VIDEOVIGILANCIA E INTELIGENCIA ARTIFICIAL: ENTRE LA UTOPÍA Y LA DISTOPÍA

Álvaro Vizcaíno Zamora*

* Doctor en Derecho por la Universidad Panamericana. Investigador invitado del Instituto Nacional de Ciencias Penales. Ex Secretario Ejecutivo del Sistema Nacional de Seguridad Pública 2015-2018 y Socio-Fundador de www.esjus.com.mx

PALABRAS CLAVE *KEYWORDS*

Seguridad pública	*Public security*
Videovigilancia	*Video surveillance*
Inteligencia artificial	*Artificial intelligence*
Prevención del delito	*Crime prevention*
Derechos humanos	*Human rights*

Resumen. El autor presenta la evolución de los sistemas de videovigilancia en México y ofrece un análisis comparado con algunos países de Europa y Asia. Analiza el escaso marco legal y narra la construcción de políticas públicas. Después, analiza el uso de la inteligencia artificial en apoyo a los sistemas de videovigilancia que motivan generar principios éticos emergentes para una revolución tecnológica en curso. Luego comenta la paradoja de la videovigilancia: vivimos en la sociedad más videovigilada de la historia y ello no se traduce en una reducción de la incidencia delictiva o la percepción de inseguridad.

Abstract. The author presents the evolution of video surveillance systems in Mexico and offers an analysis compared to some countries in Europe and Asia. He analyzes the scarce legal framework and narrates the construction of public policies. Next, he discusses the use of artificial intelligence in support of video surveillance systems that motivate the generation of emerging ethical principles for an ongoing technological revolution. He then comments on the paradox of video surveillance: we live in the most video-monitored society in history, and this does not translate into a reduction in crime incidence or the perception of insecurity.

Fecha de recepción: 20 de diciembre de 2020
Fecha de aceptación: 23 de diciembre de 2020

> Constituía un terrible peligro pensar mientras se estaba en un sitio público o al alcance de la telepantalla. El detalle más pequeño podía traicionarle a uno. Un tic nervioso, una inconsciente mirada de inquietud, la costumbre de hablar con uno mismo entre dientes, todo lo que revelase la necesidad de ocultar algo.
>
> George Orwell, *1984*

INACIPE • Revista Mexicana de Ciencias Penales • Núm. 14, mayo-agosto 2021

SUMARIO:

Abreviaturas:
Cámara de videovigilancia: CVV;
Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano de la Ciudad de México: C5CDMX;
Foro Europeo para la Seguridad Urbana: EFUS;
Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de videovigilancia para la seguridad pública: NTSVV;
Punto de monitoreo inteligente: PMI;
Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública: SESNSP;
Sistemas Tecnológicos de Videovigilancia: STV

I. INTRODUCCIÓN

"You are on a video camera over 200 times a day. Are you dressed for it?" ("Estás en una cámara de video más de 200 veces al día. ¿Estás vestido para eso?") En torno a esta pregunta giró una campaña publicitaria de la compañía de ropa Kenneth Cole NY.[1] El comercial para televisión muestra, a través de

[1] Un video de esta campaña puede verse en https://youtu.be/OHxpgcZt3TA

imágenes de cámaras de videovigilancia (CVV) públicas y privadas, a un hombre y una mujer que caminan por las calles de Nueva York para encontrarse y, cuando lo hacen, se esconden furtivamente bajo una CVV para besarse sin ser grabados.

¿Cuántas veces somos videograbados al día? Depende de varios factores. El primero se vincula con el desplazamiento de las personas. Hoy en día, la movilidad urbana se puede medir a partir del análisis del *big data* y las redes sociales (Osorio Arjona y García Palomares, 2017). El segundo factor depende del número de CVV frente a las cuales pasa una persona en un traslado ordinario. El autor de este texto hizo un simple ejercicio práctico, en una ruta cotidiana: ir a caminar al parque público ubicado a 150 metros de distancia del domicilio. El parque tiene un perímetro de 500 metros. Caminar hacia el parque y darle una vuelta completa implica un trayecto de 650 metros. En esa ruta, hay nueve CVV públicas, más doce CVV privadas, para un total de 21 CVV, a las que hay que sumar tres botones de alerta o pánico públicos. Cada lector podría hacer un ejercicio similar. Los datos cambiarán según las condiciones de la infraestructura urbana para advertir que, en la Ciudad de México, en algunos casos, la densidad de cámaras por kilómetro cuadrado es muy alta y, en otros, francamente insuficiente.

¿Cuántas CVV hay en México? En 2018 se reportaron 53,949 CVV en el país (43 por cada 100 mil habitantes), además de 71,794 botones de pánico (57.3 por cada mil habitantes) (INEGI, 2019). Cabe destacar que el Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales ofrece información aportada por las entidades federativas, no por los municipios. Habría que sumar las CVV administradas por gobiernos municipales y restar aquellas que no sirven por falta de mantenimiento. Además, el Censo 2020, que reporta datos de 2019, no ofrece información sobre videovigilancia, por lo que la información oficial más reciente es de 2018.

Conforme al Instituto Nacional de Estadística, Geografía e Informática (INEGI, 2019), 39% de las CVV se ubica en hogares, 35.2% en establecimientos o negocios, 19.8% en la vía pública, 4.9% en escuelas y 1.1% en otros lugares.

¿Cuántas CVV públicas existen en la Ciudad de México? Conforme al Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano de la Ciudad de México (C5CDMX), el estado, en 2020, de los Sistemas Tecnológicos de Videovigilancia (STV), es de 15,310 CVV

instaladas, de las cuales funcionan 14,554 y 422 presentan fallas (Gobierno de la Ciudad de México, 2020).

El mayor número de CVV instaladas se encuentra en la alcaldía Iztapalapa, con 2,293; en segundo lugar, está la alcaldía Gustavo A. Madero, con 2,027; en tercero, la alcaldía Cuauhtémoc, con 1,640; en cuarto, la alcaldía Venustiano Carranza, con 1,070 y, en quinto, la alcaldía Miguel Hidalgo, con 1,069. Además, el C5CDMX cuenta con CVV que reconocen placas vehiculares; sin embargo, el C5CDMX no especifica cuántas CVV disponen de esta tecnología (Gobierno de la Ciudad de México, 2020). Por otra parte, hay 6,500 CVV instaladas en el Sistema de Transporte Colectivo (Metro) de la Ciudad de México (Corona, 2017).

Al comparar los datos del C5CDMX (Gobierno de la Ciudad de México, 2020) con los del censo mencionado (INEGI, 2019), sin contar las CVV del Metro, la Ciudad de México cuenta con 28% de las CVV del país.

El C5CDMX reconoce que, para dar cobertura total a la Ciudad de México, se requerirían 120 mil CVV (Corona, 2017). En consecuencia, en 2020, la Ciudad de México tiene 12.5% de las cámaras que debería tener.

¿Cuántas CVV hay en el Estado de México? La entidad federativa más poblada del país cuenta con "9,052 cámaras de videovigilancia urbana distribuidas en 2,263 puntos de monitoreo inteligente (PMI's) y se cuenta con 7,124 altavoces para anuncio público y difusión de la alerta sísmica, 23 sistemas de hangar automático para dron; 31 sistemas de red inalámbrica para trasmisión de video, 158 kilómetros de red de transporte de datos de fibra óptica y 1,250 sistemas de videovigilancia para transporte público" (Gobierno del Estado de México, 2020: 254). Al comparar con los datos de INEGI (INEGI, 2019), el Estado de México tiene el 17% de las CVV del país.

Un *punto de monitoreo inteligente* (PMI) es la base del sistema de videovigilancia.

> Es el mecanismo a través del cual se adquieren datos e imágenes que permiten realizar las acciones correspondientes ante cualquier eventualidad, a partir del monitoreo en el centro de control. De forma general, un PMI se compone de: Poste y/o soporte, canalización interior para cableado eléctrico y red de datos, sistema de puesta a tierra física y de protección ante descargas atmosféricas, gabinete de equipos (caja NEMA), regulador de voltaje, supresor de sobretensiones transitorias, equipo de red, distribución eléctrica en gabinete de equipos, acometida eléctrica, soporte y cámara(s), antena y trasmisor y pararrayos (Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública [SESNSP], 2016: 61).

En pocas palabras, es todo lo que hay en un poste donde están instaladas una o varias cámaras.

¿Cuántas CVV hay en otros países? Se estima que, en Reino Unido, en 2016, había 5 millones de CVV, de las cuales medio millón se ubican en Londres (Fundación Empresa, Seguridad y Sociedad [ESYS], 2016: 86), para una población de 66 millones de habitantes. En China, en 2018, se estimaban más de 170 millones de CVV, para una población estimada en 1,395 millones de habitantes (Cámara de Valencia, 2020). En Francia, en 2007, había 340,000 mil CVV, para una población de 64 millones de habitantes. Ese mismo año, la ministra del interior anunció que se triplicaría en los siguientes dos años el número de cámaras (*El País*, 2007). En 2019, se reportan 1.65 millones de CVV (Chaverra, 2019).

Estados Unidos contaba con 50 millones de CVV en 2019, para una población de 328.2 millones de habitantes. También en 2019, Alemania contaba con 5.2 millones de CVV y una población de 83.1 millones de habitantes, mientras que Japón contaba, en 2019, con 5 millones de CVV para una población de 126.1 millones de habitantes (Chaverra, 2019)

Los anteriores datos permiten realizar una comparación en tasas de videocámaras por cada mil habitantes:

Tabla 1. Tasa de cámaras de videovigilancia por cada mil habitantes

País	Tasa por cada mil habitantes
Estados Unidos	152.3
China	121.8
Reino Unido	75.7
Alemania	62.5
Japón	39.6
Francia	25.7
México	0.41

Fuente: Elaboración propia con datos obtenidos de Fundación Empresa, Seguridad y Sociedad (ESYS, 2016), Cámara de Valencia (2020), *El País* (2007) y Chaverra (2019). Los datos de Reino Unido corresponden al año 2016, los de México y China a 2018, y los de Estados Unidos, Alemania, Japón y Francia a 2019.

La industria de la videovigilancia está en crecimiento. Según el reporte del IMS Research (2014), el mercado de la videovigilancia en América Latina mantuvo una tasa de crecimiento del 40.5% desde 2008 hasta 2013

(Xtreme Secure, 2019). Aunque el número de CVV instaladas en México presente un crecimiento exponencial, se encuentra lejos de contar con la dimensión los STV de países europeos y asiáticos.

II. VIDEOVIGILANCIA Y DERECHOS HUMANOS. EL MARCO LEGAL

La vigilancia por video puede perturbar las libertades individuales. En el otro extremo, la evolución tecnológica puede abrir muchas nuevas posibilidades a la seguridad. Se requiere equilibrio, que debe basarse en tres pilares ético-jurídicos: el derecho a la privacidad, la protección de datos personales y el libre tránsito y no discriminación de las personas (SESNSP, 2016: 2).

A) EL DERECHO A LA PRIVACIDAD

Debe existir equilibrio entre los espacios públicos seguros y el derecho a la intimidad y privacidad de las personas. Las leyes deben regular la videovigilancia en espacios públicos y en lugares privados con acceso al público, y prohibirla en espacios privados. La Declaración Universal de los Derechos Humanos establece, en el artículo 12, que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Por su parte, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento". Si bien no señala de manera expresa la protección a la vida privada o la intimidad, es evidente que los sistemas de videovigilancia pueden eventualmente implicar una injerencia arbitraria en la vida y el domicilio de las personas.

B) LA PROTECCIÓN DE DATOS PERSONALES

Las leyes de videovigilancia deben proteger a los ciudadanos frente a la posibilidad de que sus datos, voz o imagen queden expuestos. Desde 2007, la

protección de datos personales se encuentra tutelada por la Constitución. El apartado A, segundo párrafo, del artículo 6o., 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". Además, el artículo 16 señala que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos".

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México establece, en su artículo 72, como una excepción, la obtención de datos para fines policiales relacionados con la prevención de los delitos o la seguridad pública, que pueden ser recabados sin consentimiento de las personas. Las autoridades deben establecer procedimientos para que los ciudadanos puedan ejercer los derechos de acceso, rectificación, cancelación u oposición (ARCO), de tal manera que toda persona que aparezca en una grabación pueda tener acceso a esta y solicitar su cancelación.

C) EL LIBRE TRÁNSITO Y LA NO DISCRIMINACIÓN DE LAS PERSONAS

En ocasiones, los operadores de los STV realizan el video-seguimiento de personas "sospechosas" o "inusuales", con base en prejuicios tales como el color de piel, la raza o la forma de vestir. La Constitución federal protege el derecho de libre tránsito en su artículo 11. Al mismo tiempo, el artículo 1o., último párrafo, prohíbe toda discriminación motivada por "origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana".

Un estudio realizado en Interlomas, Huixquilucan, Estado de México, mostró que los operadores de los STV seguían a los trabajadores de la construcción, al entrar y salir de sus trabajos:

> El monitoreo que se hace sobre estos grupos de trabajadores se justifica, en voz de sus operadores, porque son personas que potencialmente pueden cometer algún tipo de ilícito, sobre todo introducirse en algún edificio para robar o asaltar. Para estos operadores, cualquier persona que camina por las calles de esta zona habitacional requiere de cierto monitoreo, ya que es inusual que los habitantes del lugar hagan uso de las calles para caminar (Arteaga Botello, 2016).

Otro ejemplo fue la discriminación a la comunidad LGTB+ en el centro comercial ubicado en Avenida Paseo de la Reforma 222, en la Ciudad de México:

> A los pocos días de su inauguración, los sistemas de videovigilancia funcionaron para detectar y prevenir que miembros de la comunidad lésbico-gay se besaran o abrazaran en el centro comercial del edificio. Las cámaras permitían monitorear estos comportamientos y, una vez detectados, los cuerpos de seguridad pedían a las personas que se comportaran de otra manera, y si se negaban, se les *invitaba* a salir del lugar (Arteaga Botello, 2016).

En la Universidad Nacional Autónoma de México (UNAM), en 2016, el rector Enrique Graue planteó 15 puntos específicos para mejorar la seguridad. El que más polémica causó fue instalación de STV. "Si bien un sector de los universitarios apoya esa opción, muchos otros consideran que se trata de un método invasivo" (Olivares Alonso, 2016).

D) LA CARTA PARA EL USO DEMOCRÁTICO DE LA VIGILANCIA POR VIDEO DEL FORO EUROPEO PARA LA SEGURIDAD URBANA (EFUS)

El Foro Europeo para la Seguridad Urbana (EFUS) es una red europea de 250 ciudades establecida en 1987, bajo el auspicio del Consejo de Europa. Su objetivo es procurar el respeto a los derechos humanos en la implementación de las políticas de prevención de la criminalidad, procurando que estas no impliquen la exclusión y represión de grupos vulnerables (European Forum for Urban Security, 2020). El EFUS acordó la *Carta para el uso democrático de la vigilancia por video.*

En algunos países existen regulaciones muy precisas, mientras que en otros se tiene una legislación general de protección de la vida privada y de protección de datos personales, como es el caso de México. Quienes participaron en la redacción de la Carta estiman que en algunos países será una novedad y, en otros, complementará la legislación vigente (Calfa, Sebastian y Bourgeois, 2010: 121). La carta se basa en siete principios que incluyen ejemplos para una aplicación práctica (*Ibidem*: 122-153):

> **Primero.** Legalidad. Los STV deben cumplir las leyes nacionales, estatales o locales, atendiendo a las normas aplicables a la protección de datos, la escucha de comunicaciones, la injerencia ilícita en la vida privada, la protección de la dignidad, la imagen y el domicilio. En Bélgica, Italia y España no se pueden filmar zonas privadas, como puertas y ventanas. En Reino Unido, los operadores están obligados a conocer las leyes de protección de datos.

Segundo. Necesidad. Los STV no pueden constituir un fin, sino una herramienta dentro de una estrategia de seguridad. ¿Cuál es la contribución de la videovigilancia a la resolución de un problema concreto de seguridad? El razonamiento se estructura con base en la identificación de las circunstancias, la definición de las necesidades y la necesidad de la respuesta de la videovigilancia. En Bade-Wurtemberg, Alemania, solo se puede considerar necesario un STV si estadísticamente se comprueba que una zona es criminógena.
Tercero. Proporcionalidad. La comparación entre STV suele hacerse en función del número de cámaras, lo cual no es necesariamente el mejor criterio, ya que el número de cámaras debe ser proporcional a las necesidades.
Cuarto. Transparencia. ¿Qué nivel de información debe suministrarse a los ciudadanos? En Rotterdam, cada vez que se instala una cámara, se invita a los ciudadanos a visitar el centro de control.
Quinto. Responsabilidad. El derecho de vigilancia del espacio público debe reservarse a autoridades designadas de modo restrictivo, responsables de los sistemas, que pueden merecer sanciones ante incumplimientos. Las empresas privadas y particulares que registren el espacio público deben adoptar las mismas medidas que las autoridades.
Sexto. Supervisión independiente. Vigilar a los vigilantes. En Francia existen Comités de ética en ciudades como Lyon y Havre. En Reino Unido hay programas de visitantes ciudadanos independientes a los centros de monitoreo.
Séptimo. Participación ciudadana. Toda instalación o extensión de los STV deberá considerar la participación de los ciudadanos que viven en la zona.

La Carta establece cuatro herramientas metodológicas: 1) diagnóstico previo; 2) evaluaciones periódicas; 3) formación de operadores; y 4) una autoridad de control.

E) LEGISLACIONES MEXICANAS ESPECÍFICAS

Al mes de diciembre de 2020, por orden cronológico de publicación, nueve entidades federativas y dos municipios cuentan con legislación en la materia:

- Ley que regula el uso de tecnología para la seguridad pública del Distrito Federal (publicada el 27 de octubre de 2008).
- Ley que regula la video vigilancia en el Estado de Colima (publicada el 22 de agosto de 2009).
- Reglamento de videovigilancia para el municipio de Guadalajara (publicado el 10 de junio de 2011).
- Reglamento de Video vigilancia del municipio de Durango (publicado el 14 de octubre de 2011).

- Ley que establece las bases para la video vigilancia en el Estado de Durango (publicada el 5 de julio de 2012).
- Ley que regula el uso de las tecnologías de la información y comunicación para la seguridad pública del Estado de México (publicada el 14 de mayo de 2014) y su reglamento (publicado el 30 de junio de 2015).
- Ley de Videovigilancia del Estado de Yucatán (publicada el 25 de julio de 2018).
- Ley de Videovigilancia para el Estado de Zacatecas (publicada el 22 de agosto de 2018).
- Ley de video vigilancia del Estado de Aguascalientes (publicada el 3 de septiembre de 2018).
- Ley de video vigilancia del Estado de Baja California Sur (publicada el 20 de enero de 2020).
- Ley de Videovigilancia para el Estado de Morelos (publicada el 12 de agosto de 2020).

Del análisis de esta legislación se desprenden algunos datos relevantes:

Primero. La Ciudad de México fue la primera entidad federativa en regular los STV en México. A diciembre de 2020, son 23 las entidades federativas que carecen de regulación específica en materia de videovigilancia.
Segundo. Ninguna de las legislaciones contiene disposiciones específicas sobre el uso de la inteligencia artificial en los STV.
Tercero. Las leyes comparten, en términos generales, la misma estructura: disposiciones generales y definiciones, derechos, objeto y definición de la videovigilancia, principios, disposiciones para empresas de seguridad privada y particulares, disposiciones y criterios para la instalación y retiro de cámaras, disposiciones sobre la conservación de la información, obligaciones en materia de transparencia y protección de datos, creación de registros estatales de videovigilancia y sanciones y recursos.
Cuarto. Entre los principios que establecen en términos generales las leyes, se encuentran los siguientes:

- Proporcionalidad. Evitar el uso indiscriminado e injustificado.
- Idoneidad. Utilizarla solo para los fines de la seguridad pública.
- Intervención mínima. Utilizar los STV previa ponderación de los propósitos pretendidos y las posibles afectaciones.
- Riesgo razonable. Instalar las CVV en espacios públicos o en espacios privados con acceso al público en que se considere un posible daño o afectación a la seguridad pública.
- Peligro concreto. Los STV se utilizarán para dar seguimiento específico a hechos que pongan en inminente riesgo a la seguridad pública.
- No afectación de la intimidad personal.

Quinto. Algunas leyes (Morelos y Baja California Sur) establecen la obligación a cargo de particulares de adquirir STV. Si bien las leyes locales mexicanas establecen el principio de proporcionalidad, estas y otras disposiciones parecen disponer que deben instalarse tantas CVV como sea posible.
Sexto. En Morelos, el operador de los STV adquiere el carácter de testigo sobre las imágenes que presencie. Desde el punto de vista del procedimiento penal, convendría analizar si entonces la evidencia o dato de prueba son las imágenes del video o el testimonio del operador del centro de monitoreo, o inclusive ambos.
Séptimo. No existe una ley general o federal en la materia que permitiría establecer disposiciones para homologar las normas, criterios y principios en materia de videovigilancia en México, incluyendo dispositivos en relación con el uso de la inteligencia artificial en sistemas de reconocimiento facial, identificación y seguimiento de matrículas vehiculares y el uso de vehículos no tripulados.
Octavo. Solamente dos municipios cuentan con legislación en materia de videovigilancia: Guadalajara y Durango. La seguridad pública es una atribución conferida también a los municipios, en términos del artículo 115 constitucional.

III. VIDEOVIGILANCIA COMO PARTE DE LA POLÍTICA PÚBLICA DE SEGURIDAD EN MÉXICO

Entre 2010 y 2011 me desempeñé como Secretario Ejecutivo Adjunto y, entre 2015 y 2018, como Secretario Ejecutivo del Sistema Nacional de Seguridad Pública. Pude advertir, en reuniones con los y las titulares de los poderes ejecutivos estatales y municipales, que uno de los elementos centrales de sus políticas de seguridad se basaba en establecer o fortalecer los Centros de Comando, Control, Cómputo y Comunicaciones, conocidos como C5, y en impulsar sistemas de videovigilancia. La videovigilancia se había convertido en un elemento central de la narrativa contra la inseguridad y la gestión de riesgos. Sin embargo, eran evidentes algunos problemas:

Falta de planeación estratégica

Era común escuchar frases como: "¿Para cuántas patrullas y videocámaras me alcanza?" Este problema se presenta, fundamentalmente, en el orden municipal, y no se focaliza en temas de tecnologías para la seguridad, sino en todo el ejercicio del gasto, especialmente el del subsidio (FORTASEG),[2]

[2] En 2018, 300 municipios resultaron beneficiados con el subsidio FORTASEG. Si bien representan solamente el 12% de los municipios, en ellos vive el 69% de la población, y se comete el 90% de los delitos de alto impacto, además de que cuentan con el 73% del estado de fuerza policial municipal.

que, por cierto, no fue contemplado en el Presupuesto de Egresos de la Federación para 2021. Algunas autoridades municipales, generalmente de los municipios con menor población (y menores capacidades administrativas), se presentaban al proceso de concertación de los recursos federales (que se realizaba a principios de cada año), sin una propuesta programático-presupuestal previa para etiquetar los recursos del subsidio y reflejarlo en los convenios respectivos.

Falta de diagnósticos para asignar racionalmente, con criterios de eficacia y eficiencia, recursos en materia de videovigilancia

En no pocas ocasiones, los municipios presentaban una propuesta financiera para asignar recursos federales a la adquisición de STV, basada en el dinero "que quedaba" después de atender otros temas como la adquisición de vehículos, sin un estudio que definiera cuántas cámaras requieren de acuerdo con la incidencia delictiva o la concentración poblacional. Hay diferencia entre lo que quieren y lo que necesitan.

Presión de proveedores de STV

Con frecuencia, los proveedores de STV buscan vender equipos que no corresponden con las necesidades. Por ejemplo, capacidades de almacenamiento de datos sobradas e innecesarias, o cámaras con zum potente en zonas en las cuales, por la conformación geográfica o la vegetación, es imposible usarlos. En el caso de los gobiernos estatales, se concentraban en equipar los complejos de seguridad (centros de monitoreo) con oficinas alternas, búnkeres y helipuertos para uso de los gobernadores y otros "accesorios" que encarecían el costo de los proyectos, accesorios que no eran autorizados con recursos federales.

Infiltración de la delincuencia organizada

En Acapulco, desde 2011 y durante varios años, el centro de monitoreo (C4) de las imágenes de las CVV era utilizado por operadores infiltrados por la delincuencia organizada para trasmitir los movimientos de las fuerzas federales a los delincuentes. En mayo de 2016 se anunció que el control del Centro de Monitoreo sería asumido por las fuerzas armadas (Animal Político, 2016).

A) DISEÑO, PLANEACIÓN E IMPLEMENTACIÓN DE LA POLÍTICA PÚBLICA

Era necesario impulsar una política pública que ordenara la adquisición de STV para la seguridad pública, con criterios de racionalidad y eficacia, en términos de pertinencia y de racionalidad en el uso de los recursos públicos. Por ello, en la trigésima novena sesión ordinaria del Consejo Nacional de Seguridad Pública (el 18 de diciembre de 2015), este ordenó al SESNSP (Acuerdo 08/XXXIX/15)[3] elaborar una "Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de videovigilancia pública." La Norma fue aprobada en la 40a. sesión ordinaria del Consejo Nacional de Seguridad Pública (30 de agosto de 2016) (Acuerdo 15/XL/16).[4]

En la 41a. sesión ordinaria del Consejo Nacional de Seguridad Pública (20 de diciembre de 2016), el Consejo instruyó al SESNSP (acuerdo 09/XLI/16)[5] a elaborar una Norma Técnica para homologar, a nivel nacional, características, tecnología, infraestructura y sistemas de los Centros de Control, Comando, Comunicación y Cómputo, la cual fue aprobada en la 43a. sesión ordinaria (21 de diciembre de 2017) (Acuerdo 10/XLIII/17),[6] instruyéndose convertirla en una Norma Oficial Mexicana.

La Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de videovigilancia para la seguridad pública (NTSVV) (SESNSP, 2016) fue elaborada con la participación del Instituto Politécnico Nacional. Consta de 175 páginas, más un anexo técnico de 304 páginas. Cabe destacar que la NTSVV no cuenta con una apartado específico relativo a los sistemas de inteligencia artificial que permiten el reconocimiento facial. No obstante, refiere características técnicas al respecto.

Un píxel (acrónimo de *picture element*) es "la menor unidad homogénea en color que forma parte de una imagen digital". "La resolución de las cámaras de video está en función de la naturaleza de la actividad humana a observar y se define por el número de pixeles que incluye una imagen ofrecida por un sensor de imagen". (SESNSP, 2016-2: 120)

En el anexo técnico de la NTSVV se establece que la anchura media del rostro humano es de 16 centímetros (6.3 pulgadas), por lo que, en este contexto, cuando se requiera el acercamiento a cierta área en particular, con alta calidad de imagen, para cumplir con los requisitos operacionales

[3] *Diario Oficial de la Federación* del 08/01/2016.
[4] *Diario Oficial de la Federación* del 20/09/2016.
[5] *Diario Oficial de la Federación* del 04/01/2017.
[6] *Diario Oficial de la Federación* del 06/02/2018.

de identificación, reconocimiento, detección y monitoreo, se requiere de una relación píxeles-cara, para reconocimiento facial, de 1.25 megapíxeles por centímetro y, para identificación en buenas condiciones, de 2.5 megapíxeles por centímetro, mientras que, en condiciones difíciles (mala iluminación o personas o vehículos a gran velocidad), debe ser de 5 megapíxeles por centímetro. Además, refiere el uso de video inteligente (*analytics*) para detectar en forma automática a personas y vehículos, lo que permite monitorear más imágenes con menos operadores. Asimismo, se sugiere el uso de cámaras tipo PTZ (Pan-Tilt-Zoom, por sus siglas en inglés) cubiertas con domo, que cuentan con inclinación horizontal y vertical, además de acercamientos para cubrir varios kilómetros cuadrados y capturar detalles finos, como rasgos faciales o matrículas vehiculares. Son las cámaras tipo PTZ las que deben utilizarse para seguridad urbana (SESNSP, 2016-2: 139-141).

La NTSVV define a los STV 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, 2016: 4).

La creación de la NTSVV "obedece a la necesidad de un ordenamiento que no solo garantice un mejor uso de los recursos públicos para seguridad, sino que también permita establecer criterios en la planeación, diseño, implementación y operación de los STV con base en la necesidad, proporcionalidad, e integralidad de las medidas de prevención y contención del delito" (SESNSP, 2016: 6).

La NTSVV señala que, en general, los STV se componen de tres elementos: 1) cámaras, 2) comunicaciones y 3) centro de monitoreo. Lo anterior implica la "captura de imágenes por medio de cámaras, trasmisión de datos (imagen, audio, video) por medio de una red alámbrica o inalámbrica, almacenamiento de datos y, por último, la gestión de video". El documento trata, además, las características de los postes que sostienen a las cámaras, en que influyen las características del suelo, la sismicidad, las condiciones climáticas y la velocidad del viento. Además, se considera la altura y constitución de los postes, así como la perspectiva de las cámaras (SESNSP, 2016: 8).

Por otra parte, define criterios para definir el número y posición de las CVV, en función del índice poblacional, la estructura urbana y los *hot spots* o puntos georreferenciados que concentran incidencia delictiva. Además, establece consideraciones en relación con los tipos de cámaras,

las orientaciones, resoluciones, tipos de lentes, sistemas de iluminación y el diseño de la infraestructura de comunicaciones necesaria.

La NTSVV establece criterios de mantenimiento preventivo y correctivo y, también, parámetros para medir la eficacia de los STV (SESNSP, 2016: 173-174) en relación con la disminución de índices delictivos, el aumento de detenciones, el aumento de denuncias, la reducción de los niveles de corrupción policial y los resultados de los servicios de emergencia.

B) RECURSOS FEDERALES PARA SISTEMAS DE VIDEOVIGILANCIA EN ENTIDADES FEDERATIVAS Y MUNICIPIOS

Toda política pública requiere una asignación presupuestal. Política pública sin presupuesto es demagogia y está condenada al fracaso. Al analizar los recursos federales utilizados por las entidades federativas y los municipios para STV en el período 2016-2020, resulta que los recursos suman 10,677 millones de pesos (Tabla 2).

Tabla 2. Recursos federales etiquetados para videovigilancia por las entidades federativas y los municipios entre 2016 y 2020 (cifras en millones de pesos)

Fondo de Aportaciones para la Seguridad Pública (FASP)	AÑO	MONTO	Subsidio para el Fortalecimiento de la Seguridad de los Municipios (FORTASEG)	AÑO	MONTO
	2016	462 MDP		2016	No disponible
	2017	375 MDP		2017	2,802 MDP
	2018	475 MDP		2018	3,082 MDP
	2019	316 MDP		2019	2,499 MDP
	2020	382 MDP		2020	284 MDP
	TOTAL	2,010 MDP		TOTAL	8,667 MDP
SUMA FASP Y FORTASEG	10,677 MDP				

Fuente: Elaboración propia con información del Mecanismo de Evaluación y Trasparencia de Recursos Federales (MET) del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, disponible en: https://met.sesnsp.net/

De esta tabla se desprende que las principales inversiones en materia de STV, con recursos federales, han sido realizadas por gobiernos municipales.

C) IMPLEMENTACIÓN DE LOS SISTEMAS DE VIDEOVIGILANCIA EN POLÍTICAS PÚBLICAS DE SEGURIDAD

Los STV pueden tener aplicación en la implementación de diferentes políticas públicas en materia de seguridad:

Políticas de prevención situacional del delito

La prevención situacional del delito es un "Modelo teórico-conceptual que permite la gestión del fenómeno delictivo. Parte de una perspectiva racional y económica de la actividad delincuencial, para generar estrategias que reduzcan las oportunidades de llevar a cabo un ilícito, mediante el aumento del riesgo, real o percibido, de ser detenido, y la reducción al mínimo de los beneficios potenciales del acto delictivo" (SESNSP, 2016: 17).

Un ejemplo práctico de los STV, como parte de las políticas de prevención situacional del delito, es la instalación de sistemas tecnológicos de videovigilancia en unidades de transporte público. En el Estado de México, a junio de 2019, se habían instalado en 10,300 unidades de transporte, cubriendo 826 rutas (Jiménez Jacinto, 2019). En la Ciudad de México, "el Gobierno de la Ciudad implementa el proyecto 'Monitoreo Integral y Seguridad del Transporte Público vía GPS', que consiste en la instalación de GPS, botón de pánico, contador de pasajeros y videocámaras en 16 mil unidades durante 2019. La Jefa de Gobierno, Claudia Sheinbaum, aseguró que se invierten 313 millones de pesos en la colocación del equipo" (Gobierno de la Ciudad de México, 2019).

Políticas de recuperación de espacios públicos

Solo los jóvenes, los delincuentes y los imprudentes tienen algo que hacer en una calle abandonada:

> Si está rota la ventana de una fábrica u oficina, los transeúntes observan y concluyen que a nadie le importa o que no hay un responsable. Con el tiempo, algunos empezarán a arrojar piedras para romper más ventanas. Pronto todas estarán rotas y la gente al pasar pensará

> que no solo no hay un responsable del edificio, sino además que nadie se encarga de la calle en que se encuentra (Kelling y Coles, 2001: 20).

Ante el sentimiento de ausencia de autoridad, el remedio es generar lo contrario, una percepción de presencia y orden. Para ello son necesarias mejoras en iluminación, pavimentación, limpieza, generación de corredores seguros y la sensación de vigilancia permanente de los STV.

Políticas de renovación de la infraestructura urbana

El concepto de renovación urbana

> …surgió en 1950 con el economista estadounidense Miles Calean, al referirse a la renovación de edificaciones, equipamientos e infraestructura de las ciudades, observándola como un mecanismo necesario contra su envejecimiento y a su vez se muestra como una posibilidad para mejorar y proponer nuevos usos y actividades en el suelo urbano a través de convenios de la administración pública con entidades privadas (Casas Matiz, 2014).

En México existen varios ejemplos de este tipo de intervenciones. La zona de Santa Fe, en la Ciudad de México, hace algunas décadas era un basurero y hoy es una de las zonas de mayor plusvalía. Colonias como la Condesa, la Roma o la Anzures han tomado nuevos bríos. En Toluca, con un presupuesto de 350 millones de pesos, el centro histórico será renovado con un planetario, áreas recreativas, de convivencia y culturales (Bocanegra, 2020).

Políticas de ciudades seguras

El Programa de Ciudades más Seguras (ONU-Hábitat) comenzó en 1996 a solicitud de alcaldes africanos para combatir la criminalidad. Al año 2020, ONU-Hábitat ha apoyado estas iniciativas en 77 ciudades de 24 países. El programa tiene un enfoque holístico para mejorar la habitabilidad y la calidad de vida de las personas que viven en ellas. Uno de sus aspectos es el enfoque multidimensional de prevención del crimen urbano, mediante medidas de prevención en el entorno físico y la gestión de las calles y los espacios públicos (HABITAT, 2020).

Políticas de inteligencia para la prevención

Son instrumentos y herramientas de aplicación práctica que refuerzan la operación de las instituciones de seguridad pública, resultado de la sistematización y análisis de la información cuantitativa y cualitativa recabada por los STV (SESNSP, 2016: 17).

IV. VIDEOVIGILANCIA E INTELIGENCIA ARTIFICIAL. EL RECONOCIMIENTO FACIAL

El uso de herramientas de inteligencia artificial en el ámbito de la seguridad urbana está en expansión. Por ejemplo, el reconocimiento facial de delincuentes mediante STV y la identificación y seguimiento de matrículas o placas vehiculares. Sin embargo, existe la inquietud de que la toma de decisiones operativas en materia de seguridad urbana se vuelva un proceso deshumanizado con dilemas éticos.

Un ejemplo del uso de la inteligencia artificial en materia de seguridad es el Proyecto Magneto *(*M*ultimedia* A*nalysis and correlation en*G*ine for orga*N*ised crim*E *preven*T*ions and investigati*O*n)*, financiado por el programa Horizonte 2020 de la Comisión Europea, que desarrolla un motor de correlación para la elaboración de hipótesis en la prevención e investigación del crimen organizado, a través de la inteligencia artificial, como el reconocimiento facial o la transcripción automática de audio a texto" (Fórum Español para la Prevención y la Seguridad Urbana, 2020).

El Proyecto Magneto se aplicará en 22 ciudades europeas durante 36 meses (2018-2021), generando productos como la visualización en 3D de datos georreferenciados, mapas de calor, procesos de razonamiento semántico avanzado mediante datos de informes policiales y testimoniales, reconocimiento de regiones y patrones, reconocimiento facial e identificación de patrones de interés, como tatuajes, logos, colores y la identificación de relaciones entre grupos delincuenciales (Torrado Sánchez, 2020).

La empresa tecnológica *Surfshark* analizó la videovigilancia en 194 países: 109 países utilizan el reconocimiento facial. Solo Bélgica ha declarado ilegal el reconocimiento facial, y Francia y Suecia lo prohíben expresamente en las escuelas (Atresmedia, 2020). La tecnología de reconocimiento facial se utiliza —con o sin marco legal— en 32 países de Europa. Antes de la pandemia, en enero de 2020, la policía de Londres desplegó CCV capaces

de identificar rostros. A finales de febrero de 2020 ya había realizado su primer arresto (Atresmedia, 2020).

Arvind Krishna, CEO de IBM, afirmó que la empresa "no va a contribuir a desarrollar tecnología para la vigilancia masiva, el perfil racial, las violaciones de derechos humanos y las libertades básicas o cualquier propósito que no sea coherente con nuestros valores". Agregó: "IBM entiende que en la actualidad, con los avances de la inteligencia artificial, el reconocimiento facial ha mejorado mucho pero a menudo se utiliza por compañías privadas que apenas son supervisadas." El responsable de IBM asegura que la tecnología "puede aumentar la transparencia y ayudar a la policía a proteger a las comunidades, pero no debe promover la discriminación" (Atresmedia, 2020).

El uso de la inteligencia artificial en STV presenta retos. Por ejemplo, en el control de multitudes o en aeropuertos y otras terminales de transporte. "Las herramientas basadas en inteligencia artificial deben desarrollar sistemas capaces de monitorizar en tiempo real grandes cantidades de datos obtenidos de la red, y realizar análisis de las imágenes de cámaras de seguridad en tiempo real, permitiendo la detección de ataques a la seguridad de la sociedad y las empresas." Los algoritmos deberán mejorar sus capacidades predictivas: "[E]l análisis de imágenes procedentes de cámaras de video o el análisis de las redes sociales mediante tecnologías del lenguaje y el diseño de perfiles basados en el análisis de secuencias temporales de datos, debe evitar la detección de falsos positivos." (Gobierno de España, 2019: 33)

Otras áreas de oportunidad son la detección de paquetes sospechosos, la búsqueda y localización de personas desaparecidas o ausentes y la captura de delincuentes flagrantes, mediante el procesamiento de datos que hoy recogen las cámaras y que no se procesan. "Los sistemas son un complemento a la labor policial, no un sustituto. A corto plazo, os dará más trabajo del que os quitará." (Manyá, 2020: 3)

Torrado Sánchez (2020) explica que el uso de cubrebocas con motivo de la pandemia producida por la COVID-19 ha implicado mejorar el reconocimiento facial, pues es muy difícil la identificación de personas solamente con base en los ojos o la nariz, por lo que han recurrido a tecnologías de reconocimiento de patrones o regiones, localizando marcas, logos o colores identificativos de las personas, para después buscar esos mismos rasgos en otras imágenes.

V. LA PARADOJA DE LA VIDEOVIGILANCIA

La gran paradoja de la videovigilancia consiste en que, a pesar de que vivimos bajo un panóptico[7] electrónico, en una sociedad observada por el gran *Big Brother*,[8] ello no se traduce en una mayor percepción de seguridad por parte de los ciudadanos o en una menor incidencia delictiva.

"Tal como yo lo veo, el modelo panóptico está vivo y goza de cabal salud, y de hecho está dotado de una musculatura mejorada electrónicamente, como la de un *cíborg*,[9] lo cual lo hace tan fuerte que ni Bentham, ni siquiera Focault, hubieran sido capaces de imaginarlo", afirmó Zygmunt Bauman (Bauman y Lyon, 2013: 64). David Lyon refiere un concepto denominado "banóptico", desarrollado por Didier Bigo. El prefijo *ban* se refiere a la exclusión y lo aplica a los integrantes marginales de una sociedad, "los marginales globales". En este sentido, el "banóptico" sirve "para indicar cómo las tecnologías de elaboración de perfiles se utilizan para determinar quién debe ser objeto de una vigilancia estricta". Los estudios mencionados en párrafos anteriores dan cuenta de ello.

Con un espíritu orwelliano, Lyon afirma que:

> [L]as burocracias trasnacionales de vigilancia y control sean de negocios o políticas, trabajan ahora a distancia para rastrear y controlar los movimientos de la población. En conjunto, estos discursos, prácticas, construcciones físicas y normas forman un complejo aparato interconectado, o lo que Focault llamaba un *dispositif*. El resultado no es un panóptico global sino un banóptico combinando la idea de exclusión (Bauman y Lyon, 2013: 69-70).

Bauman explica la paradoja de la videovigilancia: "…parece que (…) nos hemos vuelto adictos a la seguridad. Hemos asimilado la *weltanschauung*[10] de la ubicuidad del peligro, de la necesidad global de desconfiar y sospechar, de que sólo es concebible una cohabitación sana bajo un dispositivo de vigilancia continua." (Bauman y Lyon, 2013: 111-113)

Bauman concluye que "esta es la paradoja del mundo saturado de dispositivos de vigilancia, sea cual sea el propósito que persiguen: por un lado,

[7] Sistema de autocontrol generado por la sensación permanente de ser vigilado. El panóptico era un tipo de arquitectura carcelaria ideada por Jeremy Bentham a finales del siglo XVIII. Desde una torre central de vigilancia, el custodio puede vigilar a todos los prisioneros, ubicados en celdas y pasillos que, a manera de estrella, giran en torno a la torre central.

[8] En referencia al *Big Brother* o *Gran Hermano*, personaje de la novela *1984* de George Orwell. "De vez en cuando levantaba la mirada a la cara que le miraba fijamente desde la pared de enfrente. El Gran Hermano te vigila."

[9] Criatura compuesta de elementos orgánicos y dispositivos cibernéticos. Es un concepto híbrido de hombre y máquina.

[10] Puede traducirse como "cosmovisión".

estamos más protegidos que cualquier generación anterior; por otra parte, sin embargo, ninguna generación anterior, o preelectrónica, experimentó como la nuestra esa sensación cotidiana de inseguridad a todas horas" (Bauman y Lyon, 2013: 111-113).

Madrid firmó la Carta para el uso democrático de la vigilancia por video del EFUS. La concejala presidenta de Tetuán y Moncloa, Montserrat Galcerán, fue entrevistada sobre el porqué de la adhesión de esa ciudad a la carta. En la entrevista, reconoció los alcances limitados de la videovigilancia para la persecución del delito, aunque ayuden a aumentar la percepción subjetiva de la seguridad (European Forum for Urban Security, 2020-2):

> La criminología liberal realiza un análisis erróneo al afirmar que si se incrementa en el delincuente la certeza de que le cogerán, renunciará a su acción criminal. Parecen no tener en cuenta que la delincuencia parte de una necesidad por la obtención de recursos en el caso de robos o hurtos. Los estudios demuestran que una vez instaladas las cámaras, la tasa delincuencial se reduce en la zona, pero que una vez los delincuentes las incorporan como un elemento más dentro del paisaje urbano, los índices vuelven a sus valores anteriores. No obstante, debemos asumir que para la mayoría de la población, las cámaras de vídeo vigilancia aumentan la sensación de seguridad subjetiva. Sin embargo, esto no debe hacernos perder de vista que no son un elemento determinante tanto para la prevención como para el esclarecimiento de delitos.

La concejala Galcerán tiene razón. La alcaldía Iztapalapa, en la Ciudad de México, es la que tiene el mayor número de CVV instaladas, con 2,293 (Gobierno de la Ciudad de México, 2020), y fue, entre octubre de 2019 y octubre de 2020, la municipalidad con mayor número de secuestros del país, con 18 casos (SESNSP, 2019-2020), delito que generalmente se comete en la vía pública.

La paradoja de la videovigilancia implica que la tecnología y los avances de la inteligencia artificial son utilizados por todos, y esto incluye a los delincuentes. Basta pensar en los teléfonos celulares inteligentes, que hoy en día son material de trabajo de policías y ladrones. Un informe elaborado por EUROPOL, el Instituto Interregional de Investigación sobre Delitos y Justicia de las Naciones Unidas (UNICRI) y *Trend Micro*, publicado en noviembre de 2020, estudió los usos criminales actuales y previstos de la inteligencia artificial.

El informe concluyó que los ciberdelincuentes aprovecharán la inteligencia artificial como superficie de ataque. La suplantación de identidad es

"el uso más conocido de la inteligencia artificial como vector de ataque". No obstante, el informe advierte que será necesaria una nueva tecnología de detección para atenuar el riesgo de campañas de desinformación y extorsión, así como las amenazas dirigidas a conjuntos de datos de inteligencia artificial (Generalitat de Catalunya, 2020).

Apenas en marzo de 2018 fue reformada la Ley de Instituciones de Crédito de México, al adicionar el artículo 122 *sextus* para establecer la suplantación o robo de identidad como un delito. Esta adición fue reformada en junio de 2019.[11] El artículo 112 *séptimus*, adicionado también en marzo de 2018, sanciona a quien, usando una identidad suplantada, obtenga servicios o productos del sector financiero.

En el informe de EUROPOL, UNICRI y *Trend Micro*, citado arriba, se señala un catálogo de amenazas dirigidas a conjuntos de datos de inteligencia artificial (Generalitat de Catalunya, 2020):

- Ataques convincentes de ingeniería social[12] a gran escala.
- *Software* malicioso para obtener documentos y hacer los ataques más eficientes.
- Evasión del reconocimiento de imágenes y biométrica de la voz.
- Ataques de *ransomware*,[13] mediante orientación y evasión inteligentes.
- Contaminación de datos mediante la identificación de puntos ciegos en las normas de detección.
- Desarrollo de sistemas de inteligencia artificial para mejorar la eficacia del *software* malicioso y perturbar, así, los sistemas *antimalware* y de reconocimiento facial.

Las tres organizaciones recomiendan (Generalitat de Catalunya, 2020) aprovechar el potencial de la tecnología de inteligencia artificial como herramienta contra el crimen, continuar la investigación de tecnologías

[11] *Diario Oficial de la Federación* del 9 de marzo de 2018 y del 4 de junio de 2019.

[12] La ingeniería social consiste en técnicas de manipulación psicológica para inducir al engaño o al error a un usuario de internet, y que son utilizadas por ciberdelincuentes bajo la premisa de que es más fácil manipular a las personas que a las máquinas. Los engaños, generalmente, se despliegan por correos electrónicos o aplicaciones, utilizando como principios el respeto a la autoridad, la voluntad de ayudar, el temor a perder un servicio, el respeto social o la afectación a la imagen o dignidad personal, así como los productos o servicios gratuitos o con precios de aparente oportunidad.

[13] *Ransomware* es el secuestro de bases de datos a través de la infiltración de un programa de *software* malicioso que infecta los equipos de cómputo y muestra mensajes que exigen el pago de un rescate, generalmente mediante activos virtuales o criptomonedas.

defensivas, promover y desarrollar marcos seguros de diseño de inteligencia artificial, y potenciar las colaboraciones público-privadas multidisciplinares.

La inteligencia artificial aplicada a la seguridad urbana genera discursos antagónicos: los optimistas que creen que la tecnología va a resolver todos los problemas, y los pesimistas, que ven en la inteligencia artificial una herramienta de control que genera discriminación racial, manipulación política e invasiones a la intimidad de los ciudadanos. Estamos frente a la necesidad de un marco normativo para la inteligencia artificial, una ética para una revolución en construcción. El concepto "inteligencia artificial" es un eufemismo, pues en realidad se trata de sistemas para el tratamiento y análisis automático de la información inspirado en un desiderátum: la voluntad de emular los procesos cognitivos humanos mediante computadoras y sistemas de cómputo (Miró Llinares, 2020).

Miró Llinares (*Idem*) subraya el mito de la predicción del futuro, cuando en realidad se trata de la estimación a partir de datos del pasado. El mito de la decisión totalmente autónoma, cuando el ser humano tiene el control. El mito de la distopía del control estatal cuando la inteligencia artificial plantea los datos en manos privadas. El mito de la perfección humana frente al cerebro humano, una caja gris que tiene más sesgos y ruido que cualquier caja plateada con circuitos.

Miró Llinares (*Idem*) propone que la fiabilidad de todo sistema de inteligencia artificial se apoye en tres componentes: la inteligencia artificial debe ser lícita, esto es, apegarse a todas las leyes y reglamentos aplicables; debe ser ética, de modo que garantice el respeto de los principios y valores éticos; y debe ser robusta, tanto técnica como socialmente, pues la inteligencia artificial, incluso con intenciones buenas, pueden provocar daños accidentales o colaterales. Lo anterior implica incluir un modelo de gobernanza de la información que permita a los usuarios identificar a los responsables del tratamiento de la información y ejercitar sus derechos. Se requieren normas rígidas en cuanto a su esencia ética, pero suficientemente flexibles para permitirles adaptarse a las novedades tecnológicas.

VI. LOS DEBATES QUE VENDRÁN EN LA TERCERA DÉCADA DEL SIGLO XXI

El *deep learning* o aprendizaje profundo de redes neuronales implica un conjunto de algoritmos que busca emular el aprendizaje de los seres humanos.

Es una forma de automatizar el análisis predictivo. Manyá (2020) explica que "son cajas negras" que no dan explicaciones sobre las decisiones que toman y pueden constituir un peligro. Por ello, sugiere que siempre se exija una trazabilidad de los datos y una reflexión sobre el uso que se dará a la información, sin que implique que los datos sean utilizados para actuaciones policiales inmediatas. Pensemos en la decisión policial de utilizar armas letales en una situación de rehenes, tanto en el uso legítimo de la fuerza como ante un estado de necesidad "disculpante". ¿Cuándo y a quien disparar? No son decisiones que deban tomarse en función de algoritmos.

Otro tema de debate radica en el uso de videovigilancia y de vehículos aéreos no tripulados para videograbación en el control de masas y manifestaciones. ¿Tienen los mismos derechos y obligaciones las autoridades y los particulares? ¿Pueden los policías videograbar a manifestantes y estos no pueden videograbar a aquellos?

En noviembre de 2020, la Asamblea Nacional de Francia aprobó una Ley de Seguridad Global, cuyo artículo 24 castiga con penas de hasta un año de prisión y 45,000 euros de multa la difusión de la "imagen del rostro o de otros elementos que permitan la identificación de policías o gendarmes y que pueda perjudicar su integridad física o psíquica". Además, la ley permite el uso de drones policiales para grabar manifestaciones y el reconocimiento facial a través de CVV. Ante ello, miles de personas se manifestaron en Francia, pues consideran que la ley es un ataque a la libertad de expresión. La ley, no obstante, fue enmendada de último minuto para garantizar "el derecho a informar" (Ámbito, 2020). "En Lille llevaban pancartas con mensajes como 'Orwell tenía razón'. También hubo más de mil manifestantes en Rennes o en Montpellier, donde pidieron 'Bajen sus armas, nosotros bajaremos nuestros teléfonos'." (*La Jornada*, 2020)

En España, el Ministerio de Consumo sometió a consulta popular, en octubre de 2020, la instalación de STV en rastros y mataderos de animales, para que "se cumplan los estándares de bienestar animal y seguridad alimentaria". Argumentó que Francia, Alemania y Escocia cuentan con protocolos de videovigilancia similares (*20 minutos*, 2020). En España, el sacrificio de animales para consumo humano, en 2019, se situó en 53 millones de cerdos, 828 millones de aves, 544,000 ovinos, 94,800 caprinos y 38,000 equinos (*20 minutos*, 2020). ¿Y si después es necesario supervisar el normal desarrollo de las actividades de bares y antros? ¿Qué pasa si se requiere vigilar la correcta aplicación de vacunas contra la COVID-19 en instituciones de salud? Es necesario ponderar entre el cumplimiento

normativo en los diferentes aspectos de la vida de las empresas y la supervisión videovigilada de su cumplimiento. En junio de 2020, el parlamento suizo rechazó el uso de la videovigilancia en rastros y mataderos de animales, argumentando que la medida sería desproporcionada y simbólica. Cabe señalar que Suiza protege la dignidad animal a nivel constitucional (Swissinfo.ch, 2020).

Las empresas *Motorola* y *Avigilon* diseñaron un sistema de inteligencia artificial que permite identificar cuándo las personas, durante la pandemia de la COVID-19, no guardan la sana distancia ni portan cubrebocas (Ollero, 2020). ¿Sería posible multar a quienes no siguen las medidas de higiene? ¿Podría constituir una evidencia para imputar el tipo penal de peligro de contagio si un portador del virus, a sabiendas de que está enfermo, no usa cubrebocas?

En Moscú, Anna Kuznetsova, de 20 años, activista de los derechos humanos e integrante de la *Fundación Thomson Reuters*, compró por 170 euros un informe con 80 fotografías y ubicaciones suyas, tomadas por el sistema de videovigilancia de Moscú. Además del pago, le pidieron una fotografía de la persona a la que quisiera espiar. Las imágenes muestran dónde vive, dónde está su trabajo y cuál es su rutina diaria. Los informes se venden por la aplicación de mensajería *Telegram* y se confeccionan gracias a más de 105,000 CVV instaladas en Moscú. Esto reactivó en Rusia la controversia en torno a la videovigilancia y el reconocimiento facial, y motivó que las autoridades de Moscú investiguen accesos ilícitos a su sistema de reconocimiento facial (Aguiar, 2020). Surgen dos hipótesis: la posible utilización de imágenes y datos por quienes trabajan como operadores del sistema de videovigilancia, o un acceso lógico no autorizado orquestado por ciberdelincuentes.

Estos y otros casos motivarán los debates en torno al uso de los sistemas de videovigilancia y la inteligencia artificial, específicamente las de reconocimiento facial, en la década que inicia. Habrá que encontrar una posición intermedia entre la utopía de una sociedad vigilada democráticamente, donde se respeten los derechos humanos y donde la videovigilancia coadyuve a reducir la incidencia delictiva y mejorar la percepción de seguridad de los ciudadanos, y la distopía de una sociedad controlada y videovigilada por autoridades y delincuentes, donde la intimidad y la no discriminación queden vulneradas detrás de una pantalla.

VI. FUENTES DE CONSULTA

20 minutos. (6 de Octubre de 2020). "Consumo planea poner cámaras en los mataderos para 'que se cumplan los estándares de bienestar animal'". Recuperado el 20 de diciembre de 2020 de: https://www.20minutos.es/noticia/4408101/0/consumo-camaras-mataderos-cumplan-estandares-bienestar-animal/#:~:text=las%20noticias-,Consumo%20planea%20poner%20c%C3%A1maras%20en%20los%20mataderos%20para%20%22que%20se,los%20est%C3%A1ndares%20de%20bienestar%20

Aguiar, A. (12 de noviembre de 2020). "En Moscú puedes espiar a cualquiera por menos de 200 euros gracias a las más de 100,000 cámaras de vigilancia y reconocimiento facial que hay instaladas en la ciudad". *Bussines Insider.* Recuperado el 20 de diciembre de 2020 de: www.businessinsider.es/espiar-moscu-camaras-videovigilancia-muy-barato-754069

Ámbito. (21 de noviembre de 2020). "Francia: miles de personas se manifestaron contra nueva ley de seguridad que impide difundir imágenes policiales". Recuperado el 20 de diciembre de 2020 de: https://www.ambito.com/mundo/ley/francia-miles-personas-se-manifestaron-contra-nueva-seguridad-que-impide-difundir-imagenes-policiales-n5149952

Animal Político. (2 de mayo de 2016). "Militares controlarán las cámaras de seguridad de Acapulco, Guerrero: Osorio Chong". *Animal Político*. Recuperado el 19 de diciembre de 2020 de: 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". *Espiral, XXXIII*(66). Recuperado el 19 de diciembre de 2020 de: https://www.redalyc.org/jatsRepo/138/13844799006/html/index.html#fn14

Atresmedia. (20 de junio de 2020). "109 países utilizan o han aprobado la vigilancia de reconocimiento facial". (Atresmedia, Ed.) *Levanta la cabeza*. Recuperado el 17 de diciembre de 2020 de: https://compromiso.atresmedia.com/levanta-la-cabeza/actualidad/109-paises-utilizan-han-aprobado-vigilancia-reconocimiento-facial_202006095edf4294f8f8bb0001657e86.html

Bauman, Z., y Lyon, D. (2013). *Vigilancia líquida.* (A. Capel, Trad.) Madrid: Paidós.

Bocanegra, R. (16 de enero de 2020). *Real State Market*. Recuperado el 16 de diciembre de 2020 de: https://www.realestatemarket.com.mx/noticias/infraestructura-y-construccion/26981-centro-de-toluca-tendra-renovacion-sustentable

Calfa, R., Sebastian, S. y Bourgeois, N. (2010). "Hacia una carta por una utilización democrática de la videovigilancia en las ciudades europeas". En *Ciudadanos, ciudades y videovigilancia* (H. Birkle *et al.*, Trads., págs. 107-154). París: Foro Europeo para la Seguridad Urbana. Recuperado de: www.efus.eu/files/2013/05/CCTV_ESPAGNOL.pdf

Cámara de Valencia. (2020). "El reconocimiento facial como método de vigilancia no es exclusivo del gobierno chino. España y otros 74 países más ya lo usan de forma habitual". Recuperado el 18 de diciembre de 2020 de: https://ticnegocios.camaravalencia.com/servicios/tendencias/el-reconocimiento-facial-como-metodo-de-vigilancia-no-es-exclusivo-del-gobierno-chino-espana-y-otros-74-paises-mas-ya-lo-usan-de-forma-habitual/

Casas Matiz, E. (enero-diciembre de 2014). "Marco conceptual de la renovación urbana". (U. C. Colombia, Ed.) *Revista Questionar. Investigación científica, 1*(2), 24. Recuperado el 17 de diciembre de 2020 de: https://www.academia.edu/34108770/Marco_conceptual_de_la_Renovaci%C3%B3n_Urbana

Chaverra, D. (10 de diciembre de 2019). *Conozca los países y ciudades del mundo con mayor número de cámaras de seguridad.* Recuperado el 18 de diciembre de 2020 de: https://www.ventasdeseguridad.com/20191210118 17/noticias/empresas/conozca-los-paises-y-ciudades-del-mundo-con-mayor-numero-de-camaras-de-seguridad.html#:~:text=Estados%20Unidos%20tiene%2015.28%20c%C3%A1maras,y%20Corea%20del%20Sur%201.99.

Corona, S. (10 de noviembre de 2017). "Se necesitan 120 mil cámaras para cubrir toda la CDMX: C5". *El Economista*. Recuperado el 17 de diciembre de 2020 de: https://www.eleconomista.com.mx/politica/Se-necesitan-120000-camaras-para-cubrir-toda-la-CDMX-C5-20171110-0055.html

El País. (12 de octubre de 2007). "Francia triplicará en dos años las cámaras de videovigilancia". Recuperado el 18 de diciembre de 2020 de: https://elpais.com/diario/2007/10/13/internacional/1192226408_850215.html

European Forum for Urban Security. (2020). Recuperado el 17 de diciembre de 2020 de: www.efus.eu.es/about-us/about-efus/public/1450/

European Forum for Urban Security. (2020-2). "Madrid firma la Carta para el uso democrático de la vigilancia por video del EFUS". Recuperado el 19 de diciembre de 2020 de: www.efus.eu/es/topics/tools-and-methods/technologies/public/14298/

Fórum Español para la Prevención y la Seguridad Urbana. (9 de diciembre de 2020). *Fórum Español para la Prevención y la Seguridad Urbana.* Recuperado el 17 de diciembre de 2020 de: www.fespu.es/criterios-eticos-inteligencia-artificial

Fundación Empresa, Seguridad y Sociedad (ESYS). (2016). *La videovigilancia en la seguridad. Análisis y recomendaciones para su actualización legal.* Madrid: Fundación ESYS. Recuperado el 18 de diciembre de 2020 de: https://www.fundacionesys.com/es/system/files/documentos/VIDEOVIGILANCIA%202016_0.pdf

Generalitat de Catalunya. (14 de diciembre de 2020). *Notes de seguretat.* Recuperado el 19 de diciembre de 2020 de: www.notesdeseguretat.blog.gencat.cat/2020/12/14/amenazas-de-la-inteligencia-artificial/

Gobierno de España. (2019). *Estrategia Española de I+D+I en Inteligencia Artificial.* (Ministerio de Ciencia, Ed.) Recuperado el 19 de diciembre de 2020 de: https://cpage.mpr.gob.es

Gobierno de la Ciudad de México. (6 de agosto de 2019). "Implementa gobierno capitalino proyecto 'Monitoreo Integral y Seguridad del Transporte Público vía GPS'". Recuperado el 17 de diciembre de 2020 de: efaturadegobierno.cdmx.gob.mx/comunicacion/nota/implementa-gobierno-capitalino-proyecto-monitoreo-integral-y-seguridad-del-transporte-publico-gps

Gobierno de la Ciudad de México. (2020). "Centro de Comando, Control, Cómputo, Comunicaciones, y Contacto Ciudadano de la Ciudad de México". Recuperado el 17 de diciembre de 2020 de: www.c5.cdmx.gob.mx

Gobierno del Estado de México. (2020). *Tercer informe de resultados 2020.* Recuperado el 17 de diciembre de 2020 de: http://transparenciafiscal.edomex.gob.mx/sites/transparenciafiscal.edomex.gob.mx/files/files/pdf/rendicion-cuentas/informe-gobierno/3er-Informe-Edomex-2020.pdf

HABITAT, O. (2020). *Programa Ciudades más seguras*. Recuperado el 17 de diciembre de 2020 de: unhabitat.org/es/node/3242

Instituto Nacional de Estadística, Geografía e Informática (INEGI). (2019). *Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales.* Recuperado el 17 de diciembre de 2020 de: https://www.inegi.org.mx/contenidos/programas/cngspspe/2019/doc/cngspspe_2019_resultados.pdf

Jiménez Jacinto, R. (24 de junio de 2019). "Van mas de 10,000 unidades de transporte con cámaras y botón de pánico en Edomex". *El Universal*. Recuperado el 17 de diciembre de 2020 de: https://www.eluniversal.com.mx/metropoli/edomex/van-mas-de-10-mil-unidades-de-transporte-con-camaras-y-boton-de-panico-en-edomex

Kelling, G., y Coles , C. (2001). *No más ventanas rotas. Cómo restaurar el orden y reducir la delincuencia en nuestras comunidades.* (H. I. Gutiérrez, Trad.) México: Instituto Cultural Ludwig Von Mises, A.C.

La Jornada. (22 de noviembre de 2020). "Rechazo en Francia a iniciativa que limita fotografiar a policías". *La Jornada*, pág. 27. Recuperado el 20 de diciembre de 2020 de: https://www.jornada.com.mx/2020/11/22/mundo/027n2mun

Manyá, F. (2 de diciembre de 2020). "Aplicaciones de la inteligencia artificial en el ámbito de la seguridad ciudadana. Webinar. Relato de la jornada". Recuperado el 19 de diciembre de 2020 de: www.fepsu.es/wp-content/uploads/2020/12/Relato-webinar-2-de-diciembre.pdf

Miró Llinares, F. (Diciembre de 2020). *Fórum Español para la Seguridad Urbana.* Recuperado el 17 de diciembre de 2020 de: www.fepsu.es/wp-conten/uploads/2020/12/Fepsu-etica-inteligencia.pdf

Olivares Alonso, E. (25 de enero de 2016). "La videovigilancia acapara el debate sobre el plan de seguridad de Graue para la UNAM". *La Jornada*, pág. 36. Recuperado el 19 de diciembre de 2020 de: https://www.jornada.com.mx/2016/01/25/sociedad/036n1soc

Ollero, D. (19 de mayo de 2020). "Las cámaras de seguridad ya detectan cuando alguien no lleva mascarilla". *El mundo*. Recuperado el 19 de diciembre de 2020 de: www.elmundo.es/tecnologia/2020/05/19/5ec3db39fc6c83d41d8b45bf.html

Osorio Arjona, J., y García Palomares, J. (2017). "Redes sociales y movilidad urbana: cálculo de matrices origen-destino de viajes a partir de Twitter". *Social Big Data-CM. Using big data for social change monitoring and analysis.* Madrid: Universidad Complutense de Madrid. Recuperado el 17 de diciembre de 2020 de: researchgate.net/

publication/322931048_Redes_sociales_y_movilidad_urbana_calculo_de_matrices_origen-destino_de_viajes_a_partir_de_Twitter

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). (2016). *Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública.* Recuperado el 17 de diciembre de 2020 de: http://www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). (2016-2). *Anexo Técnico de la Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Videovigilancia para la Seguridad Pública.* Recuperado el 17 de diciembre de 2020 de: www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Anexo_Tecnico_NTSVVSP.pdf

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2019-2020). *Incidencia delictiva del fuero Común y Federal.* Recuperado el 19 de diciembre de 2020 de: https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia?state=published

Swissinfo.ch. (3 de junio de 2020). "Rechazan videovigilancia en mataderos". *Swissinfo.ch*. Recuperado el 20 de diciembre de 2020 de: www.swissinfo.ch/spa/sacrificio-animal_rechazan-videovigilancia-en-mataderos/45804552

Torrado Sánchez, A. (2 de diciembre de 2020). "Nuevas tecnologías aplicadas a la seguridad urbana. Fórum Español para la Seguridad Urbana". Recuperado el 17 de diciembre de 2020 de: www.fepsu.es/wp-content/uploads/2020/12/Magneto-Inteligencia-Artificial.pdf

Xtreme Secure. (Septiembre-octubre de 2019). "Videovigilancia y alarmas: prevención del delito y tecnología". *Xtreme Secure. El mundo de la seguridad.* Recuperado el 18 de diciembre de 2020 de: https://www.xtremsecure.com.mx/wp-content/uploads/2019/09/Xtrem-Secure-70.pdf