación. Posteriormente, en el año 2011, mediante decreto presidencial, se agregó la recolección de otros datos biométricos, tales como el iris de los dos ojos, las diez huellas digitales y la fotografía biométrica, recolectando información de millones de personas, a pesar de ser un programa al que no se le dio continuidad después del 2018.

Sin duda, estas medidas iban encaminadas a definir e identificar a la población para cuestiones estadísticas, pero también para avanzar en temas de seguridad pública. Aun cuando en el pasado se detuvo el programa para crear una cédula de identificación, ciertamente, las bases de datos de diversas instituciones públicas hacen uso de datos biométricos. Algunos ejemplos son: el Instituto Nacional Electoral, INE por sus siglas en español, el cual recopila estos datos de identificación; también lo hace el Servicio de Administración Tributaria, SAT por sus siglas en español, pues al momento de emitir la firma electrónica de los contribuyentes se recoge la información biométrica de estos.

Si bien es cierto que el uso más común de la información biométrica radica en la identificación de los individuos, también se pueden utilizar para otras actividades. Tal

es el caso de la autenticación y el otorgamiento del consentimiento; de tal modo que la conjugación de estos tres usos da lugar a un reconocimiento completo de la persona y su voluntad, como se aborda en líneas posteriores.

2. Seguridad biométrica

2.1 La inteligencia artificial en la obtención de datos biométricos

Ya se mencionó que los datos biométricos de cada ser humano poseen características universales, en virtud de que todos cuentan con estos; sin embargo, son únicos e irrepetibles. En las generalidades e historia del conocimiento de los datos biométricos se encuentran técnicas manuales que han evolucionado a técnicas automatizadas que obtienen estos datos, en el que la inteligencia artificial juega un papel de suma importancia para esta tarea, dado que su protagonismo está determinado por la rapidez y precisión con la que maneja la información. Como consecuencia de su avance a pasos agigantados, resulta imprescindible entender sus alcances, así como la urgente necesidad de su regulación en México, ya que se requiere dotar de certeza al manejo de datos personales, lo que se traduce en un tema relevante de seguridad pública.

Según Rouhiainen (2018, p. 17), la inteligencia artificial puede ser definida como “la habilidad de los ordenadores para hacer actividades que normalmente requieren inteligencia humana” o, de forma específica, “la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones, tal y como lo haría un ser humano”. Esta habilidad se mejora constantemente con el uso de la inteligencia artificial, llegando a parecer bastante humano.

Es demasiada la evolución de la inteligencia artificial en temas de manejo de datos biométricos; tan así que el jurista Lorenzo Cotino (2022, p. 70) ha documentado y argumenta que el Reglamento de Inteligencia Artificial Europeo plantea que el uso de ésta no solo se limita a la identificación del individuo, sino que va más allá, identificando o infiriendo emociones e intenciones de las personas a partir de sus datos biométricos. Tales avances, ponen en tela de juicio los riesgos que pueden ocasionar estos sistemas y se ha establecido la obligación de promover una inteligencia artificial segura que respete los derechos fundamentales.

Ahora, en el contexto de este análisis, conviene identificar cuáles son los principales riesgos del uso de la inteligencia artificial en datos biométricos. Commatteeo y Moreyra (2022, p. 32) destacan que, a pesar de que los métodos de identificación facial son una tecnología creada para fines militares, el mercado de consumidores de plataformas móviles y de *social media* utiliza esa tecnología en sus aplicaciones. Uno de los ejemplos más comunes es el etiquetado de fotografías en redes sociales, donde la base de datos de estas aplicaciones reconoce los rostros de los contactos, viéndose

afectada su privacidad, a la que, en muchas ocasiones, los usuarios no prestan la suficiente atención, al aceptar las condiciones de uso de estas aplicaciones –sin tener conocimiento sobre su contenido– con tal de estar actualizados en las redes sociales. Este tipo de utilidad puede significar problemas jurídicos, en virtud de que representan un peligro real para la privacidad personal y de terceros. Asimismo, también representan un riesgo en materia de derecho a la igualdad, debido al margen de error que los sistemas de reconocimiento facial contienen, por lo cual, quienes utilizan esta tecnología, como por ejemplo las instituciones de seguridad, deben tener presente que pueden existir fallas, precisamente para no afectar derechos fundamentales como el derecho a la libertad de expresión, el principio de inocencia, derecho a la igualdad, entre otros.

2.2 El uso de datos biométricos como medio de seguridad

La información de datos biométricos es sensible y personal, y, si bien tienen sus ventajas y facilitan cuestiones del día a día del ser humano moderno, también tienen que protegerse. El principal beneficio del uso de esta tecnología radica en la seguridad que se les da a las personas de que no se suplantarán o robarán su identidad; en el ámbito privado se refleja en las transacciones bancarias o en el uso de tarjetas de crédito, donde ya se normalizó la verificación de datos biométricos antes de realizar algún movimiento, dando certeza a la protección de la identidad y, por ende, seguridad a su patrimonio.

En nuestro país, las instituciones públicas también utilizan los datos biométricos de los ciudadanos para robustecer sus medidas de seguridad y expedir diferentes documentos oficiales, por ejemplo, el pasaporte electrónico mexicano, que, conforme al acuerdo publicado en el Diario Oficial de la Federación (2021) –por el cual se instituyó el contenido de éstos–, los pasaportes electrónicos incluyen un chip que almacena de forma electrónica datos biométricos que garantizan la seguridad de los solicitantes, pues el documento se vuelve más seguro, dificultando la suplantación de identidad.

Por su parte, el INE (2020) registra en su padrón electoral a los ciudadanos mexicanos que solicitan su inscripción para obtener su credencial para votar; asimismo, recolecta información biométrica de éstos, tales como huellas digitales y rasgos faciales para evitar la duplicidad de registros; actualmente, las credenciales para votar cuentan con un código de respuesta rápida que contiene la imagen de la huella digital de los ciudadanos.

Otro ejemplo es el servicio de acreditación biométrica del SAT (2018), que busca garantizar la identidad, integrando distintos componentes para desarrollar el proceso de acreditación de identidad a partir de la verificación y digitalización de documentos probatorios; resaltando que la información biométrica que se capturan incluye las huellas dactilares e iris; recordando que la captura y resguardo de éstos es esencial para crear la e-firma que utilizan los contribuyentes para realizar diferentes trámites.

2.3 El derecho mexicano en la protección de datos biométricos

Se ha mencionado que el uso de los datos o información biométrica es indispensable en el mundo moderno, donde la generalidad de las personas están inmersas en la digitalización de sus actividades diarias; Sin embargo, estos datos son únicos y delicados, por lo cual merecen un tratamiento especial. Al respecto, el INAI propone, en su guía para el tratamiento de datos biométricos (INAI, 2018, p. 41), obligaciones esenciales para la obligación de seguridad en el tratamiento de datos biométricos, mismos que significan efectuar medidas físicas, técnicas, incluso administrativas, indispensables para garantizar que los datos biométricos de los ciudadanos estén protegidos del acceso, procesamiento, exclusión, pérdida o usos no autorizados, por lo que es menester examinar que la tecnología biométrica observe mecanismos de cifrado en el acopio y tránsito de datos, limitar el acceso a estos datos únicamente al personal autorizado, archivar la información por medio de bitácoras, evitar cruces superfluos de información, adquirir sistemas biométricos que usen únicamente la plantilla con minucias en el caso de huellas dactilares, minimizar el uso de bases de datos centralizadas para el almacenamiento de biométricos, contar con un sitio alternativo para resguardar las bases de datos biométricos y considerar lo previsto en estándares internacionales.

Lo antes descrito se encuentra relacionado con el derecho fundamental a la protección de datos personales, que implica el derecho humano a la privacidad y a la intimidad. En nuestra Carta Magna, el artículo 6º, apartado A, fracción II, marca que la información referente a los datos personales y vida privada será protegida en los términos salvo las excepciones fijadas en la ley; asimismo, el artículo 16, párrafo segundo, establece que todas las personas cuentan con el derecho al acceso, protección de sus datos personales, cancelación y rectificación de estos; igualmente, pueden manifestar su oposición al uso de estos en los términos que establezca la ley, la cual instituirá los supuestos de excepción a los principios que rijan el tratamiento de datos por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. Por su parte, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares tiene la finalidad de graduar el tratamiento, controlado, legítimo y entendido de los datos personales, para confirmar la privacidad y el derecho a la autodeterminación, aun cuando no es específica en cuestión de datos biométricos y al ser el tratamiento de éstos uno de los retos principales del derecho mexicano, establece las funciones de protección de manera generalizada.

En relación con la idea superior, la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados busca instaurar los principios y procedimientos que avalen el derecho que poseen todas las personas a que sus datos personales sean debidamente protegidos en posesión de sujetos obligados; entiéndase por sujetos obligados por esta ley, a las autoridades en el ámbito federal, estatal y municipal, a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judi-

cial, así como los órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Esta Ley indica que organizaciones como los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, son responsables del tratamiento de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En el contexto de este análisis, se resalta que, nuevamente, esta ley no especifica el uso y administración de datos biométricos, sino que se incluyen de manera tácita como parte de los datos personales, siendo una deficiencia en la ley, misma que requiere reformarse de manera urgente, en sentido de consolidar un correcto tratamiento en el contenido de los datos biométricos como garantía de una seguridad pública y jurídica.

Dentro de los precedentes relacionados con la protección de los datos e información biométrica, la Suprema Corte de Justicia de la Nación emitió la resolución de Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 (2022), instaurada por diversos senadores de la República Mexicana, integrantes de la LXIV Legislatura, y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en la que solicitaron se declarara la invalidez del decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión en virtud de que ésta fue declarada procedente y fundada, logrando la invalidez de la totalidad del sistema normativo que integra el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el 16 de abril de 2021; precisando que en esta resolución se destacó la protección a los datos personales reconocida en el artículo 16 constitucional, y se enfatizó la inconstitucionalidad de la recopilación de datos biométricos en bases de datos masivos por parte del Padrón Nacional de Usuarios de Telefonía Móvil, dado que el empleo de éstas incide en el derecho a la privacidad y la protección de datos, por lo que tiene un alto potencial de afectar la libertad de expresión, el acceso a la información y los derechos de asociación e igualdad.

Dentro de este marco, el voto concurrente del Ministro de la Suprema Corte de Justicia de la Nación apuntó que los datos biométricos son categorizados como información personal sensible, que en los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano de la Organización de Estados Americanos, OEA por sus siglas en español, se precisa que dichos datos deben ser tratados de manera especial por lo riesgoso que puede tener un mal tratamiento o divulgación indebidos. En el mismo tenor, el Ministro también hizo mención al Reglamento Europeo General de Protección de Datos (2016) y el Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales, aprobado en México (2018), que establecen una protección para los datos biométricos que identifiquen de manera única a una persona. Posteriormente, también equiparó este derecho internacional con la Ley General de Protección de Datos Personales en Posesión de

Sujetos Obligados, que se mencionó en líneas superiores, la cual, si bien es cierto no es específica, el jurista Zaldívar señala que la información biométrica encuadra en la definición de datos sensibles prevista en la ley mexicana.

3. Manifestación de la voluntad a partir del uso de datos biométricos

Tomando la información expuesta con anterioridad, es menester establecer las diferencias entre los usos de los datos biométricos para reconocer a una persona y que ésta manifieste su voluntad, así como los posibles usos que se conjugan para determinar la voluntad, destacando que ambos pueden significar una herramienta vanguardista para manifestar la voluntad de las personas en medios electrónicos que agilizarían trámites de forma exponencial.

Ruiz Marín explica en su obra la manera en que se consigue la identificación de las personas por su información biométrica. La identificación biométrica consiste en reconocer a una persona por sus rasgos o características biofísicas o de comportamiento; se logra siguiendo un sistema de identificación biométrica que se basa en dos fases: la primera, de reclutamiento, donde se toman las muestras del usuario y se procesan para obtener un patrón y almacenar la información; y la segunda, la fase de utilización, donde, una vez almacenado el patrón, se puede usar el sistema con normalidad (2009, p. 30).

En cuanto a la autenticación biométrica, es la verificación que se hace efectiva cuando responde a interrogativas encaminadas a descubrir si el usuario o sujeto dice la verdad sobre su identidad; es decir, el sistema biométrico se encarga de dar respuesta a la interrogante bajo el patrón del usuario, comparándolo con el umbral de similitud contenido en la base de datos (2009, p. 33).

En ese orden de ideas, una vez identificado al sujeto y verificado su identidad, con base en su perfil biométrico, se puede manifestar libremente la voluntad de la persona haciendo uso de medios electrónicos. En tal sentido, conviene puntualizar lo que señala el artículo 1803 del Código Civil Federal (1928):

El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

- 1) Será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
- 2) El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad debe manifestarse expresamente.

En relación con lo anterior, uno de los principios del tratamiento de los datos biométricos es precisamente el consentimiento, que cuando se requiera, debe ir ligado a

finalidades específicas; esto es, debe ser concreto, no general. También se añade que éste debe ser informado, por lo que antes de obtenerse es indispensable que el titular conozca su aviso de privacidad.

En esta tesitura, la multicitada guía de datos biométricos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2018, p. 27) señala que, para obtener el consentimiento, se deben reunir ciertas características, por ejemplo: la libertad, donde no debe existir, error, violencia, mala fe, o dolo que perjudiquen a la manifestación de la voluntad del sujeto; asimismo, debe ser específico, pues debe referirse a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales; igualmente, tendrá que ser informado, debido a que el titular debe conocer el aviso de privacidad, previo al tratamiento al que serán sometidos sus datos personales y la consecuencia de otorgar su consentimiento; por último, será inequívoco, dado a que deben existir elementos que de manera indubitablemente demuestren su otorgamiento, en el caso del consentimiento expreso y expreso a través de un escrito.

4. El testamento otorgado por medios electrónicos

Lo hasta aquí precisado permite afirmar que existe la posibilidad de manifestar la voluntad a través de medios electrónicos, verificando la identificación, autenticación, y consentimiento obtenidos a través de los datos biométricos. Esto abre las puertas a nuevas posibilidades de automatización de trámites, que anteriormente solo se concebían como rigurosamente presenciales, pero ahora, forman parte de la revolución digital que facilitan el día a día de las personas.

Bajo tal esquema, el testamento es el documento en el que, por excelencia, se manifiesta la voluntad cuando se decide el destino que tendrá un patrimonio después de la muerte de su titular; no obstante, en México son muy pocas las personas que deciden otorgar uno, ya sea por desconocimiento, desidia, o por el tiempo que requiere realizarlo. De acuerdo con la encuesta sobre servicios notariales para el Colegio de Notarios de la Ciudad de México, realizada por el Instituto de Investigaciones Sociales Aplicadas (2022, p. 49), solo un 23% de los encuestados respondió que sí tienen un testamento; de modo que este tipo de comportamiento se puede modificar si se cuenta con herramientas que abran paso a la vanguardia y, a su vez, faciliten su otorgamiento con el apoyo de las Tecnologías de la Información y Comunicación.

El Código Civil para el Estado de Veracruz contempla diferentes tipos de testamentos: el público abierto, regulado a partir del artículo 1444 al 1451; el público cerrado, regulado a partir del artículo 1454 al 1482; el público simplificado y el ológrafo, contemplado en los artículos 1483 al 1497; el privado, que se da bajo ciertos supuestos esenciales, su regulación se encuentra a partir del artículo 1498 al 1511; el militar, verificado a partir del artículo 1512 al 1515; el marítimo, contemplado del

artículo 1516 al 1525; y el hecho en un país extranjero, dispuesto a partir del artículo 1526 al 1531.

En ese orden de ideas, el Código Civil del Estado de Veracruz, prevé diversas situaciones que implican que las personas no puedan realizar su testamento bajo las premisas comunes del testamento público abierto; sin embargo, la sociedad, sus necesidades y sus actividades diarias cambian y evolucionan de forma imprevista, tal es el caso de la pandemia por SARS CoV-2, causante de la enfermedad Covid-19, que, sin esperarlo, obligó a que todos estuviéramos en confinamiento obligatorio por la gravedad de la enfermedad y su rápida propagación y, a pesar de que la actividad notarial fue considerada por la Secretaría de Salud como esencial (2020), las circunstancias advirtieron la desactualización en la legislación al no prever ningún otro medio ajeno a la presencialidad para su verificativo. En suma, se evidenció la necesidad de que la legislación contemplara la emisión de un testamento, con apoyo de recursos electrónicos y del sistema biométrico, como medio que coadyuve a brindar seguridad y certeza jurídica.

4.1 El testamento digital: reformas al Código Civil de la Ciudad de México

Actualmente existen reformas al Código Civil de la Ciudad de México y al Código Nacional de Procedimientos Civiles que, sin duda, ponen en la lupa este tema. Un claro avance en materia de seguridad jurídica en el testamento se ve reflejado en las adiciones y reformas al Código Civil de la Ciudad de México, mediante decreto publicado el 4 de agosto del año 2021 en la Gaceta Oficial de la Ciudad de México, así como las reformas y adiciones a la Ley del Notariado para la Ciudad de México, publicado en la misma Gaceta, siendo los cambios más significativos los señalados en los siguientes artículos:

Código Civil para el Distrito Federal.

Artículo 1392 Bis. El legado también puede consistir en la titularidad sobre bienes o derechos digitales almacenados en algún equipo de cómputo, servidor, plataforma de resguardo digital, dispositivo electrónico, redes sociales o dispositivos físicos utilizados para acceder a un recurso restringido electrónicamente, los cuales pueden consistir en: I. Cuentas de correo electrónico, sitios, dominios y direcciones electrónicas de internet, archivos electrónicos tales como imágenes, fotografías, videos, textos; y II. Claves y contraseñas de cuentas bancarias o de valores, aplicaciones de empresas de tecnología financiera de los que el testador sea titular o usuario y para cuyo acceso se requiera de un nombre o clave de usuario, clave y contraseña. Los bienes o derechos digitales serán independientes de su valor económico y contenido determinable. [...]

Artículo 1520. El testamento público abierto también podrá otorgarse ante notario en el ámbito de su actuación digital, de conformidad con las disposiciones aplicables de la Ley del Notariado para la Ciudad de México. El notario, en el ámbito de su actuación digital, y de conformidad con la Ley del Notariado para la Ciudad de México, redactará las cláusulas del testamento, sujetándose estrictamente a la voluntad del testador y las leerá en voz alta para que éste manifieste su conformidad o, en su caso, también podrá reenviar el archivo electrónico al testador a efecto de que sea leído por él mismo, cualquiera de estas dos circunstancias se hará constar en el testamento. Una vez que el testador estuviese conforme, lo hará saber al notario y procederá a firmar el testamento, haciendo uso de su Firma Electrónica Avanzada reconocida conforme a la Ley del Notariado para la Ciudad de México. Se tendrá como fecha y hora de otorgamiento del testamento la que aparezca en el estampado de la hora correspondiente a la Firma Electrónica Avanzada reconocida por la Ley del Notariado para la Ciudad de México y como lugar la Ciudad de México.

Artículo 1520 bis. El testamento público abierto también podrá realizarse por medios electrónicos, siempre que el testador cuente con la posibilidad de comunicarse con el notario a través de un dispositivo electrónico y el notario pueda ver y oír al testador, así como hablar con él de manera directa, simultánea y en tiempo real durante todo el acto del otorgamiento. Lo anterior se actualizará cuando el testador se encuentre en alguno de los siguientes supuestos: I. Ante peligro inminente de muerte; II. Sufra al momento una enfermedad grave o contagiosa; III. Haya sufrido lesiones que pongan en riesgo su vida; o IV. Se encuentre en un lugar al que, por una situación excepcional, no se pueda acceder en persona. En caso de que el testador se encuentre en alguno de los supuestos a que se refieren los artículos 1515, 1516 o 1517, no podrá llevarse a cabo esta modalidad del testamento público abierto.

Del contenido anterior, resulta atractiva la posibilidad de otorgar un testamento público abierto a través de dispositivos electrónicos, teniendo como forma de identificación y autenticación la firma electrónica avanzada del testador. Aunque, de momento, el Código Civil de la Ciudad de México solo prevé cuatro supuestos para proceder a otorgar un testamento digital, representa un cambio significativo en los principios y valores en los que se solía cimentar nuestro sistema jurídico.

En cuanto a las reformas y adiciones a la Ley de Notariado para la Ciudad de México, se destacan los siguientes artículos:

Artículo 2. [...] I. Administración Pública: administración pública de la Ciudad de México; I bis. Actuación Digital Notarial: el ejercicio de la función notarial a través de medios electrónicos, ópticos o de cualquier otra tecnología, en el entorno de un protocolo digital, con equivalencia funcional al protocolo ordinario; II. [...] II bis. Apéndice del Instrumento Electrónico: sección del instrumento electrónico donde el Notario archiva y conserva, en formato digital, con su Firma Electrónica Notarial, los documentos y demás elementos relacionados con la escritura o acta de que se trate y son parte integrante del protocolo digital. Los documentos y elementos digitalizados deberán indexarse como lo determine el

Reglamento. El apéndice del instrumento electrónico es accesorio del protocolo digital y obra como complemento de los juicios y fe documental del Notario. Lo anterior no impide la validez y veracidad de los documentos o elementos archivados o indexados, ni la validez independiente de certificaciones que se hagan con base en ellos; III. a VII. [...] VIII. Certificado Electrónico: mensaje de datos o registro que confirma el vínculo entre un firmante y una clave privada; VIII bis. Ciudad: Ciudad de México; IX. a XX. [...] XXI. Firma Electrónica Notarial: Firma Electrónica Avanzada o Firma Electrónica de la Ciudad de México, según corresponda. Será empleada por el Notario a través del Sistema Informático, cuenta con el mismo valor jurídico que la firma autógrafa y su sello de autorizar en los términos de la normativa aplicable. El uso y reconocimiento de la Firma Electrónica Notarial podrá extenderse a los tres niveles de gobierno en los casos y términos que así lo determine la legislación correspondiente; XXI bis. Firma Electrónica para la Actuación Digital Notarial: Firma Electrónica Avanzada o Firma Electrónica de la Ciudad de México, según corresponda, otorgadas conforme a la normativa aplicable. Será empleada por un prestatario del servicio notarial a través del Sistema Informático, cuenta con el mismo valor jurídico de la firma autógrafa y le permite expresar su consentimiento en el otorgamiento de instrumentos electrónicos en el protocolo digital.

En el contexto de este análisis, las reformas y adiciones señaladas amplían el escenario para otorgar un testamento por medio de instrumentos electrónicos y, además, remarca la urgencia de regular también el legado digital, es decir, la gestión de toda aquella información que tenemos almacenada en la web como consecuencia de nuestra interacción en el mundo digital.

El testamento online y digital, pareciera que son términos iguales, pero no es así. Al respecto, Giner Gandía (2016, p. 56) señala que el primero, es aquel que se realiza por medios digitales, mientras que el segundo, se trata de un documento legal por medio del cual se le gira instrucciones a una persona sobre cómo debe manejar su herencia digital, designando un albacea que cumpla su última voluntad sobre activos digitales existentes, incluso para el cierre de cuentas en la web, acogándose al derecho al olvido.

En respuesta de lo anterior, la Suprema Corte de Justicia de la Nación (2022) se pronunció en su resolución del amparo en revisión número (341/2022), donde la quejosa y recurrente denominada Asociación Civil Red en Defensa de los Derechos Digitales promovió juicio de amparo contra el último párrafo del artículo 1392 bis del Código Civil para el Distrito Federal –ahora Ciudad de México– por considerar que la regulación que derivaba de dicha porción normativa respecto de la cancelación de datos personales de personas fallecidas era contraria a la libertad de expresión y al derecho al libre acceso de la información, a lo que la Primera Sala de la Suprema Corte de Justicia de la Nación determinó la inconstitucionalidad del último párrafo del artículo en cuestión, remarcando que la eliminación o cancelación de los datos de las personas fallecidas resulta contraria a la libertad de expresión y al derecho a la infor-

mación. De igual manera, remarcó su postura sobre el derecho al olvido, que no puede ser aplicado sin calificaciones en México, en razón a que la Constitución establece la presunción de que toda información pública debe permanecer con dicho carácter, sin que el tiempo sea determinante en la pérdida del interés público.

Ahora bien, la Suprema Corte de Justicia de la Nación no se ha pronunciado en contra, ni ha declarado la inconstitucionalidad del testamento otorgado por medios electrónicos, lo cual se considera un paso positivo hacia la modernización del citado trámite. Tal como se refirió en líneas superiores, es de suma importancia promover y facilitar la elaboración del testamento para brindar seguridad jurídica sobre nuestro patrimonio; sin embargo, tal hipótesis aun no es realidad para todos los estados de la República Mexicana.

4.2 El testamento otorgado por medios digitales en otros países

A continuación, se exponen algunas ideas de derecho comparado que sustentan la urgencia de la creación del testamento por medios electrónicos, que sea verificado por datos biométricos, para brindar mayor seguridad jurídica y pública.

4.2.1 Perú

En cuanto al avance que refleja Perú en la materia, el pasado 11 de agosto del año 2021 se publicó la Ley que modifica el artículo 696 de su Código Civil (2021), con el que hace más sencillo el otorgamiento del testamento por escritura pública, y modifica el artículo 38 del decreto legislativo 1049, decreto legislativo del notariado sobre la forma de llevar los registros.

Las modificaciones al artículo 696, relativas a las formalidades esenciales del testamento por escritura pública, implican el uso del sistema biométrico como medio de validación de la identidad del testador y de los testigos, establecidos por el Registro Nacional de Identificación y Estado Civil (2021), como se advierte a continuación:

Que estén reunidos en un solo acto, desde el principio hasta el fin, el testador, el notario y dos testigos hábiles. El notario está obligado a verificar la identidad del testador y los testigos a través del documento de identidad y los medios de identificación biométrica establecidos por el Reniec. Cualquiera de los testigos puede actuar como testigo a ruego del testador o testigo de identidad. [...] 3. Que el notario escriba el testamento de su puño y letra o a través de medios de tecnología informática u otros de naturaleza similar, en su registro de escrituras públicas, pudiendo insertar, de ser el caso, las disposiciones escritas que le sean entregadas por el testador. (2021, p. 3)

Ahora bien, la modificación al decreto legislativo, sobre la manera en que se deben llevar los registros, se destaca el artículo 38:

Artículo 38. Forma de llevar los Registros El registro se compondrá de cincuenta fojas ordenadas correlativamente según su numeración. Podrán ser llevados de dos maneras: [...] b) En cincuenta hojas de papel emitido por el colegio de notarios, que se colocarán en el orden de su numeración seriada, para permitir el uso de sistemas de impresión computarizado, de tecnología informática u otros de naturaleza similar, o para que el registro se efectúe a mano.

Sin duda, estas reformas y modificaciones al Código Civil de Perú dan respuesta a las necesidades de los ciudadanos peruanos, aunado a los beneficios que acarrea, como, por ejemplo, el impulso de la cultura testamentaria y reducción de costos. A pesar de los beneficios, queda la incertidumbre de si otorgar testamento por medios electrónicos garantiza la seguridad jurídica.

4.2.2 Brasil

Este país es otro ejemplo de vanguardia en modernización de las formas de presentación de testamentos, pues su legislación ya contempla la posibilidad de un testamento digital, con el apoyo del sistema biométrico.

Vaz (2019, pp. 1-5) nos cuenta que el pasado 3 de octubre del año 2021 se aprobó el proyecto de ley 5820/2019, que se justifica argumentando que el Código Civil de Brasil, formulado en la década de los 70's hasta su aprobación en 2002, no cuenta con innovaciones tecnológicas en una era donde la realidad virtual está presente en la vida cotidiana de las sociedades, se estima urgente, modernizar la ley para adaptarse a la nueva realidad social.

Este proyecto propone, entre sus modificaciones, una nueva redacción para el artículo 1881, estipulando que la disposición del testamento puede ser escrita, firmada al final o realizada por medios electrónicos con firma electrónica; asimismo, dentro de las modificaciones se incluye a la herencia digital –videos, fotos, libros cuentas de redes sociales, entre otros contenidos en la nube–; para hacer válido este documento deberá cumplir con los requisitos estipulados en la ley.

Cabe destacar que, para realizar este tipo de testamento, es indispensable utilizar un sistema digital que haga reconocimiento de sonido e imagen, que cuente con nitidez y claridad, el formato deberá grabarse en un formato compatible con los programas de lectura computarizados y autorizados para la ejecución del acto; además, es menester mencionar que el testamento deberá estar firmado digitalmente por el testado con reconocimiento facial y encriptación (Vaz, 2019, pp. 1-5).

Si bien es cierto que estas modificaciones al Código Civil brasileño son innovadoras, y necesarias, atraen escepticismo sobre su funcionamiento, veracidad, y efectividad, debido a que el testamento electrónico está sometido bajo pena de nulidad del acto, lo cual deja abierta la puerta a la incertidumbre, acerca de la aceptación o negación de la validez del documento; sin embargo, se estima que esta cláusula es necesaria debido a que, al final, este documento será evaluado por un notario público investido de fe pública, quien será quien determine que tal documento se realizó de forma correcta y le dará validez al mismo. Desde luego, el testamento otorgado por medios electrónicos es un acierto que debe tomar en consideración el uso de los datos biométricos como herramienta para verificar la autenticidad del mismo.

Continuando con la idea anterior, los datos biométricos son una herramienta útil e indispensable para realizar trámites de manera virtual, porque, si bien es cierto que muchos de los trámites que se realizan por medios electrónicos se validan con una firma electrónica personal, no menos cierto es que verificar la identidad de las personas por medio de datos biométricos le daría mayor certeza a los mismos.

4.3 La firma electrónica simple, la firma electrónica avanzada y la firma electrónica biométrica

La revolución digital que atraviesa la sociedad moderna requiere de transformaciones digitales y avances tecnológicos para agilizar sus actividades cotidianas. Debido a lo anterior, la firma digital es esencial para darle certeza a los trámites y procesos automatizados en la actualidad.

4.3.1 La firma electrónica

En su reporte técnico, Morales Sandoval, Díaz y Domínguez (2013, p. 1) nos dicen que la firma electrónica simple implica “el uso de cualquier medio electrónico para firmar un documento”, es decir, una firma realizada de forma autógrafa, escaneada y agregada a un documento digital puede ser considerada como firma electrónica; sin embargo, este tipo de firma no reúne requisitos de integridad y no repudio.

4.3.2 La firma electrónica avanzada

Esta firma, también distinguida como firma digital, se otorga por medio de un certificado digital que es emitido por una entidad con certificación acreditada. Este archivo está integrado por una serie de información electrónica que identifican al firmante a través de una llave pública, cuyo archivo está encriptado y únicamente el firmante debe tener acceso a éste; su principal uso es validar la identidad de quien envía un mensaje o firma un documento electrónico para verificar que el mismo es original y no ha sido modificado (Morales Sandoval, Díaz y Domínguez, 2013, p. 2).

4.3.3 La firma electrónica biométrica

De acuerdo con Musa Murillo (2019, p. 60), la firma electrónica biométrica es un tipo de firma electrónica avanzada que hace uso de datos biométricos, por ejemplo, la huella dactilar, u otros perfiles biométricos como los rasgos físicos, el iris, la voz, el rostro, entre otros; convirtiéndose en un mecanismo sólido de autenticación.

4.4 Retos del testamento por medios electrónicos

Anteriormente se expuso el caso del tratamiento del testamento otorgado por medios electrónicos en Brasil, que, se estima, es el país que contempla la forma más completa de otorgarlo, en comparación con la Ciudad de México y Perú, que, en sus reformas a los Códigos Civiles, dan apertura a esta modalidad para otorgar testamento, con sus excepciones, contemplándolo solo como un método de urgencia, aunado a que no prevé la autenticación del otorgante por medio de datos biométricos.

Otorgar el testamento por medios electrónicos tiene sus retos en torno a las situaciones específicas en las que se debe encontrar el otorgante para optar por esta vía, además de la resistencia de la sociedad actual que se niegue a usar este medio, por desconfianza en el trámite, porque, si bien es cierto que, para las nuevas generaciones, la opción de realizar trámites por medios electrónicos es algo que es de su preferencia y, por lo tanto, confían en el uso de estas herramientas, empero, las generaciones pasadas son renuentes a tales cambios por el desconocimiento de cómo utilizar las plataformas y dispositivos electrónicos, situación que contribuye a que aumente su desconfianza en el uso de los mismos.

El reto más importante para el testamento otorgado por medios electrónicos es el uso de una firma avanzada y la verificación de la identidad y autenticidad del otorgante por medio de un sistema de reconocimiento biométrico avanzado, pues, si bien es cierto que gran parte de las y los mexicanos contamos con e-firma, que es un documento encriptado que reúne información biométrica del individuo, no menos cierto es que este archivo se puede almacenar en unidades de memoria flash y el resguardo de este documento no llega a ser efectivo, pudiendo caer en manos de otras personas ajenas, que puedan utilizarla sin el consentimiento del dueño del archivo; por lo tanto, es indispensable que para realizar un testamento por medios electrónicos, que es un trámite de suma relevancia patrimonial, debe existir todo un mecanismo en línea que permita realizar grabaciones de video, de voz, firma electrónica avanzada y, por último, comparación de la firma con algún dato biométrico, por ejemplo, el uso de la huella dactilar a través de algún lector de huella.

Conclusión

A lo largo de esta investigación se advirtió que las necesidades de la sociedad actual requieren nuevas herramientas tecnológicas que faciliten las actividades de los individuos, usando tecnología como la biometría, que esté debidamente regulada y signifique una conjugación que ayude al país a alcanzar estándares de seguridad pública y jurídica.

Las herramientas tecnológicas existen y están al alcance de todos; sin embargo, es urgente tomar los beneficios que estas tecnologías nos ofrecen para garantizar la armonía, respeto de los derechos de los ciudadanos, crecimiento, innovación seguridad y tranquilidad, en temas relevantes como lo es el testamento emergente u otorgado por medios electrónicos, que, por la naturaleza del mismo, puede generar desconfianza en algunas personas por la falta de conocimiento de los beneficios que puede traer consigo utilizar estos medios, o por recelo a temas como la suplantación de la identidad, que puede ser previsible, precisamente utilizando los sistemas automatizados biométricos.

Finalmente, se puntualiza que, en nuestro país, el derecho avanza lento, lo cual es cierto, pero se sigue impulsando mediante investigaciones que muestran panoramas sobre qué ocurre a nuestro alrededor o cómo otros países dan respuesta a las nuevas necesidades de la sociedad. Por lo demás, con esta investigación sintetizada se considera que se explica la necesidad de conocer las tecnologías biométricas aplicadas a temas jurídicos, como lo es el otorgamiento de la última voluntad en un testamento.

Bibliografía

- Acción de Inconstitucionalidad 82/21. (2022, 26 de abril). Suprema Corte de Justicia de la Nación.
- Cámara de senadores del Honorable Congreso de la Unión. (2018). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Diario Oficial de la Federación.
- Commatteo, G., y Moreyra, P. (2022). Discriminación 4.0: una aproximación a los problemas que suscitan la biometría y los sistemas de reconocimiento facial. *Revista Internacional de Derechos Humanos*, 12(1), 15-53. <https://doi.org/2422-7188>
- Congreso de la República. (11 de Agosto de 2021). Ley que modifica el artículo 696 del código civil, facilitando el otorgamiento de testamento por escritura pública, y modifica el artículo 38 del decreto legislativo 1049, decreto legislativo del notariado, sobre la forma de llevar los registros. *Diario Oficial El Peruano*, pág. 3. <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/114101/143233/F-12802741/L%2031338%20PER.pdf>
- Cotino Hueso, L. (2022). Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal. *El cronista del estado social y democrático de derecho*(100), 68-79.

- Díaz Rodríguez, V. (Junio de 2013). Sistemas biométricos en materia criminal: un estudio comparado. *Revista IUS*, Vol. 7(No. 31), 28-47. <https://doi.org/18702147>
- Gimeno Hernández, R. (Mayo de 2010). *Escola Tècnica Superior d'Enginyeria Industrial de Barcelona*. Retrieved 6 de Mayo de 2023, from Estudio de Técnicas de reconocimiento facial: https://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC_RogerGimen_o.pdf
- Giner Gandía, J. (2016). El testamento digital sí existe y ya ha llegado. En R. Oliva León, y S. Valero Barceló, *Testamento ¿Digital?* (págs. 56-66). España: Juristas con futuro. <https://doi.org/978-84-617-4521-0>
- H. Asamblea Legislativa del Distrito Federal. (2018). *Ley del Notariado para la Ciudad de México*. Diario Oficial de la Federación.
- H. Congreso de la Unión. (1917). *Constitución Política de los Estados Unidos Mexicanos*. México: Diario Oficial de la Federación.
- H. Congreso de la Unión. (1928). *Código Civil para el Distrito Federal*. Diario Oficial de la Federación.
- H. Congreso de la Unión. (2010). *Ley Federal de protección de datos personales en posesión de los particulares*. Diario Oficial de la Federación.
- H. Congreso de la Unión. (2017). *Ley General de protección de datos personales en posesión de sujetos obligados*. Diario Oficial de la Federación.
- H. Legislatura del Estado de Veracruz. (1932). *Código civil para el estado de Veracruz de Ignacio de la Llave*. Diario Oficial de la Federación.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2018). *Guía para el Tratamiento de Datos Biométricos*. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Instituto Nacional Electoral. (24 de Enero de 2020). *Tarjeta informática: Sobre el Padrón Electoral y los Datos Biométricos*. Central Electoral: <https://centralectoral.ine.mx/2020/01/24/tarjeta-informativa-padron-electorallos-datos-biometricos/>
- INTERPOL. (2020). *INTERPOL*. <https://doi.org/COM/FS/2020-03/FS-04>
- Investigaciones Sociales Aplicadas. (Septiembre de 2022). *Investigaciones Sociales Aplicadas*. Retrieved 01 de 05 de 2023, from Encuesta sobre servicios notariales en la Ciudad de México: <https://invesoc.com/contenido/ISCN2209p.pdf>
- Jeffery G. Barnes. (2011). Capítulo 1: Historia. En E. Holder, L. Robinson, J. Laub, y A. McRoberts (Ed.), *El libro de referencia de las huellas dactilares* (págs. 7- 25). Washington, DC: Departamento de Justicia de los Estados Unidos, Oficina de Programas de Justicia.
- López Vázquez, D. (Abril- Junio de 2017). Los primeros criminalistas en México. *Visión criminológica- criminalística*, Año 5(18), 70-74. <https://doi.org/20075804>
- Martínez García, J. C. (2007). El reinado de la biometría. *¿Cómo ves?*(104), 10-14.
- Morales Sandoval, M., Díaz Pérez, A., y Domínguez Pérez, L. J. (2013). *Firma electrónica: concepto y requerimientos para su puesta en práctica*. Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional.

- Musa Murillo, N. (2019). *Mecanismos de validación de identidad y firma electrónica certificados en la adquisición de productos o servicios comercializados en medios electrónicos*. Universidad Externado de Colombia.
<https://doi.org/https://doi.org/10.57998/bdigital.handle.001.2892>
- Parlamento Europeo y del consejo. (2016). *Reglamento europeo general de protección de datos*. Parlamento europeo y del consejo.
- Rouhiainen, L. (2018). *Inteligencia artificial 101 cosas que debes saber hoy sobre nuestro futuro*. Barcelona: Planeta. <https://doi.org/978-84-17568-08-5>
- Ruiz Marín, M., Rodríguez Uribe, J. C., y Olivares Morales, J. C. (septiembre de 2009). Una mirada a la biometría. *Avances en sistemas e informática*, 6(2), págs. 29-38. <https://doi.org/1657-7663>
- Russ, D. (16 de Septiembre de 2004). *Building*. Retrieved 03 de 05 de 2023, from Biometrics myths ... six of the best.: <https://www.building.co.uk/biometricsmyths--six-of-the-best-/3040687.article>
- Sánchez Calle, Á. (2005). *Aplicaciones de la visión artificial y la biometría*. Madrid: Dykinson.
- Secretaría de Relaciones Exteriores. (2021). *Acuerdo por el que se establece el contenido de los pasaportes electrónicos mexicanos*. México: Diario Oficial de la Federación. Retrieved 8 de Mayo de 2023, from https://www.dof.gob.mx/nota_detalle.php?codigo=5630645&fecha=23/09/2021#gsc.tab=0
- Secretaría de Salud. (2020). *Acuerdo por el que se establecen acciones extraordinarias para atender la emergencia sanitaria generada por el virus SARS-CoV2*. Diario Oficial de la Federación.
- Servicio de administración tributaria. (05 de 03 de 2018). *Preguntas frecuentes*. <http://www.sat.gob.mx/personas/resultado-busqueda?words=biom%C3%A9trico&locale=1462228413195&tipobusqueda=predictiva#>
- Suprema Corte de Justicia de la Nación. (2022). *Sentencia Amparo en revisión 341/2022*. Suprema Corte de Justicia de la Nación.
- Ucciferri, L. (Abril de 2019). Tú y yo digital Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México. México. Retrieved 7 de Mayo de 2023, from <https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf>
- Vaz, E. (31 de 10 de 2019). *Projecto de lei nº 5820/2019*. Câmara dos deputados Gabinete do Deputado Federal Elias Vaz: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1829027&filename=PL%205820/2019
- Zaldívar Lelo de Larrea, A. (25-26 de Abril de 2022). *Voto concurrente que formula el Ministro Presidente Arturo Zaldívar Lelo de Larrea en la acción de inconstitucionalidad 82/21 y su acumulada 86/21*. Suprema Corte de Justicia de la Nación: <https://www.scjn.gob.mx/sites/default/files/transparencia/resoluciones/documentos/AI-82-2021-Voto-Concurrente-Ministro-Presidente-Zaldivar.pdf>

Capítulo 9

Influencia de los sistemas de videovigilancia en la formación de discursos mediáticos en materia de seguridad pública: Análisis del caso de Debanhi Escobar en Nuevo León, México

Influence of video surveillance systems in the formation of media discourses on public safety: Analysis of the case of Debanhi Escobar in Nuevo Leon, Mexico

*Araceli Espinosa Márquez**

*Carla Irene Ríos Calleja***

*Rubith Esther Gutiérrez Mejía****

Resumen

El presente trabajo tiene por objetivo analizar los sistemas de videovigilancia que influyeron en los discursos utilizados sobre seguridad pública en la prensa digital local y nacional, en particular sobre el caso de “*Debanhi Escobar*” en Nuevo León, México, y que ocupó los titulares del país y de la prensa internacional por las discrepancias existentes entre la información otorgada por el gobierno estatal y el discurso mediático debido a las imágenes presentadas por la Fiscalía del Estado. El 9 de abril, la joven Debanhi Escobar desapareció y su cuerpo fue encontrado en una cisterna de un hotel sobre una carretera y fue captada horas antes por un sistema de videovigilancia. A partir de esto, se pretende analizar las notas periodísticas entre el 9 de abril y el 15 junio del 2022 que presentaron los principales puntos de conflicto entre la comunicación gubernamental y la prensa para determinar la influencia que tiene en ellos el uso de

* Araceli Espinosa Márquez es Profesora-investigadora del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la BUAP. Sistema Nacional de Investigadores Nivel I. ORCID: <https://orcid.org/0000-0003-0475-6932>. Email: araceli.espinosa@correo.buap.mx.

** Carla Irene Ríos Calleja es Profesora-investigadora del Instituto de Ciencias de Gobierno y Desarrollo Estratégico de la BUAP. ORCID: <https://orcid.org/0000-0001-9656-4238>. Email: carla.rioscalleja@correo.buap.mx.

*** Alumna de la maestría en ciencias de gobierno y desarrollo de la BUAP. Email: bv230889@viep.com.mx

las grabaciones del sistema de videovigilancia y el impacto en la seguridad pública y en la resolución de casos.

Palabras clave: Videovigilancia; Seguridad Pública; Prensa Digital; Femicidio; Fiscalía de Nuevo León.

Abstract:

This paper aims to analyze the video surveillance systems that influenced the discourses used on public safety in the local and national digital press, particularly on the case of "Debanhi Escobar" in Nuevo León, Mexico, and which made headlines in the country and in the international press due to the existing discrepancies between the information given by the state government and the media discourse due to the images presented by the State Prosecutor's Office. On April 9, young Debanhi Escobar disappeared and her body was found in a cistern of a hotel on a highway and was captured hours before by a video surveillance system. From this, we intend to analyze the journalistic notes between April 9 and June 15, 2022 that presented the main points of conflict between government communication and the press to determine the influence that the use of video surveillance system recordings has on them and the impact on public safety and the resolution of cases.

Keywords: Video surveillance; Public Safety; Digital Press; Femicide; Nuevo Leon Prosecutor's Office.

Introducción

Los sistemas de videovigilancia se han utilizado tradicionalmente de forma pública y privada como una manera de dar certeza a los ciudadanos de que, mediante ellos, existe menos probabilidad de que sean víctimas de un delito. Para algunos, en sus viviendas, cuando una cámara capta en video lo que ocurre en tiempo real, es una forma de ganar tranquilidad en torno a su seguridad, ya que disuade a los delincuentes mediante el hecho de que serán grabados y evidenciados. Esto es un pensamiento generalizado en las sociedades latinoamericanas, en donde existen altos índices de delincuencia. Esta percepción no es fortuita; podemos encontrar diversos autores que refieren a la tecnología, en particular a los dispositivos de videovigilancia, como elementos que pueden contribuir a la disminución de los índices de delincuencia. Un estudio realizado en España (Domínguez y Ripollés, 2010) evaluó el uso de video vigilancia en zonas públicas como estrategia para reducir la delincuencia. Para ello, tomaron en cuenta los delitos registrados en la ciudad de Málaga y la opinión de habitantes de la ciudad acerca de estos dispositivos de vigilancia electrónica. En cuanto a la opinión ciudadana sobre la eficacia de las videocámaras, los resultados reportan que un 71.8% de los entrevistados tenían conocimiento que había cámaras instaladas en espacios públicos recurrentes, el 85.5% opinaron que las cámaras eran de apoyo para controlar la delincuencia, el 49.1% de ciudadanos dedicados al comercio comentaron creer que la delincuencia se redujo

tras la instalación de cámaras de seguridad. Por lo tanto, los ciudadanos, y específicamente ciudadanos comerciantes, percibían que las cámaras de seguridad ofrecen tranquilidad y que, además, solicitan la instalación de más dispositivos de vigilancia electrónica de esta índole en su comunidad.

Es pertinente señalar que existen diversas conceptualizaciones en relación con el tema de videovigilancia. Para algunos, apuntar a que son un conjunto de sistemas y, para otros, como Chong, D. (2020), señalar el objetivo, es decir, la captación de las imágenes de los hechos, que incluye el análisis automatizado, humano o una combinación de ambos procesos para identificar los riesgos en la seguridad y, con ello, tener la posibilidad de construir datos para la prevención. De ahí que, necesariamente, debe ser considerado no solo el elemento tecnológico, sino incluir la componente humana en torno al monitoreo por el análisis y el proceso de construcción de datos, ya que, al ser un medio de prevención del delito, debe tenerse una base de datos construida a partir de la observación, detección y registro de incidentes. Esto implica, además, que dicho análisis y procesamiento debe siempre incluir una mirada desde el campo de la criminología para ser pensada así (Andrade, 2022, p. 52) y, por lo tanto, para la implementación de acciones coordinadas.

Por su parte, desde la perspectiva sociológica, Arteaga-Botello (2016) señala que el sistema de video vigilancia tiene positividad en la opinión ciudadana en diferentes países, sobre todo de América Latina. Húngaros, mexicanos y brasileños consideran que las cámaras de vigilancia son efectivas para disminuir la violencia. El porcentaje de confianza en los dispositivos de video vigilancia que proveen estos habitantes son 87%, 81% y 80%, respectivamente.

Otros autores como López (2019), analizan la instalación de cámaras de video vigilancia y alarmas como medidas de protección de los hogares, considerando las opiniones resultantes de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE). Para dicho autor, el uso de dispositivos de vigilancia electrónica en materia de seguridad ciudadana es una práctica cada vez más aceptada e implementada en nuestro país, ya que se invierten grandes cantidades del presupuesto público en la adquisición de estos dispositivos que se consideran eficaces y menos intrusivos. El creciente temor de los ciudadanos de ser víctimas de delito o la considerable percepción colectiva sobre inseguridad pública provoca que se recurra a diferentes medidas de protección, entre ellas, la implementación de la tecnología. Los individuos solicitan, en algunos casos exigen, la instalación de cámaras y alarmas a las instancias gubernamentales y, por cuenta propia, también realizan esta práctica en sus hogares.

La autora Jasso López (2018) refiere en su estudio los resultados de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE), aplicada del 2012 al 2017, los cuales reportan que la inversión de estos dispositivos electrónicos

en los hogares para su protección ha incrementado al pasar de 2.2% en 2012 a un 3.5% en 2017. Otro factor reportado es la relación entre la victimización y la instalación de cámaras de video vigilancia y que es favorable, a mayor porcentaje de victimización, mayor uso de tecnología en los hogares para reducir la inseguridad. De igual manera, se encontró que, al haber percepción de delitos e incivildades que ocurren en colonias o localidades, hay mayor inversión en estos dispositivos.

I. Marco teórico

Para construir el marco teórico de este estudio, que comenzó en el 2021, se partió de los resultados proporcionados por la ENVIPE del 2020 sobre la percepción ciudadana acerca de los dispositivos de video vigilancia como política de seguridad pública, y se realizaron estadísticas descriptivas similares al estudio de López (2019), con la finalidad de considerar un panorama actualizado sobre la percepción de los mexicanos en cuanto a la seguridad pública y hacia los dispositivos de video vigilancia y poder analizar, como se desarrollará más adelante, el uso de estos dispositivos en contextos socio políticos y su influencia en el tema de la seguridad nacional.

Es por esto que se toma como eje de construcción del presente corpus teórico la intersección crítica entre la videovigilancia y los medios de comunicación, la información gubernamental, la prensa y el género, violencia y acceso a la justicia.

I.1 Videovigilancia y medios de comunicación

“[...] la videovigilancia es un recurso tecnológico que permite captar imágenes sobre hechos que ocurren sobre el campo de visión de una serie de cámaras estratégicamente colocadas y que transmite a una central de monitoreo, con el objetivo de ser un medio de prevención del delito, que, a través de acciones coordinadas, observará, detectará y registrará incidentes. Para llevar a cabo su cometido, deberá sustentarse en principios de reducción del crimen teóricamente sólidos” (Andrade, 2023). Es por esta razón, que las imágenes de videovigilancia juegan un papel fundamental en la construcción del discurso periodístico, particularmente en casos como el de Debanhi Escobar en Nuevo León, México. Estos materiales captados por cámaras de seguridad sirven como herramientas visuales para la reconstrucción de eventos y se convierten en elementos clave que alimentan y dan forma al discurso mediático. En esta misma línea, el tratamiento, edición y presentación de las imágenes como, las del caso de la presente investigación, dan cuenta de la intencionalidad de influir en la opinión pública y moldear la percepción que se tiene de los acontecimientos. “[...] los medios adoptan un lugar importante en la producción de ‘efectos de verdad’, operando en su difusión y reproducción. De hecho, estos modos de producir verdades reemplazan a los discursos científicos” (Lio, 2024).

I.2 Conflicto entre comunicación gubernamental y prensa

Otro de los aspectos que cabe resaltar es la colisión entre la prensa y la comunicación gubernamental debido a que, siendo la prensa ocasionalmente un medio para la comunicación gubernamental, permitiéndole cercanía con la ciudadanía, puede ocurrir la omisión de información o deformación de la misma en función de la conveniencia de una de las dos partes.

La articulación de la comunicación gubernamental requiere de una fundamentación teórica profundamente aplicativa con el objetivo de consolidar la estabilidad, evidenciando una condición de “gubernamentalidad” como un paradigma cognitivo distintivo. Este enfoque se caracteriza por su contribución de técnicas y racionalidad destinadas a orientar las acciones de los gobiernos. Se manifiesta en el conjunto integrado por instituciones, procedimientos, análisis y reflexiones, así como cálculos y tácticas que posibilitan el ejercicio de esta forma particular y compleja de poder (Riorda, 2009).

No obstante, en el ámbito de la comunicación gubernamental, particularmente en el contexto de la publicidad, es imperativo adoptar una perspectiva de comunicación institucionalista como contrapeso a la publicidad personalista. Se debe tener presente que la naturaleza de un gobierno implica ser propenso a crisis y tener una duración de mediano plazo. Esto conlleva la necesidad de evitar la saturación con un enfoque marcadamente personalista, ya que se deben gestionar situaciones a mediano y largo plazo sin generar fatiga en la audiencia.

Asimismo, es esencial considerar que, en caso de que un gobierno se vea inmerso en una crisis, la comunicación no puede eliminar de manera inmediata un estilo personalista previamente establecido. Este hecho conlleva riesgos significativos, ya que recordar quién es responsable de una situación delicada en cada momento y lugar podría tener repercusiones adversas. Este planteamiento se encuentra respaldado por las reflexiones de Riorda (2009).

Cabe resaltar que el esclarecimiento de los hechos de un acontecimiento importante es crucial para poder brindar información de primera mano, veraz y eficiente, y siendo mucho más preciso para la resolución óptima de conflictos legales. Sin embargo, la comunicación gubernamental no está exenta de ceder ante la presión externa de los medios para brindar declaraciones pertinentes, bien sea por una gestión o por esclarecer los hechos de un suceso trágico, como es el caso de Debahni Escobar, en el que se evidencia, a través de la construcción de la línea de tiempo, la tergiversación de la información expuesta por la Fiscalía de Nuevo León; las múltiples declaraciones ante los medios de comunicación con ciertas inconsistencias en los datos, y en evidencia se denota lo que el autor Silvio Wainsbord manifestó en su idea de que “el populismo contemporáneo continúa con su “histórica preocupación por la mediatización de la política y la politización de los medios”, que “se expresa en sus políticas de comunicación, la permanente utilización de estrategias para influir en la cobertura noticiosa,

frecuentes felicitaciones y diatribas repartidas al periodismo y la prensa, la insistencia de alimentar una narrativa política épica y el convencimiento absoluto de que ‘los medios’ tienen la llave de su suerte política” (Waisbord, 2013).

I.3 Género, justicia y violencia

Para hablar de género, se debe partir del principio de que el mismo es considerado una construcción social, es decir, que las normas, roles y expectativas de este constructo son creados y mantenidos por la sociedad. La Organización Mundial de la Salud (OMS), define el género de la siguiente forma: “Son los roles, las características y oportunidades definidos por la sociedad que se consideran apropiados para los hombres, las mujeres, los niños, las niñas y las personas con identidades no binarias. Éste es también producto de las relaciones entre las personas y puede reflejar la distribución de poder entre ellas” (OMS, 2018).

El enfoque de género, en el ámbito de las ciencias sociales, aborda su estudio y comprensión a partir de la construcción social de las identidades masculinas y femeninas, así como la inherente distribución desigual del poder entre ambos géneros. En el contexto del caso Debanhi Escobar, se reconoce que numerosas normas arraigadas en las construcciones de género perpetúan los ciclos de violencia dirigidos hacia las mujeres, ejerciendo un impacto significativo en su integridad y obstaculizando el acceso a mecanismos de protección y restitución de derechos. Desde esta perspectiva, se analiza minuciosamente cómo las expectativas culturales y las estructuras sociales contribuyen de manera sustancial a la exacerbación de la violencia, generando un entorno propicio para la perpetuación de prácticas violentas contra las mujeres.

En el contexto del caso de Debanhi Escobar, el componente de la justicia se ve influenciado de manera importante por la insistencia de sus progenitores y la presión mediática. Este fenómeno ha emergido como un factor preponderante en la búsqueda de equidad y resolución adecuada del caso hasta la fecha; la dinámica entre la autoridad judicial y la esfera mediática pone en evidencia la presencia de sesgos perceptibles en la postura adoptada por la fiscalía, evidenciando una inclinación notoria hacia la influencia ejercida por la cobertura mediática.

Al respecto de esta realidad, el autor Felipe Zuleta Lleras (2015) refiere, “Las decisiones de la Fiscalía y de los jueces las conocen primero los medios que las propias personas que están involucradas en procesos penales o en pleitos judiciales. La información se filtra, y en no pocas oportunidades, de manera selectiva. Olvidan así quienes ejercen la justicia que violan el derecho de los procesados a una defensa imparcial, pues una cosa es la realidad procesal y otra bien distinta la ‘verdad’ mediática”.

I.4 Violencia

La teoría de la violencia de Johan Galtung se centra en las estructuras sociales y económicas que perpetúan la desigualdad y generan conflictos, extendiendo el concepto de violencia más allá de los actos físicos directos (Ramírez López, 2020). El autor manifiesta una triple dimensión, en lo que él llama una afrenta a las necesidades humanas:

- La violencia directa es la violencia manifiesta, más evidente; su manifestación puede ser por lo general física, verbal o psicológica;
- La violencia estructural es la violencia intrínseca a los sistemas sociales, políticos y económicos, mismos que gobiernan las sociedades, los estados y el mundo; su relación con la violencia directa es proporcional;
- La violencia cultural abarca aquellos aspectos de la cultura, en el ámbito simbólico de nuestra experiencia (materializado en la religión e ideología, lengua y arte, ciencias empíricas y ciencias formales –lógica, matemáticas–, símbolos –cruces, medallas, medias lunas, banderas, himnos, desfiles militares, etc.–, que pueden utilizarse para justificar o legitimar la violencia directa o estructural (Calderón Rojas, 2016).

Para finalizar, la violencia de género y feminicidio puede entenderse como un síntoma de las desigualdades estructurales arraigadas en la sociedad mexicana. Las mujeres a menudo se ven afectadas de forma desproporcional por la discriminación y la falta de acceso a recursos básicos, y la presencia de altos índices de criminalidad introduce dinámicas adicionales de poder y control que afectan negativamente a las mujeres.

II. Metodología

Este trabajo de investigación se abordó desde la perspectiva cualitativa. Para realizar el análisis se eligieron dos periódicos digitales principales en el país: Milenio, con un alcance nacional y El Norte, con alcance local en el estado, principalmente. Se copiaron las notas periodísticas de estos dos medios relacionadas con el caso de Debanhi Escobar en el periodo comprendido entre el 10 de abril y el 31 de julio de 2022 y se conformó una base de datos con los encabezados y/o titulares, comparándolas con las videoconferencias transmitidas por la Fiscalía General del Estado emitidas entre el 21 de abril y el 26 de mayo de 2022. Se analizó la información y se pretendió buscar las discrepancias en el discurso a través del tiempo comprendido de estudio, para hacer una comparativa entre ellos con las siguientes preguntas de investigación: ¿Los sistemas de videovigilancia son relevantes en la generación de líneas discursivas que legitiman a las instituciones gubernamentales y para la formación de Opinión Pública? ¿Los sistemas de videovigilancia en el Caso de Debanhi marcaron una línea discursiva

Diagrama 1. Caso Debanhi Escobar





en la cobertura mediática y en la comunicación oficial entre los meses de abril y junio de 2022? ¿Existieron discrepancias entre la información otorgada por el gobierno estatal y el discurso mediático a partir del uso de las imágenes? La hipótesis planteada fue si los mecanismos de videovigilancia y las evidencias filmográficas fueron clave en la

generación de líneas discursivas, tanto en los órganos gubernamentales para generar legitimidad en el caso y fortalecer los discursos de la opinión pública a través de los medios de comunicación sobre el caso y sobre la seguridad pública en la región y/o en el país.

El 9 de abril, la joven Debanhi Escobar desapareció después de ir a una fiesta con sus amigos; desaparece frente al motel Nueva Castilla sobre la carretera Monterrey-Nuevo Laredo, en el estado de Nuevo León. Fue captada horas antes por un sistema de videovigilancia del motel Nueva Castilla, donde se ve a la joven caminando por la empresa de transporte ALCOSA. Durante los días posteriores, el motel fue registrado hasta cuatro veces por las autoridades sin rastro de la joven. Dos semanas después, tras una intensa búsqueda de las organizaciones civiles y las fuerzas policiacas estatales, el cuerpo sin vida de Debanhi Escobar aparece flotando en una cisterna de ese mismo motel. La oleada de indignación por este caso provocó que la opinión pública reabriera el tema de la inseguridad pública de la zona y, a partir de las imágenes presentadas por la Fiscalía para la construcción del caso, permitieron poner en la mesa el uso e influencia de estos dispositivos para la legitimidad de la autoridad frente a la resolución de hechos y a la percepción que se tiene sobre ellos y, por si fuera poco, también provocaron que la sociedad y los distintos colectivos de mujeres reaccionaran sobre la vulnerabilidad y la falta de seguridad que viven en el país.

Imagen 1. Se presenta el recorrido de la joven durante los últimos minutos donde se tiene registro de Debanhi Escobar con vida

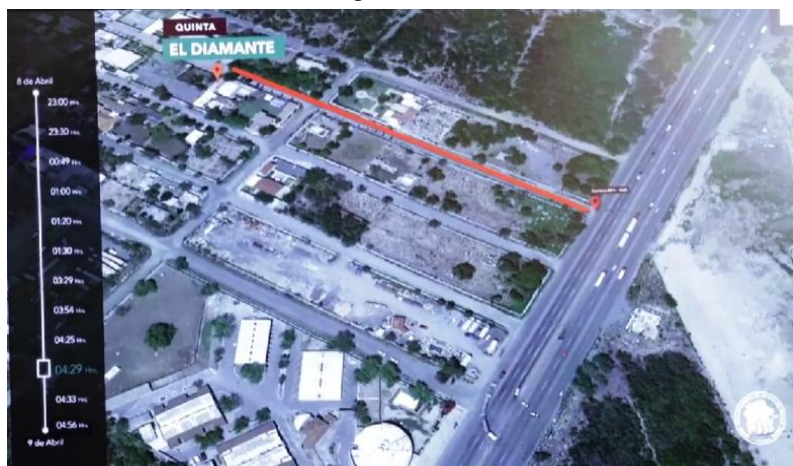


Imagen 2. Debanhi Escobar en la carretera de Monterrey a Nuevo Laredo, foto tomada por el celular del conductor que la recogió de la fiesta y la llevó ahí



Imagen 3. Debanhi Escobar caminando afuera de ALCOSA a las 4:28 - 4:30 am



Imagen 4. Debanhi Escobar caminando fuera del
Restaurante del Motel Nueva Castilla a las 4: 33 am



III. Hallazgos

Se consideró la base de datos abierta proporcionada por la ENVIPE sobre seguridad pública en la página web oficial del Instituto Nacional de Estadística y Geografía (2020). Los análisis fueron elaborados mediante el software R en su versión 4.0.5. El conjunto de datos contenía información sobre 95,161 casos, de lo que podemos señalar lo siguiente: en primer lugar, a los mexicanos les preocupa la situación de inseguridad, representado con un 19.55%; en segundo lugar se encuentra la preocupación por el desempleo, con un 15% y en tercer lugar el tema de la salud, con un 13.60%, como se señala en la Tabla 1.

Del total de casos expuestos, se seleccionaron aquellos que confirmaron haber tomado medidas preventivas en sus viviendas en materia de seguridad pública durante el 2020, siendo éstos un total de 83,620 habitantes. Las tres medidas de protección utilizadas con mayor frecuencia fueron cambiar, colocar o reforzar cerraduras y/o candados, con el 28.49%; cambiar o reforzar puertas o ventanas, con el 24.33%; y colocar o reforzar rejas o bardas, con un 16.44%. La instalación de alarmas y/o videocámaras de vigilancia ocupó el quinto lugar como medida de protección, como se señala en la Tabla 2.

Capítulo 9. Influencia de los sistemas de videovigilancia en la formación de discursos mediáticos en materia de seguridad pública

Tabla 1. Temas de preocupación expuestos por mexicanos encuestados a través de la encuesta ENVIPE 2020

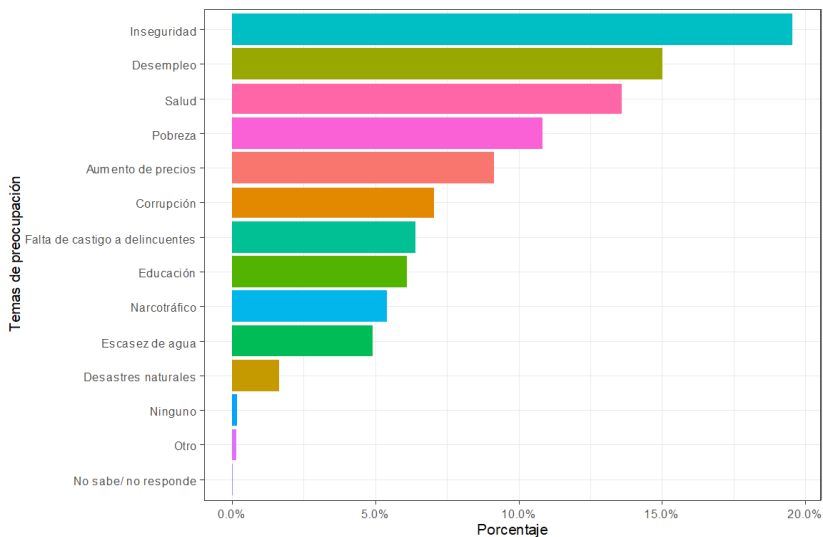
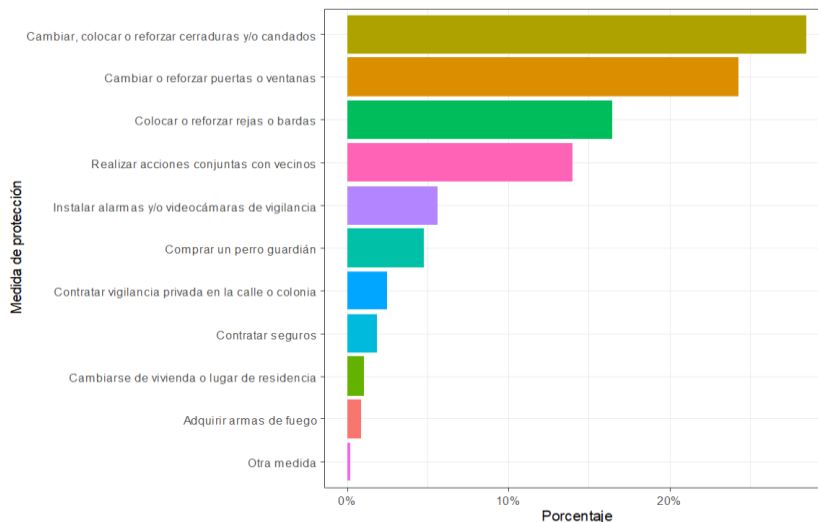
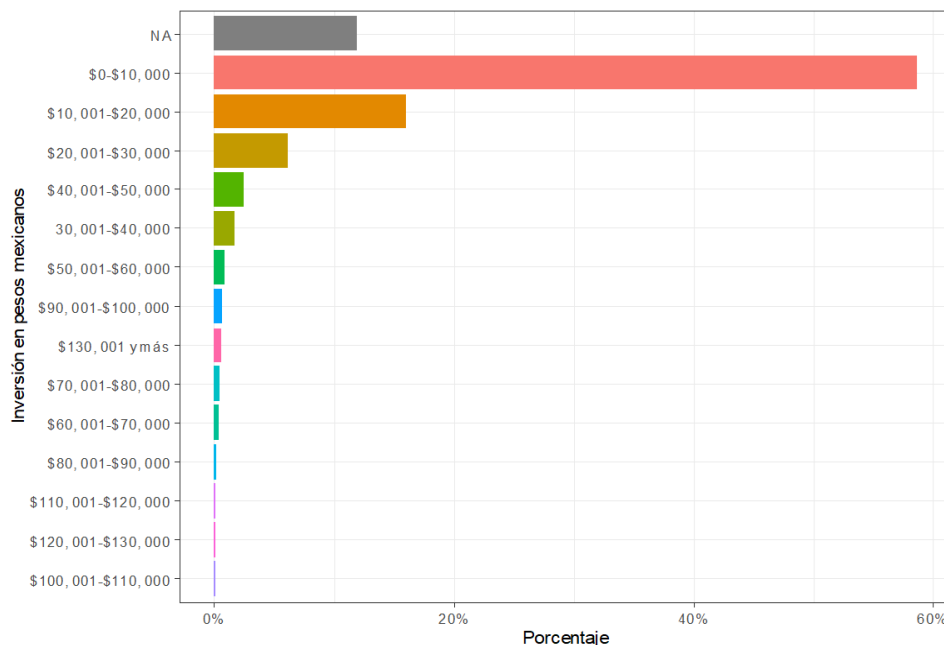


Tabla 2. Medidas de protección que se implementaron en viviendas para salvaguardarse de la delincuencia según encuestados de la ENVIPE 2020



Los individuos que optaron por instalar cámaras y/o videocámaras de vigilancia fueron 4,699, un 5.62% de la población encuestada. Un 66.58% invirtió en un rango de 0 a 10,000 pesos, el 18.16% gastó en la colocación un rango de 10,001 a 20,000 pesos y un 6.93% entre 20,001 y 30,000.

Tabla 3. Montos invertidos para la instalación de alarmas y/o cámaras de video vigilancia en los hogares de los encuestados de la ENVIPE 2020



Los ciudadanos que reportaron haber instalado alarmas y/o videocámaras en sus domicilios, en su colonia o localidad lo hicieron porque percibieron mucha inseguridad. De ellos, un 48.29% percibe inseguridad a nivel municipal o delegación, un 29.56% percibe inseguridad a nivel estado y el 22.15% percibe estar inseguro, como se observa en la Tabla 4. Podemos señalar, entonces, que la mayoría de los ciudadanos perciben inseguro el entorno donde habitan; son mayoría los que invierten en tecnología para reducir el riesgo y el temor sobre esto, por lo que los dispositivos son considerados como componentes preventivos para la disminución del riesgo a la inseguridad.

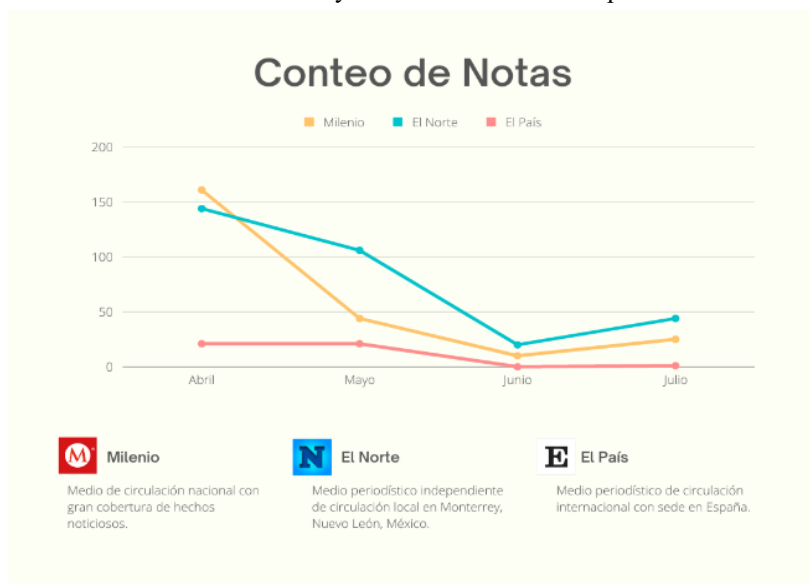
Tabla 4. Percepción de seguridad de los mexicanos en diferentes ámbitos geográficos

Ámbito geográfico	Percepción		
	Seguro	Inseguro	No sabe/ no responde
Colonia o localidad	51.41	48.29%	0.30%
Municipio o delegación	69.91	29.56%	0.53%
Entidad	77%	22.15%	0.85%

En este estudio de caso, en Nuevo León, México, se evidenció una significativa disparidad entre la información gubernamental y el discurso mediático, generando una atención tanto nacional como internacional. La desaparición de Debanhi el 9 de abril y el posterior hallazgo de su cuerpo en una cisterna de un hotel, captado por un sistema de videovigilancia, ponen sobre la mesa la necesidad de analizar las notas periodísticas entre el 9 de abril y el 15 de junio de 2022. Este lapso de tiempo presenta los puntos de conflicto clave entre la comunicación gubernamental (Fiscalía de Nuevo León) y la prensa, centrándose en el uso de grabaciones de videovigilancia y su impacto en la seguridad pública y la posibilidad de acceso a la justicia para la familia de la víctima.

El estudio contempló generar una base de datos a partir de las notas relacionadas con el caso que tuvieran cobertura en los periódicos digitales Milenio y El Norte, a partir de la fecha de la desaparición de la joven hasta el 15 de junio, fecha en la que solicita la familia de la joven una segunda autopsia necesaria para la resolución del caso. El total de notas publicadas en este tiempo, relacionadas con el caso de Debahni Escobar, por ambos medios fue de 485, de las cuales 215 realizó Milenio y 270 El Norte. En el mes de abril, a partir del día de la desaparición, Milenio publicó un total de 161 notas y El Norte 144. Durante el mes de mayo, Milenio publicó 44 notas, en comparación con El Norte, que tuvo una cobertura de 106. En el mes de junio el periódico El Norte publicó 20 notas, mientras que Milenio solo 10. En el estudio también se monitorearon las notas sobre este caso en el periódico El País para medir la cobertura internacional que se dio sobre los hechos. Se pudo observar que existieron notas durante los meses de abril y mayo, a partir de junio y julio no se encontraron. Se puede anticipar que esta ausencia se debe a la confrontación de discursos ante el caso en el Estado, perdiendo interés mediático.

Figura 1. Relación del número de notas publicadas en la prensa sobre el caso de Debahny Escobar durante el tiempo de estudio

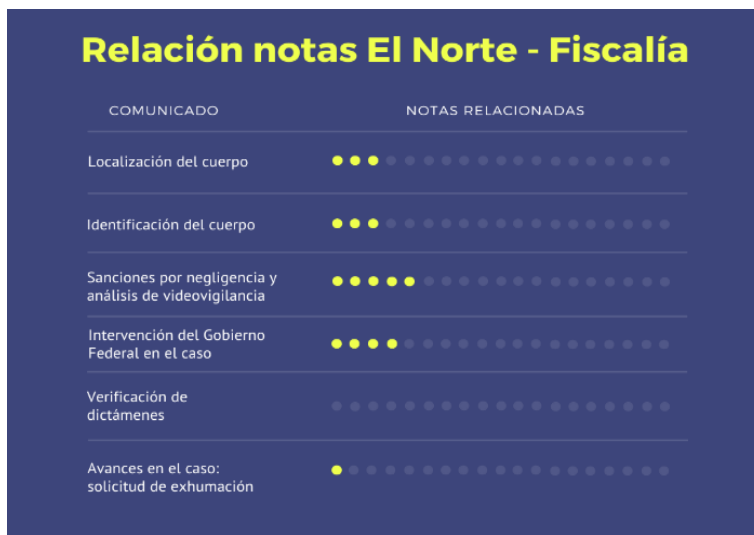


Las notas relacionadas con el caso de Debanhi Escobar se clasificaron según los encabezados de los respectivos medios que tenían lugar a partir de los comunicados de la Fiscalía, según los hallazgos encontrados en la semana. Se encontró que el periódico Milenio estuvo estrechamente vinculado con los comunicados de la Fiscalía, pero se encontraron muy pocas notas relacionadas con cada uno de los comunicados, como lo muestra la Figura 2. En cambio, el periódico El Norte publicó un número mayor de los comunicados emitidos por la Fiscalía de Nuevo León, pero la cobertura fue desigual. Algo que se encontró es que no existió cobertura sobre la verificación de dictámenes y solo una nota estuvo relacionada con la exhumación solicitada por parte de la familia. Este hecho, y el de la veracidad de las pruebas, detonó en la Fiscalía del Estado que el presidente Andrés Manuel Lopez Obrador incluyera a la Fiscalía de la República en la participación de la investigación. Se sugiere que este medio haya tenido línea editorial con la Fiscalía. Otro hallazgo importante es respecto a los comunicados referidos a la influencia de la videovigilancia en el caso, donde el periódico El Norte da mayor cobertura a los comunicados por parte de la Fiscalía sobre este tema, como se señala en la Figura 3. La Fiscalía de Nuevo León sostuvo varias hipótesis y es a partir de las cámaras de videovigilancia que se polarizan los discursos de los distintos gobiernos, estatal y federal, para la resolución del caso. Por lo que el caso en el Estado se centró mayoritariamente en el uso de los dispositivos de videovigilancia para la resolución del caso y este medio contribuyó a generar opinión respecto a ello.

Figura 2. Relación de notas publicadas por el periódico Milenio sobre los comunicados de la Fiscalía



Figura 3. Relación de notas publicadas por el periódico El Norte sobre los comunicados de la Fiscalía



Es importante señalar que la familia de Debanhi solicita desde el principio al Motel Castilla el acceso a las imágenes de las cámaras, por lo que el Motel accede. Es decir, estas imágenes que funcionaron como pruebas pasaron a ser del dominio público. Existió un efecto que perjudicó a la Fiscalía, presionada por la opinión pública y los distintos colectivos. Situó el uso de ellas en la resolución de este caso y, a pesar de esta evidencia, tuvo desaciertos en sus comunicados sobre la investigación de los hechos. Los medios evidenciaron esto. Por un lado, el periódico Milenio cubrió las notas de forma mesurada y alineada mientras que el periódico El Norte cubrió las notas de una forma detonante para que la Fiscalía de Nuevo León cambiara su discurso respecto a la seguridad pública que prevalece en el Estado y las irregularidades que imperan en la resolución de los casos.

IV. Primeras Aproximaciones

La videovigilancia, en calidad de instrumento destinado a la preservación de la seguridad pública, desempeña funciones claramente definidas y ha permeado de manera significativa en la mayoría de los sectores de la sociedad mexicana. Es por esta razón que resulta imperativo abordar cómo las grabaciones obtenidas a través de sistemas de videovigilancia inciden de manera sustancial en los discursos periodísticos y de las autoridades judiciales. Este fenómeno pone de manifiesto una estrecha co-nexión entre la observación de dichas grabaciones y la configuración de narrativas en el ámbito de la prensa y la Fiscalía de Nuevo León. Estas sinergias adquieren particular relevancia en el marco de la investigación actual.

Pero no son solo las autoridades locales las que reproducen estos discursos, también los miembros de los cuerpos de seguridad y representantes de instituciones del ámbito estatal a menudo dan por sentado que las cámaras de seguridad multiplican la capacidad de control del espacio urbano (Galdon-Clavell, 2015).

Por lo anterior, la videovigilancia no solamente es útil para el debido proceso judicial, sino también para alimentar la opinión pública, la cual, a su vez, puede llegar a convertirse en un catalizador para la pronta resolución de crímenes dada la presión social ejercida sobre las agencias de seguridad.

En las primeras conferencias, la Fiscalía se basa en las pruebas filmográficas para reconstruir la ruta de Debanhi. En este momento, la videovigilancia sirve para reforzar su línea de investigación. Sin embargo, también se emplean como instrumento de sanción dado que los involucrados omitieron presentar todas las pruebas. Es así como, a partir del 13 de mayo, los archivos de videovigilancia pasan a ser una prueba que se moviliza del gobierno local al federal y se termina su difusión en ruedas de prensa. El discurso oficial emitido por la Fiscalía determinó la agenda mediática del caso desde

la desaparición de Debanhi hasta la solicitud de la segunda necropsia. El manejo de pruebas, en este caso de los dispositivos de videovigilancia, es un aporte de Seguridad Pública, dado que es pionero en la cadena de custodia.

Referencias

- Andrade Alarcón, L. (2023). Seguridad pública y videovigilancia: Una óptica criminológica. Archivos de Criminología, Criminalística y Seguridad Privada, 11(21), 50–57.
- Arteaga-Botello, N. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. Espiral (Guadalajara), 23(66), 193-238.
- Calderón Rojas, J. (2016). Etapas del conflicto armado en Colombia: hacia el posconflicto. Latinoamérica, no. 62, Universidad del Valle-Sede Meléndez (Cali-Valle del Cauca, Colombia)
- Chavarría, B. (2022). ¿Qué es el Protocolo Alba y cuáles son sus fases en la búsqueda de mujeres desaparecidas? Quinto Poder. <https://quinto-poder.mx/tendencias/2022/4/20/que-es-el-protocolo-alba-cuales-son-sus-fases-en-la-busqueda-de-mujeres-desaparecidas-11604.html>
- Domínguez, A. I. C., y Ripollés, J. L. D. (2010). La Videovigilancia en las zonas públicas: su eficacia en la reducción de la delincuencia". Boletín criminológico, 16(121), 1.
- EL NORTE | Periodismo independiente. (s. f.). Recuperado 9 de agosto de 2022, de <https://www.elnorte.com/>
- EL PAÍS: el periódico global. (2022, 16 septiembre). El País. Recuperado 12 de agosto de 2022, de <https://elpais.com/>
- Fiscalía General de Justicia del Estado de Nuevo León, Inicio [Página de Facebook]. Recuperado el 17 de agosto de 2022 de <https://www.facebook.com/fiscaliageneraldejusticiantl>
- Galdon-Clavell, Gemma. (2015). *Si la videovigilancia es la respuesta, ¿cuál era la pregunta?* Cámaras, seguridad y políticas urbanas. EURE (Santiago de Chile), 41(123), 81-101. <https://dx.doi.org/10.4067/S0250-71612015000300004>
- Instituto Nacional de Estadística y Geografía. (2020). Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2020. Recuperado de https://www.inegi.org.mx/programas/envipe/2020/#Datos_abiertos
- Jasso López, L.C. (2018). Prevención del Delito y Tecnología: La Instalación de Cámaras de Videovigilancia y Alarmas como Medidas de Protección de los Hogares en México (p. 170). Universidad de Ciencias de la Seguridad. Recuperado de <https://revista.uco.edu.mx/wp-content/uploads/2019/04/10-prevencion-del-delito-y-tecnologia.pdf>
- Lio, V. (2019). La extensión de la videovigilancia en el territorio bonaerense. Geograficando, 15(1), 80–94. <https://doi.bibliotecabuap.elogim.com/10.24215/2346898Xe054>
- Lio, V. (2024). Imágenes del delito. Del uso preventivo a la eficacia mediática de las cámaras de seguridad. Inmediaciones de la Comunicación, 19(1), 93-115. <https://doi.org/10.18861/ic.2024.19.1.3506>

- López, L. (2019). Prevención del delito y tecnología: La instalación de cámaras de videovigilancia y alarmas como medida de protección de los hogares en México. *Revista Universidad de Ciencias de la Seguridad. Estudios de la Seguridad Ciudadana*, 2(2), 159-186.
- De la Serna Bilbao, M. N. (2016). Seguridad ciudadana y los sistemas de videovigilancia. Límites, garantías y regulación. *IUSTA*, 2(45), 129–163. <https://doi.org/10.15332/s1900-0448.2016.0045.06>
- Ma, Y., Ping, K., Wu, C., Chen, L., Shi, H. and Chong, D (2020), "Artificial Intelligence powered Internet of Things and smart public service", *Library Hi Tech*, Vol. 38 No. 1, pp. 165-179. <https://doi.org/10.1108/LHT-12-2017-0274>
- Mendoza, O. F. (2014). El Derecho a La Autodeterminación Informativa en La Era De La Llamada Videovigilancia en El Sector Privado en México. Una Perspectiva Desde La Ley Federal De Protección De Datos Personales en Posesión De Particulares Y Los Retos Pendientes. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, 12, 1–16. <https://doi.org/10.15425/redecom.12.2014.02>
- Organización Mundial de la Salud. (2018). Género y salud. Centro de prensa MILENIO | (s. f.). Recuperado 7 de agosto de 2022, de <https://www.milenio.com/>
- ONU Mujeres & Comisión Nacional de Búsqueda. (n.d.). Búsqueda de personas desaparecidas con perspectiva de género. Mexico. https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2021/twopager_desaparicion-forzada_v6.pdf
- Ramírez López, W.A. (2020). Violencia y capitalismo: regímenes de la representación y nuevas modulaciones de la violencia en la literatura colombiana reciente. Pontificia Universidad Católica de Chile. Tesis de doctorado
- Riorda, M. (2009). Comunicación Política: La comunicación gubernamental como comunicación gubernamental. Universidad Austral <https://revistas.pucp.edu.pe/index.php/politai/article/view/13956/14579>
- Romero, Jesús A. (2021). La circulación del sentido en las noticias producidas a partir del registro de cámaras de videovigilancia en Argentina. *Revista De Sociología*, 1(32), 89–102. <https://doi.org/10.15381/rsoc.n32.21550>
- Waisbord, S. (2013) *Vox populista. Medios, periodismo, democracia*. Buenos Aires: Gedisa.
- Zuleta Lleras, F. (2015). *La Justicia mediática*. El Espectador

Capítulo 10

Videovigilancia e inteligencia artificial: Implicaciones para México

Video Surveillance and Artificial Intelligence: Implications for Mexico

*Eleazar Guerrero Barrera**

Resumen

Los Sistemas de Videovigilancia (SVV), al unirse con la nueva tecnología desarrollada con Inteligencia Artificial (IA), permiten acceder a Sistemas Inteligentes de Videovigilancia (SIV) que usan macro datos y tienen el potencial de vulnerar los derechos humanos a la libertad, la intimidad, la privacidad y protección de datos personales, y usarse con fines diversos a los de la seguridad pública y nacional. Existe un debate mundial sobre el tema que en México está ausente, con las implicaciones que ello tiene. Las legislaciones que regulan SVV en el país son de orden estatal y se carece de normatividad nacional.

Palabras Clave: Sistemas de Video Vigilancia (SVV); Sistemas Inteligentes de Videovigilancia (SIV); Inteligencia Artificial (IA); Derechos humanos; Datos personales; Macro datos.

Abstract:

Video Surveillance Systems (SVV) by joining the new technology developed with Artificial Intelligence (AI), allow access to Intelligent Video Surveillance Systems (SIV) that use macro data and have the potential to violate the human rights to freedom, privacy, privacy and protection of personal data, and used for purposes other than those of public and national security. There is a worldwide debate on the subject, which in Mexico is absent with the implications that this has. The laws that regulate SVV in the country are of state order and there is a lack of national regulations.

Key words: Video Surveillance Systems (SVV); Intelligent Video Surveillance Systems (SIV); Artificial Intelligence (AI); Human rights; Personal data; Macro data.

* Doctor en Ciencias Administrativas. Maestro en ingeniería industrial. Ingeniero en sistemas computacionales.

Introducción

En el año de 1948, George Orwell (1980) escribió la novela denominada *El último hombre en Europa*, obra a la cual el editor, sin que supiera el autor, le cambió el nombre por el de *1984*. El nombre de la novela fue resultado de cambiar el orden de los dos dígitos finales que identificaban el año de edición. Esta obra trata sobre la vida de las personas en un Estado totalitario en el que la libertad es nula y el sistema de control población establecido es la videovigilancia del *Big Brother* (el Gran Hermano), que no es otro que el Estado vigilando a sus ciudadanos hasta en los más íntimos detalles de sus vidas, incluida la que se realiza al interior de sus viviendas.

La novela deja entrever el resultado de mantener una situación de videovigilancia permanente sobre las acciones que llevan a cabo las personas en todos los ámbitos de su vida y el resultado es catastrófico: la libertad en general, como las libertades particulares de expresión, información, petición, tránsito, a la intimidad y juicio, derechos humanos de las personas, defendidos desde la época la independencia de Estados Unidos, reflejada en su Constitución de 1776; la inviolabilidad del domicilio, defendida en la *Bill of Rights*, que enmendó esa constitución en 1791; así como los derechos humanos contenidos en la Declaración de los Derechos del Hombre y el Ciudadano en Francia en 1789, no existen en la novela de Orwell, fueron conculcados en esa sociedad ficticia que describe.

No obstante, la novela *1984*, si bien describe una sociedad de ficción, buscaba ser una sátira del “régimen soviético” (Eco, 2018, p. 6). Y como el mismo Umberto Eco (2018) destacaba, no era un libro profético, sino histórico, ya que el control de la libertad descrita en esta sociedad refleja las acciones de regímenes políticos que existieron. Y tiene razón; el control poblacional, la modificación de la idiosincrasia del pueblo, la restricción a la información, la manipulación de contenidos en medios de comunicación, la desinformación, la segregación, el adoctrinamiento, la imposición de un sistema de organización social o político ajeno, son manifestaciones de poder registradas en diversos pueblos desde que la humanidad empezó a usar la guerra como un medio para sojuzgar a otros. Para Orwell (1980), el referente inmediato que tuvo, además del Estado socialista, fue la construcción del *Tercer Reich* por parte de los nazis, comandados por Adolfo Hitler, en la Segunda Guerra Mundial.

La tecnología para que el *Big Brother* existiera en 1948 solo era resultado del ingenio del autor. Sin embargo, la tecnología ha avanzado a un nivel no imaginado hace apenas unas décadas atrás y lo que parecía ficción, ahora sabemos, puede convertirse en realidad. La proliferación de sistemas de videovigilancia, tanto privados como públicos, es un fenómeno vinculado con tres temas: el avance tecnológico; la aparición del internet y el incremento del fenómeno delictivo en todo el mundo.

Analizar las repercusiones que tendrá la videovigilancia como un instrumento para la prevención, detección y persecución de los delitos, invariablemente, implica análi-

zar las consecuencias que puede tener el uso de esta tecnología, pero también las limitaciones que tiene la videovigilancia frente a una sociedad que desconfía de sus autoridades y no se querella de los delitos por la incapacidad del Estado para evitar las represalias de los denunciados contra las víctimas.

Este trabajo pretende plantear tres interrogantes vinculadas con la videovigilancia:

- 1) ¿Qué implicaciones tendrá la videovigilancia al vincularse con la tecnología de inteligencia artificial?
- 2) ¿Qué impacto tiene la videovigilancia en México, ante delitos que solo son perseguidos por querella?
- 3) ¿Qué avance tiene la regulación que existe en México respecto a la videovigilancia?

Estas tres interrogantes son sustanciales para visualizar el futuro próximo del uso de las tecnologías de información y comunicación en relación con la videovigilancia vinculada a la IA y los impactos que, desde el ámbito jurídico, tendrá.

I. El concepto de videovigilancia

La Real Academia de la Lengua Española (RAL) define a la videovigilancia como: “Vigilancia por medio de un sistema de cámaras, fijas o móviles” (RAL, 2024, definición 1). A su vez, el concepto *cámaras* permite distinguir dos funciones: en la función genérica la cámara es un “aparato destinado a registrar imágenes animadas para el cine o la televisión” (RAL, 2024a, definición 16); la función específica está vinculada con lo que conocemos como cámara fotográfica, “Aparato que sirve para hacer fotografías, y que consta de un medio óptico, el objetivo, y de un medio mecánico, el obturador” (RAL, 2024b, definición 1). Al término *sistema* la RAL (2024c) lo define como: “Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto” (definición 2). El fin de la videovigilancia está implícito en el nombre del concepto: vigilar, verbo que es definido como “observar algo o a alguien atenta y cuidadosamente” (RAL, 2024d, definición 1).

Por tanto, podemos definir que un sistema de videovigilancia es un procedimiento mediante el cual se captan imágenes animadas o fotográficas a partir de cámaras fijas o móviles y que tienen como fin observar algo o a alguien de manera atenta.

La acción de vigilar mediante cámaras es un fenómeno que apareció en el siglo XX. En la década de los 40's se empezaron a usar, principalmente en el ámbito militar, para la vigilancia de espacios mediante Circuitos Cerrados de Televisión (CCTV), en instalaciones estratégicas (AAZ, 2019). Estos dispositivos se usaron en Alemania para

control de tráfico en los años 50's (Varona, 2012). En 1966, la inventora estadounidense Marie Van Brittan Brown, junto con su esposo, Albert Brown, obtienen la patente, que fue otorgada en 1969, del primer sistema de videovigilancia privado (patente número: 3,482,037). Básicamente, el sistema consistía en una cámara puesta en la puerta de la casa, como se conocen hoy en los interfonos, y servía para visualizar a quien llamara a la puerta. La patente lo describe como:

Un sistema de seguridad de video y audio para una casa bajo el control de un ocupante de la misma. El sistema incluye un dispositivo de escaneo de video en la puerta de entrada de la casa para escanear a un visitante fuera de la puerta, e incluye un equipo de intercomunicación de audio dentro y fuera de la puerta para conversar con el visitante fuera de la puerta. Se proporciona una cerradura para la puerta con medios de liberación de la cerradura controlados manualmente por el ocupante de la casa (*Patented 3,482,037, 1969, abstract of the disclosure*).

La definición introduce un concepto importante, *escáner*, el cual es definido por la RAL (2024e) con tres acepciones de las cuales las primeras dos son útiles para el presente trabajo: 1) “Dispositivo que explora un espacio o imagen y los traduce en señales eléctricas para su procesamiento”; 2) “Aparato que, por medio de ultrasonidos, resonancia magnética, radiaciones ionizantes o rayos X, proporciona una imagen de órganos o partes internas del cuerpo” (Definiciones 1 y 2). La importancia de estos conceptos es que la videovigilancia es, además, un proceso de escáner de las personas que se realiza por dispositivos eléctricos o de otra índole, que permiten, incluso, ver las partes internas de una persona, como ya sucede en los aeropuertos en la videovigilancia contra el tráfico de drogas.

El avance de la videovigilancia va a registrar un gran impulso en los años 90's del siglo pasado cuando se crea la videovigilancia mediante cámaras IP (*Internet Protocol*). Las cámaras IP utilizan el internet para poder transmitir las imágenes captadas por la cámara mediante la red y transmitida a un punto remoto, por lo que ya no es necesario estar en el mismo lugar donde está la cámara para poder vigilar. Ello implicó incluir a las computadoras como elemento sustancial para poder hacer la videovigilancia IP (Cadavid, 2017) y aquí es donde se intersectan las tecnologías de videovigilancia con la tecnología de la IA.

I.1 El concepto de inteligencia artificial

De manera similar al concepto de videovigilancia, se abordará el de *inteligencia artificial*, usando las definiciones que establece la Real Academia de la Lengua Española. El término *inteligencia* es definido como: “1) Capacidad de entender o comprender” y “2) Capacidad de resolver problemas” (RAL, 2024f, definiciones 1 y 2). Cuando

se habla de la IA hay que distinguir la inteligencia que busca reproducir las capacidades mentales de la persona, particularmente, vinculadas a la primera definición: entender, comprender y sentir emociones. Esta función cognitiva que realizan las personas es difícil de reproducir y estamos muy lejos de conseguirlo, aunque los esfuerzos buscan lograrlo. A esta inteligencia artificial se le denomina Inteligencia Artificial Fuerte (IAF) y fue explicada por John R. Searle en 1980 en su artículo *Minds, brains, and programs*. Por contraparte, también describe la Inteligencia Artificial Débil (IAD), a la cual denomina “weak or cautious” (Searle, 1980, p. 417). La IAD está vinculada con la utilización de información para toma de decisiones; en este sentido, un programa informático puede usar la IAD para establecer procedimientos y lograr una meta o un objetivo, es decir, “construir programas que realicen tareas específicas” (López, 2018, p. 46). En este sentido, la IAD está más cerca de la segunda definición que de inteligencia hace la RAL (2024f), es decir, la inteligencia que permite resolver un problema, para el cual se requiere información y procesamiento de ésta.

Por su parte, la Real Academia de la Lengua Española define el concepto de *artificial* como: “Producido por el ingenio humano” (RAL, 2024g, definición 3). En otras palabras, es un dispositivo, producto o idea que no es originado por la naturaleza, sino que requiere del procesamiento cognitivo de los humanos, único ser del planeta que puede tener autoconciencia, entendimiento, razonamiento, capacidad de resolver problemas de forma intuitiva, de sentir emociones, de comprender a partir de la experiencia.

En su origen, el concepto de inteligencia artificial fue planteado de manera general por Turing (1950) en su artículo *Computing Machinery And Intelligence*, en el cual se hace la pregunta: ¿Pueden pensar las máquinas? Esta pregunta surge a partir de la aparición de la computadora: “el presente interés en “máquinas que piensan” se ha incrementado en particular por esa clase de máquinas, usualmente llamadas ‘computador electrónico’ o ‘computador digital’” (Turing, 1950, p. 3). El artículo de Turing en realidad planteaba un método para testar si las máquinas llamadas computadoras podrían pensar y su planteamiento se acerca más a la psicología que a la computación.

Años más tarde, el 31 de agosto de 1955 John McCarthy hizo una convocatoria conocida como “*A proposal for the Dartmouth summer research project on artificial intelligence*”. A esta reunión realizada en *Dartmouth College* se le conoce como la Conferencia de Dartmouth y se realizó en 1956 con el financiamiento de la Fundación Rockefeller. Ahí, McCarthy acuñó el término “inteligencia artificial” (Leahey, 2013, p. 361).

Por inteligencia artificial, dado que la IAF está muy lejos del alcance de la ciencia actual y no sabemos si algún día se logrará, podemos entenderla a partir de la IAD, como la capacidad de los dispositivos hechos por los humanos (cámaras, computadoras y software) para procesar datos y obtener un resultado que permita tomar decisiones autónomas a partir de la información obtenida y tener una retroalimentación para la

corrección de la decisión tomada sin la intervención humana en dicho proceso. En este sentido, la IA es definida como un sistema.

I.2 La videovigilancia con inteligencia artificial

Mucho se ha avanzado desde el primer circuito de videovigilancia patentado en 1966 por Marie Van Brittan Brown. En el siglo XXI la videovigilancia se ha potenciado: no solo el Estado realiza videovigilancia, sino también los particulares. Ahora se hace en los espacios del hogar, la oficina y la calle. Se ha convertido en móvil, por los dispositivos artificiales con que contamos en la era de la información: teléfonos celulares, *tablets*, computadoras portátiles y drones.

La historia de la videovigilancia indica que estamos a un paso de dar un salto cuántico, al combinar la videovigilancia con la IA.

La IA en la analítica de videos “es uno de los temas más controvertidos en el sector de la videovigilancia. Algunas de las aplicaciones pueden acelerar considerablemente el análisis de datos y automatizar tareas repetitivas” (Axis, 2021, p. 3). La combinación de tecnologías de videovigilancia más IA permite analizar el *Big Data* poblacional, generando una capacidad de análisis de la información visual (imagen, movimiento, tipo de vestimenta, dispositivos que se cargan, micromovimientos faciales, etc.) para la toma de decisiones que no existió en ninguna otra época de la historia de la humanidad.

La videovigilancia tradicional permite obtener información testimonial sobre hechos, actos o eventos sucedidos, en tiempo real o grabados. Se tiene una imagen, que no aporta más información que la percibida por el ojo que la observa. Cuando se trata de la videovigilancia de una persona, como en el caso de un interrogatorio policial, los elementos de análisis son fácilmente observables: movimientos gestuales y faciales, tono de voz, actitudes, estados de ánimo, entre otros. Pero cuando se está ante la imagen de miles de personas tomadas por una cámara, por ejemplo, en un estadio de fútbol, todos esos elementos y otros más son imposibles de analizar por el ojo humano abarcando a todos los asistentes, por lo que la tecnología permite acceder a la videovigilancia con IA.

La IA, mediante un algoritmo, palabra de origen árabe que significa, según la RAL (2024) “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema” (Definición 1), puede realizar los cálculos que un ser humano o conjunto de ellos no podría hacer para analizar la información de miles de personas de manera simultánea, en un periodo de tiempo corto. Los algoritmos que pueden aplicarse en la videovigilancia son: a) cuantitativos o de búsqueda, que comparan las imágenes captadas para identificar un patrón preestablecido que reconozca el procesador de datos; b) cualitativos o de comportamiento, estableciéndose patrones de movimiento corporal y voz que el procesador de datos reconoce como parte de una secuencia. Sin embargo,

se han clasificado, desde la complejidad de la IA, dos algoritmos: “Un algoritmo de aprendizaje automático ha aprendido la combinación de características visuales que define estos objetos. Un algoritmo de aprendizaje profundo es más sofisticado y, con el entrenamiento adecuado, puede detectar objetos mucho más complejos” (Axis, 2021, p. 3).

En ambos casos, en el proceso de aprendizaje del programa de IA se expone a la cámara los elementos que debe detectar, hasta que, mediante un proceso de repetición y adquisición de la información, se genera un proceso de aprendizaje, que en el caso del aprendizaje automático es finito; termina una vez que se ha hecho la exposición. Sin embargo, en el aprendizaje profundo el programa sigue *aprendiendo*, mediante sistemas redundantes, pudiendo cambiar la toma de decisiones en tanto más exposición de elementos se le dotan. En este caso, parte del control que tienen los operarios del sistema se pierde, por lo que puedan dar falsos positivos.

Para entender este proceso vale un ejemplo. Para el aprendizaje automático, se expone a una cámara operada con IA figuras que debe detectar (datos de entrenamiento): armas blancas, pistolas, ametralladoras, botellas, punzones y la cámara, con capacidad de análisis de rayos x, puede detectar este tipo de elementos en una zona de escáner, lo que sabemos sucede en los aeropuertos y se usan para detectar droga, armas o explosivos. La detección se limita a aquellos elementos o figuras previamente sospechosas. En el caso del aprendizaje profundo, la exposición sigue el mismo camino, solo que el proceso de entrenamiento que se establece hace que, con cada escaneo, el programa reconoce los elementos previamente dispuestos, así como otros que puedan acercarse a la figura establecida, entre más exposiciones tiene más aprende y más potente se hace.

Con el uso de software sofisticado, sistemas de almacenamiento de información en grandes volúmenes (*Big Data*) y programas redundantes que generan aprendizaje, ya sea automático (el proceso es finito hasta concluir la tarea), o profundo (el proceso de comparación no para y se retroalimenta), se pueden establecer lo que definiremos como Sistema Inteligente de Videovigilancia (SIV), el cual lo definimos como un procedimiento mediante el cual se captan imágenes animadas o fotográficas a partir de cámaras fijas o móviles, que tienen como fin observar algo o a alguien de manera atenta, para detectar elementos previamente configurados, que generan una representación estadística o gráfica, para la toma de decisiones o una respuesta de un dispositivo mecanizado. En este último caso, por ejemplo, un dispositivo que detecta que una persona va armada, manda una decisión al dispositivo mecanizado de no girar la puerta o torniquete para el acceso de la persona en un espacio determinado. Sirven para detectar, si lo que se analiza son movimientos corporales, cuáles movimientos son considerados agresivos y, por tanto, clasificarlos para generar puntos rojos de posibles conflictos en una gran concentración poblacional.

Adicionalmente a esta posibilidad, la IA permitirá que la información captada por cámara pueda generar búsqueda de información en otras bases de datos masivos, macro datos o *Big Data*, como los que disponen las redes sociales *Facebook* o *Instagram*, por citar algunos, para generar perfiles de los rostros detectados y compararlos con los rostros publicados en esas redes sociales, así como la información personal complementaria. A este proceso se le conoce como “*massive data-driven AI*, [...] acceder a cantidades masivas de datos y poderlos procesar con hardware [...] para descubrir relaciones entre ellos, detectar patrones y realizar inferencias y aprendizaje mediante modelos probabilísticos como los sistemas de aprendizaje profundo” (López, 2018, p. 50).

I.3 Impactos de la videovigilancia usando IA

La tecnología permitirá analizar una gran cantidad de macro datos, no solo para reconocer quiénes son las personas que se captan en la cámara de videovigilancia, sino que también podrá analizar sus costumbres, relaciones virtuales, amigos, familiares, información personal, gustos o preferencias sexuales, entre otras cosas, a partir de la información que expone en redes sociales, etc.; en suma, la pérdida de la intimidad es uno de los resultados iniciales.

La videovigilancia vinculada con la IA implica retos importantes:

- 1) La inteligencia profunda deberá incorporar sistemas que permiten entender cómo se llegó a una decisión, inferencia o conclusión, dado que el proceso de aprendizaje es infinito, y los parámetros de análisis van cambiando sin intervención del operador del sistema, a fin de que no se tomen falsos positivos como verdaderos; vgr., que un sistema detecte a una persona como terrorista, sin que lo sea;
- 2) Se diseña software que pueda analizar a la inteligencia profunda, así como la toma de decisiones que hace a partir de las imágenes captadas con una cámara, con el fin de detectar errores en el programa experimental (López, 2018); considérese el sistema de IA en autos sin conductor, que debe reconocer desde objetos, personas, niños, animales, así como situaciones de riesgo, que emitan una decisión al sistema del auto para frenar o acelerar, según sea el caso; la falta de control del sistema de inteligencia profunda podría generar accidentes dramáticos;
- 3) El desarrollo de la IA, vinculada con la videovigilancia ha provocado que el mundo alce la voz respecto a los derechos humanos a la intimidad, al honor, a la protección de la propia imagen y voz como dato personal, así como otras implicaciones jurídicas que tendrá la nueva tecnología, particularmente en materia de discriminación, que se puede generar por “un sesgo discriminatorio (por ejemplo, cuando las herramientas de reconocimiento registran un mayor índice de identi-

ficaciones faciales incorrectas en el caso de sujetos de determinadas razas o etnias)” (Feldstein, 2022, p.7).

II. La videovigilancia en el contexto internacional

Europa atendió desde décadas atrás el tema de la videovigilancia, particularmente usada en espacios públicos como sistemas disuasivos o preventivos de la comisión de delitos, así como para el establecimiento de sanciones administrativas (multas por exceso de velocidad, no respeto de señales de tránsito, etc.).

Sin duda, Europa es el continente que tiene más experiencia en el uso de SVV, particularmente la Gran Bretaña: “el Reino Unido es uno de los países que más usa y de manera creciente las videocámaras en espacios públicos. En 1960 la policía Metropolitana de Londres fue la primera en utilizar *Closed Circuit Television* CCTV en la plaza Trafalgar” (Martínez, 2017, p. 50).

El terrorismo internacional, a partir de los atentados de 2001 en Nueva York, alentó el uso de los SVV para la inteligencia policial, militar y para la seguridad pública y nacional, prácticamente en todos los países del mundo. Los países que más cámaras instaladas tienen, en millones, son: China, 200; Estados Unidos, 50; Alemania, 5.2; Reino Unido, 5; Japón, 5; Vietnam, 2.6; Francia, 1.65; Korea del Sur, 1.05; Holanda, 1; y Australia, 1 (Chaverra, 2019).

Las ciudades que más cámaras por kilómetro cuadrado tienen son: Londres, 399.27; Nueva Delhi, 289.42; Pekín, 277.1; París, 254.59; Guadalajara, 170.1; Buenos Aires, 77.34; Moscú, 76.86; Barcelona, 71.01; Ciudad de México, 58.59; y Nueva York, 25.97 (Chevalier, 2021).

Desde que empezó el uso de los SVV el tema de la pérdida de la privacidad y la intimidad de las personas en el espacio público se hizo manifiesto. Así lo deja entrever las expresiones de diversos foros que han empezado a analizar las implicaciones de la videovigilancia usando IA: “Al habilitar la supervisión pública omnipresente, dichas herramientas pueden facilitar la represión sistemática de grupos específicamente identificados, alentar la extralimitación investigativa o tener un efecto paralizante en los derechos de expresión y asociación” (Kerley, 2022, p. 3), siendo China en donde los ojos del mundo tiene la vista puesta por la tendencia represora del régimen de Xi Jinping, presidente de ese país.

II.1 Regulación internacional

En el entorno mundial, el desarrollo de la tecnología ha sido tema central de la Organización de las Naciones Unidas, particularmente por la diferencia que existe entre países desarrollados y subdesarrollados respecto al acceso a la tecnología. En este sentido, los SVV y los SIV forman parte de las nuevas tecnologías de comuni-

cación e información (TIC's), mismas que han sido reconocidas como medios para el desarrollo, pero también una fuente de distanciamiento entre los países ricos y pobres.

En noviembre de 2021, frente a los peligros que implica el uso de la IA; 193 países miembros adoptaron las *Recomendaciones para la Ética de la Inteligencia Artificial*, emitidas por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). Este documento, sin querer establecer una definición de IA, indica que son “sistemas que tienen la capacidad para procesar datos e información de manera que se parece al comportamiento inteligente, y por lo general incluye aspectos de razonamiento, aprendizaje, percepción, predicción, planificación o control” (UNESCO, 2021, p. 10). Respecto al reto ético que representa la IA, el documento deja en claro que:

Los sistemas de IA plantean nuevos tipos de cuestiones éticas que incluyen, pero no se limitan a, su impacto en toma de decisiones, empleo y trabajo, interacción social, cuidado de la salud, educación, medios de comunicación, acceso a la información, brecha digital, datos personales y protección del consumidor, medio ambiente, democracia, estado de derecho, seguridad y policía, uso dual, y los derechos humanos y las libertades fundamentales, incluida la libertad de expresión, la privacidad y la no discriminación. Además, los nuevos desafíos éticos son creados por el potencial de los algoritmos de IA para reproducir y reforzar los sesgos existentes y, por lo tanto, exacerbar las formas de discriminación ya existentes, prejuicios y estereotipos (UNESCO, 2021, p. 10).

Una de las recomendaciones de la UNESCO para el uso de la IA, particularmente vinculada a la videovigilancia, resalta la necesidad de proteger la privacidad como un “derecho esencial para la protección de los derechos humanos, dignidad [y] la autonomía humana” (UNESCO. 2021, p. 21).

Es claro que a nivel mundial el tema de la videovigilancia, usando tecnología de IA, genera temor por la capacidad que tiene esta tecnología para apoyar sistemas de control poblacional, detección de grupos o minorías raciales, uso de detección de perseguidos políticos o discriminación, no solo por agencias gubernamentales, sino también por grupos fácticos de poder del orden privado. De ahí que el tema del derecho a la privacidad e intimidad sea prioritario, porque aún en los espacios públicos puede haber privacidad respecto a aquellos que no se encuentran en el área, privacidad que se rompe con las cámaras y el uso de internet, que permiten difundir imágenes en tiempo real en las antípodas del mundo. Un ejemplo de ello son los servicios de Qik, Bamber, Livestream, Meerkat y Periscope. Estas aplicaciones informáticas y de internet permiten que los usuarios violen el derecho de intimidad cuando se usan sin consentimiento de las personas que están siendo tomadas en video.

Ante la amenaza que implica los SIV, regiones como la Unión Europea han tomado en serio el asunto, tanto en la Carta de los Derechos Fundamentales de la Unión Euro-

pea, artículos 7 y 8, que protegen el derecho a la privacidad y a los datos personales, como en la actualización de la Política de Videovigilancia del Parlamento Europeo (PE), aprobado por Secretaría General Adjunta del PE en 2014, reconoce que se deben proteger los datos personales, y la privacidad, es decir, el derecho a la intimidad (PE, 2014). Este tema no es nuevo, los medios de comunicación, tanto televisivos como impresos, hacen uso de imágenes de personas sin el consentimiento de éstas, al presentar información o noticias sobre un suceso. En materia de transparencia, el PE distingue el acceso restringido a la información captada por cámaras (rostros, voz, comportamientos, etc.) y la información pública, que se puede acceder por internet, ya sea en tiempo real o en tiempo diferido. Esta distinción es importante, ya que las imágenes que se captan en SVV en espacios públicos, de ninguna forma deberían ser transmitidas en tiempo real por internet, ya que se estarían violando los derechos humanos a la intimidad y privacidad, así como de protección de datos personales.

Los espacios a vigilar con cámara deben ser espacios de alta afluencia de personas como: accesos, salas de espera, salidas de emergencia, aparcamientos; pero deben evitarse en otros espacios en donde se puede violar la intimidad y la privacidad como: baños, salas de descanso de los trabajadores o espacios de ocio (PE, 2014).

II.2 La videovigilancia: el caso de España

Un ejemplo de que puede existir conflicto de derechos en las leyes de los países que regulan los datos personales y la videovigilancia es España, en donde la *Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad*, en su preámbulo, indica que con la utilización de estos dispositivos “se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas” (párrafo 2). No obstante, destaca que el uso de esta tecnología debe regularse a fin de evitar se perturban los derechos de las personas por “un exceso de celo en la defensa de la seguridad pública” (Párrafo 3), en aplicación del principio de proporcionalidad (idoneidad e intervención mínima), temas que son tratados en el artículo 6 de dicho ordenamiento:

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 solo 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 artículo 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 (Ley Orgánica 4/1997).

Al analizar la Ley Orgánica 4/1997 de España, queda en evidencia que el uso de la videovigilancia está restringida a un uso tradicional de vigilancia con video. No incorpora el procesamiento del *Big Data*, por lo que existe una laguna legal que no solo España tiene, sino la mayor parte de los países, que regulan la instalación de SVV no están considerando el uso de la IA, aunque los objetivos que persiguen necesitan de ella para lograr sus metas.

Al analizar la *Ley 19/2007 contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte*, en su preámbulo, al referirse el gobierno español a los SVV, considera que: “Es obligatorio que éstos cuenten con un dispositivo de vigilancia permanente mediante videocámaras, que permite localizar, identificar y sancionar a las personas autoras de actos violentos” (p. 7). Lo que busca esta ley es evitar la discriminación y la “violencia, el racismo, la xenofobia, el antisemitismo y la intolerancia o cualquier otra manifestación inaceptable de discriminación” (p.7) en los espacios deportivos o de alta concentración poblacional. Sin embargo, esta norma, de manera implícita, alienta el uso de los SIV, ya que los objetivos planteados no podrían ser alcanzados de otra forma. El artículo 2, fracción 1, define qué debe entenderse por “actos o conductas violentas o que incitan a la violencia en el deporte”, entre los que se encuentran: participación activa en altercados, riñas, peleas; exhibición de pancartas, símbolos, emblemas o leyendas que inciten, fomenten o ayuden a la realización de comportamientos violentos, terroristas o discriminatorios; la entonación de cánticos que inciten a la violencia, al terrorismo o a la agresión en los recintos deportivos; la irrupción no autorizada en los terrenos de juego; las declaraciones, gestos o insultos proferidos en los recintos deportivos; cánticos, sonidos o consignas así como la exhibición de pancartas, banderas, símbolos u otras señales, que contengan mensajes vejatorios o intimidatorios.

El artículo 12, fracción 1, inciso b) establece la obligación de “instalar cámaras en los alrededores, en los tornos y puertas de acceso y en la totalidad del aforo a fin de grabar el comportamiento de las personas espectadoras”; por su parte, el inciso d) plantea la obligación de “instalar circuitos cerrados de televisión para grabar el aforo completo

del recinto a lo largo de todo el espectáculo desde el comienzo del mismo hasta el abandono del público”. El artículo 13 ayuda a entender cómo el uso de la IA, en combinación con los SVV, es promovido por esta Ley, la cual requiere: Promover sistemas de verificación de la identidad de las personas que traten de acceder a los recintos deportivos, implantación de sistemas de emisión y venta de entradas que permitan controlar la identidad de los adquirentes de entradas y la instalación de mecanismos o dispositivos para la detección de las armas e instrumentos análogos.

El *Real Decreto 203/2010 por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte*, en su artículo 66, fracción 1, al describir el SVV, señala que el “circuito contará con cámaras fijas y móviles” y la fracción 3 da la libertad para que las cámaras móviles se sitúen en los lugares “que el Coordinador estime necesario controlar especialmente en cada acontecimiento deportivo”. En otras palabras, las cámaras móviles podrían estar en zonas restringidas para la privacidad personal, como son los baños, violentando con ello el derecho humano a la intimidad.

España es un ejemplo que permite tener presente que la regulación y protección de los datos personales pueden chocar con las normatividades que buscan prevenir y combatir la violencia en todas sus manifestaciones. El problema central es que la protección de datos personales es considerada un derecho humano, en tanto que la regulación de los SVV son normas técnicas o procedimentales.

II.3 La videovigilancia: el caso de Francia

El 19 de mayo de 2023, se publicó en el diario Oficial de la República de Francia la *Ley número 2023-380 relativa a los Juegos Olímpicos y Paraolímpicos de 2024 y otras disposiciones*, en cuyo artículo 10 Francia aprueba un articulado que contradice las disposiciones europeas de protección de datos personales y que, de forma experimental, aprueba la videovigilancia usando algoritmos y macro datos o *Big Data*. Así, el artículo 10, fracción I, dispone:

I.- Con carácter experimental y hasta el 31 de marzo de 2025, con el único fin de garantizar la seguridad de las manifestaciones actividades deportivas, recreativas o culturales que, por el grado de su asistencia o por sus circunstancias, sean especialmente expuesta al riesgo de actos de terrorismo o amenazas graves para la seguridad de las personas, la imágenes captadas mediante sistemas de videoprotección autorizados en virtud del artículo L. 252-1 del código de seguridad interno o por medio de cámaras instaladas en aeronaves autorizadas sobre la base del capítulo II del título IV del libro II del mismo código, en los lugares sede de estos eventos y en sus alrededores, así como que en los derechos de paso de los vehículos y del transporte público y en las vías que les sirvan, podrán ser objeto de procesamiento algorítmico. El único objetivo de este tratamiento es detectar, en tiempo real, eventos medidas predeterminadas que puedan presentar o revelar estos riesgos y reportarlos con

miras a la implementación de medidas necesarias por parte de la policía nacional y los servicios de gendarmería nacional, los servicios de bomberos y los servicios de emergencia, los servicios de policía municipal y los servicios de seguridad interna de la SNCF y la Régie Transporte Autónomo de París en el marco de sus respectivas misiones.

Lo anterior contradice la Carta de los Derechos Fundamentales de la Unión Europea en sus artículos 7 y 8, la cual no establece excepciones en la protección de los datos personales; también va en contra de las recomendaciones que hace la UNESCO para el uso de la IA. Para tratar de enmendar el impacto que tiene esta normatividad, la cual será usada para detectar posibles actos terroristas, es que la fracción IV del artículo 10 aclara que no se usarán datos biométricos, no se aplicarán técnicas de reconocimiento facial, que no habrá conciliaciones, interconexiones o enlaces automatizados con otros tratamientos de datos personales y que no se harán enjuiciamientos a partir de la información detectada. Y remata: en todo momento habrá personas encargadas de su implementación, por lo que no se refiere a sistemas automatizados. Después de haber leído hasta aquí el presente trabajo, seguramente todo lector se hará la pregunta: ¿Entonces para que usar procesamiento algorítmico? Es claro que van a usar inteligencia automática para detección de instrumentos portados por las personas que puedan ser peligrosos en cada evento deportivo, pero también que deberán usar inteligencia profunda para poder “detectar, en tiempo real, eventos medidas predeterminadas que puedan presentar o revelar estos riesgos” (fracción I).

El caso francés abre la puerta al debate público. ¿Puede haber excepciones temporales al tratamiento de los datos personales? El responder sí implica reconocer que los derechos humanos pueden ser violentados por un Estado de manera temporal, argumentando labores de seguridad pública o seguridad nacional o, como lo hace Francia, sumándole que tiene un carácter experimental.

III.4 La videovigilancia en México

En México la videovigilancia como una política pública se inscribe en la aparición de un sistema vinculado al tema de la seguridad pública. En 1995 se reforma el artículo 21 Constitucional, en donde se establece la creación del Sistema Nacional de Seguridad Pública [SNSP] (CESOP, 2006). Ese mismo año, en cumplimiento a la reforma antes mencionada, se publica, en diciembre, la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, en la que se crea un Secretariado Ejecutivo que operará el nuevo Sistema Nacional de Seguridad Pública. En este marco, se promueve el Programa de Servicio Telefónico de Emergencias Ciudadana 066, el nuevo programa de atención de emergencias ciudadanas al estilo del número telefónico estadounidense 911 (que a la postre México terminó por homologar), hecho que requirió la integración de los C4 (Centro Estatal de Control, Comando,

Comunicaciones y Cómputo), que tienen como una de sus labores centrales, la atención y el monitoreo de las llamadas de emergencia.

Bajo el Programa Nacional de Equipamiento del SNSP, los estados del país impulsaron el uso de SVV operados por los C-4, precarios al inicio, aunque han evolucionado a verdaderos sistemas complejos, sobre todo en la Ciudad de México y en la ciudad de Guadalajara, la cual tiene un número importante de cámaras por kilómetro cuadrado, lo que la ha colocado en el ranking mundial de ciudades con mayor videovigilancia.

Los Sistemas de Video Vigilancia (SVV), como los denomina el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), en la *Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública*, son definidos 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” (SESNSP, 2017, p. 4).

Cabe destacar que, al analizar la norma técnica, es evidente que no integra en la recolecta de la información visual el uso de software vinculado a la IA, ya que los SVV solo se busca sean homologados en cuanto a las características del equipo que se va a adquirir. El incremento en la instalación de cámaras de vigilancia públicas, además, se alentó debido a que el: “Subsidio para la Seguridad Pública en los Municipios (SUBSEMUN) contempla un rubro específico para la adquisición de cámaras” (Arteaga, 2016, p. 196).

En un país en donde el fenómeno delictivo parece incrementarse cada vez más, la opción de la cámara de vigilancia no solo es solicitada por el ciudadano a la autoridad, sino que también es promovida en los ámbitos privados, ya que “las cámaras aparecen como la respuesta –si bien no la única, sí la mejor– a los problemas de inseguridad” (Arteaga, 2016, p. 197). No obstante, no hay evidencias de que la videovigilancia tengan algún efecto real en la prevención del delito.

Los SVV que define la norma técnica no se ocupan para prevenir el delito, en la mayoría de los casos, sino como sistemas de apoyo vial, que permiten ver donde hay más tráfico. No obstante, cuando una cámara de los sistemas permite captar un evento o hecho delictivo:

- 1) Permite dirigir el apoyo policial hacia el lugar de los hechos;
- 2) Ayuda a la logística policial cuando hay una persecución policial para capturar a un presunto delincuente;
- 3) Sirve de prueba pública, dado que la grabación es una captura hecha en equipos oficiales, para los procesos ministeriales o judiciales que se inicien.

El *Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2016*, indica que había en el país 33,643 cámaras de videovigilancia, pertenecientes a las corporaciones policiales, en las que la Ciudad de México tiene 136 cámaras por cada 100 mil habitantes y el Estado de México 57. Es significativo, si se considera que un año antes el Censo reportaba que había 25,631 cámaras de videovigilancia, lo que representa que en solo un año se instalaron ocho mil nuevas cámaras. Sin embargo, la tendencia de instalaciones de cámara no indica que la delincuencia esté disminuyendo ahí donde se colocan.

La videovigilancia permite contar con “Sistemas Tecnológicos de Videovigilancia: STV” (Vizcaíno, 2021, p. 9), esos sistemas que en este trabajo hemos denominado SIV (Sistemas Inteligentes de Videovigilancia). Para el caso de México, no existe mención en las leyes al uso de IA combinada con sistemas de videovigilancia, por lo que existe la posibilidad de intromisión a la intimidad y violación del uso de datos personales, como ya sucede en España o Francia.

En México, las entidades que tienen una ley de videovigilancia son: Ciudad de México, Colima, el municipio de Guadalajara, Durango y el municipio de Durango, Estado de México, Yucatán, Zacatecas, Aguas Calientes, Baja California Sur y Morelos (Vizcaíno, 2021). Las características que este autor destaca de estos marcos normativos son las siguientes:

- 1) Coinciden en regular la instalación de los equipos vinculados a los SVV;
- 2) Limitan el uso de las cámaras a temas vinculados con la seguridad pública, es videovigilancia en tiempo real, aunque la información puede ser grabada como medio de prueba;
- 3) Solo consideran su instalación en espacios públicos, a fin de no violar el derecho a la intimidad;
- 4) No mencionan el tema de la IA para el tratamiento de la información.

Cabe destacar que no existe una regulación federal en la materia, aunque existe un proyecto presentado en el año 2015 para crear la Ley General de Videovigilancia, misma que coincide con las normatividades establecidas en las entidades federativas que ya cuentan con éstas.

Destaca que, en la exposición de motivos, los Senadores de la República reconocieron un hecho destacado: que había SVV en Tamaulipas, que eran operadas y habían sido instaladas por la delincuencia organizada, por lo que habían desmontado 190 cámaras en Reynosa y Ciudad Victoria, siendo este suceso un riesgo de la falta de regulación nacional en el uso de SVV (PAN, 2015).

La iniciativa, en su artículo 3, recoge los principios fundamentales que se han estado defendiendo en Europa:

- a) Proporcionalidad - basado en la idoneidad (uso necesario) e intervención mínima;
- b) Riesgo razonable - prever que se pueda presentar un daño, ya sea por un hecho o acto delictivo o por un desastre.

La iniciativa de Ley General de Videovigilancia termina duplicando conceptos que ya están establecidos en las normas que protegen datos personales; su aportación es menor, ya que regula acciones que están conferidas a la autoridad municipal, como los lugares en donde pueden instalarse cámaras del Estado, pero es omisa, al igual que las legislaciones locales, en lo referente al uso de la IA, por ejemplo, mediante sistemas de reconocimiento facial o biométricos, tema de la mayor importancia al referirnos a la videovigilancia, sobre todo porque ya se integran a los dispositivos de reconocimiento biométrico para el registro de asistencia laboral.

III. Los SVV y la prevención del delito

Los SVV han sido alentados como parte de una política pública en el marco del Sistema Nacional de Seguridad Pública, como lo reconoce Vizcaíno (2021), el Programa de Fortalecimiento para la Seguridad Pública (FORTASEG) permitía a los municipios destinar recursos para la adquisición de cámaras de vigilancia, sin tener un programa claro de cómo se utilizarían, al no contar con un diagnóstico del problema que querían atender. Ello llevó a que se suscitaran problemas como el caso de Acapulco, en donde el SVV del C-4 era operado por infiltrados del crimen organizado (Animal Político, 2016).

No obstante la presencia de SVV en México, aún no es evidente cómo se usan estos dispositivos. Es claro que la función de vigilancia vial prevalece en los C-4, ya que la información que generan sobre conflictos viales, incluso, son reportados diariamente en programas de televisión y radio. Es por estos medios que se difunden eventualmente imágenes de delincuentes sometiendo a personas con armas de fuego, robos, acoso sexual en la calle y espacios públicos, asaltos en calles y avenidas, entre otros delitos. Del total de delitos que se comenten, de acuerdo con la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2022, en el año 2021 “en 93.2% de delitos no hubo denuncia o no se inició una carpeta de investigación” (p. 40). Este resultado no tuvo cambio respecto a la misma ENVIPE 2021, que reporta una cifra negra similar en el año 2020, lo cual indica que la población no tiene confianza en que sus autoridades realmente hagan algo para detener a los delincuentes, además de que el costo de oportunidad por la atención cuando se decide denunciar es alto,

siendo éstas las dos principales razones por las que un ciudadano no decide denunciar: “pérdida de tiempo con 33.5% y desconfianza en la autoridad con 14.8%” (ENVIPE, 2022, p. 44). El tiempo que lleva la denuncia produce pérdidas hora-hombre, ya que ENVIPE (2022) reporta que 32.6% de los denunciantes indican que les llevó más de 4 horas presentar su denuncia ante el ministerio público, 20.2% de dos a cuatro horas, 29.5% entre una y dos horas y solo 15.1% consideró que se le llevó menos de una hora hacer su denuncia. Ello provoca que la percepción de inseguridad entre las personas de 18 años o más sea de 61.2 por ciento.

Estos datos, de manera indirecta, indican que, aun con la presencia de los SVV públicos o privados, la incidencia delictiva no disminuye, por lo que el argumento de que estos sistemas permiten prevenir y combatir el delito está en entredicho y forma parte del discurso político, que no es demostrado con hechos concretos.

Las cámaras ayudan, en caso de que registren un hecho delictivo, a reconocer a los delincuentes, pero sin que haya una denuncia por parte de los afectados, esas imágenes no dejan de ser solo anécdotas visuales, que sirven a los programas televisivos, pero no a la autoridad.

¿Por qué no denuncian las víctimas? En el caso de delitos menores, ya se vio que la razón es la desconfianza a la autoridad y el costo de oportunidad de perder tiempo. Pero hay otra razón adicional. La beligerancia de la delincuencia organizada y no organizada, respecto a los sistemas de protección de víctimas. El denunciante se encuentra indefenso frente a su agresor a partir de un procedimiento que permite que el denunciado enfrente su proceso penal en libertad, pudiendo tomar revancha en contra de su denunciante. Esta posibilidad se encuentra en todas las democracias que aplican el principio de presunción de inocencia, la diferencia con México es que, a pesar de que el artículo 12, fracción X de la Ley General de Víctimas, otorga derecho a medidas cautelares a las víctimas para su protección respecto a su agresor, en la práctica éstas no evitan el poder enfrentar violencia de parte del denunciado, lo que inhibe la denuncia ciudadana ante ministerio público Avendaño *et al.* (2021) explican esta situación: “tiene diferentes causas: considerar que es una pérdida de tiempo, desconfiar de la autoridad, considerar el delito de poca importancia, no tener pruebas para presentar una denuncia, trámites largos, o miedo a represalias” (p. 3).

Conclusiones

A través de los SSV es posible crear inteligencia estratégica en materia de seguridad pública, misma que posibilita a las instituciones encargadas del orden identificar situaciones de alerta, para posteriormente proponer acciones que logren eficiencia en el uso de los recursos operativos con los que cuenta el Estado.

El análisis de la vinculación de los SVV, aunado a la IA que integran los SIV, indica que México aún tiene un rezago importante en materia legislativa para atender las

implicaciones que tiene combinar dos sistemas tecnológicos, hecho que está siendo abordado en otros países por las posibles violaciones a los derechos humanos vinculados a la privacidad, la intimidad y la protección de datos personales.

El análisis de las normas de España y Francia ejemplifica que el problema de la videovigilancia usando inteligencia artificial puede tener contradicción al vincularse al tema de la seguridad pública o la seguridad nacional, por lo que no es suficiente que se legisle en materia de protección de datos personales. En este sentido México ya tiene legislación que le permite proteger los datos personales, pero no tienen una legislación específica de carácter nacional, que regule los SVV, así como a la IA, por lo que el riesgo de actos de discriminación usando la nueva tecnología está potencialmente presente.

La IA se constituye como uno de los desarrollos tecnológicos que más podrían lesionar el derecho a la privacidad y a la intimidad, sobre todo por el uso de estos sistemas en el reconocimiento de la persona, por ejemplo, el facial, y su eventual vinculación a información disponible en bases de datos que constituyen *Big Data*, particularmente las que disponen las redes sociales.

No existe evidencia contundente que los SVV permitan disminuir la incidencia delictiva, como una política general de gobierno, sobre todo por las deficiencias de éste para proporcionar garantías de protección a la víctima de un delito, aun cuando existan las medidas cautelares legalmente.

Es un hecho que la tecnología seguirá su desarrollo y que los dispositivos que integran una cámara seguirán diversificándose como una estrategia de detección de hechos que pudieran ser constitutivos de un delito, sobre todo en el ámbito privado. No obstante, en el sector público no existe claridad de hacia dónde se dirigirá la política pública de videovigilancia.

La vinculación entre los SVV y la IA, que permiten tener SIV, genera más preguntas que respuestas en estos momentos, como son las dos siguientes:

- 1) ¿Cuál será la ponderación que darán los gobiernos nacionales y subnacionales al uso de los SIV ante una delincuencia organizada nacional y transnacional, que empieza a hacer uso también de esos sistemas?
- 2) ¿Cómo se evitará llegar a vivir en un mundo orwelliano en donde el Estado tenga un control poblacional usando los SIV?

Sin duda, México tiene mucho por hacer, particularmente en materia legislativa, la cual no ha atendido el tema de los SVV y, mucho menos, de la IA. El hecho de que se haya presentado una iniciativa desde el año 2015 y no haya sido dictaminada y aprobada, indica que el tema no está presente aún en la agenda política nacional como un

factor importante para la defensa de los derechos humanos vinculados con la libertad, la privacidad, la intimidad y la protección de datos personales.

Referencias

- Alarmas Automáticas de Zacatecas [AAZ]. (2019). *Historia de los sistemas de videovigilancia*. <https://www.centraldealarmasdezac.com/historia-de-los-sistemas-de-videovigilancia.html>
- Animal Político. (2 de mayo de 2016). *Militares controlarán las cámaras de seguridad de Acapulco*, Guerrero: Osorio Chong. <https://www.animalpolitico.com/2016/05/militares-controlaran-las-camaras-de-seguridad-de-acapulco-guerrero-osorio-chong/>
- Arteaga Botello, N. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. *Sociedad, XXIII*, 66, 193-238. <https://www.scielo.org.mx/pdf/esprial/v23n66/1665-0565-esprial-23-66-00193.pdf>
- Avendaño, F. Montes, P. y Santana, M. (2021). Pilares de integridad empresarial. IMCO. https://imco.org.mx/wp-content/uploads/2021/11/Cultura-de-denuncia_PilarV_.pdf
- Axis-Communications. (2021). *La IA en la analítica de video. Consideraciones para una analítica basada en aprendizaje automático y aprendizaje profundo*. <https://www.axis.com/dam/public/50/5d/7b/la-ia-en-la-anal%C3%ADtica-de-v%C3%ADdeo--consideraciones-para-una-anal%C3%ADtica-basada-en-aprendizaje-autom%C3%A1tico--es-ES-267958.pdf>
- Cadavid Parra, J. C. (2017). *Videovigilancia: Historia*. <https://www.americacomunicaciones.com/videovigilancia-historia/>
- Carta de los Derechos Fundamentales de la Unión Europea. (2000). Diario Oficial de las Comunidades Europeas. https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/EU_mCarta_Derechos_Fundamentales_Uni%C3%B3n_Europea_2000_ES.pdf
- Centro de Estudios Sociales y de Opinión Pública [CESOP]. (2006). *Seguridad Pública*. Cámara de Diputados, México. http://archivos.diputados.gob.mx/Centros_Estudio/Cesop/Comisiones/7_publica.htm
- Chaverra Agudelo, D. (2019). *Conozca los países y ciudades del mundo con mayor número de cámaras de seguridad*. <https://www.ventasdeseguridad.com/2019121011817/noticias/empresas/conozca-los-paises-y-ciudades-del-mundo-con-mayor-numero-de-camaras-de-seguridad.html>
- Chevalier Naranjo, S. (2021). *¿Qué tan vigiladas están las grandes metrópolis del mundo?* Estadista. <https://es.statista.com/grafico/23979/camaras-de-seguridad-por-km2-en-una-seleccion-de-ciudades/>
- Eco, U. (2018). Orwell, o la energía visionaria (prólogo). En G. Orwell (1949). *1984*. Editor digital: libra.
- ENVIPE. (2021). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2021*. INEGI. https://www.inegi.org.mx/contenidos/programas/envipe/2021/doc/envipe2021_presentacion_nacional.pdf

- ENVIPE. (2022). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2022*. INEGI. https://www.inegi.org.mx/contenidos/programas/envipe/2022/doc/envipe2022_presentacion_nacional.pdf
- Feldstein, S., (2022). La lucha global ante la vigilancia con IA. En B. Kerley (Coord.). *La lucha global ante la vigilancia con IA. Nuevas tendencias y respuestas democráticas*. National Endowment For Democracy / International Forum For Democratic Studies
- INEGI. (2016). Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2016.
- Kerley, B. (Coord.) (2022). *La lucha global ante la vigilancia con IA. Nuevas tendencias y respuestas democráticas*. National Endowment For Democracy / International Forum For Democratic Studies
- Leahey, T. H. (2013). *Historia de la psicología*. Pearson.
- Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte. Boletín Oficial de Estado, España. <https://www.boe.es/buscar/pdf/2007/BOE-A-2007-13408-consolidado.pdf>
- Ley General de Víctimas. Cámara de Diputados. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGV.pdf>
- 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. Boletín Oficial de Estado, España. <https://www.boe.es/buscar/pdf/1997/BOE-A-1997-17574-consolidado.pdf>
- LOI no 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions. Journal Officiel de la République Française. https://www.legifrance.gouv.fr/download/pdf?id=yUQ_DLw0skm8dWcA3FHSXNCWae1u63ZO6Nh5ySR3wgs=
- López de Mántaras, R. (2018). Hacia la inteligencia artificial progresos, retos y riesgos. *Métode Science Studies Journal*, 99, 45-51. DOI: 10.7203/metode.9.11145
- Martínez Meza, K. N. (2017). *Video vigilancia como política de seguridad pública en la ciudad de Puebla (2002-2016* [Tesis doctoral]). BUAP. <https://hdl.handle.net/20.500.12371/1058>
- McCarthy, J. (1955). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>
- Orwell G. (1980). *1984*. Salvat Editores.
- Partido Acción Nacional [PAN]. (2015). *Iniciativa por la que se expide la Ley General de Videovigilancia*. Senado de la República. https://infosen.senado.gob.mx/sgsp/gaceta/63/1/2015-11-26-1/assets/documentos/Ini_PAN_Video_vigilancia_Nueva_Version.pdf
- Patented 3,482,037. (1969). *Home security system utilizing television surveillance*. United States Patent Office. <https://patentimages.storage.googleapis.com/d0/0f/f7/5ef6cc1c77139d/US3482037.pdf>
- PE. (2014). *Política de Videovigilancia del Parlamento Europeo*. <https://docplayer.es/6545616-Politica-de-videovigilancia-del-parlamento-europeo.html>
- RAL. (2024). *Videovigilancia*. <https://dle.rae.es/videovigilancia>

- RAL. (2024a). *Cámara*. <https://dle.rae.es/c%C3%A1mara#L8Mfv91>
- RAL. (2024b). *Cámara fotográfica*. <https://dle.rae.es/c%C3%A1mara?m=form#9NK03WT>
- RAL. (2024c). *Sistema*. <https://dle.rae.es/sistema?m=form>
- RAL. (2024d). *Vigilar*. <https://dle.rae.es/vigilar?m=form>
- RAL. (2024e). *Escáner*. <https://dle.rae.es/esc%C3%A1ner>
- RAL. (2024f). *Inteligencia*. <https://dle.rae.es/inteligencia>
- RAL. (2024g). *Artificial*. <https://dle.rae.es/artificial>
- Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte. Boletín Oficial de Estado, España. <https://www.boe.es/buscar/pdf/2010/BOE-A-2010-3904-consolidado.pdf>
- Searle, R.J. (1980). Minds, brains, and programs. *The behavioral and brain sciences*, 3, 417-456. <https://home.csulb.edu/~cwallis/382/readings/482/searle.minds.brains.programs.bbs.1980.pdf>
- SESNSP. (2017). *Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública*. https://secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf
- Turing, A. M. (1950) Computing Machinery And Intelligence. *Mind* 49, 433-460. <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>
- UNESCO. (2021). Recomendaciones para la Ética de la Inteligencia Artificial. ONU. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Varona Martínez, G. (2012). *Estudio exploratorio sobre los efectos del uso policial de la videovigilancia en lugares públicos: propuesta criminológica de un sistema de indicadores sobre su adecuación y proporcionalidad en materia de seguridad*. Instituto Vasco de Criminología.
- Vizcaíno Zamora, A. (mayo-agosto 2021). Videovigilancia e inteligencia artificial: entre la utopía y la distopía. *Revista Mexicana de Ciencias Penales*, 14. INACIPE. <https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/432/346>

Capítulo 11

La videovigilancia en el estado de Veracruz: anomia jurídica e inexistencia de política pública

Video surveillance in the State of Veracruz: legal anomie and lack of public policy

*Alejandro de la Fuente Alonso**

*Karol Karim Mar Alonso***

Resumen

La videovigilancia se ha convertido en una política pública con la finalidad de disminuir los índices delictivos en los territorios donde ha sido aplicada; sin embargo, se confronta con las libertades del individuo y su esfera más privada: la intimidad. En ese orden de ideas, se plantean las razones que sustentan la existencia de la política pública de videovigilancia, teniendo como base fundamental la seguridad del ciudadano como causa teleológica de ésta y coexistiendo con el respeto a los derechos humanos de los individuos. Posteriormente a ese estudio teórico, se plantea el contexto del estado de Veracruz y la necesidad no solo de la creación de una política pública de videovigilancia en la entidad federativa, sino también la legislación en la materia por parte del Congreso Local.

Palabras clave: Videovigilancia; Políticas públicas; Veracruz; Legislación.

Abstract

Video surveillance has become a public policy to lower crime rates in the territories where it has been applied, however, it is confronted against the freedoms of the individual and their most private sphere: privacy. In this order of ideas, the reasons that support the existence of the public policy of video surveillance are raised, having as a fundamental base the security of the citizen as a teleological cause of this and coexisting with respect for the human rights of individuals. Subsequent to this theoretical study, the context of the State of Veracruz and the

* Doctor en Derecho por la UNAM, Investigador Nacional Nivel 1 y perfil PRODEP.

** Becario Conacyt en el IIJ de la Universidad Veracruzana.

need not only for the creation of a public policy of video surveillance in the federal entity but also the legislation on the matter by the Local Congress are indicated.

Keywords: Video surveillance; Public policies; Veracruz; Legislation.

Introducción

El ser humano ha ido avanzando tecnológicamente durante su andar por esta tierra. Así, ha logrado construir artefactos que le han simplificado la realización de sus actividades, pero, al mismo tiempo, han devenido en replantearse ciertas ideas. La evolución de los saberes lógico-matemáticos, que ha devenido en el avance en las disciplinas de las Ciencias Exactas y Biológicas, ha sido igual que la que se ha dado en las Ciencias Sociales. En ese orden de ideas, este progreso ideológico deviene en colisiones de dogmas, creencias, razonamientos, esquemas y doctrinas.

Hoy en día, las Tecnologías de la Información y la Comunicación permiten a quien las utiliza realizar lo inimaginable hace cuatro décadas, corto el periodo en la historia de la humanidad e insignificante en la edad cósmica; en ese sentido, las cámaras de video se han consagrado como un medio de garantía de la seguridad ciudadana o, al menos, una herramienta de reducción de la actividad delictiva.

No obstante, en la actualidad, existe un debate sobre las políticas públicas que han decidido o desean adoptar la videovigilancia; porque, si bien tienen la intención de proteger la paz social de la comunidad, también, es cierto que llegan a incidir en la transgresión del derecho a la intimidad de las personas. Todo lo anterior, complementado en el *status quo* nacional y estatal donde el legislador, tanto federal como local, ha sido incapaz de delimitar las reglas, leyes o normas con las cuales se guíe el poder Ejecutivo para la construcción de estas políticas públicas dentro del rango de su competencia.

No se discute sobre si existe el capital para financiarlo, no se ahonda sobre si las soberanías de la federación o las municipalidades lo contemplan dentro de sus planes de desarrollo, ni, mucho menos, sobre la implementación, coordinada o no, en territorio nacional; sino que se enuncia una anomia en el sistema jurídico mexicano derivada no solo de una ineficacia de los congresos para legislar, sino también de un conflicto doctrinal o colisión de dos principios o derechos humanos (en un primer momento).

He aquí que se plantea un análisis teórico de lo que “debe ser” frente a lo que está sucediendo en la realidad social del estado de Veracruz de Ignacio de la Llave, para no solo comprender, sin justificar, por qué el Congreso Local no ha planteado una legislación sólida sobre la videovigilancia, enfocándonos en la pugna entre el derecho a la seguridad frente al de la intimidad.

Siendo lo anterior replicado a nivel nacional, pues en el orden federal no existe una normatividad que regule la coordinación o colaboración de los diferentes órdenes de gobierno para una política pública más eficiente y garante de la protección de los derechos del individuo. Es decir, no emana una iniciativa desde el poder legislativo ni tampoco desde las diferentes secretarías de Estado que inciden en el tema de la seguridad de nuestra nación, siendo un tema que ha sido ignorado en la agenda pública del país. No es el fin de este texto plantear un análisis a esta situación, sin embargo, en las siguientes líneas se comprenderá por qué se enuncia esto.

I. Las políticas públicas

Para la comprensión de la adopción de la videovigilancia en las políticas públicas y su relación con el poder legislativo, se debe entender el concepto de forma independiente. He aquí que se puede indicar que, aludiendo a Pulido Chaves (2017, p. 16), la política pública “se refiere al vínculo general entre el Estado y la sociedad [...] en función de los intereses y necesidades concretas que convocan a los distintos grupos humanos a la acción política”.

Ahora bien, desde la visión vanguardista de Velásquez Gavilanes (2009, p. 156), la política pública “[...] es un proceso integrador de decisiones, acciones, inacciones, acuerdos e instrumentos, adelantado por autoridades públicas con la participación eventual de los particulares, y encaminado a solucionar o prevenir una situación definida como problemática”.

Es decir, son las acciones y decisiones que toma el Estado con el propósito de solucionar o prevenir un problema público, coordinándose con los particulares cuando lo crea necesario para la consecución de sus objetivos.

Sin embargo, se debe recordar que el poder en el Estado democrático y de Derecho, en el cual nos encontramos, no es absoluto ni se concentra en un solo órgano, pues bien lo indicaba el barón de Montesquieu (1845) cuando escribió:

Todo estaría perdido, si el mismo hombre, el mismo cuerpo de personas, de los nobles o del pueblo ejerciera los tres poderes: el de hacer las leyes, el de ejecutar las resoluciones públicas y el de juzgar los delitos o las diferencias entre los particulares.

Por ello, existe un poder que crea la ley, pero no la aplica ni juzga con ella, otro que la aplica, pero no juzga con ella ni es el facultado de crearla y uno último que juzga con ella, pero no la aplica ni la crea. He ahí el principio de la división o separación tripartita del poder que sigue vigente hasta nuestros días.

En ese sentido, es el poder Ejecutivo el encargado de crear y aplicar las políticas públicas; sin embargo, debe edificarlas bajo la normatividad vigente o bajo los linea-

mientos que ha dictado el poder Legislativo. He aquí la relación e interdependencia de los poderes para alcanzar lo que Porrúa Pérez (2005) denomina bien público temporal y es la causa teleológica de cualquier Estado desde su génesis.

II. Las políticas públicas y la videovigilancia

De acuerdo con Luis Andrade Alarcón (2023, p. 52), la videovigilancia “[...] es un recurso tecnológico que permite captar imágenes sobre hechos que ocurren sobre el campo de visión de una serie de cámaras estratégicamente colocadas y que transmite a una central de monitoreo, con el objetivo de ser un medio de prevención del delito, que, a través de acciones coordinadas, observará, detectará y registrará incidentes”.

Las precedentes líneas encierran la causa teleológica de la videovigilancia como un punto importante dentro de las políticas públicas para prevenir el delito. Es así como Ricardo Morales (2004, p. 1720) indica que la videovigilancia “tiene como finalidad bien la prevención de conductas ilícitas, bien la prevención de riesgos”. En concordancia con lo anteriormente enunciado, sin embargo, ¿qué sucede cuando se utilizan como pruebas?

Es el mismo Morales (2004, p. 1720) quien indica que “[...] Cuando se utiliza una videocámara, no para prevenir, sino para investigar a posteriori y obtener pruebas relacionadas con delitos ya cometidos o recabar información sobre cuestiones específicas no cabe hablar, en sentido estricto, de videovigilancia, sino simplemente de tomas videográficas”.

Por lo anterior, tras la presente disyuntiva, se debe precisar que el enfoque de la videovigilancia como política pública para Este estudio será para la prevención de los índices delictivos, siendo ello su parte teórica, no obstante, el acercamiento con la realidad social para complementar la doctrina será el contexto en el estado de Veracruz de Ignacio de la Llave.

En ese sentido, se retoma lo que indica Alexis González Acuña (2021, p. 48) en su tesis para optar al Magíster de Derecho en la Universidad de Valparaíso Chile:

La implementación de sistemas de televigilancia por parte de organismos del Estado encuentra su justificación en la protección de la seguridad pública, y viene a ser parte del enfoque de Prevención Situacional, asumida como política pública transversal.

En ese orden de ideas, se observa a la videovigilancia como un punto importante dentro de los planes y estrategias gubernamentales para lograr esa paz social tan anhelada; Santiago Mir Puig (2004), en su libro “Derecho Penal: parte general”, indica que “La idea del Estado social sirve para legitimar la función de prevención en la medida en que sea necesaria para proteger a la sociedad”.

Ello nos hace retomar la idea de que el Estado tiene como uno de sus fines la protección y seguridad de sus habitantes, a costa de la libertad de la comunidad, puesto que se han sometido a la potestad de este ente superior e intangible por algo que no han de poder conseguir en lo individual; lo precedente quizás tenga una visión sesgada de lo que representa el Estado y, sobre todo, la relación entre gobernantes y gobernados; sin embargo, coadyuva a comprender la idea del actuar del Estado a través de las políticas públicas para prevenir los delitos.

En el contexto mexicano, la política pública de videovigilancia en México “se ha articulado principalmente a partir del diseño local de los estados y municipios que, de acuerdo a sus expectativas, necesidades, problemas y alternativas han implementado sistemas de videovigilancia en las ciudades” (Jasso López, 2018, p. 216). En ese orden de ideas, el gobierno de México ha edificado la política de videovigilancia para garantizar la seguridad al ciudadano y, a pesar de ver los problemas y alternativas posibles, han omitido si esto limita (aún más) la libertad del ciudadano en su vida cotidiana.

Y aquí se erige otro problema que plantea Jasso López (2018, pp. 216-217): “no existe una política pública consolidada a nivel nacional que homologue los procesos y permita una comunicación fluida entre los diferentes sistemas de videovigilancia en aras de la seguridad ciudadana”. Por lo que México presenta no solo la pugna entre los principios o derechos previamente marcados (seguridad, intimidad), sino también la nula coordinación de la federación con las entidades y los municipios por la inexistente normatividad en la materia; ya sea que se plante uno nacional, como indica Jasso, o uno de forma federal, como el actual Sistema Nacional de Coordinación Fiscal.

III. El derecho a la seguridad frente al de la intimidad en el contexto de las políticas públicas de videovigilancia

Para poder ponderar la seguridad (puesto que es el argumento de existencia de estas políticas públicas) sobre la intimidad de las personas, se debe, en un primer lugar, comprender por qué se ha estimado con un mayor valor (en el plano jurídico, social y de la Teoría del Estado) la seguridad sobre la libertad.

En ese marco, se retoman las palabras asentadas por González Acuña (2021, p. 35) en su tesis para obtener el grado de Magister en Derecho, iniciando por mencionar que “La libertad es un derecho «débil» que se relativiza fácilmente de cara a la problemática de la inseguridad”, y, a pesar de que menciona que “La libertad y la seguridad son bienes constitucionales de primer orden en la medida que constituyen un presupuesto indispensable para el efectivo disfrute y cumplimiento de todos los demás” (González Acuña, 2021, p. 35), puede existir una diferencia por su relativización.

Se comprende que “En la práctica se presentan como un binomio en constante tensión, en donde siempre es necesario sacrificar en mayor o menor medida una de sus

partes” (González Acuña, 2021, p. 35). Es decir, si se tiene que decantar la autoridad por alguna de ellas, lo podrá ser si el beneficio es mayor; por ello sometemos nuestra libertad por la seguridad y certeza que se tiene cuando se vive en sociedad o bajo a lo que hemos denominado nuestra nación, entidad federativa, municipalidad o comunidad.

La Declaración Universal de Derechos Humanos se refiere a la «seguridad de la persona» dentro del art. 3, en los siguientes términos: “Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona”. Es decir, se vuelve a poner en el mismo nivel la libertad con la seguridad y, a la manera de Dworkin o Alexy, se debe definir qué principio/derecho se debe ponderar con un mayor valor en casos específicos.

En síntesis, en un primer momento, identificamos que la acción estatal ha ponderado limitar la libertad del habitante para garantizar (de una forma más efectiva) la seguridad de los conciudadanos, en pequeñas acciones y bajo la jerarquización de los habitantes en ciertas actividades y potestades que devienen en el buen funcionamiento de la sociedad, es decir, lo que sucede en nuestra vida cotidiana por la estructura orgánica del Estado y el ejercicio de los poderes públicos a través de sus depositarios.

Ahora bien, transitando de la confrontación libertad-seguridad y previo al ingreso a la pugna del presente apartado, se debe precisar la definición de la seguridad desde la óptica humana y no jurídica, puesto que todo lo anterior vertido se basa desde una concepción más cercana a la primera y no tanto a la seguridad.

Así, se puede enunciar que la seguridad humana “[...] intenta establecer aquellas dimensiones que afectan a la seguridad de las personas (alimentarias, ambientales, salud, económicas, personales, comunitaria y política) e identifica amenazas y vulnerabilidades tradicionales y no convencionales que afectan a las personas, superando los marcos meramente criminológicos” (PNUD, 1994).

En ese ambiente, el Estado no solo garantiza la seguridad jurídica del ciudadano o la reducción de las acciones criminales de los individuos, sino también busca brindar las facilidades (e inclusive su garantía) de todo lo que rodea la esfera humana para su desarrollo como persona.

Y, si bien no es una regla establecida, se puede indicar que los Estados modernos lo realizan pensando en las necesidades que se encuentran establecidas en la llamada Pirámide de Maslow, desde las básicas como las fisiológicas, transitando por las de seguridad, así como de afiliación y de reconocimiento, hasta las de autorrealización.

En ese orden de ideas, cuestiones como las libertades (humana, de expresión, de reunión, entre otras) y la seguridad (humana, jurídica, social, entre otras) se establecen en un mismo nivel; por lo que, ya no solamente desde el ámbito jurídico o la Filosofía del Derecho, sino también desde la psicología, se puede apreciar que se debe ponderar su valor porque en términos absolutos se encuentran en el mismo nivel y, por tanto, un caso concreto/particular establece la posibilidad de su relativización.

Así se sobrepone la seguridad humana de los conciudadanos de un Estado o demarcación para la creación de las políticas públicas de videovigilancia por parte de las autoridades; empero, surge el cuestionamiento si el uso de las cámaras de video transgrede el derecho a la privacidad de cada uno de los individuos que puedan ser grabados con ellas.

Por lo anterior, se debe realizar un recorrido sobre la concepción de la intimidad humana. En ese orden de ideas, la intimidad, desde el punto de vista de derecho fundamental, “[...] protege la esfera más privada del individuo, dotada de caracteres reservados que pueden o no compartirse mediante autorización, así encontramos el derecho a la intimidad, con intentos de conceptualizaciones subjetivas, unas más acertadas que otras” (Villalba Fiallos, 2017, p. 27).

No obstante, la anterior definición no complace o es suficiente para poder comprender el término analizado; es así como se retoman las palabras del tratadista Germán Bidart Campos (1998, p. 137), quien se refiere a la intimidad y a la privacidad de la siguiente manera: “la intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero [...] y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos”.

De lo antes planteado, concebimos a la intimidad como lo más personal y privado del individuo, siempre y cuando no afecten la esfera de lo público o comunitario. He aquí que se indica que (la intimidad) puede encontrarse transgredida en la época actual, tal cual nos lo explica Villalba Fiallos (2017, p. 41) al referir que “El avance tecnológico genera nuevas formas de vulneración de derechos personales, transgrediendo la protección de datos individuales y el bien jurídico fundamental de la intimidad”. He aquí que se plantea el problema del cual se ha venido hablando, la videovigilancia puede transgredir la esfera más íntima de las personas.

Por lo anterior, se genera “[...] la necesidad latente de la promulgación de normativa y políticas públicas que establezcan límites a ciertas libertades humanas que generen un equilibrio entre los derechos propios y ajenos” (Villalba Fiallos, 2017, p. 41).

Empero, no se debe limitar el problema a la intimidad, sino también a la nueva tendencia de la protección de los datos personales, a la forma de Puccinelli (1999, p. 68), “El derecho a la protección de datos tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc”.

Es decir, en el contexto contemporáneo, es inherente la relación protección de datos personales y la intimidad de las personas. No obstante, en anteriores líneas indicamos que se considera que un asunto es íntimo, personal y privado del individuo cuando no

existe relación con la vida pública, en sociedad o comunitaria. En ese ambiente, ¿qué sucede con las políticas públicas?

La respuesta a la interrogante es que, por todo lo vertido y analizado en las líneas precedentes, las políticas públicas de videovigilancia del Estado mexicano trascienden del “problema” de la transgresión (si existiese) de lo personal por preservar y defender el llamado bien público temporal, el cual, en la presente tesitura, es la seguridad del individuo puesto que su causar teleológica es la prevención del delito en donde son colocadas, siempre y cuando se usen para el fin por el cual fueron colocadas.

Para comprender lo anterior, se presenta la siguiente explicación: si bien, una cámara pudiera afectar la intimidad de las personas, su fin y su uso no responde a ello, sino a la prevención del delito, las videograbaciones que pudieran afectar la vida privada de las personas, debieran estar protegidas por la ley debido a que el Estado mexicano debe velar por esta protección de los datos personales de sus habitantes; en ese sentido, el problema de la política no es de forma, sino de fondo; no es donde se coloquen, sino el uso que se le de a lo grabado.

El Estado mexicano tiene la responsabilidad inalienable de velar por los derechos humanos de su población y, por tanto, el derecho a la intimidad y protección de sus datos personales. Sin embargo, como han versado los párrafos anteriores, no son motivo para evitar la creación de las políticas públicas de videovigilancia, sino que, quienes creen, normen, regulen y apliquen éstas, deben hacerlo respetando los derechos humanos de todo quien pudiera ser grabado con esta red de aparatos tecnológicos.

IV. La videovigilancia en México

Se deben realizar dos puntualizaciones, previo al análisis de la realidad social del estado de Veracruz de Ignacio de la Llave, las cuales son: 1) la videovigilancia se presenta como un fenómeno aislado en algunas entidades federativas, mientras, en otras como una acción coordinada; 2) y, en un segundo momento, no en todas las soberanías está legislado aunque cuenten ya con equipos de videograbación.

La primera aseveración se sustenta en lo que nos expresó alguna vez Lucía Carmina Jasso López, integrante del Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México, cuando expresó “mientras en Campeche se instalan cámaras en poblaciones de acuerdo a los índices delictivos y crecimiento urbano, en Tlaxcala lo hacen en puntos de desarrollo económico, incluso las utilizan como blindaje fronterizo” (Reyes Díaz, 2018).

Lo precedente nos lleva a afirmar que no hay una homologación en los procesos para la edificación de las políticas públicas de videovigilancia y, aunque se puede afirmar que lo realizan de acuerdo con su contexto (objetivos, necesidades, problemas y

realidades), no existe un marco normativo claro y tangible que guíe el actuar de las autoridades para la creación de políticas públicas más eficaces y eficientes.

No obstante, a pesar de la ausencia de un marco normativo nacional, algunas soberanías han devenido en legislar en la materia, ya sea por la necesidad que les creó la cantidad de videocámaras colocadas por su poder ejecutivo estatal o lo hicieron previo a ser superados por la realidad social; es decir, la fuente de los primeros es la combinación de la formal (por el proceso legislativo necesario) y la material (por lo que estaba sucediendo en su realidad social), mientras, los segundos encuentran su segunda fuente en una cuestión histórica, porque retoman los pensamientos de legisladores locales que lo realizaron previo a ellos.

De acuerdo con Martínez Meza y Armenta Ramírez (2019), “a nivel estatal, las entidades federativas que regulan la implementación de video vigilancia en los espacios públicos son Ciudad de México (2008), Aguascalientes (2009), Colima (2009), Durango (2012), Chihuahua (2012), Baja California Sur (2014), Estado de México (2014 y 2015), San Luis Potosí (2015) y Yucatán (2018)”.

Lo expresado en el párrafo anterior nos denota el proceso de positivizar lo que está sucediendo en la realidad social, siendo importante precisar que este proceso legislativo se realiza por la necesidad de que la política pública de videovigilancia coexista con la protección y respeto a los derechos humanos que realiza y es deber del Estado mexicano.

En ese sentido, Martínez y Armenta precisan que los cuerpos normativos (no todos y mucho menos de manera homogénea) que regulan la videovigilancia en las diferentes entidades federativas se desarrollan “[...] bajo los principios rectores de protección al derecho de la privacidad: legalidad, proporcionalidad, idoneidad, intervención mínima, el de riesgo razonable y el de protección a la privacidad personal salvo consentimiento del titular u orden judicial”.

Es así como las diferentes legislaturas reconocen que la videovigilancia es una excelente herramienta para que el poder ejecutivo, en el ámbito de sus atribuciones, pueda garantizar la seguridad de sus habitantes. No obstante, siempre deben velar por el respeto a los derechos humanos para que no transgredan, con su actuar, los principios de constitucionalidad y convencionalidad al cual están sometidos las leyes nacionales y, por tanto, su población en general.

Ese es el contexto teórico y de la realidad social en nuestro país; sin embargo, a la forma en que expresan algunos y por nuestra forma de Estado (Estado Federal y, a su vez, Estado Pluricultural), no podemos afirmar (como se ha denotado desde el ámbito jurídico) que existe un solo México puesto que cada soberanía define lo que ha de ser mejor, a su criterio, hacia su gobierno interior y la videovigilancia *a priori* se encuentra en ello.

Si bien, podemos pensar en la coordinación nacional de la videovigilancia dentro del Sistema Nacional de Seguridad Pública, no se puede negar que primero se requiere de una consolidación del sistema a nivel estatal y, en consecuencia, una regulación del mismo en cada una de las entidades federativas; ello, sin contar que debe existir la colaboración entre el gobierno estatal (a través de su símil de la Secretaría de Seguridad y Protección Ciudadana) con cada una de sus municipalidades.

V. La videovigilancia en el estado de Veracruz de Ignacio de la Llave

Ahora bien, después del recorrido teórico en el cual han versado las páginas que anteceden este subtópico, se han asentado las bases doctrinales y el contexto nacional para poder comprender el *status quo* del estado de Veracruz de Ignacio de la Llave en el marco de las políticas públicas de videovigilancia.

En ese sentido, se plantea la explicación del contexto actual de la entidad federativa en tres premisas: 1) percepción ciudadana; 2) legislación vigente y 3) situación de las cámaras con las que cuenta el gobierno actualmente.

Para lo que conlleva la primera premisa, se han de enunciar diferentes hechos que, a criterio personal, parecen importantes y denotan la opinión pública que se manifiesta en las diferentes latitudes de las entidades federativas:

- 1) En Poza Rica, siendo una de las ciudades más grandes e importantes de la zona norte, el presidente del Consejo Coordinador Empresarial del Norte de Veracruz, Sergio Hernández Rivera, “dijo que el sistema de cámaras es fundamental para la seguridad de la ciudad de Poza Rica. Cabe mencionar que este servicio fue parte de inversión que los empresarios realizaron para coadyuvar a reducir índices delictivos” (López, 2022);
- 2) En el sur de la entidad, el delegado de la Cámara Nacional del Autotransporte de Carga (Canacar) en Veracruz, Luis Exsome Zapata, propuso “la instalación de cámaras de videovigilancia en la autopista Orizaba-Puebla con la finalidad de evitar que grupos de la delincuencia roben unidades pesadas que movilizan mercancías” (García, 2022);
- 3) En Xalapa, en la colonia “Progreso Macuiltépetl, delincuentes robaron cinco cámaras instaladas por los vecinos, precisamente por los constantes robos en las calles Oaxaca, Nuevo León y Guanajuato” (Caiceros, 2023).

Estos tres casos permiten realizar diferentes aseveraciones que posibilitan realizar deducciones de lo que piensa el veracruzano sobre las políticas públicas de videovigilancia. En un primer momento, se está solicitando la colocación y funcionamiento de las cámaras de videovigilancia para reducir los índices delictivos, es decir, en el

imaginario colectivo concuerda la teoría con la praxis: la política pública funciona como un control del Estado para reducir la actividad delictiva en los territorios donde se han colocado.

La idea anterior se refuerza cuando observamos que, en la ciudad capital, en una colonia que ha ido a la alza en el tipo penal de robo, los delincuentes ven como un obstáculo a las cámaras de videovigilancia puesto que los harían identificables cuando delinquen.

En síntesis, tanto ciudadanos como delincuentes reconocen que la política pública coadyuvaría al actuar de las autoridades para dar con los transgresores de la ley y, por tanto, reduciría el índice delictivo porque se convierten en vigía o centinela permanente en donde sea colocado, sin la necesidad de que esté un oficial de seguridad pública de forma física en la zona.

No obstante, hay un punto importante en el caso Orizaba: las carreteras ya no competen al fuero municipal y, por lo tanto, emerge la precisión que se hacía en páginas anteriores, es el gobierno estatal que debe dirigir la política pública en toda la entidad federativa y las municipalidades deben coordinarse con ella.

Ahora bien, el ciudadano ignora u omite la cuestión de la privacidad y protección de datos personales; implícitamente han de sentir que se encuentra respaldada su seguridad mediante un cuerpo normativo y, aún con mayor importancia, la actividad de la videograbación lo hacen por su seguridad, por lo que el nivel de confianza en la política pública se establece si bien no alto, por lo menos superior al promedio.

Aún así, el párrafo inmediato anterior nos permite iniciar con la segunda premisa: la legislación vigente. Si bien, se puede argumentar que existen cantidad infinita de cuerpos normativos que hacen referencia a la videograbación, la realidad es que no existe una adecuada regulación de este tópico en normatividad veracruzana, nos encontramos ante una anomia jurídica puesto que existe una ausencia de normas en este ámbito.

Es cierto que existen los cuerpos normativos que delimitan el actuar del poder ejecutivo en su labor para garantizar la seguridad pública; también, se puede afirmar que existen un marco jurídico que protege y vela por las libertades y los derechos humanos de los habitantes de nuestra entidad federativa; y se puede aseverar que pueden existir reglamentos, códigos de ética y demás cuerpos normativos menores que regulan lo referente a la videovigilancia; sin embargo, la realidad concreta veracruzana es que lo único que se puede enunciar es el artículo 292 de la Ley del Sistema Estatal de Seguridad Pública para el Estado de Veracruz de Ignacio de la Llave:

Artículo 292. En los términos de la ley de la materia, la información que se obtenga a través de la operación de videocámaras y equipos para grabar o captar imágenes con o sin sonido

por las corporaciones policiales y las empresas prestadoras de servicios de seguridad privada y particulares deberá integrarse el Sistema Estatal de Información en Seguridad Pública.

Solamente ello, lo cual es insuficiente para poder regular la actuación de la autoridad y los límites de lo que se debe o no realizar con el contenido de las cámaras de videovigilancia; empero, el legislador no ha legislado en la materia bajo la siguiente lógica: si no existe lo que requieren que regule con una ley, para crear una ley que no tenga objeto y, por tanto, observancia.

La afirmación anterior tiene su génesis en la tercera premisa, puesto que, de acuerdo con una evaluación del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, “La red de vigilancia de Veracruz es la que tiene el menor número de cámaras entre las de las entidades de todo el país” (Ramos, 2021).

Ello se sostiene porque Veracruz contaba, en 2020, con tan solo 94 cámaras de videovigilancia, una situación crítica que denota un rezago gigantesco cuando se compara con otras entidades federativas, como lo realiza el periodista al indicar que: “El Estado de México cuenta con 20 mil cámaras, seguido de Jalisco con 6 mil 340 y Michoacán con 5 mil 316” (Ramos, 2021).

Si bien, pareciera que es una omisión por parte de las autoridades actuales, en este caso es un problema de antaño. Podemos precisar que Veracruz llega tarde a las políticas públicas de videovigilancia; no obstante, el problema deviene en una situación que ha denunciado la administración actual: “En 2019 la Administración del gobernador [...] denunció un fraude por la compra de más de 6 mil cámaras de vigilancia durante la administración [anterior] [...], el cual representó un daño patrimonial por mil 116 millones de pesos” (Ramos, 2021).

Es decir, el gobierno anterior percibió el problema y el atraso, por lo que decidió realizar una inversión. La partida ha sido devengada pero las cámaras no han sido colocadas y, aunque el gobernador “destacó que se tienen cámaras suficientes y están funcionando en lugares estratégicos para dar con quien comete algún delito” (García, 2023), la realidad es que no son suficientes las que están colocadas a lo largo y ancho de la entidad federativa.

En lo que se resuelve el problema del gobierno con la empresa contratada para el servicio, cientos de kilómetros cuadrados tienen ausentes las cámaras que han de servir como los centinelas de la Secretaría de Seguridad Pública del Estado de Veracruz y, al mismo tiempo, el Congreso Local no pone prioridad en establecer un marco normativo para su regulación por la inexistente red de videocámaras que debería existir en una entidad federativa tan grande y con un nivel alto de población a comparación de las otras soberanías que conforman nuestra federación.

Hoy en día, Veracruz carece no solo de una legislación que proteja sus derechos humanos frente a lo que representa la videovigilancia sobre su esfera más personal y

privada del individuo, sino también carece de la videovigilancia para garantizar su seguridad en un gobierno que, como es de todos conocidos, se está viendo rebasado en esta área.

Sin embargo, es preciso indicar que, con el panorama actual, se debería legislar en la materia para asentar las bases del actuar del poder ejecutivo y que, con fundamento en ese cuerpo normativo, elaboren la política pública, sin la necesidad de tener que cambiar el rumbo por una ley emergente posterior a la aplicación de su política pública. Siendo un reto dual para el Gobierno del Estado de Veracruz de Ignacio de la Llave: la regulación con una ley por parte de su poder legislativo y la creación e implementación de una política pública de videovigilancia por parte de su poder ejecutivo.

Conclusiones

El acelerado avance del desarrollo tecnológico humano ha devenido en la creación de cámaras de videos que, en conjunto y coordinación de las instancias de seguridad pública del Estado, forman sistemas que pueden servir para la prevención del delito; a eso le llamamos videovigilancia.

Esta videovigilancia se ha convertido en una política pública del Estado para poder garantizar la seguridad de los habitantes de las demarcaciones donde tiene presencia y, por lo tanto, tiene eficacia tras ser instalado. Su función es poder ser un medio de control de las Secretarías de Seguridad Pública o sus similares estatales, con lo que disminuyen la tasa delictiva de la zona sin estar presentes físicamente, pero vigilando a la distancia.

Esta nueva forma de vigilancia, a la cual se puede hacer referencia como televigilancia, encuentra una serie de confrontaciones con algunos derechos humanos; no obstante, en líneas anteriores se ha podido comprobar su factibilidad para ser ejercido por el Estado y, sobre todo, su coexistencia con los derechos humanos, pues se argumentaba podía violentarlos pero el análisis comprobó que no.

Se recordó que el ciudadano sacrificó un poco de su libertad a cambio de la seguridad, abandonó las ideas de la ley del Talión o la ley del más fuerte para someterse a la potestad de aquel ente intangible y abstracto al que denominamos Estado y ser cubierto por su manto protector al que llamamos Derecho.

Y, en esa búsqueda del Estado para garantizar la seguridad de sus habitantes, se encuentra con la condición de realizarlo bajo las normas jurídicas que lo rigen, y los derechos humanos inherentes a cualquier persona; puesto que, si no fuera así, a la manera del pensamiento de San Agustín de Hipona, el Estado se convertiría en una banda de ladrones porque lo único que lo diferencia de ello es la justicia, siendo esa utopía alcanzable únicamente a través del establecimiento de un sistema jurídico que permita el orden, la paz, el progreso y dar a cada quien lo que le corresponde.

En ese sentido, el otro problema presentado ha sido precisamente la cuestión de determinados derechos humanos que se indicaba que se encontraban en contraposición a la videovigilancia: la privacidad y la protección de los datos personales.

Sin embargo, se respondió que la causa teleológica de las políticas públicas de videovigilancia es la reducción del índice de delitos y, por tanto, la seguridad; la información se debe utilizar únicamente con esos fines y, por ende, debe haber un control por parte del propio Estado con respecto a cómo se utilizan los datos recabados en las cámaras de videovigilancia.

He aquí que, tomando en cuenta el análisis teórico realizado, se enuncia la situación actual del Estado de Veracruz, el cual ha demostrado tener dos graves problemas que debe resolver con respecto a las políticas públicas de videovigilancia: 1) existe una anomia jurídica en la materia y 2) no se cuenta con el suficiente recurso técnico-tecnológico-material para poder atender la demanda de atención del problema público que resuelve la política pública planteada.

Lo primero se expresa en la ausencia de leyes que normen el actuar de la Secretaría de Seguridad Pública del Estado de Veracruz con respecto a la videovigilancia, limitándose a incorporar los videos de las videocámaras al Sistema Estatal de Información en Seguridad Pública, sin prever realmente una verdadera regulación del actuar de la autoridad con respecto al uso de estas tecnologías tanto para la prevención del delito como el respeto a la intimidad de las personas.

El problema no versa en que puede violentar la esfera más privada y personal de los individuos, sino que no existe un marco jurídico que imponga la forma en la cual se debe conducir la autoridad al momento de planear, aplicar y evaluar las políticas públicas de videovigilancia.

En ese sentido, el Congreso Local veracruzano podrá argumentar que no existe normatividad debido a que no hay materia para hacerlo, es decir, al no contar con un sistema estatal lo suficientemente grande y la ausencia de sistemas municipales bien estructurados, pueden indicar que no se puede regular algo inexistente; en otras palabras, no existe fuente material o real que de vida al cuerpo normativo planteado.

No obstante, a la forma que Winston Churchill ve al político, el parlamentario se erige como aquel ciudadano que debe predecir el futuro para poder crear el marco normativo que mantenga el orden en la sociedad y su justo equilibrio; si bien, no existe un sistema de videovigilancia estatal en Veracruz, el porvenir augura que, con el avance tecnológico que estamos experimentando y la situación en otras entidades federativas, la videovigilancia se convierta en el medio de control de los índices delictivos por parte de las autoridades, por lo que su regulación previa a su aplicación es un deber para los legisladores.

Lo anterior se fundamenta en que debería existir la regulación de la política pública previa a su creación, planeación y, sobre todo, antes de su aplicación y evaluación,

puesto que, en caso contrario, se les obligaría a realizar modificaciones por violentar alguna norma administrativa o, en un caso peor, transgredir una esfera normativa de mayor envergadura o, inclusive, algún derecho humano de forma indirecta por el sesgo de la autoridad de desear el éxito de la política pública.

Por lo vertido en las líneas precedentes, se comprende que el H. Congreso del Estado de Veracruz de Ignacio de la Llave debe solventar la anomía jurídica existente para dar las bases al Ejecutivo de realizar una verdadera política estatal en coordinación con las 212 municipalidades.

En ese orden de ideas, la coyuntura actual obliga a la administración estatal 2018-2024 y a la próxima (2024-2030) a ser válida la inversión realizada por el gobierno anterior (2016-2018) sobre las cámaras de videovigilancia devengadas más no recibidas; asimismo, la política pública debe enfocarse en los puntos que se enuncian a continuación: 1) identificar las ciudades y zonas con mayores índices delictivos; 2) coordinarse con los municipios identificados para estudiar a fondo los lugares estratégicos para su colocación; 3) evaluar e identificar que los puntos evaluados resultan una excelente forma de ponderación o se debe reinventar la forma de definir la colocación de los aparatos; 4) replicar el método exitoso hasta cubrir cada una de las municipalidades.

Ello es un proceso largo, pero es imperativa su aplicación en las zonas metropolitanas y, sobre todo, no limitar la edificación de la política pública a las autoridades estatales y municipales, sino también a la sociedad civil, es decir, académicos, empresarios, comerciantes, entre otros que puedan aportar a reducir el sesgo en su planeación y, por tanto, aumentar su éxito.

Ahora bien, se planteó la idea de un sistema nacional de videovigilancia; sin embargo, esta utopía solo podrá ver la luz cuando se cuente con 32 sistemas estatales de videovigilancia que funcionen de forma correcta y eficiente; y, actualmente, Veracruz tiene la responsabilidad de consolidar el suyo antes de pensar en proponer uno nacional.

La videovigilancia ha comprobado su eficiencia; algunos gobiernos estatales han fortalecido y engrosado su capacidad de política pública. El Gobierno del Estado de Veracruz debe hacerlo su prioridad en su agenda de seguridad pública estatal. No solo la teoría, sino la praxis, ha comprobado que es lo mejor para alcanzar la plena percepción de seguridad de las y los veracruzanos.

Referencias

- Andrade Alarcón, L. (2023). Seguridad pública y videovigilancia: Una óptica criminológica. *Archivos de Criminología, Seguridad Privada y Criminalística*, 50-57.
- Caicerós, C. (14 de marzo de 2023). *Con cubetas, roban cámaras de seguridad en colonias de Xalapa, Veracruz*. Obtenido de La Silla Rota Veracruz: <https://lasillarota.com/veracruz/local/2023/3/14/con-cubetas-roban-camaras-de-seguridad-en-colonias-de-xalapa-veracruz-419202.html>
- Camota, W., & Bidart, G. (1998). *Derecho constitucional comparado*. Ediar.
- De Secondat Montesquieu, C. L. (1845). *Del espíritu de las leyes (Vol. I)*. Imprenta de Marcos Bueno.
- García, A. (30 de enero de 2023). *Avance en revisión e instalación de cámaras es apenas del 30%: Cuitláhuac García*. Obtenido de Diario de Xalapa: <https://www.diariodexalapa.com.mx/local/que-ocurrio-con-las-camaras-de-vigilancia-contratadas-durante-el-gobierno-de-miguel-angel-yunes-linares-9544742.html/amp>
- García, J. (13 de septiembre de 2022). *Canacar propone instalar cámaras en la autopista Orizaba-Puebla para frenar robo al autotransporte*. Obtenido de Avcnoticias: <https://www.avcnoticias.com.mx/noticias-veracruz/centro/334059/canacar-propone-instalar-camaras-en-la-autopista-orizaba-puebla-para-frenar-robo-al-autotransporte.html>
- González Acuña, A. F. (2021). *Videovigilancia y seguridad pública, una mirada constitucional*. Universidad de Valparaíso Chile.
- Jasso López, L. C. (2018). Hacia la transterritorialización de la política pública de videovigilancia en México. *Anuario de espacio urbanos, historia, cultura y diseño*, 199-220.
- López, L. (6 de junio de 2022). *Empresarios piden se active el sistema de videovigilancia para Poza Rica*. Obtenido de Radio Fórmula Poza Rica: <https://www.radioformula.com.mx/poza-rica/2022/6/6/empresarios-piden-se-active-el-sistema-de-videovigilancia-para-poza-rica-718862.html>
- Martínez Meza, K. N., & Armenta Ramírez, P. (2019). *Diagnóstico situacional del marco jurídico que regula la implementación de Video Vigilancia como Política de Seguridad Pública en México y propuesta de directrices para un modelo que garantice el respeto por los Derechos Humanos*. VI Simposio Internacional Lavits 2019: asimetría y (in)visibilidades: violencia, género y raza.
- Mir Puig, S. (2004). *Derecho penal: Parte general*. B de F.
- Morales, R. (2004). El derecho a la intimidad: grabaciones con videocámaras y microfonía oculta. *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, 1718-1725.
- PNUD. (1994). *Informe sobre desarrollo humano 1994: Nuevas dimensiones de la seguridad humana*. Fondo de Cultura Económica.
- Porrúa Pérez, F. (2005). *Teoría del estado*. México: Editorial Porrúa.
- Puccinelli, O. (1999). *El Habeas Dara en Indoiberoamérica*. Temis.

- Pulido Chaves, O. O. (2017). Política pública y política educativa: una reflexión sobre el contexto. *Educación y ciudad* 33, 13-28.
- Ramos, Á. (8 de diciembre de 2021). *Veracruz el estado con menos cámaras de vigilancia en el país*. Obtenido de e-consulta Veracruz: <https://www.m.e-veracruz.mx/nota/2021-12-08/estado/veracruz-el-estado-con-menos-camaras-de-vigilancia-en-el-pais>
- Reyes Díaz, K. d. (29 de noviembre de 2018). *Política de videovigilancia debe homologarse*. Obtenido de Universo. Sistema de noticias de la UV: <https://www.uv.mx/prensa/general/politica-de-videovigilancia-debe-homologarse/>
- Velásquez Gavilanes, R. (2009). Hacia una nueva definición del concepto "política pública". *Desafíos* 20, 149-187.
- Villalba Fiallos, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Revista de Derecho* 27, 23-42.

Capítulo 12

Diseño de un sistema prototipo de prospección inteligente con doble propósito: vigilancia para seguridad ciudadana, Control de GEI, PVs Y COVs. para monitoreo de cambio climático en ciudades inteligentes de los municipios conurbados de la Cd. de Puebla, Amozoc, Cuautlancingo, San Andrés Cholula, San Pedro Cholula, San Martin Texmelucan, Huejotzingo, Coronango y San Miguel Xoxtla, por los efectos toxicológicos del Rio Atoyac, GEI y Volcán Popocatepetl

Design of a prototype intelligent prospecting system with dual purpose; Surveillance for citizen security, GHG control, PVSn and VOCS. for climate change monitoring in smart cities. Of the conurbated municipalities of Puebla, Amozoc, Cuautlancingo, San Andrés Cholula, San Pedro Cholula, San Martin Texmelucan, Huejotzingo, Coronango and San Miguel Xoxtla. For the toxicological effects of the Atoyac River, GHG and Popocatepetl Volcano

*Cuitláhuac Alfonso Roviroso Madrazo**
*Armando Guadarrama L.***
*Pablo Saldivar Martinez****

Resumen

Al valorar el *cambio climático* del 13 al 15 de mayo del 2019 en Puebla (SEDEMA-INAOE) en material vegetativo impactado por fenómeno atmosférico conjugado; Desde la reactivación geológica del Popocatepetl, no sucedía, con una composición de GEI, PVs y COVs procedentes de la cuenca hidrológica del Rio Atoyac. Se usaron edificios para prospección de $PM \leq 2.5$. Se formó una capa densa con partículas PM 2.5 sobre la atmosfera conurbada de Puebla. Se hizo prospección en tejidos forestales como indicadores de toxicidad para determinar posibles ries-

* INAOE, CONACYT, CONCYTEO, cuitlahuacrovirosa@hotmail.com

** INAOE, CONCYTEP.

*** BUAP. Facultad de Ciencias Agrícolas y Pecuarias.

gos en vías respiratorias por silicosis. Se aplicaron SIG con imágenes de la NASA y ESA en combinación con técnicas Raman. Encontrando azufre (S) volcánico, COVs como *Benzyl disulfide*, CAS: 150-6-7 y PVs PM 0.5 a 2.5 μm incrustadas en tejido forestal. Se caracterizaron con *AccuSizer A700 Particle Sizing Systems*, recolectadas *in situ*. Arrojando una cifra preocupante: 2,981,334/Q15ml.15min de las cuales 962,881 son PM $\geq 0.5 \mu\text{m}$, que representan un 32.29%/15ml, y 191,556 $\geq 2.5 \mu\text{m}$ el 6.4%/15ml. Con un total del 38.39% de partículas peligrosas. Presencia de PVs, COVs combinados citotóxicos para las poblaciones urbanas. De este estudio, se derivó en la necesidad de la IA para la prospección y control con sistemas de alerta de futuros fenómenos similares en Puebla.

Palabra clave: IA-GEI; COVs; PVs. Puebla.

Abstract

When assessing climate change from May 13 to 15, 2019 in Puebla (SEDEMA-INAOE) in vegetative material impacted by conjugated atmospheric phenomenon; Since the geological reactivation of Popocatepetl, it did not happen, with a composition of GHGs, PVs and VOCs from the hydrological basin of the Atoyac River. Buildings were used for prospecting for PM ≤ 2.5 . A dense layer with PM 2.5- particles formed over the metropolitan atmosphere of Puebla. Forest tissues were surveyed as indicators of toxicity to determine possible respiratory risks due to silicosis. GIS with NASA and ESA imagery was applied in combination with Raman techniques. Finding volcanic sulfur (S), VOCs such as Benzyl disulfide, CAS: 150-6-7 and PVs PM 0.5 to 2.5 μm embedded in forest tissue. They were characterized with AccuSizer A700 Particle Sizing Systems, collected *in situ*. Yielding a worrying figure: 2,981,334/Q15ml.15min of which 962,881 are PM $\geq 0.5 \mu\text{m}$, representing 32.29%/15ml, and 191,556 $\geq 2.5 \mu\text{m}$ 6.4%/15ml. With a total of 38.39% of hazardous particles. Presence of PVs, cytotoxic combined VOCs for urban populations. From this study, it was derived in the need for AI for prospecting and control with warning systems of future similar phenomena in Puebla.

Keywords: IA-GEI; COVs; PVs. Puebla.

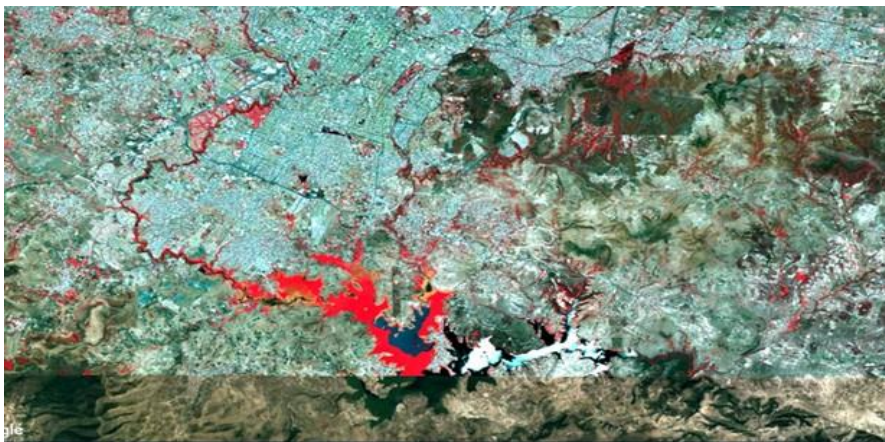
I. Introducción

La ciudad de Puebla está integrada a la Cuenca del Alto Atoyac, que pertenece a la Región Hidrológica del río Balsas. Es una de las 37 regiones hidrológicas de México con mayor contaminación hídrica (Alvarez B. *et al*, 2023). Esta cuenca se conforma por cuatro subcuencas: **Atoyac, Zahuapan, Alseseca y la presa Manuel Ávila Camacho**, mejor conocida como **Valsequillo**. Cubren un área de alrededor de cuatro mil kilómetros cuadrados sobre 70 municipios de los estados de Puebla y Tlaxcala (Soto, 2009), gran parte de forma urbana y periurbana. Es una de las ciudades urbanas de México con serios problemas de contaminación atmosférica, hídrica y pedológica, que impactan en la salud humana y sus ecosistemas. Su cercanía al volcán Popocatepetl la hace vivir adicionalmente un problema atmosférico complejo, sumando a las emisiones atmosféricas de Gases efecto invernadero (GEI) por los parques vehiculares e

industriales, la grave presencia de gases volcánicos. Uno de los efectos pueden ser las precipitaciones con lluvia ácida, incluso a cientos de kilómetros de la fuente emisora; excesivas emisiones de SO_2 que pueden implicar disminuir la temperatura, mientras que el CO_2 atmosférico se convierte en GEI. Adicionalmente, se conjugan Compuestos Orgánicos Volátiles (COVs) procedentes del río Atoyac y partículas sedimentables $\text{PM}_{2.5}$ a $\text{PM}_{0.5}$ (Rovirosa *et al*, 2019). Razones, por las que se hace urgente la prospección y monitoreo con IA de las condiciones ecosistémicas para prevenir el incremento de enfermedades crónico degenerativas como Leucemia, Cáncer y Enfermedad Renal Crónica en los habitantes de Puebla (Alvarez B. *et al*, 2023). Adicionalmente, con el problema de seguridad ciudadana, la demanda de vigilancia con IA es un reto y oportunidad para fortalecer el desarrollo social urbano.

II. Antecedentes, resultados y evidencias de daño ambiental con análisis espacial de contaminación hídrica, determinada con ayuda de satélites para detectar COVs en la cuenca alta del Río Atoyac

Figura 2.1. Imagen del satélite *sp. Sentinel 2* de la agencia espacial ESA, con bandas multiespectrales, infrarrojo cercano (B-IRC)



La Figura 2.1. permite ver los niveles de contaminación hídrica en rojo de la cuenca hidrológica del Río Atoyac-Zahuapan fuente principal de los COVs en la zona urbana y conurbada en Coronango, Cuautlancingo, Huejotzingo, Puebla, San Martín Texmelucan, San Pedro y San Andrés Cholula hasta la Presa Valsequillo.

II.1. Zona urbana Impactada por COVs en Puebla

Figura 2.2. Imagen del satélite (sp. Sentinel 2)



Fuente: Agencia Espacial ESA.

En la Figura 2.2., con aplicación de bandas multiespectrales e infrarrojo cercano (B-IRC), se aprecian niveles de contaminación hídrica en color rojo dentro de zona urbana y conurbada de Puebla.

II.2. Edificios que sirvieron en la prospección *in situ*

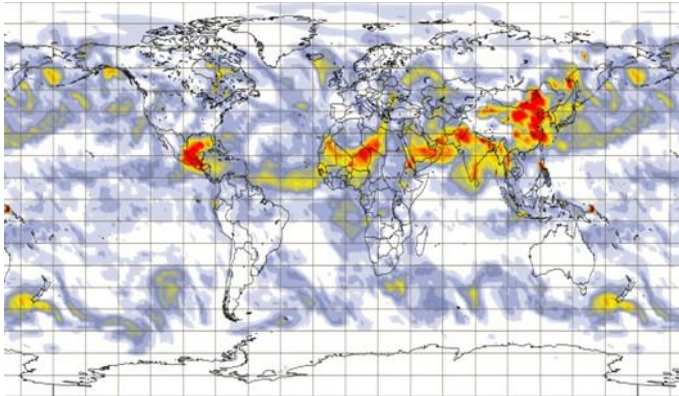
Figura 2.3. Impacto atmosférico por PVs $PM_{\leq 2.5}$
de los días 13,14 y 15 mayo del 2019



En la Figura 2.3. se aprecian emisiones de cenizas del Popocatépetl en Puebla.

II.3. Determinación geográfica de zonas impactadas por el fenómeno atmosférico con $PM \leq 2.5$ dentro del Valle de México y Puebla en el año 2019

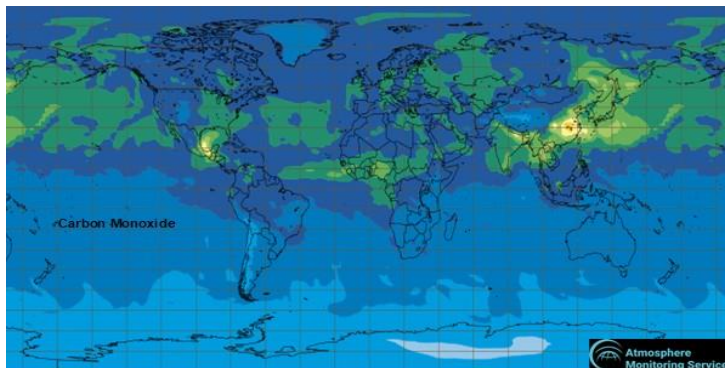
Figura 2.4. Estudio global con imágenes de satélite de la ESA de los Días 13,14 y 16 de mayo del 2019 del Valle de México



Fuente: Copernicus Atmosphere Monitoring Service UE, 2019.

En la Figura 2.4 se aprecian niveles de contaminación similares a los de Asia, África y Rusia. Bandas infrarrojo cercano.

Figura 2.5. Estudio con ayuda de imágenes satelitales de los días 13,14 y 16 de mayo del 2019



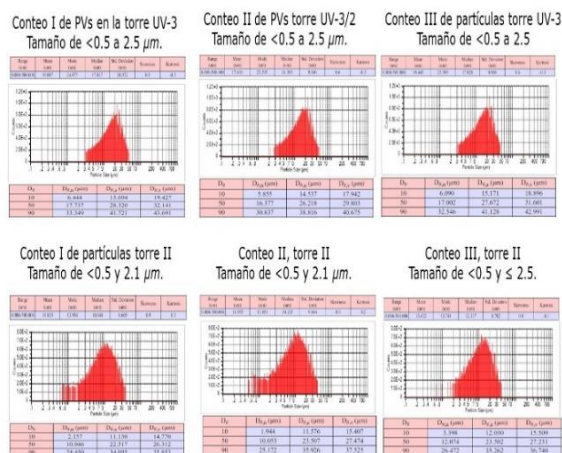
Fuente: Copernicus Atmosphere Monitoring Service UE, 2019.

En la Figura 2.5 se pudo observar la presencia de monóxido de carbono (CO_2) presente en el Valle de México, con concentraciones similares a las de Asia, África y Rusia.

II.4. Análisis cuantitativo por tipo de partículas PM ≤ 2.5 detectadas y recolectadas *in situ*

II.4.1. Metodología del *Particle Sizing System-AccuSizer*, 2019

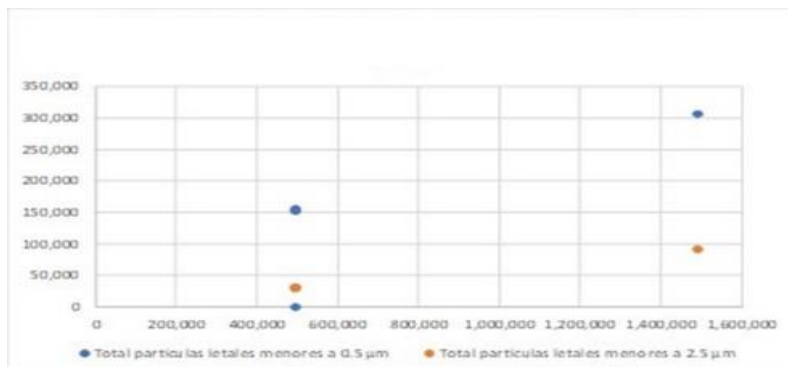
Figura 2.6 Cuantificación estadística de partículas citotóxicas PM 2.5 y $<0.5 \mu\text{m}$



En la Figura 2.6 se puede observar una uantificación estadística de partículas citotóxicas PM 2.5 y $<0.5 \mu\text{m}$, generadas por GEI, COVs y PVs, presentes en las azoteas de las torres UV-3 y II, en Angelópolis, Puebla.

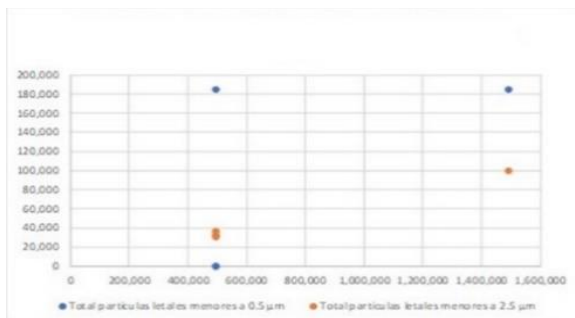
II.4.1.1. Análisis cuantitativo gráfico de partículas PM ≤ 2.5

Figura 2.7. Gráfica de totales de PVs, COVs y GEI



En la Figura 2.7 se puede observar la ráfica de totales de PVs, COVs y GEI detectados en el sistema *Particle Sising Sistem-AccuSizer* por número, área y volumen, de las cuales 462,736 resultaron ser menores a $0.5\ \mu\text{m}$ equivalentes al 83.333% y 92,548 a $\geq 2.5\ \mu\text{m}$ al 16.666%.

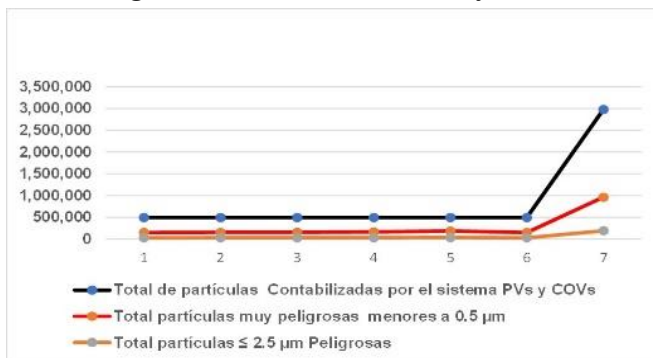
Figura 2.8. Grafica de totales de PVs, COVs y GEI



En la Figura 2.8 se puede observar la gráfica de totales de PVs, COVs y GEI detectados en el sistema *Particle Sising Sistem-AccuSizer* por número, área y volumen, de las cuales 585,145, $< 0.5\ \mu\text{m}$ equivalentes al 85.528% y 99,008 a $\geq 2.5\ \mu\text{m}$ al 14.465%.

II.4.1.2. Concentrado de la cuantificación de partículas recolectadas *in situ* de PM ≤ 2.5 y PVs, COVs y GEI contabilizadas por el *Particle Sising Sistem-AccuSizer*

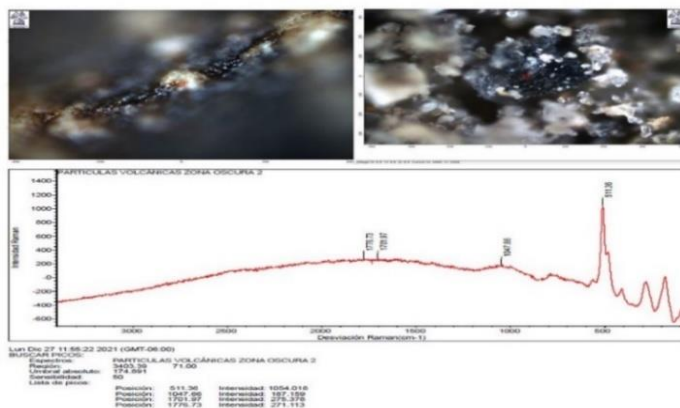
Figura 2.9. Partículas totales PVs y COVs



La Figura 2.9 muestra las partículas totales PVs y COVs = 2,981,334; Total PM <0.5 μm 962,881 y Total PM $\geq 2.5 \mu\text{m}$ 191,556 y observadas en microscopía Raman (figuras 1.1. a 1.13).

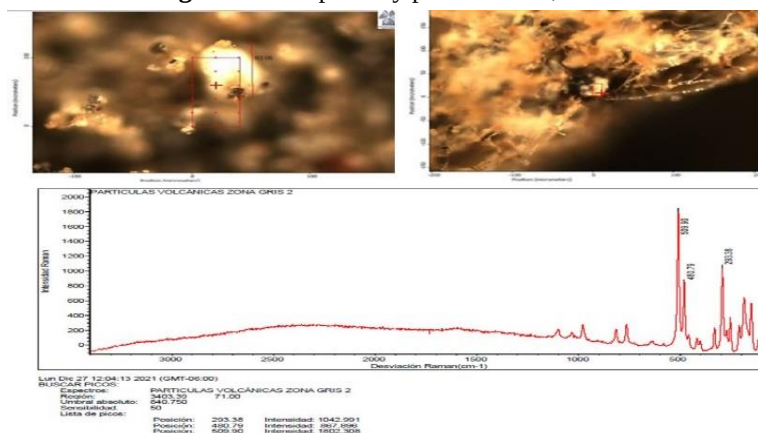
II.4.2. Análisis Raman PVs PM ≤ 2.5

Figura 2.10. Espectro con la interfaz de la librería sistema OMNIXi



En la Figura 2.10 se observa el espectro con la interfaz de la librería sistema OMNIXi, señales de los blancos PVs de azufre (S), en tejidos intersticiales y microvellosidades de la inflorescencia forestal urbana. Imágenes en x10 en microscopía Raman.

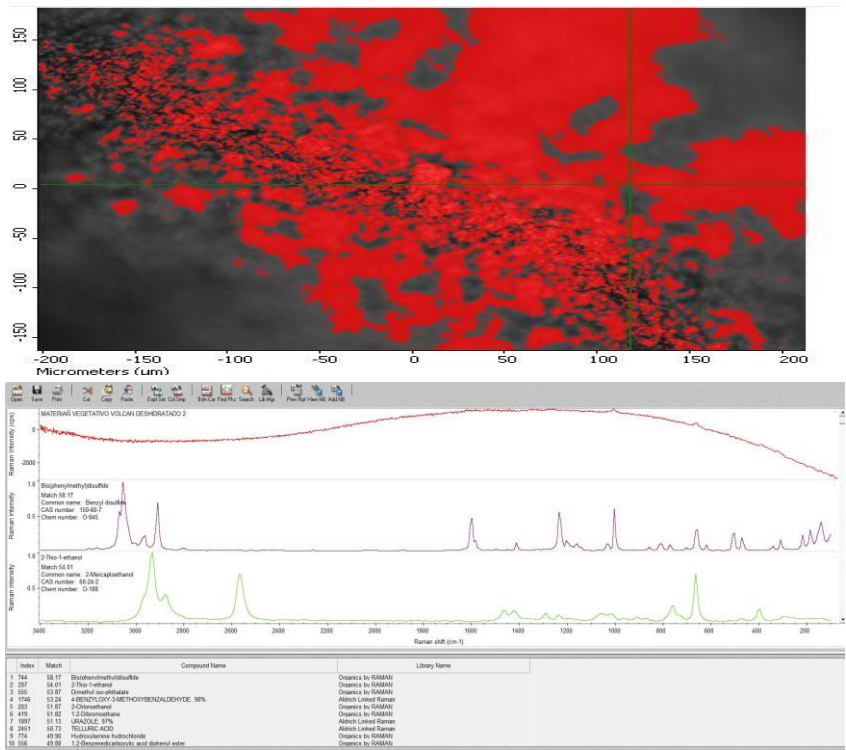
Figura 2.11 Espectro y picos de PVs, COVs



En la Figura 2.11 se observan el espectro y picos de PVs, COVs a partir de la interfaz con la librería del sistema OMNİcxi, blanco cristales de azufre (S) en ramas forestales urbanas. Imágenes en x10 en microscopía Raman.

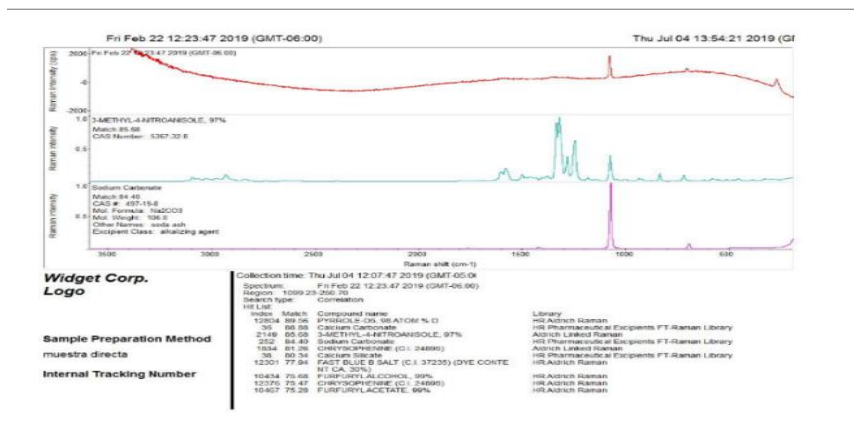
II.4.3. Análisis Raman de COVs

Figura 2.12. Micrografía de estructuras de inflorescencia en ramas forestales y, espectro de su contenido



En la Figura 2.12 se puede observar una micrografía de estructuras de inflorescencia en ramas forestales y, espectro de su contenido a partir de la interfaz con librería del sistema OMNİcxi; Señales de COVs. Se detecta presencia de Benzyl disulfide, CAS: 150-6-7 y Mercaptoethanol, CAS: 60-2 4-2. Imagen en rojo con dispersión espacial de COVs del tejido en x20 de microscopía Raman.

Figura 2.13. Espectro a partir de la interfaz



En la Figura 2.13 se puede observar el espectro a partir de la interfaz con librería del sistema OMNICxi. señales en blanco de Raman, COVs: 3-Methyl -4-Nitroanisol al 98%, CAS:5367-32-8 y Sodium Carbonate, CAS:497-19-8) en tejidos de inflorescencia forestal.

III. Introducción a la Inteligencia artificial (IA)

La Inteligencia Artificial (IA) es una tecnología avanzada que permite la combinación de herramientas múltiples de monitoreo y prospección como el presente caso, que permitirá diversos aspectos sociobiológicos y ecológicos como son la seguridad integral de la sociedad que habita en las ciudades de Amozoc, Coronango, Cuautlancingo, Huejotzingo, Puebla, San Andrés Cholula, San Martín Texmelucan, San Miguel Xoxtla y San Pedro Cholula como municipios conurbados de Puebla.

III.1 Antecedentes sobre la inteligencia artificial (IA), (Grigori Sidorov, 2011)

Agencia TSS – En 1968, el físico argentino e impulsor de buena parte de su programa nuclear, Jorge Sabato, junto con el politólogo Natalio Botana, formularon un modelo de interacción triangular entre tres vértices: Gobierno.

Infraestructura Científico-Tecnológica. Conformada en gran parte por la academia y sector productivo, integrado por las empresas públicas y privadas, como base para el- desarrollo y la innovación en materia tecnológica. El modelo pasó a ser conocido internacionalmente como el “Triángulo de Sabato”. El miércoles 15 de agosto, en el marco de la feria Expotrónica 2018, la muestra de tecnología que cada dos años realiza en la Ciudad de Córdoba la Cámara de Industrias Informáticas, Electrónicas y de

Comunicaciones del Centro de Argentina (CIECCA), se presentó oficialmente el Nodo de Colaboración Científico Industrial para la Investigación y el Desarrollo de la Inteligencia Artificial.

El “Nodo” es una iniciativa de cooperación entre la Facultad de Matemática, Astronomía, Física y Computación (FAMAF) de la Universidad Nacional de Córdoba (UNC) y el Córdoba Technology Cluster, de la que participa el Centro de Computación de Alto Desempeño (CCAD), también de la UNC.

*Construcción de modelos de la inteligencia humana,
tales que se puede implementarlos en las computadoras*

Se puede hacer una analogía con la física —antes de que se empezara a aplicar el aparato matemático en la física, ésta última era una ciencia descriptiva; después de aplicar los conceptos matemáticos, la física se convirtió en una ciencia exacta. Lo mismo sucedió con la inteligencia artificial, antes de que aparecieran las computadoras, la inteligencia artificial era parte de la filosofía —aunque no se utilizaba este nombre. Con las computadoras, la inteligencia artificial se convirtió en una ciencia exacta, ya que apareció la posibilidad de verificar sus teorías. Además, como siempre sucede con las computadoras, se agregó la posibilidad de procesar unas cantidades enormes de datos, lo que da una nueva calidad a la ciencia de la inteligencia artificial. Nótese que la palabra artificial precisamente subraya la idea de construir los modelos que se pueda implementar en algún artefacto, normalmente, la computadora. Una definición conocida es “sistemas basados en conocimientos”. Como ya sabemos, el conocimiento es precisamente el modelo del mundo externo, sin embargo, esa definición se centra en el conocimiento, e ignora los algoritmos que también son una parte importante de la IA. Otra posible definición es “sistemas basados en heurísticas”. Las heurísticas son las reglas o procedimientos que se aplican cuando no existe un método exacto para resolver un problema dado. Esa definición enfatiza la relación entre los métodos donde existe una solución exacta y los métodos donde no se sabe de antemano el camino a la solución, y para encontrar tal camino se usa la inteligencia, basada en el conocimiento y el razonamiento. Entre otras distinciones frecuentemente aceptadas, que se presentan, por ejemplo, en las definiciones de la inteligencia artificial se agrupan en cuatro categorías, a saber, la IA se define como:

- Sistemas que piensan como humanos;
- Sistemas que actúan como humanos;
- Sistemas que piensan racionalmente;
- Sistemas que actúan racionalmente.

Analizando esas definiciones, nos damos cuenta que todos se refieren a los sistemas, es decir, a los modelos implementados en las computadoras. Del otro lado, las diferencias entre las definiciones están relacionadas con el uso de las palabras “actuar” vs. “pensar” y “como humanos” vs “racionalmente”. Nos parece que las diferencias entre ambas pares de palabras se refieren en la realidad al mismo rasgo. De hecho, tanto actuar como pensar se refieren al modelo del mundo-, donde actuar implica la realización de ciertas acciones, mientras que en pensar no- se realizan las acciones, pero se decide que hay que realizarlas; notemos que en actuar tampoco se realizan las acciones al azar, sino dado algunas consideraciones previas, es decir, existe algún tipo de pensamiento —sea “racional” o “como humanos”. Entonces, la única diferencia entre actuar y pensar en este caso es la implementación física de las acciones, lo que nos parece irrelevante en el contexto de análisis ya que eso no está realmente relacionado con la propia inteligencia. Ahora bien, ¿y qué significa racionalmente? Según el mismo diccionario es “relativo a la razón”, y la razón es la “facultad de discurrir”; discurrir en su turno significa “inferir, conjeturar, reflexionar, pensar, aplicar la inteligencia”. Sin embargo, nos parece que la clave de la diferencia entre “racionalmente” y “como humanos” está en las palabras “como humanos”, porque está claro que este enfoque también es racional, por lo menos todas las cosas irracionales, como sentimientos, emociones, etc. que poseemos los seres humanos no son objetos de estudio de la inteligencia artificial tradicional.

Estructura operativa del área de la inteligencia artificial

La inteligencia artificial está compuesta por varias áreas bastante grandes. Las diferencias entre las áreas se basan en qué parte de la inteligencia se modela. Para imaginar todo el proceso debemos evaluar como funcionamos nosotros mismos, lo que se hace con el método de la introspección —es decir, tratando de observar nuestros propias acciones, pensamientos, etc. Nuestro funcionamiento e interacción con el mundo externo consiste en:

- a) Percepción basada en la información obtenida de nuestros sentidos son cinco sentidos - la visión, la audición, el olfato, el gusto, el tacto; pero el sentido más importante es la visión, según algunas evaluaciones más del 90% de la información recibida es visual —pensamiento basado en el modelo actual del mundo, que consiste en la ubicación de las percepciones en el modelo del mundo y del razonamiento sobre este modelo para resolver problemas;
- b) Acciones que realizamos a través de nuestro cuerpo y lenguaje;
- c) Uso de lenguaje natural para el pensamiento y para la transmisión/recepción de información en la sociedad.

El lenguaje natural es una capacidad única de los seres humanos. El lenguaje nos hace lo que somos. Ningún animal tiene un lenguaje; claro, los animales tienen sus sistemas de comunicación, pero nunca llegan a nivel de abstracción que desarrollaron los humanos. Entonces, de un lado, los humanos reciben la información a través del lenguaje y absorben toda la experiencia de la sociedad grabada en los textos y en palabras de los otros individuos. Del otro lado, el lenguaje natural es nuestra principal manera de representar el conocimiento en nuestro modelo del mundo. También podemos reaccionar no solo con las acciones físicas, sino en forma verbal entrando en un diálogo.

III.2 El Nodo

El convenio que dio origen al Nodo fue firmado por Mirta Iriondo, decana de la FAMAF, y Diego Casali, presidente del Cluster, el 14 de marzo de 2018, e inmediatamente la cooperación comenzó a materializarse a través de una Diplomatura en Ciencias de Datos, Aprendizaje Automático y sus Aplicaciones, destinada al personal de las empresas socias del Cluster, a docentes e investigadores académicos, estudiantes y empleados gubernamentales. Iriondo, doctora en Matemática e investigadora adjunta del CONICET, comenzó su exposición enmarcando la idea del Nodo en el esquema del Triángulo de Sabato. En ese contexto, enfatizó que uno de los roles del Estado es “traccionar con proyectos que impulsen a las pymes” para el desarrollo de nuevas tecnologías y capacidades productivas.

IV. Introducción y justificación en materia ambiental y ecológica para la prospección atmosférica frecuente en la ciudad de Puebla con IA

Los desastres, motivados por la acción del hombre, contribuyen hoy en día al deterioro del desarrollo socioambiental. Cerca del 75 % de la población mundial se encuentra en situación de riesgo ante desastres provocados por fenómenos naturales. Las estimaciones mundiales apuntan a que el crecimiento urbano, la degradación ambiental y el calentamiento global amplificarán el impacto de las catástrofes naturales; La pérdida de vidas humanas, la destrucción de medios de subsistencia y la devastación de áreas naturales, son algunas de las secuelas que se revelan en aquellos países con alto índice de huracanes, erupciones volcánicas, terremotos o conflictos bélicos. Es más, las regiones más desfavorecidas se muestran especialmente vulnerables a este tipo de situaciones. La gestión del riesgo es una estrategia fundamental para la reducción de eventos desfavorables en los sistemas socioambientales, así como para la generación de procesos de adaptación y resiliencia ante acontecimientos incontrolables por el humano (Bello *et al*, 2014) En el caso de México como cualquier otro país, no escapa a tener sus propios eventos de riesgo inminente, como el caso del centro del país en donde existe un volcán activo, el volcán Popocatepetl, el cual se encuentra históricamente rodeado de poblaciones humanas muy cercanas y vulnerables a cualquier evento

volcánico (González y Carranza, 2015). Adicionalmente la presencia grave de partículas y contaminantes urbanos, metano por el complejo problema del río Atoyac (Figuras 2 y 3). Estos contaminantes hidrológicos y atmosféricos causan a vías- respi-ratorias y oftálmicas, provocando irritación e inflamación (ATSDR Toxic Substances Portal Agency, 2019). Se describe el elevado nivel de contaminación que registran las aguas del río Atoyac y de su confluente, el río Zahuapan (Bravo et al., 2015). La contingencia atmosférica de mayo 13, 14 y 15 del año 2019, en la zona urbana de Puebla fue grave, fundado en los análisis por estaciones de prospección fijas, semifijas y móviles, que operaron conjuntamente el Gobierno del Estado y la Federación. En el presente estudio se mostraron pronósticos y monitoreos de concentraciones letales de exposición humana a la contaminación por gases efecto invernadero (GEI) en la zona metropolitana de Puebla. Al determinar la concentración de contaminantes citotóxicos (Sandoval Villasana *et al.*, 2009), (Saldaña y Gómez., 2006), (Bravo *et al.*, 2015) (Morales et al., 2015); Ozono (O₃), PVs partículas volcánicas sedimentarias y COVs compuestos orgánicos volátiles (Figuras 4 a 11), derivados del efecto antropogénico conjugado con fenómenos naturales (hidrometeorológicos, climáticos, geológicos) (IVHNN, Gas Guide Line, 2019) e incendios forestales (Salamanca, 2019); Impactaron en la salud de las poblaciones y medio ambiente urbano (medios físicos y bióticos). Cuando se presentan concentraciones de gases como el ozono (O₃) y partículas PM₁₀ y PM_{2.5} (Blanco Jiménez, 2015) y compuestos orgánicos volátiles (COVs) conjuntamente, epidemiológicamente ponen en riesgo la salud humana de animales y especies forestales (Wasim., 2014) –en este contexto–, es necesario hacer énfasis en las responsabilidades de las dependencias, empresas, entidades y autoridades en materia ambiental. La transversalidad, coherencia y concordancia con actuaciones oportunas entre la Ciudad de México, Estado de México, Hidalgo, Morelos, Tlaxcala y Puebla ante fenómenos que impactan igual en todas las entidades en zonas fronterizas de forma ecológica, y atmosféricamente a los municipios de Puebla; Amozoc, Cuautlancingo, San Andrés Cholula y San Pedro Cholula, San Martín Texmelucan, Huejotzingo, Coronango, San Miguel Xoxtla (Catalogación en la fuente INEGI, 2019).

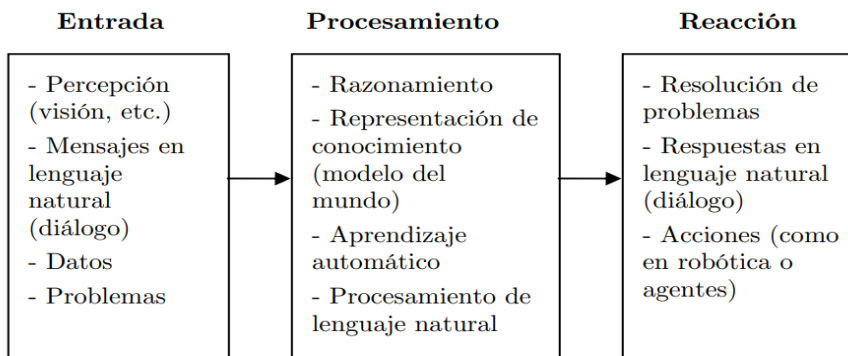
V. Material y Métodos

A continuación se muestra la propuesta para la prospección atmosférica de partículas suspendidas GEI, PVs y COVs sedimentables y sociobiológica en materia de seguridad pública de la zona urbana de Puebla con IA. (Rovirosa, Guadarrama y Saldivar, 2022).

Figura 5.1. Imagen de zona urbana de EUA en prospección con altos índices de monóxido de carbono (CO₂) y Dióxido de Nitrógeno (NO₂)



Figura 5.2. Diseño de flujo de información convencional en la IA



Fuente: (Grigori Sidorov (2011).

A continuación se muestran las estadísticas de conducta sociobiológicas en materia de seguridad pública de la ciudad de Puebla que justifican el uso de la Inteligencia artificial (IA) doble propósito (Grigori Sidorov, 2011), con base en las bases de datos de la encuesta nacional de victimización y percepción sobre seguridad pública, principales resultados, Puebla, para aplicar la IA en materia de seguridad humana (ENVIPE-INEGI, 2021).

Gráfico 5.1. Prevalencia delictiva en hogares de Puebla



Gráfico 5.2 Tasa de víctimas en Puebla

Tasa de víctimas

Víctimas¹ *por cada 100 000 habitantes* para la población de 18 años y más en el estado de **Puebla**.

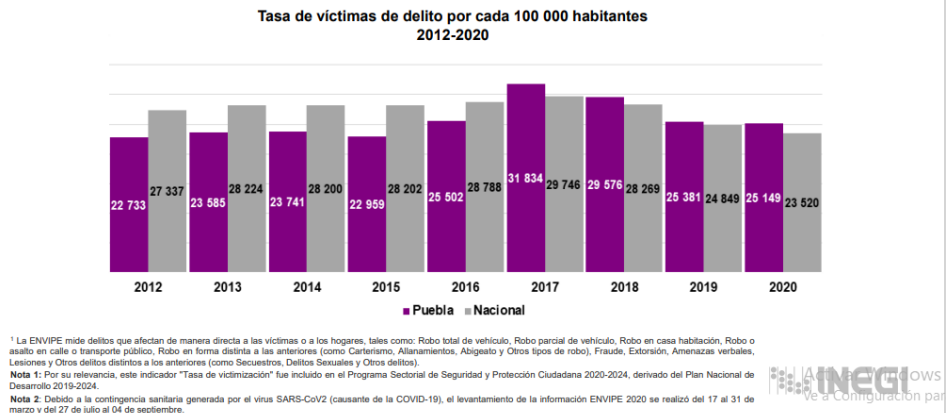


Gráfico 5.3 Incidencia delictiva en Puebla



Gráfico 5.4. Incidencia delictiva robo y asalto en Puebla

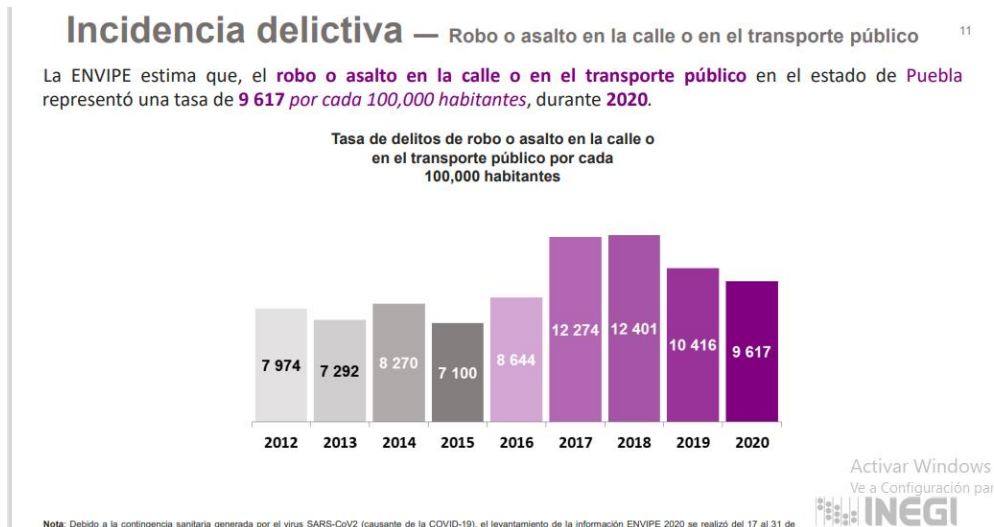
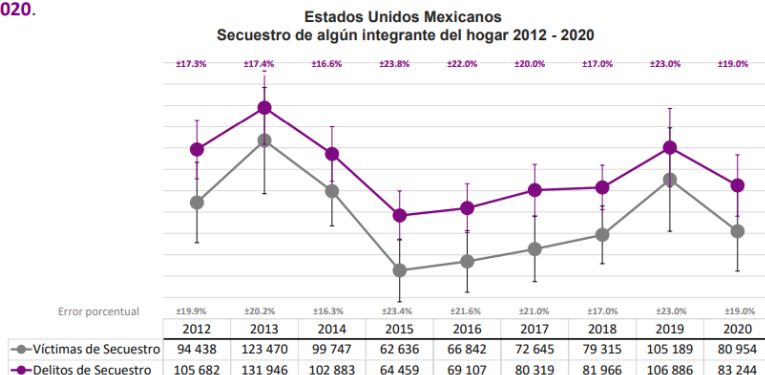


Gráfico 5.5. Incidencia delictiva y secuestro en Puebla

Incidencia delictiva — Secuestro de algún integrante del hogar

12

A nivel nacional, se estiman **83 244 secuestros de algún integrante del hogar** sufridos por **80 954 víctimas** durante **2020**.



Nota 1: La estimación de víctimas de secuestro para el año 2012 tiene un intervalo de confianza de (78 095; 110 781); para 2013 de (102 017; 144 923); para 2014 de (83 183; 116 311); para 2015 de (47 742; 77 530); para 2016 de (52 162; 81 522); para 2017 (58 250; 87 040); para 2018 (65 632; 92 998); para 2019 (80 672; 129 706) y para 2020 (85 405; 96 503). Por su parte, la estimación de delitos de secuestro para el año 2012, tiene un intervalo de confianza de (84 605; 126 759); para 2013 de (105 252; 158 640); para 2014 de (86 107; 119 659); para 2015 de (49 341; 79 577); para 2016 de (54 146; 84 068); para 2017 (63 826; 96 812); para 2018 (67 979; 95 953); para 2019 (82 222; 131 550) y para 2020 (87 331; 99 157).

Nota 2: Debido a la actualización estadística realizada por el INEGI (Cálculo de la FICHA 10) al procesamiento de la información ENADE 2020 en octubre del 17 al 24 de

Gráfico 5.6. Características de la incidencia delictiva

Incidencia delictiva — Características

13

De los **1 447 936** de delitos estimados para **2020**, la **víctima estuvo presente**¹ en **57.3%** de los casos, lo que representa en términos absolutos **830 032**.



De los delitos donde la víctima estuvo presente, **14%** de ellos involucró **algún tipo de agresión**².

¹ Corresponde aquellos delitos donde la víctima estuvo presente en el momento en que éste se cometió y en los que observó la realización del delito.

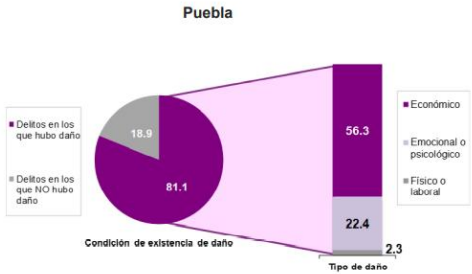
² La condición de agresión física es la situación que refiere la víctima respecto de haber o no sufrido una acción deliberada para provocarle un daño físico por parte del agresor.

Gráfico 5.7 Características de la incidencia delictiva

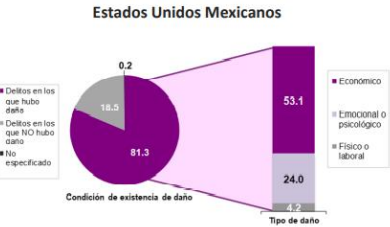
Incidencia delictiva — Características

14

De los **1 447 936** delitos estimados en el estado de **Puebla**, **81.1%** de los casos la víctima manifestó haber sufrido un **daño***.



A nivel nacional, **81.3%** de las víctimas manifestó haber sufrido un **daño***.



De los delitos donde la víctima manifestó haber sufrido un daño, **56.3%** de los casos el **daño** fue de tipo **económico**.

* Los daños incluyen económico, emocional o psicológico, físico o laboral.

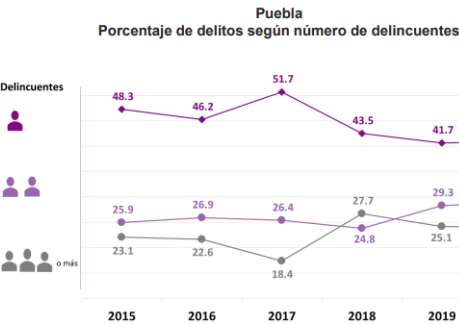
INEGI

Gráfico 5.8. Victimarios VS. Delincuentes en Puebla

Victimarios — Número de delincuentes

15

De los delitos estimados en el estado de **Puebla** donde la **víctima estuvo presente**, en **41.9%** de los casos la víctima manifestó que participó **sólo un delincuente**.



Delitos por sexo de los delincuentes participantes			
Año	Sólo Hombres	Sólo Mujeres	Hombres y Mujeres
2015	80.8	6.1	10.9
2016	82.0	5.3	10.8
2017	83.5	5.8	7.9
2018	80.1	4.2	12.8
2019	85.6	3.0	9.2
2020	84.4	4.7	9.1

Nota: Debido a la contingencia sanitaria generada por el virus SARS-CoV2 (causante de la COVID-19), el levantamiento de la información ENVPE 2020 se realizó del 17 al 31 de marzo y del 27 de julio al 04 de septiembre.

INEGI

Gráfico 5.9. Costos económicos del delito en Puebla

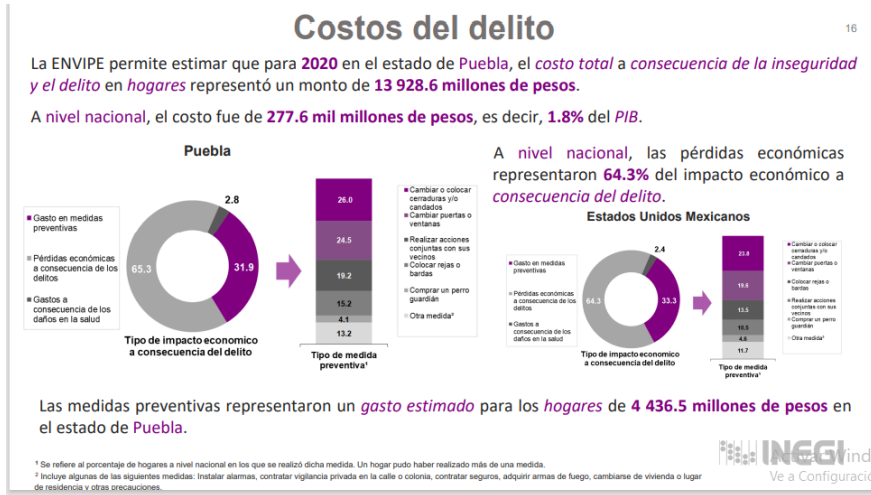


Gráfico 5.10. Cifra negra de delincuencia en el estado de Puebla

carpeta de investigación, entre el total de delitos por cien.

Entidad	Cifra Negra (%)								
	2012	2013	2014	2015	2016	2017	2018	2019	2020
NACIONAL	92.1	93.8	92.8	93.7	93.6	93.2	93.2	92.4	93.3
Puebla	92.5	94.3	93.2	92.3	94.9	93.2	91.6	91.3	94.7

Nota: Debido a la contingencia sanitaria generada por el virus SARS-CoV2 (causante de la COVID-19), el levantamiento de la información ENVIPE 2020 se realizó del 17 al 31 de marzo y del 27 de julio al 04 de septiembre.

INEGI
Activa Wind
Ve a Configuración

VI. Descripción de la tecnología del sistema de inteligencia artificial y seguridad sociobiológica en las zonas conurbadas de la CD. De Puebla

El sistema, aunque presenta distintas funcionalidades que corresponden a diversas áreas de la administración, estará enfocado principalmente en la seguridad social. La misma infraestructura puede ser utilizada para incorporar todo tipo de sensores al sis-

tema incluyendo los de prospección de $PM \leq 2.5$ de GEI, PVs y COVs, sin la necesidad de desplegar nueva y costosa infraestructura paralela. Utiliza una plataforma unificada para el monitoreo y control de distintas variables. El sistema utilizará infraestructura existente y nueva para la video vigilancia, incorporando tecnología de inteligencia artificial para la activación de alarmas que permitan un uso más efectivo y eficiente de los recursos digitales. La información generada por medio de analíticos permitirá automatizar acciones en función de diversas reglas previamente establecidas. Así como identificar patrones y acciones disruptivas que requieren atención. De esta manera, se pueden accionar, de forma automática, medidas preventivas y reactivas para apoyar las funciones de seguridad social, ecológica y ambiental.

La plataforma permitirá incorporar, entre otras funciones:

- 1) La identificación de personas en bases de datos preexistentes, para llevar trazas de su desplazamiento o permitir el acceso a zonas controladas;
- 2) La identificación de las placas y otras características de los vehículos (color, tipo, marca, modelo), para contar con trazas sobre sus desplazamientos, corroborar destinos, permitir el acceso, etc. Con la debida integración a bases de datos existentes, se pueden identificar vehículos robados, placas sobrepuestas, infractores, etc.;
- 3) La identificación de comportamientos o eventos atípicos, tales como conducción de vehículos en contrasentido, exceso de velocidad, concentración de personas, personas corriendo, objetos olvidados, vueltas prohibidas, acceso indebido a zonas restringidas, etc.;
- 4) La identificación y clasificación de vehículos (automóviles, motocicletas, bicicletas, camiones de pasajeros y carga), personas y animales, así como el conteo de concentraciones, frecuencias, etc.;
- 5) La detección de armas de distintas características, tanto ocultas (multisensor de infrarrojo cercano), como visibles (video);
- 6) La identificación por sensorización de variaciones fuera de rango en variables de partículas $PM 2.5$, gases efecto invernadero (GEI), compuestos orgánicos volátiles (COVs) y partículas volcánicas sedimentaria (PVs); Pureza atmosférica, temperaturas, humedad relativa, iluminación, flujos de agua y pronóstico de precipitaciones.

VI.1 Sensorización espacial urbana por tipo de prospección ambiental de partículas $PM \leq 2.5$ de GEI, PVS y COVs; caracteres e indicadores climáticos y conducta sociobiológica humana de comportamiento urbano

Figura 6.1. Tipos de sensores y estaciones múltiples de prospección urbana combinados con BIGDATA, Internet de las cosas y Intelicity V2 propuestos para zona urbana



VI.2. Centro de operaciones de inteligencia artificial (COIA) para la ciudad de Puebla. Estaría a cargo de la SEDEMA en coordinación con Gobiernos Municipales

Figura 6.2. Centro de operaciones prototipo de inteligencia artificial para la ciudad de Puebla a cargo de la SEDEMA-Gobiernos Municipales



VI.3. Funciones del Centro De Operaciones De Inteligencia Artificial (COIA) de la CD. De Puebla

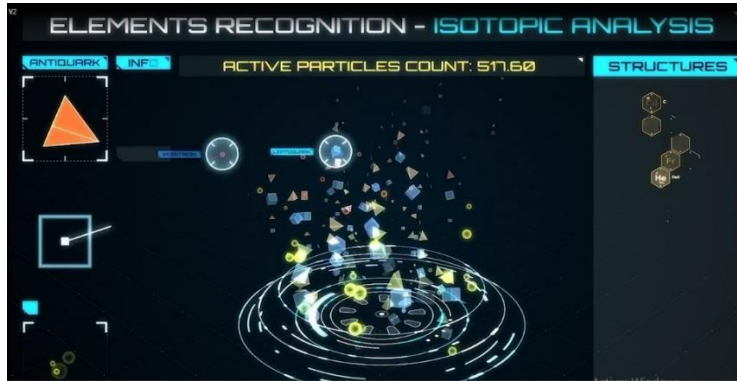
- a) Colecta y ordenamiento de bases de datos recolectados para procesamiento digital y emisión de alertas por medio de Nodos y algoritmos;
- b) Implementar sistemas digitales de operación de BIGDATA, Internet de las cosas y Intelicity V2.
- c) Implementar y controlar funciones de prospección por sensorización urbana.
- d) Generar alertas y semaforización social, ambiental y de seguridad biológica.
- e) Reportar a la sociedad y autoridades transversalmente de todos los fenómenos ambientales y sociobiológicos detectados en la zona urbana de Puebla con bases de datos probabilísticos de los Patrones estadísticos de la sensorización en tiempo real.
- f) Registro estadístico de todos los fenómenos ambientales y sociobiológicos y de conducta humana en la zona conurbana de Puebla. Incluyen violencia y crisis emocional por pánico colectivo.
- g) Emisión comunitaria de alertas de cualquier actividad anormal ambiental y sociobiológica que ponga en riesgo a grupos sociales y grupos comunitarios en colonias o barrios y zonas de alta concentración urbana.
- h) Transferencia social de conocimiento generado por experiencia de crisis sociales en general. *Causa-Efecto*, crisis ambiental y aprendizaje evolutivo de la conducta humana en zonas conurbadas de Puebla.

Para todas estas funciones se pueden programar alertas y acciones en tiempo real, mejorando la velocidad y capacidad de respuesta humana. Eliminando errores humanos y procesando grandes volúmenes de información para la identificación de patrones de comportamiento sociobiológico y ambiental de forma conjunta autoridades sociedad.

El proyecto estaría montado sobre una red digital gubernamental de enlaces robustos y estables con uso de satélites y drones de forma combinada. Para garantizar la continuidad en las operaciones de monitoreo prospección y vigilancia urbana. La plataforma única de monitoreo digital con infraestructura permite detectar fallas y problemas por medio de la retroalimentación del sistema en tiempo real. Igualmente hacer diagnósticos remotos y acelerar los procesos de mantenimiento para contar con altos niveles de eficiencia y disponibilidad del sistema, por encima del 98% de eficiencia y rendimiento.

VI.3.1. Colecta y ordenamiento de bases de datos recolectados para procesamiento digital y emisión de alertas por medio de Nodos y algoritmos

Figura 6.3. Sistema de generación de bases de datos a partir de sensorización y Nodos para procesarse por medio de algoritmos y convertirlos en datos estadísticos



VI.3.2. Implementación de sistemas digitales de operación de BIGDATA, Internet de las cosas y Intelicity V2

Figura 6.4. Distribución geográfica prototipo de la sensorización urbana prototipo controlado por Centro de Operaciones para uso social y ambiental utilizando BIG DATA, Internet de las cosas y Intelicity V2

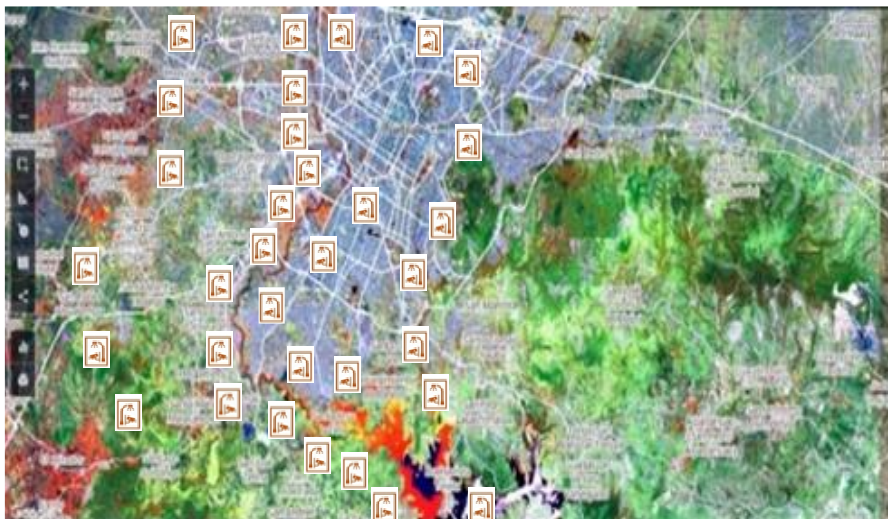


Figura 6.5. Distribución geográfica urbana de la sensorización prototipo controlado por Centro de Operaciones para uso social y ambiental utilizando BIG DATA, Internet de las cosas y Intelicity V2



VI.3.3. Prospección satelital y con Drones hídrica de la cuenca urbana del Atoyac

Figura 6.6. Mapeo con puntos de prospección con Nodos climáticos y ambientales atmosféricos e hidrológicos de la cuenca urbana del Río Atoyac.



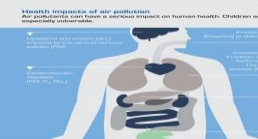
VI.3.4. Prospección urbana de movilidad sociobiológica con inteligencia artificial

Figura 6.7. Puntos clave en esquinas urbanas de monitoreo ambiental por sensorización enlazada con satélites climáticas y ambientales



VI.3.5. Semaforización contingente ambiental de la sensorización atmosférica e hidrológica

Figura 6.8. Semáforo advertencia poblacional urbana de partículas $PM \leq 2.5$ del sistema de control y prospección de GEI, PVs Y COVs

SEMAFORO AQI (Air Quality Index).	NIVELES DE CONCENTRACIÓN	VALORES DEL INDICADOR	DESCRIPCIÓN DE LA CALIDAD DEL AIRE.
			
Verde	Bueno-Sano	0 a 50	La calidad del aire es satisfactoria, y la contaminación del aire representa poco o ningún riesgo.
Amarillo	Moderado	51 a 100	La calidad del aire es aceptable. Sin embargo, puede haber un riesgo para algunas personas, particularmente aquellas que son inusualmente sensibles a la contaminación del aire.
Naranja	Insalubre para grupos sensibles	101 a 150	Los miembros de grupos sensibles pueden experimentar efectos en la salud. Es menos probable que el público en general se vea afectado.
Rojo	Insalubre	151 a 200	Algunos miembros en general pueden experimentar efectos más graves para la salud; pueden experimentar efectos en la salud; miembros de grupos sensibles.
Purpura	Muy insalubre para todos.	201 a 300	Alerta de salud: El riesgo de efectos en la salud aumenta considerablemente.
Marón	Peligrosos	301 y Más	Advertencia sanitaria de las condiciones de emergencia: es más probable que todos se vean afectados por altas concentraciones.

VI.3.6. Sensorización y prospección de COVs. Hidrológica del río Atoyac

Figura 6.9. Sensorización y prospección hidrológica de COVs e índices de calidad del agua del río Atoyac



VI.3.7. Prospección del río Atoyac con cámaras hiperespectrales en Drones y transmisión de datos por radio frecuencia a tiempo real para localizar puntos de descargas y contaminación de empresas y Ayuntamientos combinadas con imágenes del satélite multiespectrales

Figura 6.10. Dron con cámaras hiperespectrales para prospección del rio Atoyac en la cuenca urbana de la ciudad de Puebla y teletransmisión de datos al centro de operación



Figura 6.11. Emisión de alertas de pánico de respuesta rápida a la sociedad y autoridades urbanas de zona conurbada de Puebla por riesgos sociobiológicos y ambientales



Figura 6.12. Detección de armas de fuego y armas blancas en individuos con conductas inapropiadas y tendencias psicológicas delincuenciales



VI.3.8. Prospección sociobiológica *in situ-ex situ* de la conducta psicológica en zonas de alta concentración urbana en zonas conurbadas de Puebla por IRC y Rayos X

Figura 6.13. Detección por IRC y Rayos X la portación de armas de fuego y armas blancas en personas potencialmente peligrosas



VI.3.9. Control urbano por prospección y sensorización en la movilidad poblacional con armas y actitudes agresivas o anormales para emisión de alertas tempranas

Figura 6.14. Modelo de prospección sociobiológica por IRC y Rayos X de actitudes anormales y portación de armas de fuego y armas blancas y grupos delincuenciales organizados en su movilidad



Figura 6.15. Caracterización integral digital con IA morfológica de rostros y rasgos faciales, con técnicas forenses de personas sospechosas para la identificación temprana de posibles tendencias normales de conductas



VI.3.10. Seguimiento con IA de vehículos vinculados y sospechosos en actos delincuenciales con técnicas IRC y Rayos X para detección de armas y emisión de alertas tempranas.

Figura 6.16. Prospección y seguimiento con IA de vehículos vinculados y sospechosos en actos delincuenciales con técnicas IRC y Rayos X

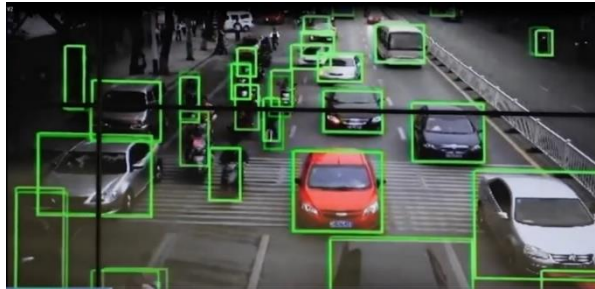


Figura 6.17. Transferencia de conocimiento sociobiológico urbano en crisis ambientales y de seguridad pública de las zonas conurbanas de Puebla



VI.4. Componentes de NODOS del sistema de inteligencia artificial (IA) y tecnología de la información (TI y SIG) para el procesamiento de señales y datos *ex situ-in situ*

Figura 6.1. Diseño de los componentes del sistema de IA y prospección urbana.

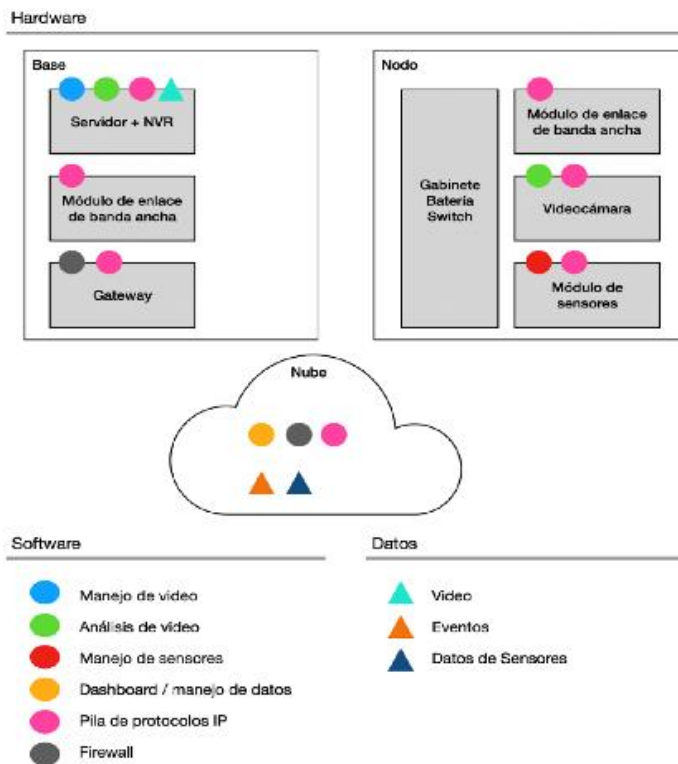
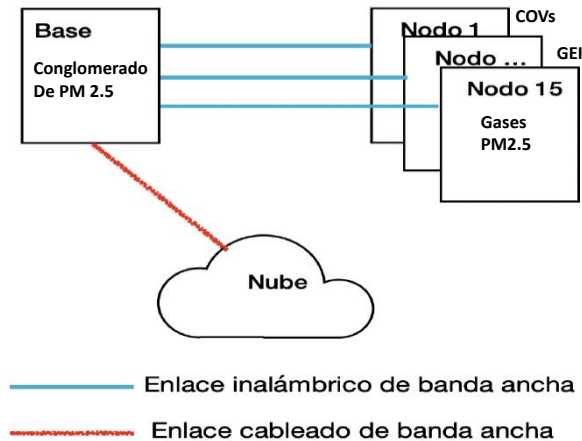


Figura 2. Componentes del sistema

VI.4.1. Diseño de postes inteligentes del sistema de la inteligencia artificial distribuidos en las zonas conurbadas de la ciudad de Puebla.

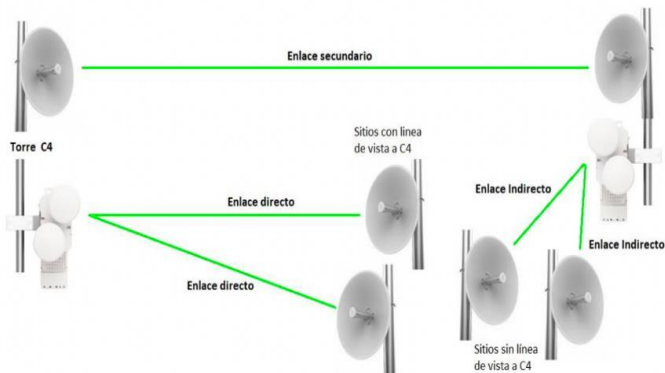
A continuación se presente el sistema de sensorización de la IA en postes de acero reforzados *in situ* para ser instalados en Puebla; Amozoc, Coronango, Cuautlancingo, Huejotzingo, Puebla, San Andrés Cholula, San Martín Texmelucan, San Miguel Xoxtla Y San Pedro Cholula para montar detectores de señales de BIGDATA, Internet de las cosas y Intelicity V2.

Figura 6.3. Dinámica de funcionamiento de NODOS e IA del sistema integral en zonas conurbadas de Puebla



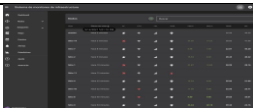
VI.4.2. Transmisión de datos por medio de radiofrecuencia y transducción de señales combinados con Drones y satélites

Figura 6.3. Sistema de radiofrecuencia de transducción transmisión de datos recolectados *in situ* a partir de postes ubicados en zonas conurbadas de Puebla



VII. Componentes electrónicos de la tecnología del sistema de IA aplicable al sistema de vigilancia, monitoreo y prospección sociobiológica de seguridad ambiental y seguridad pública

A continuación se presentan los equipos del sistema integral de IA y tele transmisión de datos al sistema de IA con bases de procesamiento datos para plataforma de captura y procesamientos con la transducción de señales de frecuencias e imágenes.

1) Antenas de distribución	
2) Switch para enlaces	
3) Cámara fija.	
4) Lente Ópt. de señales. de comunicación.	
5) Camaras PTZ.	
6) Servidores	
7) Dashboard de monitoreo.	
8) Plataforma de monitoreo de de videos y alertas de datos analíticos. de infraestructura.	

9) Pilares de tecnología multisensor	
10) Antenas para enlaces	
11) Poste y cámaras en arroyo para detección de armas ocultas. Inalambricos. Vehicular.	
12) Gabinetes y electrónica en sitio.	
13) Detectores y sensores Raman de PM 2.5	

VIII. Conclusiones

La ciudad de Puebla y los municipios conurbados de Amozoc, Coronango, Cuautlancingo, Huejotzingo, Puebla, San Andrés Cholula, San Martín Texmelucan, San Miguel Xoxtla Y San Pedro Cholula. están viviendo conjuntamente una situación muy compleja entre los problemas sociobiológicos; Que implican, una crisis de salud ambiental por fenómenos atmosféricos e hidrológicos conjugados, la presencia grave de GEI, COVs y PVs requieren de forma urgente un monitoreo y prospección a tiempo real para evitar complicaciones de salud pública con COVID, Silicosis y otras enfermedades crónico degenerativas como IRC y Cáncer, así como afectación a sus ecosistemas forestales, hidrológicos, pedológicos y atmosféricos.

Las estadísticas del INEGI evidencian una situación de seguridad sociológica frágil y vulnerable a la delincuencia organizada que demanda una estrategia con todos los medios tecnológicos disponibles que fortalezcan la gestión de las autoridades responsables de la impartición de vigilancia y justicia.

Con la tecnología propuesta se logrará un control estratégico para revertir los daños a los ecosistemas y garantizar la seguridad e integridad de la zona conurbada de Puebla.

Referencias

- Grigori Sidorov (Ed.). 2011. Métodos modernos de Inteligencia Artificial. Laboratorio de Procesamiento de Lenguaje Natural Instituto Politécnico Nacional (IPN. México D.F.
- Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública. Principales Resultados. Puebla. (ENVIPE)-INEGI. 2021.
- Rovirosa Madrazo C.A., Guadarrama L. A.; Escobar R. D. 2019. Indicadores forestales relacionados con partículas de un fenómeno atmosférico conjugado urbano en Puebla, México en la crisis atmosférica de mayo del 2019 en la ciudad de Puebla. Convenio de Investigación Científica, INAOE-SEDEMA/CONCYTEP, Thermo Scientific México. Puebla, México.
- Rovirosa Madrazo C. A. 2021. Sistema Integral de Inteligencia Artificial (SIIA) Para El Desarrollo Turístico Litibú, Nayarit. FONATUR-EYPO. México 2021.
- Vigevano Marta R. 2021. Inteligencia artificial aplicable a los conflictos armados: límites jurídicos y éticos. RBOR Ciencia, Pensamiento y Cultura. Vol. 197 Núm. 800 (2021). Argentina.

Capítulo 13

El aviso de privacidad de datos personales en la era digital de la videovigilancia

The privacy notice of personal data, in the digital era of video surveillance

*Dennisse de los Ángeles Uribe Obregón**

Resumen

El objetivo del presente capítulo es identificar que los sistemas de videovigilancia son una herramienta tecnológica útil e indispensable que permiten reforzar la seguridad tanto en espacios públicos como privados. La protección de datos personales, a través de los avisos de privacidad en la implementación de los sistemas de videovigilancia, ha llevado en algunos casos a ponderar sobre qué derechos son más valiosos, si el derecho a la privacidad e intimidad o el derecho a la seguridad.

Lo anterior se analizará a través de un análisis teórico utilizando el método cualitativo con la finalidad de analizar la legislación en materia de protección de datos personales y los avisos de privacidad.

Palabras clave: Videovigilancia; Aviso de privacidad; Datos personales; Derecho privacidad e intimidad.

Abstract

The objective of this chapter is to identify that video surveillance systems are a useful and indispensable technological tool that allows security to be reinforced in both public and private spaces. The protection of personal data, through privacy notices in the implementation of video surveillance systems, has led in some cases to consider which rights are more valuable, whether the right to privacy and intimacy or the right to security. The above will be analyzed through a theoretical analysis using the qualitative method in order to analyze the legislation on the protection of personal data and privacy notices.

Keywords: Video surveillance; Privacy notice; Personal data; Privacy; Privacy rights.

* Doctora en Derecho Público por el Instituto de Investigaciones Jurídicas de la Universidad Veracruzana.

Introducción

El incremento actual de los niveles de inseguridad que se presenta en el sector público, así como en el privado, han llevado a desarrollar nuevas alternativas en la implementación de sistemas de videovigilancia, lo que ha permitido a las personas encargadas de la seguridad poder actuar de manera rápida y eficiente en el control y, en su caso, en la prevención de delitos y, así, disminuir los índices de inseguridad.

Aceves Bernal señala, que: “actualmente se cuenta con sociedades más globalizadas, donde el control gubernamental sobre la población está aumentando; razón por la cual, es importante no perder de vista que los métodos de vigilancia por parte del estado sean cada vez más estrictos, especialmente después de los actos del narcotráfico y del terrorismo alrededor del mundo que se han llevado a cabo” (2013, p. 39).

Es posible asegurar que el derecho a la privacidad e intimidad, con la implementación de los sistemas de videovigilancia, en algunas ocasiones se han visto restringidos; sin embargo, el objetivo principal de la seguridad es el garantizar las libertades, la paz y la tranquilidad, sin menoscabar los derechos humanos de las personas.

En el presente trabajo se analizará el concepto de videovigilancia, así como sus antecedentes, utilizando el método comparado; posteriormente, a través del método cualitativo y sistemático se conocerán diversas legislaciones relacionadas con la protección de datos personales y sus principios, el aviso de privacidad y sus tipos, la videovigilancia, el derecho de privacidad e intimidad en México.

1. La videovigilancia

La Real Academia de la Lengua Española define a la videovigilancia como el medio de un sistema de cámaras, fijas o móviles (RAE, 2023).

Es importante mencionar que el término de videovigilancia es una palabra compuesta por la palabra video, la cual proviene del vocablo inglés, misma que deriva del latín *video*, que quiere decir “yo veo”; y la palabra vigilancia, que proviene del latín *vigilantia*, la cual significa “dispuesto para vigilar”. Por lo tanto, el verbo vigilar, proviene del latino *vigilare*, que significa “acción de velar”.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), describe a la videovigilancia como:

el uso de cámaras de video fijas o móviles con o sin sonido, o de sistemas cerrados de televisión que involucren la colocación de una o varias cámaras en espacios privados o públicos, limitadas a la supervisión o monitoreo de ese espacio y de las personas que en él se encuentran (INAI, 2016).

La videovigilancia es una herramienta de control y vigilancia pública, misma que también se utiliza en los espacios privados. Este tipo de sistemas consiste en implementar cámaras de video fijas o móviles, con la finalidad de observar de manera remota (desde un celular) y/o videograbar áreas geográficas (uso de drones) o áreas designadas con el propósito de prevenir, disuadir o sancionar comportamientos inusuales o documentar incidentes y situaciones de emergencia.

Hoy en día, los sistemas de videovigilancia se han utilizado como métodos que ayudan a prevenir y en algunos casos para poder sancionar aquellas conductas contrarias a ley o para garantizar la seguridad de personas o, en su caso, bienes materiales. Por lo que, al usar el sistema de la videovigilancia es posible capturar imágenes de personas que las identifiquen o las hagan identificables, cuya recopilación y almacenamiento impliquen un manejo de datos personales (INAI, 2019).

2. Antecedentes de la videovigilancia

La implementación de los sistemas de videovigilancia tuvo su origen en las pruebas realizadas por el ingeniero estadounidense Frank B. Gilbreth, con el principal objetivo de llevar a cabo el monitoreo a operarios y a profesionales destacados a comienzos del siglo XX. El científico Frank Gilbreth, pretendía optimizar aquellos procesos productivos y aumentar la eficacia, utilizando tecnologías visuales y cámaras cinematográficas con la finalidad de mejorar la producción industrial (Ramírez, 2021, p. 79).

A partir de 1971, en Estados Unidos se comenzaron a utilizar los sistemas de videovigilancia para conocer, prevenir y contender aquellas manifestaciones que ocasionaban desórdenes públicos. Este monitoreo se realizaba a través de circuitos cerrados de televisión, por lo que, a partir de esa época, diversos países en el mundo comenzaron a utilizar los citados sistemas.

La primera práctica de implementación en espacios públicos se desarrolló en los años 1970, “cuando se estableció el primer sistema público de vigilancia en la ciudad turística británica de Bournemouth en 1985 como parte de la reunión anual del Partido Conservador del Reino Unido” (Soto Galindo, 2023).

En los años 80, en Norteamérica, el uso de sistemas de videovigilancia no era empleado en la mayoría de los casos para las áreas públicas, pero en el sector privado los propietarios de tiendas y bancos comenzaron a utilizar dichos sistemas, para contrarrestar la inseguridad.

Con los atentados ocurridos el 11 de septiembre de 2001 en Estados Unidos, se impuso el tema de la seguridad como una de las prioridades de la agenda mundial, por lo que los sistemas de videovigilancia se han ido implementando en los medios que se consideran vitales para la lucha contra el terrorismo.

Actualmente, en diversos países se ha instaurado la tecnología de video vigilancia con CCTV, la cual es utilizada como un instrumento para supervisar y monitorear los sistemas de transporte, vigilar el mantenimiento de la infraestructura, prevenir incendios y supervisar espacios públicos. Suiza en los 90 adoptó de manera amplia la tecnología de CCTV con la finalidad de manejar el sistema operativo de áreas públicas (Security, n.d.).

En el año 2006, en China se adoptó el programa “Ciudades más invirtiendo en sistemas biométricos”; éste fue implementado en 660 localidades. Dichos avances tecnológicos fueron primordiales para la organización, desarrollo, vigilancia y seguridad de las Olimpiadas de Beijín en el año 2008, sistema que ayudo a monitorear las actividades que se desarrollaron durante el citado evento deportivo y prevenir cualquier anomalía que pusiera en alto riesgo a la población (Security, n.d.).

Según diversos informes, Inglaterra se ha catalogado como el país más vigilado del mundo, pues cuenta con un promedio de 4.2 millones de cámaras instaladas, las cuales se encargan de seguir cada movimiento de sus pobladores.

El 27 de octubre de 2008 fue publicada, en la Gaceta Oficial de la Ciudad de México, la Ley que regula el uso de tecnología para la Seguridad pública del Distrito Federal, la cual, en su artículo 1, dispone lo siguiente:

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

- I. Regular la ubicación, instalación y operación de equipos y sistemas tecnológicos a cargo de la Secretaría de Seguridad Pública del Distrito Federal;
- II. Contribuir al mantenimiento del orden, la tranquilidad y estabilidad en la convivencia así como prevenir situaciones de emergencia o desastre e incrementar la seguridad ciudadana;
- III. Regular la utilización de la información obtenida por el uso de equipos y sistemas tecnológicos en las materias de seguridad pública y procuración de justicia; y
- IV. Regular las acciones de análisis de la información captada con equipos o sistemas tecnológicos para generar inteligencia para la prevención de la delincuencia e infracciones administrativas.” (Ley que regula el uso de tecnología para la Seguridad pública del Distrito Federal, 2008)

La citada Ley ha permitido la instalación de cámaras de videovigilancia en la Ciudad de México. De conformidad con los datos disponible con el Portal del Gobierno de la Ciudad de México, en 2018 se tenía registro de 18 mil 410 cámaras del C5; al año 2000 se han instalado un total de 64 mil 807, por lo que se cuenta con vigilancia en tiempo real, lo que ha contribuido al soporte de las carpetas de investigación y seguimiento de diversos delitos en la capital (CDMX, 2022).

3. Protección de datos personales

El primero de junio del año 2009 se publica en el Diario Oficial de la Federación (DOF) el decreto por el que se incorpora en la Constitución Política de los Estados Unidos Mexicanos (CPEUM) el derecho de cada individuo a la protección de sus datos personales, al acceso, corrección y eliminación de los mismos, así como a expresar su objeción, adicionando en esta reforma al artículo 16° segundo párrafo del texto constitucional

A través del reconocimiento en la CPEUM de la protección del derecho a la protección de datos personales, se inicia una nueva etapa proteccionista en materia de derechos humanos en su vertiente de protección de datos, y que este nuevo derecho proporciona la libertad para autodeterminarse, es decir la libertad de elegir con quién compartir sus datos después de haber sido informado de sus reglas tratamiento (términos y condiciones) mediante los avisos de privacidad, lo que significa la previa información del responsable del manejo de los mismos propósitos y seguridad que monitorean, de modo que, de manera consciente, decida a quién y para qué proporciona sus datos.

El reconocimiento constitucional de la protección de datos personales busca armonizar la tecnología, el comercio y la salvaguardia de la privacidad e intimidad de las personas. Para lograr esto es crucial establecer límites, deberes y obligaciones en el tratamiento de datos personales a través de leyes reglamentarias. Este proceso debe basarse en el consentimiento libre y la aceptación debidamente informada de los titulares, quienes han proporcionado sus datos como requisito para llevar a cabo alguna transacción comercial. De este modo, la autodeterminación informativa se entiende como la capacidad de decidir sobre los propios datos personales.

El cinco de julio de 2010 fue publicada en el DOF la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual, en el artículo 3, fracción V, define el concepto de dato personal: “Cualquier información concerniente a una persona física identificada o identificable” (LFPDPPP, 2010).

Posteriormente, el veintiséis de enero de 2017 fue publicada en el DOF la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en el artículo 3, fracción X se define el concepto de datos personales, estableciendo lo siguiente: “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” (LGPDPPSO, 2017).

Hoy en día, las personas pueden disponer de la información que de su persona exista en los archivos de registros de bases de datos: “a fin de que dicha información sea veraz, íntegra, actualizada, no intrusiva y con las garantías de seguridad pertinentes conforme a la finalidad para la cual hayan sido recolectados” (Aveleyra, 2003, p. 27).

En conclusión, se puede advertir que el derecho a la protección de datos personales es un derecho autónomo y contempla los derechos ARCO (de acceso, rectificación, cancelación y oposición); aunado a ello, se permite la autodeterminación informativa, la cual permite a la persona tener el control de sus datos personales y, con ello, el que puedan garantizar el respeto a su privacidad e intimidad.

Para Carranza, el reconocimiento constitucional y legal del derecho a la protección de los datos personales, menciona que “pretende garantizar el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaban y utilizan sus datos personales” (Araujo Carranza, 2009, p. 57).

3.1. Principios de la protección de datos personales

Los principios de protección de datos son un conjunto de reglas que dictan cómo deben recopilarse, procesarse y compartirse los datos personales tanto por entidades públicas como privadas; por lo que es importante reflexionar si a estos principios deben recurrir supletoriamente las personas titulares de salvaguardar y proteger los datos personales en los casos que encuentren vacíos o lagunas legales y éstas, en uso de sus atribuciones, tengan la obligación de proponer una determinación.

Dado lo expuesto, es relevante destacar que el derecho a la protección de datos personales se fundamenta en ocho principios esenciales que regulan las responsabilidades y compromisos de aquellos encargados de salvaguardar los datos personales, los cuales se detallan a continuación.

- 1) **Principio de licitud:** “establece que todo tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera” (IDAIQROO, 2023).
- 2) **Principio de finalidad:** “señala que todo tratamiento de datos personales que efectué el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, en relación con las atribuciones expresas que la normatividad aplicable les confiera” (IDAIQROO, 2023).
- 3) **Principio de lealtad:** “este principio está vinculado con el de licitud o principio de lealtad y legalidad que obliga al responsable a que los datos recolectados se usen para finalidades lícitas y legales, que no atenten contra su titular ni contra terceros” (Instituto Nacional de Transparencia, 2023).
- 4) **Principio de consentimiento:** “Es uno de los principios de mayor importancia, ya que, sin el consentimiento, no sería posible tratar de manera lícita los datos personales” (Instituto Nacional de Transparencia, 2023).
- 5) **Principio de calidad:** “implica que, el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos

personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento” (IDAIQROO, 2023).

- 6) **Principio de proporcionalidad:** “refieren que los datos personales que se recolectan, deben ser proporcionales según lo exija la relación con el titular, y no deberán recolectarse más datos de los que resulten adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad, de igual manera, supone el esfuerzo razonable del responsable por limitar el uso de los datos sensibles al periodo mínimo e indispensable para el cumplimiento de la finalidad para la cual sean recolectados” (Instituto Nacional de Transparencia, 2023).
- 7) **Principio de información:** “El principio de información, implica que el responsable deberá informar al titular a través del aviso de privacidad la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto” (IDAIQROO, 2023).
- 8) **Principio de responsabilidad:** “Los responsables del tratamiento de tus datos personales no solo deben tomar las medidas necesarias para cumplir con los principios y obligaciones antes señaladas, sino que además es deseable que realicen un esfuerzo adicional para observar las mejores prácticas y estándares en la protección de datos personales, y para que rindan cuentas con relación al uso y cuidado de la información personal que esté en su posesión” (Instituto Nacional de Transparencia, 2023).

En resumen, los principios mencionados previamente definen la responsabilidad asociada con el manejo de datos personales para asegurar la adecuada protección de la privacidad e intimidad de aquellos que proporcionan sus datos. Además, estos principios resaltan la necesidad de implementar medidas de seguridad (administrativas, técnicas y físicas) para garantizar la privacidad, integridad y seguridad de los datos personales. Se establecen sanciones por parte del Estado en caso de incumplimiento por parte del responsable de proteger los datos personales, según lo informado en el aviso de privacidad y los deberes y obligaciones derivados del tratamiento de datos personales.

4. Derecho a la privacidad e intimidad

En esta sección se examinarán los conceptos de privacidad e intimidad y su vínculo con los datos personales en los avisos de privacidad. Es importante señalar que, en la actualidad, el derecho a la intimidad personal está regulado en el sistema constitucional mexicano; sin embargo, dicha regulación es bastante general y poco precisa, como se puede observar en los artículos 6, 7 y 16 de la Constitución Federal del estado mexicano.

El artículo 16 de la CPEUM establece que, para que un individuo pueda ser perturbado en su vida privada, es decir, en su derecho a la intimidad, se requiere necesariamente una orden emitida por una autoridad autorizada por la ley. Por lo tanto, dicho artículo se aplica únicamente a las autoridades judiciales o administrativas, excluyendo a los particulares, como los medios de comunicación, que con frecuencia violan la privacidad de las personas al divulgar información que solo concierne al individuo en cuestión.

Es notable mencionar que la Constitución mexicana no menciona la intimidad como un derecho. La palabra intimidad, de acuerdo con el diccionario de la Real Academia Española, se refiere a la “zona espiritual, íntima y reservada de una persona o de un grupo, especialmente de una familia” (RAE, 2023).

Diversos autores, como Ernesto Villanueva y Vanessa Díaz, se han dado a la tarea de diferenciar entre privacidad e intimidad, y estipulan que:

La intimidad es el derecho a no ser conocidos, en ciertos aspectos por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos. En ese mismo sentido, anidan otras cuestiones que vinculan como derechos personalísimos, tales como el honor, la imagen, la dignidad el perfil frente al público o la opinión personal que de uno se tiene, etc. (2015, p. 25).

Así mismo, Guzmán García refiere que “el derecho a la intimidad se puede caracterizar por el contenido eminente negativo para salvaguardar aquel conocimiento ajeno, en la cual lleva implícita una parte de nuestra vida personal y familiar; en pocas palabras, aquella información personal que deseamos tener en el lado más reservado o secreto de nuestra vida” (2013, p. 90).

Néstor Torres reflexiona que “la intimidad es el espacio exclusivo que todas las personas sean personajes públicos o personas comunes tienen derecho a gozar sin la injerencia de los demás” (2009, p. 120). Es importante mencionar que la intimidad es un derecho innato, “el cual surge cuando nacemos y comenzamos a realizar nuestras primeras actividades personales en la vida, esas actividades es la intimidad que representa a cada una de las personas” (Arenas, 1998, p. 189).

En este sentido, es relevante destacar que la intimidad representa un derecho que faculta a los individuos a desenvolverse sin restricciones en su ámbito personal, manteniendo el derecho exclusivo de mantener en privado sus pensamientos, creencias religiosas, preferencias, inclinaciones políticas, entre otros aspectos. Estas cuestiones solo pueden ser compartidas a discreción de cada individuo, ya sea en contextos familiares o íntimos, con el propósito de evitar que terceros adquieran conocimiento sobre asuntos que podrían dar lugar a la animosidad o la discriminación hacia la persona.

La intimidad, que constituye la esfera más privada de cada individuo, es el espacio donde se encuentran todos los datos sensibles, es decir, aquella información que no es imprescindible para el desarrollo social y que solo puede ser revelada por el titular a su discreción, ya sea en un entorno familiar o con amigos de confianza.

El reconocimiento en la LFPDPPP del derecho a la intimidad en nuestro sistema legal mexicano, es un avance en la materia de protección y salvaguarda de los derechos humanos; por lo que, “hoy en día se cuenta con mecanismos de protección idóneos y suficientes que garantizan la protección real (material) y no solo virtual que proporcionan las leyes” (Lozano Vega, 2013, p. 57).

5. Aviso de privacidad: tipos

El aviso de privacidad se encuentra definido en el artículo 3, fracción I de la LFPDPPP: “Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley” (LFPDPPP, 2010). En similares términos, se encuentra descrito en el artículo 3, fracción II de la LGPDPPSO, que dispone: “Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos” (LFPDPPP, 2010).

El artículo 16 de la LFPDPPP, establece los requisitos que deben contener el aviso de privacidad, disponiendo lo siguiente:

Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:

- I. La identidad y domicilio del responsable que los recaba;
- II. Las finalidades del tratamiento de datos;
- III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
- V. En su caso, las transferencias de datos que se efectúen, y
- VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.
- VII. En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos (LFPDPPP, 2010).

Asimismo, en la citada Ley se advierte la forma en la cual debe ponerse a disposición de los titulares del derecho a la protección de datos, señalando lo siguiente:

Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

- I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y
- II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad (LFPDPPP, 2010).

En similares términos, la LGPDPPSO, en el artículo 27, señala los requisitos que deben de cumplir los avisos de privacidad, narrando lo siguiente:

Artículo 27. El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información:

- I. La denominación del responsable;
- II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
- I. III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y b) Las finalidades de estas transferencias;
- III. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y
- IV. El sitio donde se podrá consultar el aviso de privacidad integral (LGPDPPSO, 2017).

Además de los requisitos citados anteriormente, la Ley señala requisitos adicionales que se deben de cumplir:

Artículo 28. El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información:

- I. El domicilio del responsable;
- II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
- V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- VI. El domicilio de la Unidad de Transparencia, y
- VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad (LGPDPPSO, 2017).

La LGPDPPSO, señala tres tipos de avisos de privacidad, los cuales cuentan con características específicas:

- 1) El aviso de privacidad integral - en este tipo de aviso el usuario cuenta con toda la información concerniente a las finalidades de la obtención de los datos, su medida de seguridad de los citados datos y, en su caso, procedimientos para ejercer sus derechos ARCO, entre otras características;
- 2) El aviso de privacidad simplificado - este tipo de aviso es reducido de pocas líneas (una especie de síntesis); sin embargo, redirecciona al aviso de privacidad integral;
- 3) El aviso de privacidad corto - este aviso por lo regular se da a conocer a los usuarios, a través de mensajes de textos en dispositivos móviles, mensajes de audio, entre otros; asimismo, también suele redireccionar al aviso de privacidad integral.

El aviso de privacidad juega un papel fundamental en el principio de información, ya que es el instrumento a través del cual el responsable de los datos personales proporciona al titular de dichos datos toda la información requerida por la ley. Esto es esencial para permitir que el titular ejerza su derecho a decidir cómo se utilizan sus datos personales.

El principal objetivo del aviso de privacidad es definir y delimitar el alcance, términos y condiciones del manejo de los datos personales. Esto se hace para que el titular esté capacitado para tomar decisiones informadas sobre sus datos personales y pueda mantener el control y la disposición de la información que le pertenece.

5.1. Aviso de privacidad: videovigilancia

El consentimiento representa un principio fundamental en la protección de datos personales. Es la expresión de la voluntad libre, específica e informada del titular de dichos datos, mediante la cual autoriza su tratamiento por parte de los responsables correspondientes. Este principio requiere que el titular esté debidamente informado, por lo que antes de obtener su consentimiento y de llevar a cabo cualquier tratamiento de sus datos personales, es crucial que el titular tenga conocimiento del aviso de privacidad.

Dependiendo del tipo de datos personales involucrados, el consentimiento puede ser tácito o expreso (en el caso de datos personales no sensibles), o expreso y por escrito (para datos personales sensibles), y se adquiere conforme a lo estipulado en el artículo 21 de la LGPDPPSO: tácito, expreso y por escrito.

En aquellos casos en los que no se puedan recabar datos personales de índole sensible, se ha recomendado que así se debe estipular en el aviso de privacidad.

El INAI ha recomendado que la presentación de un aviso de privacidad, cuando se realice dentro de espacios privados como un domicilio particular, se deberá informar a las personas que están siendo captadas por el sistema de video (Soto Galindo, 2023).

En España, la Agencia Española de Protección de Datos (AEPD) es la autoridad encargada de la protección de datos, quien ha recomendado que: “se realice un tratamiento de imágenes con fines de seguridad a través de los diversos sistemas existentes de captación, debe valorarse en primer lugar la legitimación para utilizar dichos sistemas de captación, así como los principios de limitación de la finalidad y minimización de datos (AEPD, 2018).

Asimismo, Soto Galindo refiere que “el INAI ha distinguido dos tipos de videovigilancia: en tiempo real, sin grabaciones de por medio, y la que guarda (graba) las imágenes en dispositivos de almacenamiento digital o análogo” (Soto Galindo, 2023).

El tratamiento de datos personales de personas que los hagan identificables constituye un dato personal y el tratamiento de sus datos personales puede conllevar a visualizar mediante los dispositivos de videovigilancia a cualquier actividad que realicen, mismas que podrán ser almacenadas, transferidas, consultada, etc. (INAI, 2016).

Diversos estudiosos en materia de transparencia y protección de datos personales han referido que, cuando se emplea adecuadamente, la videovigilancia se convierte en uno de los recursos más utilizados para garantizar la seguridad de individuos, empresas y otros entornos. Por tanto, al implementar la videovigilancia en lugares públicos y privados, es imperativo que uno de sus principales objetivos sea salvaguardar el respeto a la privacidad, el honor y la imagen personal de las personas. Sin embargo, es importante tener en cuenta que la videovigilancia puede ser intrusiva, ya que tiene el

potencial de identificar patrones de comportamiento y otros aspectos de la vida privada de las personas.

Es crucial destacar que el responsable del manejo de datos personales en sistemas de videovigilancia es la empresa o individuo que contrata a otro –el encargado– para instalar y operar dichos sistemas, siguiendo sus directrices. Según la LFPDPPP, el responsable es la persona física o moral de naturaleza privada que toma decisiones sobre el tratamiento de los datos personales.

6. Caso relevante sobre aviso de privacidad y videovigilancia: Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero 2018, asuntos núms. 1874/13 y 8567/13 (Asunto López Ribalta y otros contra España)

Es importante destacar que una sentencia de particular relevancia en el ámbito de la videovigilancia y la protección de datos personales en los avisos de privacidad, especialmente cuando se instalan cámaras de vigilancia en el entorno laboral, es la emitida por el Tribunal Europeo de Derechos Humanos el 9 de enero de 2018 (TEDH, 2018). El caso refiere sobre un negocio de supermercados, en el cual se sospechaba que existían discrepancias entre las ventas y lo que existía en el inventario. Por lo tanto, la empresa se vio obligada a instalar cámaras visibles, notificando previamente tanto a los empleados como al Comité de empresa. No obstante, la puesta en marcha y funcionamiento de dichas cámaras no fue comunicado ni a los trabajadores ni al Comité.

Es importante destacar que, en diversas sentencias emitidas por el Tribunal Constitucional Español, en casos similares se había venido adoptando la intromisión justificada de cámaras ocultas; sin embargo, el Tribunal de Estrasburgo, órgano judicial, tras un pormenorizado análisis y estudio de los hechos y las circunstancias concurrentes, manifestó su discrepancia:

Este Tribunal no puede compartir la visión de los tribunales nacionales sobre la proporcionalidad de las medidas adoptadas por el empleador [...]. La videovigilancia llevada a cabo por el empleador, teniendo lugar durante un tiempo prolongado, no cumple con las exigencias del art. 5 –de la entonces vigente LOPD–, y en particular con la obligación de informar sobre todo lo concerniente a la existencia y particulares características del sistema de recogida de datos personales’ (Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero 2018, núms. 1874/13 y 8567/13 (Asunto López Ribalta y otros contra España)).

Por consiguiente, es obligatorio que los tribunales nacionales fundamenten sus decisiones conforme a los criterios establecidos por el Tribunal de Estrasburgo en materia de protección de datos personales, especialmente cuando se trate de videovigilancia fija o permanente.

Conclusiones

En la actualidad, en el sistema jurídico del Estado mexicano no existe una ley de carácter general o federal que regule la instalación y el uso de los sistemas de videovigilancia, y con ello se asegure y garantice que la información que es generada por la implementación e instalación de equipos y sistemas de videovigilancia se deberá tratar respetando los principios de: confidencialidad, integridad, proporcionalidad, idoneidad y seguridad (Soto Galindo, 2023).

Considerando lo expuesto, con el fin de salvaguardar y garantizar el derecho a la privacidad e intimidad, se sugiere la implementación de un modelo de aviso de privacidad tanto en el ámbito público como privado. Este aviso debería ubicarse en un lugar visible y redactarse en un lenguaje claro y comprensible para todos, especialmente en las áreas donde se lleve a cabo la videovigilancia, con el propósito de garantizar la seguridad del área vigilada.

Al día de hoy, la videovigilancia se ha vuelto un fenómeno donde se enfrentan o colisionan varios derechos debido al tratamiento de información de datos personales que pueden identificar o se vuelven identificables a una o varias personas, e inclusive a los sectores de la sociedad más vulnerables, en este caso niñas, niños, adolescentes, personas con discapacidad; por un lado, el derecho a la seguridad y, por el otro, los derechos de privacidad e intimidad, libertad, libre asociación y manifestación de las ideas y la protección de datos personales.

El reconocimiento del derecho a la privacidad y la intimidad, así como la protección de datos personales a nivel constitucional y legal, busca resolver los problemas de violación de la privacidad e intimidad. Sin embargo, las ambigüedades y lagunas presentes en las leyes LFPDPPP y LGPDPSO respecto al consentimiento y uso de datos personales, junto con la falta de aplicación del aviso de privacidad de la videovigilancia en espacios públicos y privados, comprometen la eficacia de estas leyes como herramientas para proteger el derecho a la autodeterminación informativa.

Lo anterior se sostiene de la lectura de los artículos 18 de la LFPDPPP y 21 de la LGPDPSO. El análisis de estos artículos revela que, aunque los datos se recopilen con fines históricos, estadísticos o científicos, a menudo terminan en manos de múltiples personas cuya intención y forma de tratamiento de estos datos son desconocidas. Esto incluye actividades como encuestas de opinión y sondeos. Esta situación representa un riesgo para la intimidad e integridad de las personas, ya que existe la posibilidad de un uso indebido de los datos.

La excepción a los principios que regulan el tratamiento de datos en relación con la seguridad nacional, así como las disposiciones de orden público (seguridad y salud públicas o la protección de los derechos de terceros, según lo estipulado en el párrafo segundo del artículo 16 constitucional), no es clara. Esto se debe a la falta de un procedimiento reglamentado para el uso de los datos personales, lo que genera incertidum-

bre. En consecuencia, cualquier modificación en el aviso de privacidad puede ocurrir sin garantizar el derecho de audiencia a las partes involucradas, lo que podría resultar en una vulneración directa de los derechos de privacidad e intimidad en algunos casos.

Una de las observaciones que también se contemplan en los artículos 18 de la LFPDPPP y 21 LGPDPPSO, es en el entendido de la puesta a disposición del aviso de privacidad, en este caso de la videovigilancia. Los referidos ordenamientos señalan que el citado aviso se deba encontrar alojado en la página electrónica (o en la página web) de la institución pública y privada; es pertinente proponer que los referidos avisos deberán prever mecanismos de fácil lectura y lenguaje inclusivo y, sobre todo, fácil localización de los usuarios.

En conclusión, es crucial destacar que el empleo de sistemas de vigilancia, tanto en el sector público como en el privado, seguirá incrementándose con el tiempo, con el objetivo de proporcionar seguridad y tranquilidad a las personas que habitan en un determinado espacio físico. Por ello, las autoridades encargadas de resolver los conflictos relacionados con la protección de datos personales deberán aplicar los principios de ponderación y proporcionalidad, evaluando su idoneidad y necesidad, para asegurar la protección de los derechos humanos de las personas afectadas por estos conflictos de derechos.

Referencias bibliográficas

- Aceves Bernal, F. A. (enero de 2013). Tesis Maestría: Sistema de videovigilancia para la Ciudad de México. IPN. Instituto Politécnico Nacional.
- AEPD. (2018). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. Obtenido de <https://www.aepd.es/media/guias/guia-videovigilancia.pdf>
- Araujo Carranza, E. (2009). *El derecho a la información y la protección de datos personales en México*. Porrúa.
- Arenas, A. L. (1998). *Derecho a la intimidad*. Valencia: Tirant Lo Blanch.
- Aveleyra, A. M. (2003). El Derecho de Acceso a la Información Pública vs. el Derecho de Libertad Informática. *Jurídica-Anuario, Revista de la Universidad Iberoamericana*, 403-443.
- CDMX, G. d. (10 de agosto de 2022). *Crece el número de cámaras del C5*. Obtenido de <https://gobierno.cdmx.gob.mx/noticias/crece-el-numero-de-camaras-del-c5/>
- De Marcos Davara F., I. (noviembre de 2019). *Diccionario de Protección de Datos Personales. Conceptos fundamentales*. Recuperado el 17 de mayo de 2023, de <https://inai.janium.net/janium/Portadas/3487.pdf>
- Díaz, E. V. (2015). *Derecho de las Nuevas Tecnologías*. México: Oxford University Press.
- García González, A. (2007). *La protección de datos personales: derecho fundamental del siglo XXI, un estudio comparado* (septiembre-diciembre ed.). Instituto de Investigaciones Jurídicas UNAM.

- González, C. G. (2019). Control empresarial de la actividad laboral mediante la videovigilancia y colisión de los derechos fundamentales del trabajador. *Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Revista Aranzadi Digital*, 14.
- Guzman García, María de los A., (2013). *El derecho fundamental a la protección de datos personales en México. Análisis desde la influencia del ordenamiento jurídico español*. Madrid: Universidad Complutense de Madrid.
- GPCD. (2010). *Dictamen de la Comisión de Gobernación, con proyecto de decreto por el que se expide la LFPDPP* (Vols. número 2984-IV). Cámara de Diputados.
- IDAIQROO. (30 de abril de 2023). *Instituto de Transparencia y Acceso a la Información de Quintana Roo*. Obtenido de <https://transparencia.congresoqroo.gob.mx/principios-proteccion-datos/>
- INAI. (16 de agosto de 2016). *Modelo de aviso de privacidad corto para video-vigilancia*. Recuperado el 30 de abril de 2023, de Instituto Nacional de Transparencia, Acceso a la Información y a la Protección de Datos Personales: <https://home.inai.org.mx/wp-content/documentos/ABCAvisoPrivacidad/Modelo%20de%20aviso%20de%20privacidad%20corto%20para%20V-V.pdf>
- INAI. (2016). *Modelo de aviso de privacidad corto para V-V. Ciudad de México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Obtenido de <http://inicio.inai.org.mx/AvisoPrivacidad/Modelo%20de%20aviso%20de%20privacidad%20corto%20para%20V-V.pdf>
- INAI. (2019). *Diccionario de Datos Personales* (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ed.).
- INAI. (3 de mayo de 2023). *El ABC del aviso de privacidad*. Obtenido de http://abcavisosprivacidad.ifai.org.mx/#seccion1_02P
- INEGI (Ed.). (2018). *Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2017*. Instituto Nacional de Estadística y Geografía.
- Instituto Nacional de Transparencia, A. a. (2023). *Guía para Titulares de los Datos Personales. Principios rectores de la Protección de Datos Personales* (Vol. 2). México: INAI.
- Ley del Estatuto de los Trabajadores, Real Decreto Legislativo 2/2015 (15 de octubre de 2015).
- Lozano Vega, S. (2013). *El "Aviso de Privacidad" como un mecanismo ineficaz de protección del derecho a la autodeterminación informativa* (Vol. 12). Tribunal Federal de Justicia Fiscal y Administrativa, Revista de Investigación Jurídica-Técnico Profesional, Praxis de la JFyA.
- Lucas Durán, M. (1997). *El acceso a los datos en poder de la administración tributaria*. Aranzadi.
- Néstor Torres, Franco (2009). *Libertad de expresión y derecho de autor. Guía legal para periodistas*. Bogotá, Colombia: Universidad del Rosario.
- GPCD. (2010). *Dictamen de la Comisión de Gobernación, con proyecto de decreto por el que se expide la LFPDPP* (Vols. número 2984-IV). Cámara de Diputados.

- IDAIQROO. (30 de abril de 2023). *Instituto de Transparencia y Acceso a la Información de Quintana Roo*. Obtenido de <https://transparencia.congresoqroo.gob.mx/principios-proteccion-datos/>
- INAI. (16 de agosto de 2016). *Modelo de aviso de privacidad corto para video-vigilancia*. Recuperado el 30 de abril de 2023, de Instituto Nacional de Transparencia, Acceso a la Información y a la Protección de Datos Personales: <https://home.inai.org.mx/wp-content/documentos/ABCAvisoPrivacidad/Modelo%20de%20aviso%20de%20privacidad%20corto%20para%20V-V.pdf>
- INAI. (2016). *Modelo de aviso de privacidad corto para V-V. Ciudad de México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Obtenido de <http://inicio.inai.org.mx/AvisoPrivacidad/Modelo%20de%20aviso%20de%20privacidad%20corto%20para%20V-V.pdf>
- INAI. (2019). *Diccionario de Datos Personales* (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ed.).
- INAI. (3 de mayo de 2023). *El ABC del aviso de privacidad*. Obtenido de http://abcavisosprivacidad.ifai.org.mx/#seccion1_02P
- INEGI (Ed.). (2018). *Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2017*. Instituto Nacional de Estadística y Geografía.
- Instituto Nacional de Transparencia, A. a. (2023). *Guía para Titulares de los Datos Personales. Principios rectores de la Protección de Datos Personales* (Vol. 2). México: INAI.
- Ley del Estatuto de los Trabajadores, Real Decreto Legislativo 2/2015 (15 de octubre de 2015).
- Lozano Vega, S. (2013). *El “Aviso de Privacidad” como un mecanismo ineficaz de protección del derecho a la autodeterminación informativa* (Vol. 12). Tribunal Federal de Justicia Fiscal y Administrativa, Revista de Investigación Jurídica-Técnico Profesional, Praxis de la JFyA.
- Lucas Durán, M. (1997). *El acceso a los datos en poder de la administración tributaria*. Aranzadi.
- Néstor Torres, Franco (2009). *Libertad de expresión y derecho de autor. Guía legal para periodistas*. Bogotá, Colombia: Universidad del Rosario.
- RAE. (2023). *Diccionario de la Real Academia de la Lengua Española*. Madrid: RAE.
- Ramírez, M. S. (abril de 2021). La protección y el tratamiento de datos personales. El derecho humano a la privacidad y a la intimidad. *Mirada Legistativa No. 201*(Instituto Belisario Domínguez/Senado de la República, Ciudad de México.), 1-20.
- SCJN. (2018). *Tribunales Colegiados de Circuito. Décima Época. Gaceta de Semanario Judicial de la Federación*. (Vol. Tomo VI).
- Security. (s.f.). Recuperado el 17 de May de 2023, de Antecedentes de la video vigilancia e importancia: <https://www.securitycom.mx/blog/antecedentes-de-la-video-vigilancia-e-importancia>
- Soto Galindo, José (20 de enero de 2023). ¿Qué es la videovigilancia? Recuperado el 05 de enero 2023, de *economicon*: <https://economicon.mx/blog/que-es-la-videovigilancia/>
- TEDH. (2018). *Asuntos núms. 1874/13 y 8567/13 (Asunto López Ribalta y otros contra España)*. Estraburgo, Francia. Recuperado el 2018 de enero de 9

El cuidado de la obra estuvo a cargo de Montiel & Soriano Editores
S.A. de C. V. El tamaño del archivo es de 8.8 MB

La obra que el autor tiene en sus manos ofrece una exploración integral de los desafíos y oportunidades asociados con la implementación de dispositivos de vigilancia electrónica en México. A través de trece capítulos detallados, el libro aborda la percepción de inseguridad en áreas vigiladas, el marco jurídico que regula estos dispositivos, y la interacción entre la videovigilancia y los derechos humanos. Este recurso es esencial para académicos, profesionales del derecho, y tomadores de decisiones interesados en comprender las implicaciones legales, sociales y éticas de la vigilancia electrónica.

Desde la normatividad de la videovigilancia y su impacto en la privacidad, hasta los retos de implementar políticas públicas que equilibren seguridad y derechos humanos, este libro presenta un análisis profundo y multifacético. Capítulos dedicados a la videovigilancia en contextos específicos, como la protección de los derechos de la niñez y el uso de inteligencia artificial, proporcionan una visión amplia de las implicaciones de estos sistemas en la sociedad mexicana. Además, estudios de caso como el de Debanhi Escobar y análisis de políticas en el estado de Veracruz y la ciudad de Puebla, ofrecen perspectivas prácticas y actuales sobre los retos que enfrenta la seguridad pública en México.

