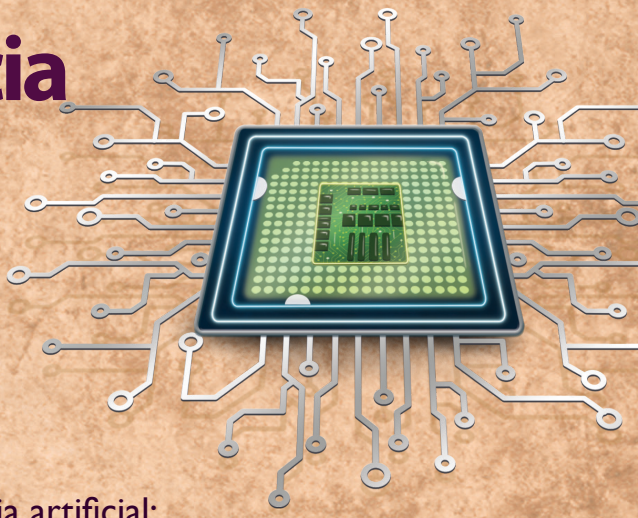
# Revista Mexicana de Ciencias Penales

Año 4 • Número 14 • mayo-agosto de 2021

## Ciencias Penales e inteligencia artificial



- Videovigilancia e inteligencia artificial: entre la utopía y la distopía
  *Álvaro Vizcaíno Zamora*
- Inteligencia artificial, derecho penal y *compliance*
  *Diego Fernando Martínez Hernández*
- Panorama general de la *e-justice* en México y su utilización en el procedimiento penal acusatorio: avances y retos para su consolidación
  *Hugo Oscar Granja Pérez*
- La posibilidad de la policía predictiva
  *Víctor Shaí Nóhpal Rodríguez*

·INACIPE·
INSTITUTO NACIONAL DE CIENCIAS PENALES

# REVISTA MEXICANA DE CIENCIAS PENALES

REVISTA MEXICANA DE CIENCIAS PENALES es una publicación del INACIPE, cuyo objetivo es dar a conocer investigaciones, análisis, reflexiones y opiniones acerca de las ciencias penales en México y en el mundo. En esta revista se dan cita los autores más reconocidos en estas disciplinas.

**Año 4. Número 14. Mayo-agosto 2021**
**ISSN 0187-0416**

· INACIPE ·
INSTITUTO NACIONAL DE CIENCIAS PENALES

# DIRECTORIO




**Diseño editorial**
**Lizeth Violeta Méndez Guadarrama**
**Daniel Leyte Muñiz**

**Cuidado editorial**
**Irene Bárcenas Jara**
**Víctor Fernando Gálvez García**

**Diseño de portada**
**Israel Eliseo Martínez**

REVISTA MEXICANA DE CIENCIAS PENALES, año 4, No. 14, mayo-agosto 2021. Es una publicación trimestral editada por el Instituto Nacional de Ciencias Penales, a través de la Dirección de Publicaciones y Biblioteca. Calle Magisterio Nacional núm. 113, Col. Tlalpan, Alcaldía Tlalpan, C. P. 14000, Ciudad de México, México. Tel. 5487 1571; www.inacipe.gob.mx; e-mail: publicaciones@inacipe.gob.mx. Reservas de Derechos al Uso Exclusivo No. 04-2017-080214584200-102. ISSN: 0187-0416, ambos otorgados por el Instituto Nacional del Derecho de Autor. Licitud de Título y contenido: 17106. Expediente: CCPRI/3/TC/18/21019 otorgado por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación.

Impresa por Lito Roda S.A. de C.V., calle Escondida no. 2, Col. Volcanes, Alcaldía Tlalpan, C.P. 14640, Ciudad de México. Este número se terminó de imprimir en junio de 2021 con un tiraje de 500 ejemplares.





Instituto Nacional de Ciencias Penales

@ INACIPE

**www.inacipe.gob.mx**

# CONTENIDO

## VISIONES PARA EL FUTURO

# EDITORIAL





Empeñado en lograr objetivos que rebasan los límites de sus fuerzas, el ser humano ha creado máquinas que, además de realizar labores arduas con mayor eficacia de la que alcanzaría un mortal, se encaminan a imitar la capacidad cognitiva de sus hacedores hasta donde sea posible. Lo anterior representaría el culmen de la inteligencia artificial y cimbraría al entramado social de modo inédito. La amenaza al concepto jurídico de persona y, desde luego, a sus derechos y a los medios para protegerlos, obligaría a la ciencia jurídica a reinventarse para moderar una realidad nueva que, al igual que la actual, precisaría arrojo institucional y principios éticos para sostenerse.

En el caso de las ciencias penales, la evolución de los sistemas de cómputo ha facilitado la procuración de justicia, al perfeccionar diversos métodos para prevenir el delito o, en su caso, aprehender al perpetrador. Sin embargo, estos avances no siempre observan la obligación estatal de resguardar los derechos humanos; a modo de ejemplo, la videovigilancia extrema en las urbes y la recolección masiva de datos personales repercuten en el ejercicio del derecho a la privacidad y a la identidad, entre otros, lo cual socava la confianza en las instituciones y polariza a la sociedad, poniendo ideas tecnófilas en pugna con el afán de resguardar la dignidad por la vía jurídica.

Si a lo anterior se agrega la opción de que la función judicial quede a merced de máquinas, so pretexto de que la subjetividad humana se traduce siempre en errores, es probable que en el futuro destaque un sistema de integración jurisprudencial "por algoritmos", que sepulte de una vez la evolución del pensamiento ponderativo enderezado a impartir *justicia*. En cierta medida, escenarios de esta índole aún son hipotéticos, como se desprende de los artículos contenidos en este número de la *Revista Mexicana de Ciencias Penales*, dedicado al impacto que la inteligencia artificial ha tenido y acaso tendrá en las disciplinas que analizan y pretenden controlar el fenómeno delictivo.

Tocará al lector, en su fuero interno, cavilar sobre el tipo de valores que le gustaría mantener y fomentar en las generaciones venideras, y que difícilmente se apreciarán alguna vez en criaturas *no humanas*.

Sergio Alonso Rodríguez
Director de la *Revista Mexicana de Ciencias Penales*

Obituario

# L. Rafael Moreno G.

(28/nov/1931- 7/mar/2021)

Luis Rafael Moreno González nació en 1931. Médico cirujano por la Universidad Nacional Autónoma de México (UNAM), se especializó en ciencias forenses y criminalística, disciplina de la cual fue pionero en el país y divulgador constante,[1] como se advierte de los 15 libros y más de 75 artículos que publicó, así como de las innumerables conferencias impartidas en universidades y foros nacionales. En total, dedicó 56 años al ejercicio profesional en materia de criminalística y disciplinas afines.[2]

Brilló como investigador e innovador; incorporó avances en laboratorios de grafoscopía y polígrafo, genética forense, odontología legal, antropología física, microscopía electrónica, fotografía de alta definición e inventario de fármacos, entre muchos otros.[3] En 1970 asumió la Dirección de Servicios Periciales de la entonces Procuraduría General de Justicia del Distrito Federal, y demostró sus dotes de modernizador de procedimientos periciales; por ejemplo, a la sazón todavía se aplicaba

[1] Alemán Velasco, M. (2021). "In Memoriam del Dr. Rafael Moreno González". En https://www.eluniversal.com.mx/opinion/miguel-aleman-velasco/memoriam-del-dr-rafael-moreno-gonzalez. Consultado el 13 de abril de 2021

[2] "Rafael Moreno González. *In Memoriam*". En https://www.revistaabogacia.com/rafael-moreno-gonzalez/. Consultado el 13 de abril de 2021

[3] Alemán Velasco, M., *loc. cit.*

la "prueba de la parafina" en las investigaciones sobre disparo de armas de fuego; Moreno González desechó esa prueba y la sustituyó por métodos modernos, con lo cual impulsó el desarrollo de la criminalística.[4] Es de notar que fue el encargado del dictamen pericial del asesinato de Luis Donaldo Colosio.[5]

Por otra parte, propugnó la importancia de conocer el desarrollo histórico de la criminalística, así como su objeto de estudio, sus fines y su utilidad. Asimismo, introdujo el método científico en la investigación de campo, acierto que fomentó la objetividad en las intervenciones periciales. No menos relevante fue que alentara el aprendizaje de la criminalística más allá de la ciencia, para acercarla a temas como la cultura y las artes, especialmente la literatura, que lo movió a analizar las aportaciones de Arthur Conan Doyle y Edgar Allan Poe a la materia.[6]

En el ámbito académico, fungió como profesor de medicina forense, criminalística y criminología en la Facultad de Derecho de la UNAM. En 1976, al alimón con Celestino Porte Petit, fundó el Instituto Nacional de Ciencias Penales (INACIPE), del cual fue director adjunto (labor que el INACIPE le reconoció en 1981), profesor de criminalística, investigador emérito (desde 2010) y, a partir de 2003, doctor *honoris causa*. Cabe agregar que, en 2009, el instituto denominó "Dr. L. Rafael Moreno González" a su Laboratorio de Criminalística.

Su bibliografía fue ingente. Entre sus libros fundamentales destacan *Ensayos criminológicos y criminalísticos* (1971), *El método científico y la investigación criminalística* (1974), *Metodología e investigación científica* (1979), *La investigación científica* (1986), *Balística forense* (1990), *Notas de un criminalista* (1996), *Introducción a la criminalística* (2006) y *Los indicios biológicos del delito* (2007). Por lo demás, publicó más de cien artículos en revistas especializadas.

Por lo que hace a reconocimientos, se hizo acreedor a una cantidad copiosa, a la que se alude acto seguido de manera enunciativa. La Sociedad Mexicana de Criminología le otorgó la Medalla al Mérito Criminológico "Alfonso Quiroz Cuarón"; a su vez, la Procuraduría General de Justicia de Tlaxcala le hizo un reconocimiento por 20 años de labor científica en el campo de la criminalística (1980); la UNAM lo reconoció con las "Palmas Académicas" por 25 años de labor docente (1988), y la PGJDF por 30 años de servicios (1990); otras

[4] "Rafael Moreno González. *In Memoriam*", *loc. cit.*

[5] Alemán Velasco, M., *loc. cit.*

[6] Lázaro Ruiz, E. (2021). "*Laudatio ad perpetuam memoriam* del Dr. L. Rafael Moreno González". En https://drive.google.com/file/d/1DjsnoDYEPi2nu64hvfUbaMmmLSPb4on5/view. Consultado el 13 de abril de 2021

instituciones que lo honraron fueron el extinto Departamento del Distrito Federal (1992) y el Instituto de Ciencias Forenses y Periciales de Puebla (1998).

Fue miembro fundador, expresidente y presidente honorario vitalicio de la Academia Mexicana de Criminalística; académico de número de la Academia Mexicana de Ciencias Penales; miembro de la American Academy of Forensic Sciences, de la Association of Firearm and Tool Mark Examiners, de la Asociación Panamericana de Ciencias Forenses y del Instituto Mexicano de Cultura. Adicionalmente, se desempeñó como vicepresidente honorario del capítulo mexicano de la Asociación Latinoamericana de Medicina Legal y Deontología Médica e Iberoamericana de Ciencias Forenses.[7]

Falleció el 7 de marzo de 2021. En una elegía publicada en *El Universal*, Miguel Alemán Velasco apuntó: "En su nombre y su memoria se habrán de conservar sus peritajes como referentes obligados que dieron evidencias contundentes en la lucha permanente en la investigación de los delitos y la impartición de justicia."[8]

Sergio Alonso Rodríguez[9]

[7] "Dr. L. Rafael Moreno González. Síntesis curricular". En https://www.inacipe.gob.mx/assets/docs/investigacion/claustro/Rafael-Moreno-Gonzalez-INACIPE.pdf. Consultado el 13 de abril de 2021.

[8] Alemán Velasco, M., *loc. cit.*

[9] Instituto Nacional de Ciencias Penales.

# TENDENCIAS ACTUALES

# 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*Ni*sed 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_NTS-VVSP.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

# DESPLAZAMIENTO FORZOSO Y DESPLAZAMIENTO INTERNO FORZADO DE PERSONAS. UNA VISIÓN DESDE EL MARCO DE LA POLÍTICA CRIMINAL, LOS DERECHOS HUMANOS Y LA INTELIGENCIA ARTIFICIAL

Eduardo Lozano Tovar*

* Universidad Autónoma de Tlaxcala

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Desplazamiento forzoso** | *Forced displacement* |
| **Derechos humanos** | *Human rights* |
| **Inteligencia artificial** | *Artificial intelligence* |
| **Derecho internacional humanitario** | *International humanitarian law* |
| **Política criminal** | *Criminal policy* |



**Resumen.** La inteligencia artificial, en el ámbito de la política criminal, tiene que jugar un papel importante en la producción de nuevas estrategias para la lucha contra el crimen; de ahí la propuesta contenida en este artículo, consistente en un método de búsqueda de nuevos estándares para el mejoramiento de la realidad social.

**Abstract.** Artificial intelligence in the field of criminal policy must play an important role in the production of new strategies for fighting crime; hence the proposal contained in this article, consisting of a method of searching for new standards for the improvement of social reality.


Fecha de recepción: 20 de enero de 2021
Fecha de aceptación: 15 de abril de 2021

SUMARIO:







## I. INTRODUCCIÓN

Para efectos didácticos de esta investigación, merece la pena considerar que el desplazamiento forzoso y el desplazamiento forzado interno deben ser estudiados desde planos distintos del orden internacional, toda vez que hay elementos diversos que los conforman, y que deben ser tomados en cuenta para entender la diferencia que existe desde el plano conceptual hasta el plano fenomenológico.

En primer lugar, analizaremos el *desplazamiento forzoso de personas*, y para ello aludiremos al artículo 5o. del Estatuto de Roma y los crímenes que son de su competencia. En ese sentido, se debe atender a lo siguiente:

> Artículo 5.
> Crímenes de la competencia de la Corte
> 1. La competencia de la Corte se limitará a los crímenes más graves de trascendencia para la comunidad internacional en su conjunto. La Corte tendrá competencia, de conformidad con el presente Estatuto, respecto de los siguientes crímenes:
> a) El crimen de genocidio;
> b) Los crímenes de lesa humanidad;
> c) Los crímenes de guerra;
> d) El crimen de agresión.
> 2. La Corte ejercerá competencia respecto del crimen de agresión una vez que se apruebe una disposición de conformidad con los artículos 121 y 123 en que se defina el crimen y se enuncien las condiciones en las cuales lo hará. Esa disposición será compatible con las disposiciones pertinentes de la Carta de las Naciones Unidas (Estatuto, 2002).

El artículo citado señala que los crímenes de lesa humanidad —en inglés, *crimes against humanity*—[1] serán de la competencia de la Corte Penal Internacional (CPI), y se desarrollan en el articulado subsecuente del Estatuto:

[1] Deberían traducirse sencillamente como *crímenes en contra de la humanidad*.

Artículo 7.
Crímenes de lesa humanidad
1. A los efectos del presente Estatuto, se entenderá por "crimen de lesa humanidad" cualquiera de los actos siguientes cuando se cometa como parte de un ataque generalizado o sistemático contra una población civil y con conocimiento de dicho ataque:
a) Asesinato;
b) Exterminio;
c) Esclavitud;
d) Deportación o traslado forzoso de población;
e) Encarcelación u otra privación grave de la libertad física en violación de normas fundamentales de derecho internacional;
f) Tortura;
g) Violación, esclavitud sexual, prostitución forzada, embarazo forzado, esterilización forzada o cualquier otra forma de violencia sexual de gravedad comparable;
h) Persecución de un grupo o colectividad con identidad propia fundada en motivos políticos, raciales, nacionales, étnicos, culturales, religiosos, de género definido en el párrafo 3, u otros motivos universalmente reconocidos como inaceptables con arreglo al derecho internacional, en conexión con cualquier acto mencionado en el presente párrafo o con cualquier crimen de la competencia de la Corte;
i) Desaparición forzada de personas;
j) El crimen de apartheid;
k) Otros actos inhumanos de carácter similar que causen intencionalmente grandes sufrimientos o atenten gravemente contra la integridad física o la salud mental o física.
2. A los efectos del párrafo 1:
a) Por "ataque contra una población civil" se entenderá una línea de conducta que implique la comisión múltiple de actos mencionados en el párrafo 1 contra una población civil, de conformidad con la política de un Estado o de una organización de cometer ese ataque o para promover esa política;
b) El "exterminio" comprenderá la imposición intencional de condiciones de vida, entre otras, la privación del acceso a alimentos o medicinas, entre otras, encaminadas a causar la destrucción de parte de una población;
c) Por "esclavitud" se entenderá el ejercicio de los atributos del derecho de propiedad sobre una persona, o de algunos de ellos, incluido el ejercicio de esos atributos en el tráfico de personas, en particular mujeres y niños;
d) Por "deportación o traslado forzoso de población" se entenderá el desplazamiento forzoso de las personas afectadas, por expulsión u otros actos coactivos, de la zona en que estén legítimamente presentes, sin motivos autorizados por el derecho internacional;
e) Por "tortura" se entenderá causar intencionalmente dolor o sufrimientos graves, ya sean físicos o mentales, a una persona que el acusado tenga bajo su custodia o control; sin embargo, no se entenderá por tortura el dolor o los sufrimientos que se deriven únicamente de sanciones lícitas o que sean consecuencia normal o fortuita de ellas;
f) Por "embarazo forzado" se entenderá el confinamiento ilícito de una mujer a la que se ha dejado embarazada por la fuerza, con la intención de modificar la composición étnica de una población o de cometer otras violaciones graves del derecho internacional. En modo

> alguno se entenderá que esta definición afecta a las normas de derecho interno relativas al embarazo;
> g) Por "persecución" se entenderá la privación intencional y grave de derechos fundamentales en contravención del derecho internacional en razón de la identidad del grupo o de la colectividad;
> h) Por "el crimen de apartheid" se entenderán los actos inhumanos de carácter similar a los mencionados en el párrafo 1, cometidos en el contexto de un régimen institucionalizado de opresión y dominación sistemáticas de un grupo racial sobre uno o más grupos raciales y con la intención de mantener ese régimen;
> i) Por "desaparición forzada de personas" se entenderá la aprehensión, la detención o el secuestro de personas por un Estado o una organización política, o con su autorización, apoyo o aquiescencia, seguido de la negativa a admitir tal privación de libertad o dar información sobre la suerte o el paradero de esas personas, con la intención de dejarlas fuera del amparo de la ley por un período prolongado.
> 3. A los efectos del presente estatuto se entenderá que el término "género" se refiere a los dos sexos, masculino y femenino, en el contexto de la sociedad. El término "género" no tendrá más acepción que la que antecede (Estatuto, 2002).

A la luz de lo plasmado en el Estatuto de Roma, por desplazamiento forzoso de población se entenderá el desplazamiento forzoso de las personas afectadas por expulsión u otros actos coactivos de la zona en que estén legítimamente presentes, sin motivos autorizados por el derecho internacional; es ahí donde tenemos el primer concepto que sobre este tema debe ser considerado para el estudio de esta conducta como crimen en contra de la humanidad.

Asimismo, respecto de la jurisprudencia de la CPI, hay un aspecto que debe ser tomado en cuenta, el cual se describe en los siguientes criterios:

> Las Salas de Primera Instancia del Tribunal han sostenido en varias sentencias que la deportación se define como el desplazamiento forzado de personas por expulsión u otros actos coercitivos del área en la que están legalmente presentes, a través de una frontera nacional, sin fundamentos legales […] La Sala de Primera Instancia está de acuerdo con estos hallazgos (CPI, 2003).

La Sala de Primera Instancia, por mayoría de votos, está convencida de que el *actus reus* de "deportación", según el artículo 5 (d) del Estatuto, consiste en el desplazamiento forzado de personas a través de una frontera estatal, desde el área en la que están legalmente presentes, sin motivos permitidos bajo el derecho internacional (CPI, 2004).

Así, a la vera de los criterios emanados de la jurisprudencia de la CPI, se puede identificar un elemento clave para diferenciar el desplazamiento

forzoso de población con el desplazamiento forzado interno de personas, ya que la CPI ha estimado que el primer criterio atiende al desplazamiento que se da a través de una frontera estatal, situación que amplía el panorama desde el cual debe considerarse el concepto que el Estatuto de Roma brinda desde su interpretación literal y estricta, y, desde el punto de vista político-criminal internacional (prevención y represión), el alcance del estatuto solamente se extiende a las personas que son desplazadas forzosamente a través de una frontera internacional, haciendo necesaria la construcción de un instrumento internacional que extienda su protección a las personas internamente desplazadas.

En ese sentido, desde una visión político-criminal se puede apreciar una clara distinción entre el desplazamiento forzoso de población y el desplazamiento interno forzado de personas, aunque, para obtener una distinción más clara de esta disparidad en los conceptos, tendríamos que atender a la Convención de la Unión Africana para la Protección y la Asistencia de los Desplazados Internos en África ([CUAPADIA] Convención de Kampala), en la cual se construyen dos conceptos que constituyen una medida de política criminal que auxilia a los Estados a encontrar los mecanismos para la prevención y la represión de las conductas que llevan a las personas a desplazarse, conceptos que, a la vez, dan claridad respecto de la diferencia entre el marco conceptual analizado, los cuales se sujetan a lo siguiente, conforme al artículo 1 (incisos k y l) de ese documento:

> k. Se entiende por "desplazados internos" a las personas o grupos de personas que se ven forzadas u obligadas a huir, a abandonar sus hogares o lugares de residencia habitual, en particular como resultado de, o en el fin de evitar, los efectos del conflicto armado, de situaciones de violencia generalizada, de violaciones de los derechos humanos o de catástrofes naturales o producidas por el ser humano, y que no han cruzado una frontera de Estado internacionalmente reconocida;
> l. Se entiende por "desplazamiento interno" el movimiento involuntario o forzado, la evacuación o la reubicación de personas o grupos de personas dentro de las fronteras de Estado internacionalmente reconocidas (CUAPADIA, 2012).

En consecuencia, se desprende que los mismos sujetos, como medida de política criminal, deciden huir o dejar su lugar de residencia habitual para evitar ser alcanzados por los efectos de la violencia generalizada por la que atraviesa el Estado (represión); todo ello tiene que ver con la inacción del Estado sobre tomar disposiciones de prevención y represión en un

contexto sistemático y generalizado de violencia y, en general, en un conflicto armado.

De lo dispuesto por el ordenamiento anterior que, dicho sea de paso, ha sido el primero que hace las veces de *hard law* en el derecho regional, como enteramente vinculante a una cuestión de desplazamientos internos (Pérez *et al.,* 2019: 15) —y que juega un papel importante para la prevención de la violencia del ser humano—, es en ese punto donde se pueden comprender las consideraciones de lo que debemos entender por desplazamiento interno, y de lo que se tiene que entender por desplazados internos.

Así, el desplazamiento forzoso de población es construido a partir de la consideración de que ese fenómeno se da en un radio que supera las fronteras del país en el que se encuentran legalmente presentes las personas, debido a su expulsión u otros actos coactivos.

En tanto, el desplazamiento forzado interno de personas no sobrepasa las fronteras del Estado en donde las personas se encuentran legalmente constituidas; esto es, son personas que, si bien huyen de un determinado fenómeno (en particular como resultado de, o con el fin de evitar, los efectos del conflicto armado, de situaciones de violencia generalizada, de violaciones de los derechos humanos o de catástrofes naturales o producidas por el ser humano), no han cruzado una frontera de Estado internacionalmente reconocida (CUAPADIA, 2012).

## II. CONTEXTO DEL TEMA DE ESTUDIO EN MÉXICO

Una vez delimitado el marco conceptual que existe entre el desplazamiento forzoso de población y el desplazamiento forzado interno, es necesario establecer que, para poder comenzar con el estudio del tema en cuestión, es imprescindible hacer un análisis breve sobre las causas que han desarrollado un problema de gran magnitud, de tal suerte que hasta estos días se puede constatar, no solamente como un fenómeno latente y que en los últimos años ha tomado cada vez más relevancia en la discusión pública, sino más bien como un fenómeno en crecimiento, que, a su vez, no ha encontrado un esquema que permita al Estado garantizar una solución a corto y mediano plazo a través de criterios que deben ser atendidos por la política criminal.

Pareciera que la opinión pública se ha inclinado hacia la discusión de los desplazamientos forzosos de la población y los desplazamientos internos

forzados de personas en la última década, con la aparición de movimientos sociales tales como las caravanas migrantes, que encuentran en México un país de mero tránsito que les permita su llegada a los Estados Unidos de América, aunque el desplazamiento forzoso de población es un tema que encuentra su explicación desde hace décadas en México, como un problema que ha trascendido a lo largo de generaciones.

Debe considerarse que este fenómeno no solamente ha avanzado desde fuera hacia dentro de las fronteras de nuestro país, sino que es un problema que se ha mantenido en la memoria del último siglo. Por ejemplo, desde la década de 1970 ya se podía percibir una tendencia clara sobre desplazamientos internos forzados dentro del Estado mexicano, en acontecimientos que tenían una relación con la intolerancia religiosa (CNDH, 1994), que por mucho tiempo fue un factor de discriminación en México de parte de grupos católicos (en su mayoría, que a su vez tenían, por supuesto, un mayor número de seguidores), en contra de las comunidades indígenas, por un lado y, por el otro, de los grupos protestantes que han ganado una mayor representación en la población mexicana. Asimismo, esta situación encuentra sus orígenes en los distintos conflictos sociales que se relacionan con problemáticas meramente comunales y conflictos por predios y recursos naturales, entre otros (CMDPDH, 2014: 3).

En ese tenor, habría que atender a los distintos movimientos sociales que se originaron hace varios lustros, debido a que es en cada uno de ellos en donde encontramos comportamientos específicos que derivan en desplazamientos internos forzados; una muestra de ello es el movimiento del Ejército Zapatista de Liberación Nacional (EZLN), surgido en 1994 en Chiapas, que dio lugar al desplazamiento de alrededor de 30,000 personas, quienes se encontraron en un desplazamiento forzado prolongado (CMDPDH, 2014: 3).

La información apuntada debe llevarnos a considerar que, en cada movimiento social que conlleva a un conflicto armado, el Estado debe estudiar uno de los rubros más relevantes: la situación de desplazamientos internos forzados, que resultan como consecuencia directa de los hechos victimarios que detonan la necesidad de las personas de abandonar su lugar de origen, o bien, donde se encontraban asentados antes de tener que huir de tal territorio.

El Estado debe, además, estudiar las causales de dichos desplazamientos, a fin de aplicar políticas criminales que permitan evitar tales contextos de violencia generalizada para prevenir los desplazamientos forzados.

Dicho esto, es necesario que el Estado atienda tales cuestiones, debido a que se encuentra obligado a promover, respetar, proteger y garantizar los derechos humanos de todas las personas que se encuentren en el territorio mexicano (CPEUM, 2020).

Asimismo, se deben poner en marcha los distintos mecanismos tendentes a emplear sistemas de inteligencia artificial que detonen un nuevo esquema de prevención del delito en el Estado mexicano, como forma de dar cumplimiento a sus obligaciones, señaladas en el párrafo anterior.

En este escenario, debemos determinar lo imprescindible de hacer alusión al fenómeno que se estudia desde un punto de vista cualitativo, que permita una comprensión de las verdaderas dimensiones de la problemática que debe atender el Estado mexicano en aras de salvaguardar los derechos humanos; es así como impacta en el aparato de gobierno el contar con estadísticas que permitan dar prioridad a asuntos que le son atribuibles desde el punto de vista del derecho internacional, para evitar caer en una responsabilidad ante distintos tribunales internacionales, derivada de conductas contrarias a los tratados internacionales en derechos humanos de los que el Estado mexicano es parte.

Cabe señalar que, como se ha mencionado en otros textos (Lozano, 2010 y 2020), los instrumentos que permiten medir la percepción de la realidad que se vive en México sobre la situación de ciertos delitos de gran relevancia, no son los más idóneos para obtener mediciones aceptables respecto de lo que ocurre para su posible abordamiento.

Y sin lugar a controversia, esa es la situación de los instrumentos utilizados para la medición de los desplazamientos internos forzados en México, que calculan —según mediciones de la sociedad civil— en 6.76 el porcentaje de personas que se encuentran en el territorio mexicano, y que se han visto obligadas a abandonar su lugar de residencia como resultado de la situación de violencia. Lo anterior, de acuerdo con información arrojada por la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) (Pérez *et al.*, 2019: 12).

Con los datos que anteceden, se puede tener una idea de la importancia del tema que se discute en estas líneas, así como de los espacios de investigación que estén encaminados a buscar nuevos rumbos que exploren la situación real que los desplazamientos internos forzados juegan en el rol de las personas establecidas en el territorio mexicano, y la situación de desplazamiento forzoso que aqueja a una gran parte de la sociedad centro y sudamericana, que se encuentra obligada a huir de sus países de origen y

encontrar en México un país de tránsito en la búsqueda del cada vez más ilusorio "sueño americano".

Si el Estado no cuenta con mecanismos de medición adecuados respecto de los desplazamientos forzados internos acompañados de esquemas de inteligencia artificial, se encuentra incapacitado para realizar un diagnóstico general, que permita, a su vez, que desde la dogmática jurídico-penal se construyan esquemas efectivos de política criminal que puedan ser determinantes en la erradicación del contexto que lleva a las personas a desplazarse, y que, derivado de la situación de vulnerabilidad en la que se encuentran, sean revictimizadas durante el proceso de desplazamiento. Asimismo, en el Estado queda reflejada la incapacidad para crear planes y programas que generen condiciones para dar atención a las personas internamente desplazadas.

Tales planes y programas tienen que ser implementados desde el marco de la inteligencia artificial; por ejemplo, debe insistirse en la creación de una plataforma digital que permita al Estado mexicano obtener datos certeros sobre las personas internamente desplazadas, en un primer momento, para poder garantizar el respeto al derecho a la personalidad jurídica de tales personas y, en segundo lugar, sería fructífero que tal plataforma fuera desarrollada para poder transmitir la evolución del desplazamiento de las personas, y que tuviera la capacidad de determinar por sí misma el número de insumos necesarios y de recursos humanos pertinentes para aportar apoyo humanitario en distintas fases del trayecto, como modelo de prevención del fenómeno delictivo.

Además de que, en tiempos de pandemia, se tiene que garantizar el derecho al acceso a la salud de las personas desplazadas, en el entendido de que el organismo dedicado a atender a la migración podría llevar a cabo la operación de esta plataforma a partir de distintos puntos de atención en toda la república, con miras, también, a saber cuántas personas que se encuentran en esta situación están afectadas por la COVID-19 y, en ese tenor, la plataforma debería tener la capacidad de calcular los materiales necesarios para poder aportar sistemas de alerta, que permitan que los espacios que carecen de tales materiales sean provistos de todo lo necesario para atender a los desplazados.

Incluso, el Poder Legislativo debería considerar elevar a rango constitucional la obligación del Estado de mantener un plan de política criminal transexenal, el cual permita a las personas conocer cuáles serán los criterios que los gobiernos tendrán que seguir para prevenir y reprimir el delito,

para que, con el auxilio de la dogmática jurídico-penal, se construya una mejor realidad social no solo para los desplazados, sino para todas las personas que se encuentran en México.

## III. CRITERIOS RELEVANTES DE LA CORTE IDH





Ahora, después del abordaje conceptual de la temática que interesa en el presente documento, se debe establecer una conexión entre la realidad sociológica mexicana, en el espacio de los desplazamientos internos forzados de personas, y la realidad que otros países tienen con los mismos fenómenos. Todo ello, a fin de realizar ejercicios de derecho comparado que permitan una visión de política criminal y derechos humanos para que, eventualmente, se puedan adaptar distintas medidas que garanticen la prevención y la no repetición de los hechos que son del conocimiento de tribunales internacionales, tribunales que, con sus criterios, dan un sendero a los Estados para poder prevenir y erradicar estos eventos de manera contundente, y sancionar a los culpables que ejecutan dichas conductas.

Sobre esta base reflexiva, abordaremos parte de los criterios que la Corte Interamericana de Derechos Humanos (Corte IDH) ha establecido sobre desplazamientos internos forzados y sus consideraciones jurídicas respecto de la afectación que se genera a los derechos humanos.

En el caso *Chitay Nech y otros vs. Guatemala*, la Corte IDH realizó un análisis de lo establecido por la Convención Americana sobre Derechos Humanos (CADH), cuyo artículo 22 indica:

> Artículo 22. Derecho de Circulación y de Residencia
> 1. Toda persona que se halle legalmente en el territorio de un Estado tiene derecho a circular por el mismo y a residir en él con sujeción a las disposiciones legales.
> 2. Toda persona que tiene derecho a salir libremente de cualquier país, inclusive del propio.
> 3. El ejercicio de los derechos anteriores no puede ser restringido sino en virtud de una ley, en la medida indispensable en una sociedad democrática, para prevenir infracciones penales o para proteger la seguridad nacional, la seguridad o el orden públicos, la moral o la salud públicas o los derechos y libertades de los demás.
> 4. El ejercicio de los derechos reconocidos en el inciso 1) puede asimismo ser restringido por la ley, en zonas determinadas, por razones de interés público.
> 5. Nadie puede ser expulsado del territorio del Estado del cual es nacional, ni ser privado del derecho a ingresar en el mismo.
> 6. El extranjero que se halle legalmente en el territorio de un Estado Parte en la presente Convención, sólo podrá ser expulsado de él en cumplimiento de una decisión adoptada conforme la ley.

> 7. Toda persona tiene el derecho de buscar y recibir asilo en territorio extranjero, en caso de persecución por delitos políticos o comunes conexos con los políticos y de acuerdo con la legislación de cada Estado y los convenios internacionales.
> 8. En ningún caso el extranjero puede ser expulsado o devuelto a otro país, sea o no de origen, donde su derecho a la vida o a la libertad personal está en riesgo de violación a causa de raza, nacionalidad, religión, condición social o de sus opiniones políticas.
> 9. Es prohibida la expulsión colectiva de extranjeros (CADH, 1969).

En este artículo se plasma el reconocimiento del instrumento respecto del derecho de circulación y de residencia (Corte IDH, 2010); tal reconocimiento ha sido referido por la Corte para determinar que el ordenamiento en cuestión protege el derecho a no ser desplazado forzadamente dentro de un Estado Parte (Corte IDH, 2010).

Desde esta consideración, se debe indicar que la sentencia de la Corte IDH, en el caso *Chitay Nech y otros vs. Guatemala*, tiene como punto medular lo siguiente: el Tribunal ha considerado que los Principios Rectores de los Desplazamientos Internos de las Naciones Unidas resultan particularmente relevantes para determinar el contenido y alcance del artículo 22 de la Convención Americana, principios que definen lo que sigue:

> (…) se entiende por desplazados internos las personas o grupos de personas que se han visto forzadas u obligadas a escapar o huir de su hogar o de su lugar de residencia habitual, en particular como resultado o para evitar los efectos de un conflicto armado, de situaciones de violencia generalizada, de violaciones de los derechos humanos […], y que no han cruzado una frontera estatal internacionalmente reconocida (Corte IDH, 2010: párr. 140).

El fragmento anterior se caracteriza por el desarrollo de un estándar de derecho internacional que invoca como su base los aludidos principios rectores, en el sentido de que se toma en cuenta que tales principios sirven de lo que en derecho internacional se conoce como *soft law*, que, a pesar de ser un criterio no vinculante, determina el contenido y el alcance del artículo 22 de la CADH, en aras de proporcionar una definición de lo que se debe entender por "desplazados internos".

Resulta necesario para la Corte enlazar sus criterios con los principios aludidos, ya que fueron fruto del trabajo que, a petición de la entonces Comisión de Derechos Humanos de las Naciones Unidas, se llevó a cabo desde 1992, y donde la Secretaría General nombró un representante que tuvo a su cargo la investigación del fenómeno del desplazamiento interno forzado de personas, investigación que ha tenido un impacto en la apreciación que los mismos Estados han tenido sobre este fenómeno. Por lo

anterior, la Corte IDH determinó establecer la definición que se considera a continuación:

> 2. A los efectos de estos Principios, se entiende por desplazados internos las personas o grupos de personas que se han visto forzadas u obligadas a escapar o huir de su hogar o de su lugar de residencia habitual, en particular como resultado o para evitar los efectos de un conflicto armado, de situaciones de violencia generalizada, de violaciones de los derechos humanos o de catástrofes naturales o provocadas por el ser humano, y que no han cruzado una frontera estatal internacionalmente reconocida (ONU, 1998).

De lo anterior se desprende que la Corte IDH consideró, en esa línea argumentativa, que los desplazamientos internos forzosos guardan especial relación con la situación de vulnerabilidad que tiene la mayoría de las personas desplazadas, lo cual constituye una condición *de facto* de desprotección (Corte IDH, 2010, párr. 141); en ese sentido, hay que recalcar que el documento que presenta los Principios Rectores de los Desplazamientos Internos de las Naciones Unidas comienza con una nota introductoria, que posiciona el aspecto de la vulnerabilidad de las personas como un eje central que debe ser observado, tal como se señala a continuación:

> Nota de presentación de los Principios Rectores.
> 1. Existe hoy día el convencimiento general de que los desplazamientos internos, que afectan en todo el mundo a más de 25 millones de personas, se han convertido en uno de los fenómenos más trágicos de nuestro tiempo. Los desplazamientos, consecuencia habitual de experiencias traumáticas de conflictos violentos, violaciones manifiestas de los derechos humanos y causas similares en las que la discriminación tiene un papel significativo, generan casi siempre condiciones de sufrimiento y penalidad para las poblaciones afectadas. Provocan la ruptura familiar, cortan los lazos sociales y culturales, ponen término a relaciones de empleo sólidas, perturban las oportunidades educativas, niegan el acceso a necesidades vitales como la alimentación, la vivienda y la medicina, y exponen a personas inocentes a actos de violencia en forma de ataques a los campamentos, desapariciones y violaciones. Los desplazados internos, tanto si se agrupan en campamentos como si huyen al campo para ponerse al abrigo de posibles fuentes de persecución y violencia o se sumergen en comunidades igualmente pobres y desposeídas, cuentan entre las poblaciones más vulnerables y más necesitadas de protección y asistencia (ONU, 1998).

En otros casos, la Corte IDH ha señalado que esa desprotección debe entenderse como una condición individual respecto de las personas que se encuentran en situaciones semejantes; en ese entendido, también debe atenderse a la consideración de la Corte sobre que la vulnerabilidad tiene una dimensión social que se relaciona estrechamente con el contexto

histórico del país en el cual el fenómeno se desarrolla (Corte IDH, 2015: párr. 177).

Así las cosas, se debe atender a que existe una situación diferenciada en la que están inmersos los desplazados, situación que debe obligar a los Estados a tomar medidas para revertir los efectos de tal vulnerabilidad (Corte IDH, 2015: párr. 179, y Corte IDH, 2010: párr. 141). Además, llama la atención que el análisis de la Corte señale que es deber del Estado tomar medidas de carácter positivo para revertir los efectos de la condición en la que se encuentran, incluso *vis à vis*, actuaciones y prácticas de terceros particulares (Corte IDH, 2015: párr. 179).

Ese criterio debe llamar la atención, porque presupone una aportación doctrinal en el sistema regional de derechos humanos, en el que los instrumentos de protección de estos amplían su protección, no solo contra actos del Estado que vulneran derechos humanos, sino que, además, sostiene un planteamiento sobre la eficacia de aquellos en las relaciones entre particulares.

Con lo anterior, de ninguna manera se quiere decir que el criterio señalado en la jurisprudencia de la Corte IDH sean el único ni el primer estándar desarrollado por este órgano en este sentido (Corte IDH, 1988); lo que sí se argumenta en estas líneas, es que el tribunal continental sigue sosteniendo una doctrina en la que el alcance de la protección de los derechos humanos trasciende incluso las fronteras de los actos del Estado para permear también los de las propias personas. Incluso, la Corte ha señalado, sobre el tema abordado, lo que sigue:

> 62. Podría, sin embargo, argumentarse que la circunstancia de que la Corte considere, por vía de inferencia, que la detención de la víctima fue ilegal, debería llevarla, igualmente, a concluir que hubo una violación del derecho a la vida por parte de Surinam porque, de no haber sido detenida la persona, probablemente no habría perdido la vida. Sin embargo, la Corte piensa que en materia de responsabilidad internacional de los Estados por violación de la Convención [l]o decisivo es dilucidar si una determinada violación a los derechos humanos reconocidos por la Convención ha tenido lugar con el apoyo o tolerancia del poder público o si éste ha actuado de manera que la transgresión se haya cumplido en defecto de toda prevención o impunemente.
>
> En definitiva, de lo que se trata es de determinar si la violación a los derechos humanos resulta de la inobservancia por parte de un Estado de sus deberes de respetar y garantizar dichos derechos, que le impone el artículo 1.1 de la Convención (Caso Velásquez Rodríguez, supra 49, párr. 173; Caso Godínez Cruz, supra 49, párr. 183). En las circunstancias de este caso, no es posible fijar la responsabilidad del Estado en los términos descritos, en virtud, entre otras razones, de que la Corte está determinando una responsabilidad por detención ilegal por inferencia y no porque haya sido demostrado que la detención fue, en

> efecto, ilegal o arbitraria o que el detenido haya sido torturado. Y así lo declara (Corte IDH, 1994).

Lo que se debe hacer notar en el criterio anterior de la Corte IDH, es que se debe determinar la responsabilidad internacional de la violación a derechos humanos resultante de la inobservancia por parte de un Estado de medidas de prevención, que de manera natural constituyen esquemas basados en política criminal y, en consecuencia, del deber de respetar y garantizar los derechos humanos a la luz de la CADH.

En ese sentido, es inevitable señalar que el Estado mexicano debe adoptar una serie de medidas que se encaminen a la prevención del fenómeno de los desplazamientos forzosos, lo cual no se puede lograr si no es a través de estudios dogmáticos en política criminal y criminológica, fundamentando tales medidas en la jurisprudencia de la Corte IDH, toda vez que en ese supuesto se podrá construir un esquema de protección a los desplazados con una perspectiva de derechos humanos y política criminal, permitiendo que el Estado encuentre la forma de reducir los casos de violaciones a la dignidad humana de las personas desplazadas y de delitos cometidos en contra de estas.

## IV. CRITERIOS RELEVANTES UTILIZADOS POR LA CRUZ ROJA INTERNACIONAL

El 17 de mayo de 2016, el Comité Internacional de la Cruz Roja (CICR) aprobó un documento que aporta mucho al combate del desplazamiento interno de las personas, el cual previó una duración que abarca el periodo 2016-2019. Esta contribución, intitulada *Desplazamientos internos: estrategia del CICR para 2016-2019*, es digna de ser atendida, debido a que motiva la búsqueda de una mejor respuesta operacional —así se le denomina en el documento—, que puede recogerse como un criterio que el Estado mexicano debería observar para ampliar su respuesta en la protección de los derechos humanos de las personas internamente desplazadas.

En dicho documento se contextualiza la problemática de las partes en conflicto, y los intentos que los Estados y la comunidad internacional han hecho para tratar de erradicar la presencia de desplazamientos, además de ofrecer soluciones a las personas que han sido desplazadas (CICR, 2019).

El análisis del CICR se realiza desde una perspectiva en la que se plasma la preocupación por el fracaso de las medidas implementadas a nivel internacional para el combate a esta problemática, toda vez que se ha develado que incluso los conflictos armados han desarrollado, dentro de sus características, ser cada vez más prolongados y crónicos.

Sobre esa misma línea, habrá que destacar que el CICR encuentra que, dentro de los debates sobre este tema, se ha concordado que entre las causales del desplazamiento se encuentran las raíces de los conflictos armados, sin mirar las causas de los desplazamientos internos durante los conflictos armados (CICR, 2019).

Lo anterior presupone que, cuando se pone a discusión el tema de las causales de los desplazamientos forzosos, se tiende a dejar de lado en el análisis —como ya se dijo— la temporalidad de los conflictos armados. La consideración anterior no pone en tela de juicio si los desplazamientos encuentran sus orígenes en conflictos armados, sino que, más bien, atiende a los momentos en que se estudian los desplazamientos; así, deben estudiarse, en un primer momento, las raíces de un conflicto armado como causal primordial de los desplazamientos en un determinado lugar, relacionándolo con una población determinada y, en ese sentido, continuar el análisis durante el desarrollo del conflicto. Derivado de ello, se ha percibido por parte del CICR que ha existido:

> (…) una falta de reconocimiento en la relación entre violaciones del Derecho Internacional Humanitario (DIH) y los desplazamientos; en consecuencia, el compromiso de la comunidad internacional en general con los Estados y las partes en conflicto a menudo no ha destacado la necesidad de respetar y hacer respetar el DIH y prevenir, en primer lugar, los desplazamientos (CICR, 2019).

Una vez más se hace hincapié en que los Estados no han adoptado medidas para respetar y hacer respetar el DIH, aunque se destaca por parte del CICR que la acción primordial debe ser llevada a cabo a través de la prevención. Esto es, que en principio el Estado, si tiene la voluntad de realizar acciones para erradicar los desplazamientos, debe empezar materializando esquemas que permitan la prevención de aquellos, lo cual debe integrar medidas basadas en criterios político-criminales.

En este sentido, es prudente señalar que de ninguna manera se sugiere que la única causal de los desplazamientos sean los conflictos armados, toda vez que el documento que se ha ocupado para abordar la perspectiva del comité, de igual forma ha mencionado que, desde hace mucho tiempo,

se han hecho esfuerzos para brindar protección y asistencia a las personas internamente desplazadas, en el marco del cometido que tiene la Cruz Roja de ayudar a las personas afectadas por los conflictos armados y otras situaciones de violencia.

Cuando el comité se refiere a las personas afectadas por otras situaciones de violencia, se refiere a un estándar que se desarrolló en 2014 en un documento denominado *El papel del Comité Internacional de la Cruz Roja (CICR) en situaciones de violencia que no alcanzan el umbral de los conflictos armados*, y que tiene como función primordial desarrollar el estándar de interpretación de lo que se debe entender por "otras situaciones de violencia", y cuáles son exactamente esas situaciones.

Dentro de ese esquema, habrá que señalar que el comité comienza el análisis de las otras situaciones de violencia, argumentando que se debe establecer una diferencia primordial entre los conceptos de conflictos armados no internacionales, y los de otras situaciones de violencia colectiva, para determinar no solamente la ley que le será aplicable, sino la fuente de la misión que deberá atender el CICR (IRRC, 2014: 278).

Además, dentro de las situaciones que abarcan la violencia colectiva, destacan dos supuestos que son analizados por el comité:

> 1.- Los disturbios internos.
> Esto implica situaciones en las cuales no hay un conflicto armado no internacional como tal, pero existe una confrontación dentro del país, que se caracteriza por una cierta seriedad o duración y que implica actos de violencia. Estos últimos pueden asumir diversas formas, desde la generación espontánea de actos de revuelta a la lucha entre grupos más o menos organizados y las autoridades en el poder.
> En estas situaciones, que no necesariamente se generan en una lucha abierta, las autoridades en el poder recurren a amplias fuerzas policiales, o incluso fuerzas armadas, para restablecer el orden interno. El alto número de víctimas hace necesaria la aplicación de un mínimo de normas humanitarias (IRRC, 2014: 279).
> 2.- Las tensiones internas.
> Se podría decir que incluyen en particular situaciones de grave tensión (política, religiosa, racial, social, económica, etc.), pero también las secuelas de conflictos armados o de disturbios internos. Tales situaciones pueden tener una o más de las siguientes características, si no es que todas al mismo tiempo:
> -Arrestos a gran escala;
> -Un gran número de presos "políticos";
> -La probable existencia de malos tratos o condiciones inhumanas de detención;
> -La suspensión de garantías judiciales fundamentales, ya sea como parte de la promulgación de un estado de emergencia o simplemente de hecho;
> -Denuncias de desapariciones (IRRC, 2014: 279).

Estas definiciones no figuran en una convención o tratado, sino que forman parte de la doctrina del CICR. Si bien están diseñadas para un uso práctico, pueden servir para argumentar sobre estos términos que aparecen en un instrumento de derecho internacional por primera vez (IRRC, 2014: 279).

Por tanto, resulta necesario que los Estados atiendan a este tipo de estándares, ya que, aunque no sean vinculantes, dotan de contenido, a través de un estándar, a un determinado derecho humano, que, a la vera de la CADH, para el caso de los Estados americanos, este instrumento internacional carece de sentido jurídico.

La relación que existe entre estos conceptos y la operatividad que se sostenía al principio es clara, ya que, para identificar las posibles vías de prevención del desplazamiento forzado interno, es útil que los Estados conozcan qué tipo de violencia es la que se está suscitando, derivada de cualquier acontecimiento. En ese sentido, a lo largo del siglo XX el CICR intensificó gradualmente sus actividades en situaciones en las que el DIH no era aplicable, y modificó el marco de sus actividades en tales situaciones, a la luz de su práctica y textos de referencia interna. Esos textos internos afirman que, además de la calificación legal de la situación, "la existencia o la probabilidad de situaciones humanitarias graves es suficiente para justificar la oferta de servicios" (IRRC, 2014: 283).

Es por la necesidad de intervención para la oferta de servicios que el comité ha llevado a cabo las medidas necesarias para poder extender la justificación de esa oferta, con miras a poder generar las condiciones de poder respetar y hacer respetar el derecho internacional humanitario.

Lo anterior abre la puerta a que, en el caso del Estado mexicano, se adopten medidas que permitan una mejor respuesta operacional con fundamento en los criterios del CICRI, aunado a las aportaciones que el propio Estado pueda desarrollar conforme a su realidad social y, en este caso, el desarrollo de tecnologías que permitan que, mediante esquemas de inteligencia artificial, se facilite su tarea; por ejemplo, el Estado puede:

1. Añadir una perspectiva desde el plano de la victimología, reconociendo que la asistencia que el Estado debe prestar no solamente debe ser extendida a las víctimas directas, sino que se debe llevar a cabo un estudio de las personas que han sido afectadas, derivado del fenómeno de desplazamiento del que se trate, recabando los datos en una plataforma digital que opere el Estado, y desarrollando una aplicación para que los servidores públicos encargados de brindar atención tengan la oportunidad de tener datos certeros y, de igual forma, actualicen los datos de las personas atendidas de forma inmediata.

A lo anterior se suma el hecho de que todas las víctimas tienen necesidades particulares que deben ser identificadas en aras de poder establecer distintos esquemas que permitan garantizar la protección de los derechos humanos.

De igual forma, la razón primordial de ser de la plataforma sería la identificación de las personas internamente desplazadas, aumentando la capacidad de respuesta del Estado para atender a la colaboración internacional de búsqueda de connacionales, y ayudar a evitar que las personas desaparezcan. Lo anterior conlleva una medida de política criminal que permite prevenir que surjan distintas conductas delictivas contra la población que es internamente desplazada, o de las personas referidas entre sí.

En ese tenor, la plataforma que estamos planteando tendría que tener la capacidad de poder llevar a cabo distintos análisis, con base en las estadísticas de las cifras del Estado mexicano para ayudar a prevenir la desaparición de los desplazados; dicho de otro modo, tendría que tener la capacidad de que, con base en cifras de inseguridad, la plataforma pueda predecir cuántas personas son susceptibles de ser desaparecidas, y hacer una estimación de los lugares del país en donde esa susceptibilidad pueda ayudar a la autoridad a ganar tiempo, en caso de la consumación de un delito de esta naturaleza.

2. El Estado tiene que construir esquemas de protección para las personas internamente desplazadas, en los que no solamente se atienda a la problemática desde fases aisladas, sino desde una mirada integral, en donde el Estado estudie todas las fases del desplazamiento, como lo son desde las circunstancias precedentes hasta el regreso, la integración local o el reasentamiento de las personas.

3. Se debe poner la mirada en la prevención de la problemática de los desplazamientos forzados, enfocándose en las causales del fenómeno, lo cual funciona como una política criminal eficaz, prestando atención, así, a la prevención como una medida fundamental para la erradicación del desplazamiento forzado. Es claro que el trabajo empieza por la prevención, aunque, cuando los desplazamientos se detonan por cualquier conflicto armado u otras formas de violencia que no sobrepasan el umbral de un conflicto armado, se deben adoptar operaciones conjuntas que den seguimiento a la prevención de múltiples desplazamientos producto de los que ya existen, siguiendo así una política criminal internacional (de prevención y represión), evitando su multiplicación.

Además, en el caso de la presencia de un conflicto armado, el Estado debe garantizar la entrada de cuerpos que permitan la protección de las personas que integran a la población civil, para protegerlas de hostilidades por parte de otros grupos.

4. El Estado debe facilitar las condiciones para que se adapten diversas zonas de acogida para que las personas internamente desplazadas puedan, eventualmente, acceder a servicios básicos, y que en las zonas remotas se pueda contar con personal de asistencia para aminorar los efectos del desplazamiento.

Por otro lado, se debe llevar a cabo una gestión necesaria de campamentos, aunque esto no haya de considerarse una solución predeterminada para los desplazamientos (Perrín, 1998).

Cabe señalar que es necesario comenzar a elaborar un andamiaje legal, a través de un esquema de inteligencia artificial desarrollado por una plataforma digital que permita la construcción de un aparato encargado

de individualizar e identificar a las personas víctimas de desplazamiento en México, para que así el Estado cuente virtualmente con la información necesaria para estar en aptitud de encontrar una mejor respuesta operacional, ya que, través de la identificación de las personas, sería más fácil conocer las necesidades particulares de cada individuo desplazado y, con ello, llevar a cabo distintos programas de acompañamiento que sean realmente eficaces.

En ese sentido, hay que señalar que es imprescindible que tales procesos, de identificación y de apoyo en servicios, se brinden a través de las condiciones de acogida ya señaladas, y que la operación de la plataforma sea operada por los servidores públicos encargados de tales espacios, en aras de actualizar la evolución de los desplazamientos y los datos de las personas desplazadas. Dicho de otro modo, en cada zona de apoyo, además de brindar la asistencia humanitaria, se tendría la aptitud de contar con un sistema que permitiera conocer la ayuda que se le ha brindado a las personas desplazadas a través de la plataforma en cuestión, estableciendo una proximidad de la autoridad con las necesidades que eventualmente hayan podido ser atendidas y las que aún falten.

El desarrollo de esta plataforma y su eventual aplicación son una propuesta en el rubro del rotundo éxito que se ha obtenido a partir de la creación de plataformas digitales en sistemas que tienen que ver con aspectos de mejora de atención en relación con las necesidades de los mercados; por ejemplo, plataformas para telecomunicaciones, radio, financieras, de transporte, de mapas, etcétera; razonamiento que nos lleva a creer que el éxito ya señalado puede refrendarse en la operación del Estado de tales tecnologías, en problemas que pueden hallar solución a mediano plazo a través de la implementación de sistemas de inteligencia artificial.

Todo lo que se ha comentado implica que el Estado adopte criterios de modernización dentro de sus acciones para generar condiciones, en primer término, de acceso a la salud y, en segundo, para que las personas desplazadas internamente encuentren oportunidades para su eventual retorno.

El Estado mexicano debe estar preparado para realizar una serie de acciones con perspectiva de política criminal que contemplen los efectos de los desplazamientos, para poder brindar a las personas la certeza jurídica de que no se vulneren sus derechos, y de que no se revictimice a aquellos cuyos derechos ya se hayan vulnerado.

En esa virtud, las medidas de prevención deben obedecer a un sistema dogmático, dado que la política criminal se vuelca en tales construcciones,

que funcionan como instrumento adecuado para la realización de esa política (García, 2004: 547, 555 y 595); en otras palabras, si no hay un análisis dogmático correcto que acompañe a las medidas de política criminal, entonces esta no tendrá bases sólidas y estará destinada al fracaso, lo cual condenaría a las personas a estar subyugadas a un espacio en donde no se encontraría un esquema eficaz para la prevención de los delitos en contra de las personas internamente desplazadas, o de ellos entre sí, ni mucho menos un espacio en donde se prevea la atención ante una contingencia sanitaria.

Hay que reiterar que el único camino por el cual se puede materializar una eficaz política criminal es a través del Poder Legislativo; en ese tenor, la medida que se ha propuesto consiste en legislar en la materia, en aras de poder construir modelos integrales que permitan la prevención y la atención del desplazamiento forzado interno en México, además de que este país se convierta en punta de lanza, delante de la comunidad internacional, para la implementación de un nuevo instrumento internacional que se vuelva vinculante para los Estados americanos, en función de la prevención y la atención del desplazamiento interno forzado, además del éxito operacional que existiría a partir de la implementación de esquemas de inteligencia artificial.

## V. CONCLUSIONES

En el tema estudiado subsisten dos cuestiones de significativa importancia y, a su vez, polarizadas en cierto sentido: por un lado, la necesidad de salvaguardar el acceso ordenado, documentado y no pernicioso del desplazamiento que pueda darse al interior de México, como puente de paso hacia los Estados Unidos de América. Y, por el otro, la necesidad de garantizar los derechos humanos de las personas internamente desplazadas en el territorio nacional, de lo cual el Estado es responsable en función de la normativa constitucional, legal y convencional.

Pero, además, estos factores se ven dimensionados con mayor agudeza, cuando se trata de la migración motivada por el desplazamiento forzoso y forzado de las poblaciones desde fuera y al interior del país, por causas, sobre todo, de índole social, criminal y política.

Al colindar diferentes factores en la problemática aludida a lo largo de este texto, no podemos sino remitir nuestra preocupación hacia las medidas

que deben tomar las diferentes instituciones del Estado mexicano para, en un contexto estructural de política criminal, disponer las medidas preventivas tendentes a aminorar los efectos nocivos, tanto para la población desplazada como para las regiones en que esta situación se manifiesta, y que buscan rentabilizar agentes extraños al fenómeno.

Consideramos que la política criminal sustantiva que debe permear en este escenario fenomenológico, exige la necesaria intervención no solo de las instancias tradicionales, como la Secretaría de Gobernación a través del Instituto Nacional de Migración; la Comisión Nacional de los Derechos Humanos, por medio de sus Visitadurías responsables del auxilio a migrantes; o de los gobiernos estatales, donde se advierta una presencia significativa de la problemática, entre otras, sino de la sociedad civil multiplicada en cientos de oenegés, de organismos empresariales, de universidades, de asociaciones religiosas, y configurar, en este sentido, una política criminal con las instituciones del Estado, que cumpla con los requerimientos establecidos en las normativas aludidas en líneas anteriores.

Todas estas políticas deben ir respaldadas con el aporte de la inteligencia artificial, con *software* que haga posible el registro de las personas desplazadas que, en todo momento, tienen contacto con los diferentes servidores públicos y asociaciones civiles que deben convertirse en receptores de esa información. Existen, dentro del mercado internacional, varias firmas que ofrecen este tipo de tecnología informática para poder acceder a un registro puntual y permanente de las personas en estas condiciones de desplazamiento.

En Perú hay un Registro Nacional para las Personas Desplazadas, y no vemos por qué en México no pudiese llevarse a cabo un esquema de registro semejante, a menos que sigamos considerando a la migración de personas como un fenómeno al cual se le puede rentabilizar desde la corrupción de los agentes del Estado, o desde las ambiciones de la criminalidad organizada y en la cual, por circunstancias aviesas, también participan no pocos funcionarios públicos.

## VI. FUENTES DE CONSULTA

Comisión Mexicana de Defensa y Promoción de los Derechos Humanos (CMDPDH) (2014). *Desplazamiento interno forzado en México*. México:

Comisión Mexicana de Defensa y Promoción de los Derechos Humanos, A.C.

Comisión Nacional de los Derechos Humanos (CNDH) (1994). Recomendación 58/1994, sobre expulsión de pobladores en el Municipio de San Juan Chamula, Chiapas, por no profesar la religión predominante en la zona. México: CNDH.

Constitución Política de los Estados Unidos Mexicanos (CPEUM) (2020), última reforma el 24 de diciembre de 2020, Ciudad de México: Servicios Parlamentarios, Secretaría General, Cámara de Diputados, H. Congreso de la Unión.

Corte Interamericana de Derechos Humanos (Corte IDH) (1988). Caso *Velázquez Rodríguez vs. Honduras*. Sentencia de 29 de julio de 1988. San José: Corte IDH.

Corte Interamericana de Derechos Humanos (Corte IDH) (1994). Caso *Gangaram Panday vs. Surinam*. Sentencia de 21 de enero de 1994. San José: Corte IDH.

Corte Interamericana de Derechos Humanos (Corte IDH) (2010). Caso *Chitay Nech y otros vs. Guatemala*. Sentencia de 25 de mayo de 2010. San José: Corte IDH.

Corte Interamericana de Derechos Humanos (Corte IDH) (2015). Caso *Masacre de Mapiripán vs. Colombia*. Sentencia de 15 de septiembre de 2015. San José: Corte IDH.

Corte Penal Internacional (CPI) (2003). *El Fiscal c. Simić. Tadić y Zarić*. Caso No. IT-95-9, Sala II de Primera Instancia del TPIY, sentencia del 17 de octubre de 2003, párrafo 122. La Haya: CPI.

Corte Penal Internacional (CPI) (2004). *Fiscalía v. Brđanin*, Caso No. IT-99-36-T, sentencia del 1 de septiembre de 2004, párrafo 544. La Haya: CPI.

Comité Internacional de la Cruz Roja. *Desplazamientos internos: estrategia del CICR para 2016-2019* (Desplazamientos) (2019). Ginebra: Comité Internacional de la Cruz Roja. Disponible en: https://www.icrc.org/es/document/desplazamientos-internos-estrategia-del-cicr-para-2016-2019. Consultado el 3 de enero de 2021.

García Ramírez, S. (Mayo-agosto, 2004). "Crimen y prisión en el nuevo milenio", en *Boletín Mexicano de Derecho Comparado*, nueva serie, año XXXVII, (110).

*International Review of the Red Cross* (IRRC) (febrero de 2014), 96(893). Ginebra: Comité Internacional de la Cruz Roja. Disponible en: https://www.

icrc.org/es/document/desplazamientos-internos-estrategia-del-cicr-para-2016-2019. Consultado el 2 de enero de 2021.

Lozano Tovar, E. (2010). *Manual de Política Criminal y Criminológica*. México: Porrúa.

Lozano Tovar, E. (2020). *Política criminal aplicada. El aspecto material de las políticas públicas contra la delincuencia en México*. México: Porrúa.

Organización de Estados Americanos (OEA) (1969). Convención Americana sobre Derechos Humanos (CADH). Washington, D.C.: OEA.

Organización de las Naciones Unidas (ONU) (1998). *Principios Rectores de los Desplazamientos Internos de las Naciones Unidas (Principios)*. Nueva York: Comisión de Derechos Humanos de Naciones Unidas.

Organización de las Naciones Unidas (ONU) (2002). Estatuto de Roma de la Corte Penal Internacional (Estatuto). Nueva York: ONU.

Organización de las Naciones Unidas (ONU) (2012). Convención de la Unión Africana sobre la Protección y Asistencia de los Desplazados Internos en África (CUAPADIA). Ginebra: Alto Comisionado de las Naciones Unidas para los Refugiados.

Pérez, B., De Aquino, L. y Castillo, M. (2019). *Entre la invisibilidad y el abandono: un acercamiento cuantitativo al desplazamiento interno forzado en México.* México: Comisión Mexicana de Defensa y Promoción de los Derechos Humanos, A. C.

Perrín, P. (1998). "Efectos de la ayuda humanitaria sobre la evolución de los conflictos", en *Revista Internacional de la Cruz Roja*. Ginebra: Comité Internacional de la Cruz Roja. Disponible en: https://www.icrc.org/es/doc/resources/documents/misc/5tdlpa.htm. Consultado el 2 de enero de 2021.

# INTELIGENCIA ARTIFICIAL, DERECHO PENAL Y *COMPLIANCE*

Diego Fernando Martínez Hernández*

* Director del despacho Martínez Hernández Legal & Compliance y alumno de la Maestría en Juicio Oral y Proceso Penal Acusatorio en el Instituto Nacional de Ciencias Penales (INACIPE). Contacto: abogadiegofmh@gmail.com

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Derecho penal** | *Criminal law* |
| **Inteligencia artificial** | *Artificial intelligence* |
| ***Compliance* penal** | *Criminal compliance* |
| **Responsabilidad penal de la persona jurídica** | *Criminal liability of the legal entity* |
| **Prevención del delito** | *Crime prevention* |



**Resumen.** En este artículo se analizarán la inteligencia artificial, la naturaleza preventiva del *compliance* penal, y si es posible que exista alguna relación entre el derecho penal y la inteligencia artificial; asimismo, se tratarán algunos supuestos en los cuales una persona jurídica podría ser responsable penalmente por los actos de máquinas que utilicen inteligencia artificial, en caso de que estas llegaran a considerarse sujetos del derecho penal.

**Abstract.** This article will analyze artificial intelligence, the preventive nature of criminal compliance, and if it is possible that there is any relationship between criminal law and artificial intelligence. Likewise, some cases will be dealt with in which a legal person could be criminally liable for the acts of machines that use artificial intelligence, if these were to be considered subjects of criminal law.



Fecha de recepción: 15 de enero de 2021
Fecha de aceptación: 17 de febrero de 2021

SUMARIO:







## I. INTRODUCCIÓN

El tema de la inteligencia artificial es, sin duda, uno de los que más interés y curiosidad generan hoy en día; sin embargo, al momento de involucrarlo con el derecho, a más de uno le puede causar conflicto que exista relación entre sí, y más aún si se trata de derecho penal.

No obstante, lamentablemente pareciera que la relación entre inteligencia artificial y el derecho penal comienza a tomar un camino similar al que en su momento tuvo la responsabilidad penal de las personas jurídicas, la cual fue negada rotundamente por más de un estudioso del derecho; en efecto, aun cuando dicha responsabilidad se encuentre regulada por normativas específicas, sigue sin comprenderse del todo; se le sigue poniendo en duda, aunque sea una realidad en el sistema jurídico mexicano.

En las líneas que siguen se realizará un estudio somero de la inteligencia artificial, se abordará la naturaleza jurídica preventiva del delito en la aplicación del *compliance* penal, y se analizarán algunos supuestos a partir de los cuales podría determinarse si una persona jurídica puede, o no, ser penalmente responsable por los actos u omisiones que realice una máquina que utilice inteligencia artificial.

El derecho, como toda ciencia social, tiene la característica de ser dinámico y atiende a las necesidades de la sociedad para que cumpla su función de regular la conducta; sin embargo, debemos aceptar que, como si fuere "película futurista", paulatinamente el futuro (valga la redundancia) nos alcanzó y la responsabilidad del estudio de la relación entre el derecho y la inteligencia artificial es tarea de todo jurista que busca mantenerse actualizado, sin importar la rama del derecho en la cual se especialice.

## II. LA INTELIGENCIA ARTIFICIAL

Pareciera que hablar de "inteligencia artificial" equivaliera a referirse a alguna película o serie de ciencia ficción; es decir, a un tema futurista, con el cual tendrán relación las generaciones siguientes; sin embargo, lo cierto es que —se repite— el futuro nos alcanzó y que, día a día, se tiene contacto directo o indirecto con la inteligencia artificial.

El principal objetivo de esta es que las computadoras puedan competir intelectualmente con los seres humanos y, de ser posible, que puedan sobrepasarlos en cuanto a desarrollo y destreza mental (Poblete, 2020). Al respecto, es importante tomar en consideración que, hasta cierto punto, lo que se busca es el desarrollo dentro de un plano de igualdad en el aspecto intelectual.

De igual forma, es importante señalar que, aun cuando esta inteligencia sea independiente o autónoma de la del ser humano, la robótica, por ejemplo, se asocia a tres "leyes" (Poblete, 2020) que deben de ser respetadas en todo momento. Dichas leyes fueron propuestas por el escritor ruso-estadounidense Issac Asimov (1920-1992) en su obra *Yo, robot* (1950), y señalan:

1. Un robot no puede hacer daño a un ser humano o, por su inacción, permitir que un ser humano sufra daño.
2. Un robot debe obedecer las órdenes dadas por los seres humanos, excepto si estas órdenes entran en conflicto con la Primera Ley.
3. Un robot debe proteger su propia existencia siempre que dicha protección no entre en conflicto con la Primera o la Segunda Ley. (Poblete, 2020)

En cambio, dejando de lado a la literatura y jurídicamente hablando, cabe mencionar la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2013 [INL]),[1] que a grandes rasgos prevén lo siguiente:

1. Proteger a los seres humanos del daño causado por los robots.
2. Respeto a la negativa de atención por parte de un robot.
3. Respeto y protección de la libertad del ser humano frente a los robots.
4. Protección de la humanidad en contra de las violaciones a la privacidad cometidas por un robot.

[1] Consultable en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html#top (N. del E.) Estas recomendaciones pueden considerarse un punto de partida para una posible futura legislación en la materia.

5. Tratamiento de datos personales procesados por un robot.
6. Protección de la humanidad contra el riesgo de manipulación por robots.
7. Evitar toda disolución de vínculos sociales.
8. Igualdad en el acceso al progreso de la robótica.
9. Restringir el acceso humano a las tecnologías de mejora.





## III. EL *COMPLIANCE* PENAL

Las políticas corporativas preventivas del delito, también denominadas *Criminal Compliance Program*, son las herramientas por antonomasia para lograr un control correcto y efectivo dentro de la organización, pues a partir de su implementación se busca que se actúe dentro del orden jurídico nacional, tanto al interior como al exterior de la propia organización, buscando prevenir en todo momento la actualización de un delito.

En relación con lo anterior, y tomando en cuenta las características y objetivos del *compliance* penal, puede señalarse que es:

> …la implementación voluntaria, correcta y efectiva de un Programa Corporativo sobre Prevención del Delito al interior de una organización (persona jurídica), con base en la normativa jurídica vigente de naturaleza penal y de igual forma, con base en cualquier ordenamiento que implique obligaciones para la Persona Jurídica que, en el supuesto de no cumplirse, pudiera actualizar un hecho que la ley señala como delito; teniendo como finalidad que en caso de que la Persona Jurídica se encuentre implicada en un proceso de naturaleza penal, dicha responsabilidad pueda ser atenuada o en el mejor de los casos, excluida. (Martínez, 2019)

Ahora bien, debe tomarse en cuenta que si bien, como tal, la implementación de estas políticas corporativas preventivas del delito (*compliance* penal) no es una obligación de las personas jurídicas, también es verdad que implementarlas atendería a las prácticas de buen gobierno e integridad corporativa.

De igual manera, dichas políticas, al ser desarrolladas exclusivamente para cada organización en particular y atendiendo a sus necesidades, actividades y objeto social, implican que, para el caso en cuestión (el uso de la inteligencia artificial), deban estar sumamente controladas, y que sus funciones y objetivos estén claramente definidos.

## IV. RESPONSABILIDAD PENAL Y PREVENCIÓN DEL DELITO EN LA INTELIGENCIA ARTIFICIAL

Antes de hablar sobre la prevención del delito y la inteligencia artificial, primero debemos definir si realmente es posible que exista alguna relación entre dicha inteligencia y el derecho penal, de tal forma que pueda ser posible que aquella cometa un hecho que la ley señala como delito. Si bien es verdad que la inteligencia artificial, al ser "la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano" (Iberdrola, 2019), supone que hasta cierto punto tenga una forma de pensar autónoma, distinta e independiente de la del ser humano, para poder plantearnos si su proceder o su omisión realmente pueden tener relación directa con el derecho penal (de modo que sí se pueda actualizar un hecho que la ley señala como delito), debe descubrirse si es posible que una máquina que utilice inteligencia artificial pueda actuar de forma dolosa o culposa (tipicidad subjetiva), así como que pueda desarrollar, hasta cierto punto, una capacidad de culpabilidad (Ontiveros, 2017), pues entonces será responsabilidad de los estudiosos de las ciencias penales establecer de qué forma debe aplicarse la teoría del delito en supuestos donde las máquinas que utilicen inteligencia artificial se involucren en un hecho delictuoso.

Con base en lo anterior y suponiendo, sin conceder, que una máquina que utilice inteligencia artificial cuente con lo descrito, es decir, en el supuesto de que cometa un hecho que la ley señala como delito, ¿la máquina debe ser considerada responsable directa, o solo se le tendrá como instrumento del delito? En este último caso, ¿será posible que se actualice una agravante en la utilización de máquinas que usen la inteligencia artificial para la comisión de un hecho delictivo?

Desde el punto de vista de quien esto escribe, todo dependería, principalmente, de la programación de la inteligencia artificial que se utilice, pues si no se programa con la finalidad de cometer un delito, podría considerarse un simple instrumento para ello; sin embargo, si la comisión del delito se realiza a partir del pensamiento previo de la máquina (programación de fábrica), y al final decide, de forma autónoma, realizar determinada conducta u omisión y, como resultado, comete un delito, se estima que sí sería responsable penalmente, liberando de cualquier tipo de responsabilidad a la persona física o jurídica que se ocupe de ella, a menos que dicha persona pudiera limitar los alcances de "los actos" de la máquina.

Ahora bien, en relación con esto último, las políticas preventivas del delito deben tomar en cuenta, ante todo, a la legislación actual, pues a partir de esta se sabrá el alcance y hasta qué punto la persona jurídica puede ser penalmente responsable por utilizar máquinas que tengan inteligencia artificial. Hasta la fecha, este aspecto no ha sido abordado del todo en el sistema jurídico mexicano; sin embargo, si el desarrollo de la inteligencia artificial mantiene el ritmo que ha tenido en los últimos años, es posible que el legislador mexicano se vea en la necesidad de ocuparse del tema, basándose, quizá, en las Normas de Derecho Civil sobre Robótica de la Unión Europea.

Otro aspecto importante que también debe tomarse en cuenta es saber qué sistema de imputación se utilizará para llevar a cabo el estudio de la responsabilidad penal de la persona jurídica una vez que se legisle en esta materia, en virtud de que, al contar con un catálogo de delitos dentro de los cuales se puede hacer penalmente responsable a una persona jurídica, hará que se pueda delimitar de mejor forma el proceder de la organización, impactando principalmente en los protocolos para la toma de decisiones y en los manuales de operación al momento de la creación de las políticas corporativas preventivas del delito (*compliance* penal). Sin embargo, la labor fundamental radicará en establecer un límite en el pensamiento y la actuación de las máquinas que utilicen inteligencia artificial al momento de programarlas, de tal forma que, si no se puede evitar cualquier conducta delictiva desde la programación de fábrica, entonces será obligación de la persona jurídica hacerlo, evitando así riesgos futuros.

## V. CONCLUSIONES

Sin duda, la relación que pudiera existir entre el derecho penal y la inteligencia artificial es una tema complejo. En México no se dispone todavía de una legislación que se aplique efectivamente a las máquinas que utilicen inteligencia artificial, por lo que en materia de teoría del delito, la cual es general, sistemática y precisa, será responsabilidad de los juristas y estudiosos del derecho penal trabajar en dicha normativa, de manera que se pueda aplicar de forma armónica tanto a personas físicas y jurídicas como a las máquinas que utilicen inteligencia artificial (Posada, 2019), en caso de que estas últimas lleguen a ser consideradas sujetos del derecho penal.

Una vez que se establezca lo señalado con anterioridad, las ciencias penales se enfrentarán al siguiente reto: ¿cómo se sancionaría a las máquinas?, ¿tendrían derechos? Y, en términos del artículo 18 de la Constitución Política de los Estados Unidos Mexicanos, ¿habría lugar a la reinserción social? Es evidente que aún no se tienen respuestas; sin embargo, lo que sí puede hacerse es utilizar, como base de la legislación faltante, los avances que el Parlamento Europeo ha realizado en la materia.

## VI. FUENTES DE CONSULTA

Asociación Peruana de Compliance (2019, agosto 28). "Tiempos de Compliance- Episodio 18- El Derecho Penal frente a los Agentes de Inteligencia Artificial (AI)." Recuperado de: https://www.youtube.com/watch?v=d_yvrvBMH4k&t=445s

Iberdrola. (2019). "¿Qué es la Inteligencia Artificial?". *Iberdrola*. Recuperado de: https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial

Martínez Hernández, D.F. (2019). "Compliance penal: actos de corrupción y el lavado de dinero en la responsabilidad penal de la persona jurídica." En *Memoria del Primer Congreso Internacional de Derecho Penal 2018: Terrorismo, trata de personas y nuevas formas de esclavitud, corrupción y tráfico de drogas.* Volumen 3, p. 1193.

Ontiveros Alonso, M. (2017). *Derecho penal: parte general*. México: Ubijus. pp. 330 y 331.

Poblete Sáenz, O. (2020) "¿Quién regulará la Inteligencia Artificial?". *Ciencias UNAM*. Recuperado de: http://ciencia.unam.mx/leer/952/-quien-regulara-la-inteligencia-artificial-

Resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones de la Comisión sobre normas de derecho civil sobre robótica (2015/2103[INL]), Estrasburgo, 16 de febrero de 2017.

# VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL Y EL *BIG DATA:* RETOS Y OPORTUNIDADES PARA GARANTIZAR LOS DERECHOS HUMANOS

Oswaldo Rosalío Aguilar Rivera*

* Académico del Instituto Nacional de Ciencias Penales.

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Inteligencia artificial** | *Artificial Intelligence* |
| **Derechos humanos** | *Human rights* |
| **Macrodatos** | *Big data* |
| **Vigilancia** | *Surveillance* |
| **Víctimas** | *Victims* |



**Resumen.** La vigilancia a través de la inteligencia artificial y el *big data* se ha vuelto común. Diversos sistemas tecnológicos y digitales se han desarrollado de manera gradual, hasta superar los mecanismos de supervisión éticos y normativos para garantizar el respeto a los derechos humanos. En este artículo se exploran las tendencias del desarrollo, uso y vigilancia de las tecnologías de la información en materia de inteligencia artificial, para dar un diagnóstico desde un enfoque real y normativo. Se mostrarán los excesos, limitaciones y desafíos que enfrenta la vigilancia, así como la protección a los derechos humanos y la posible aparición de víctimas por violaciones a aquellos, a fin de coadyuvar al desarrollo de la investigación y la protección normativa de este fenómeno.

**Abstract.** Surveillance through artificial intelligence and big data has become common. Various technological and digital systems have been developed gradually, to overcome the ethical and regulatory supervision mechanisms to guarantee respect for human rights. This article explores the trends in the development, use and surveillance of information technologies in terms of artificial intelligence, to give a diagnosis from a real and normative approach. The excesses, limitations and challenges faced by surveillance will be shown, as well as the protection of human rights and the possible appearance of victims of human rights violations, to contribute to the development of the investigation and the normative protection of this phenomenon.


Fecha de recepción: 16 de enero de 2021
Fecha de aceptación: 12 de abril de 2021

SUMARIO:





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

## I. COMPONENTES BÁSICOS DE LA IA: EL *BIG DATA*, ALGORITMOS, *MACHINE LEARNING*, *DEEP LEARNING* Y *BLACK BOX*

Para hablar de inteligencia artificial, hay que remontarse a sus inicios, cuando el hombre empezó a desarrollar tecnología en aras de mejorar procesos en busca de comodidad, ahorro de mano de obra y/o de recursos. Particular y desafortunadamente, la guerra siempre ha contribuido de manera rápida a implementar nuevas tecnologías para el combate y lo relacionado con él. En este rubro, puede mencionarse que, durante la Segunda Guerra Mundial, la máquina que inventó Alan Turing fue uno de los primeros artefactos de IA en utilizarse para descifrar códigos nazis. Funcionaba a través de un número finito de estados internos para realizar cualquier operación que estuviera representada mediante un algoritmo, y estos datos se almacenaban en una cinta bidireccional en forma de dos marcas, lo cual también creo un precedente no solo para los ordenadores que vendrían posteriormente, sino también para el *big data.*

Los *algoritmos* son el motor fundamental de esta tecnología: según la Real Academia Española, la palabra "algoritmo", del latín *algobarismus*, significa "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". En relación con la inteligencia artificial, estas operaciones se hacen posibles gracias a la cantidad de datos recolectados que pone en marcha este engranaje para resolver modelos complejos a partir de un problema determinado. De manera general, un algoritmo se compone de tres etapas: 1) datos de entrada; 2) un proceso lógico-formal; y 3) la solución

que se da según la problemática planteada. Así, podemos ejemplificar un algoritmo cuando un abogado espera la resolución de un asunto (dato de entrada); al notificarse, puede tomar distintos rumbos según sus intereses (proceso lógico-formal); y, si es abogado del imputado y la sentencia es condenatoria, hay una alta probabilidad de que interponga un recurso de apelación; y si, por el contrario, la sentencia es absolutoria, no promoverá recurso alguno (soluciones).

Estos procesos, que son comunes en la vida diaria, suelen ser recogidos por la inteligencia artificial, con el valor agregado de que, entre más complejo y más datos disponibles haya, sale de la esfera de resolución inmediata del hombre e ingresa en la de las máquinas, que son capaces de resolver en cuestión de segundos.

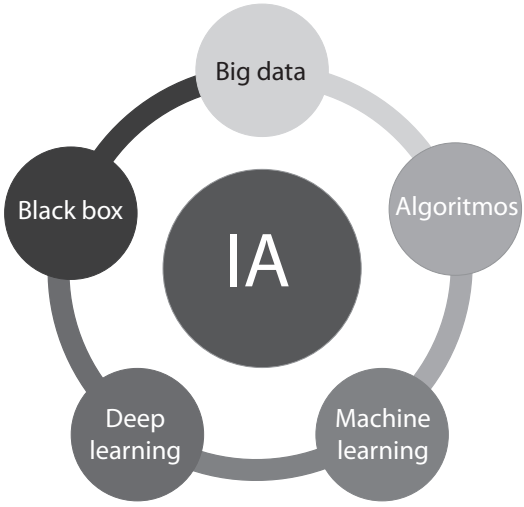
La recolección de datos de la cual se sirve la inteligencia artificial para generar los procesos traducidos en algoritmos se conoce como *big data*. Aunque el término se usó por primera vez en 1997, sus antecedentes se remontan a 1958, cuando Hans Peter Lung, investigador de IBM, utilizó el término *business intelligence* (inteligencia de negocios), que en la década de 1980 se utilizó para referirse a sistemas de *software* que intervenían en la toma de decisiones de negocios, con base en la recogida de análisis de datos o hechos. Al final de esa década surgió el término *data mining* (minería de datos), como analogía a la extracción de yacimientos, tales como bancos de datos, de lo cual se obtiene un conocimiento en concreto, equiparado como un material valioso. En 1989 empezó a utilizarse la expresión *knowledge discovery in databases* (descubrimiento de conocimiento en bases de datos), que no es otra cosa que delimitar el valioso resultado final de esa extracción (Niño e Illarramendi, 2015).

Otro integrante de suma trascendencia de la IA es el *machine learning* (aprendizaje automático), que es la capacidad de un sistema o máquina para aprender automáticamente a partir de la experiencia de la extracción de datos y la resolución de problemas de acuerdo con experiencias programadas, presentes o futuras. Con procesos más profundos, y entendido como subcampo del *machine learning*, se desarrolló el *deep learning* (aprendizaje profundo), que se define como "la actividad automática de adquisición de conocimiento a través de máquinas que usan varios niveles para la extracción". El adjetivo "profundo" no se aplica en sí al conocimiento adquirido, sino a la forma en el que el conocimiento se adquiere (Gómez Gil, 2015).

Un concepto que mueve a debatir sobre la posibilidad de violentar derechos humanos a través de la inteligencia artificial es *black box* (caja negra), que funciona con los algoritmos programados y el análisis proporcionado por el *big data*, y cuyas entradas y operaciones no son visibles para el usuario y, en algunos casos, ni para el propio operador; en pocas palabras, es impenetrable, por lo que "esta alta dimensionalidad evita que los humanos conozcan cómo la IA está tomando sus decisiones o predice cómo tratará los nuevos datos" (Bathaee, 2018).

Estos términos se estiman fundamentales para la comprensión de la inteligencia artificial, y servirán para el desarrollo de este artículo.

Gráfico 1.




Fuente: Elaboración propia

## II. VIGILANCIA POR INTELIGENCIA ARTIFICIAL Y EL *BIG DATA*

Con el avance tecnológico en materia de inteligencia artificial, cada vez son más los mecanismos de los que la humanidad se auxilia para llevar a cabo todo tipo de tareas. Es común convivir con medios tecnológicos que dan respuestas rápidas y precisas a muchas necesidades; desde una búsqueda sencilla en Google hasta una instrucción a los asistentes inteligentes, como

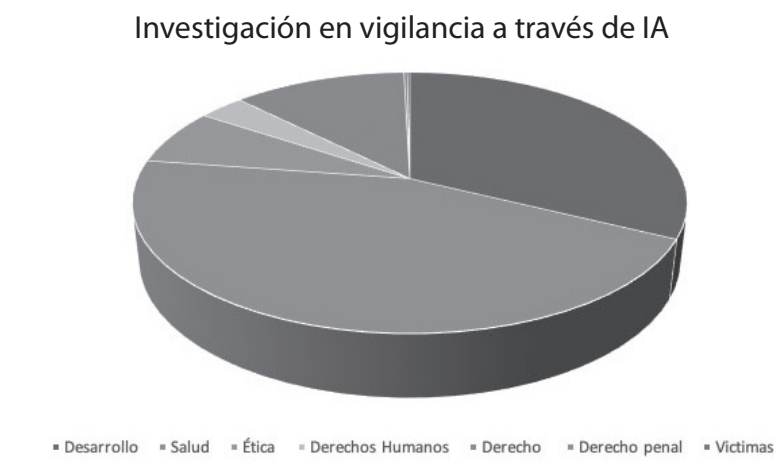
*Siri* o *Alexa*, mecanismos de IA hacen la vida más fácil. El desarrollo de este tipo de tecnología se vuelve determinante para "ayudar" de mejor manera al usuario. Para el uso de estos sistemas, solo es necesario tener un dispositivo a la mano y su correspondiente aplicación. Otros casos de utilización de inteligencia artificial son las páginas web, cámaras de videovigilancia en la calle, redes sociales, etcétera. Todo esto se genera a partir de una construcción social de la realidad que, de acuerdo con varios análisis interdisciplinarios, creó necesidades, como utilizar un navegador para evitar el tráfico o compartir un estado de ánimo en las redes sociales, y también obligaciones, como compartir los datos biométricos en algún trámite gubernamental como requisito para completarlo. Sin embargo, este desarrollo de la inteligencia artificial, ¿crece para informar oportunamente y, sobre todo, para proteger los derechos humanos de los usuarios que, poco a poco, han ido entregando su privacidad hasta quedar "vacíos"?

La vigilancia a través de la inteligencia artificial debe analizarse con base en el auxilio que aquella presta en la cotidianidad, ya que, bajo un esquema de facilitadora de tareas diarias o que se han vuelto indispensables para el usuario, a través del *big data* recolecta y concentra datos de cualquier tipo. Si bien es cierto que la vigilancia a partir de la geolocalización es una de las más importantes, no lo es menos el monitoreo de compras *online*, visitas a determinados sitios web y, más delicado aún, del modo de pensar a partir de las publicaciones que definen una postura política, social o religiosa, entre otras.

El *big data* es trascendental en el desarrollo de la inteligencia artificial y se define como "el acumulamiento de datos generados de manera masiva" (Casas Roma, Nin Guerrero, y Julbe López, 2019); plantea distintos retos, de los cuales no están exentas las ciencias penales y, particularmente, quienes pudieran tener la calidad de víctimas en el sistema penal acusatorio mexicano. Es de llamar la atención el grado de desarrollo de la inteligencia artificial en comparación con el de la protección de los derechos humanos relacionados con esta: en un estudio bibliográfico, partiendo de las variables en inglés *artificial intelligence* + *surveillance* (inteligencia artificial + vigilancia) dentro del buscador digital *Discovery Service* del sistema bibliotecario digital de la UNAM, delimitando la temporalidad entre los años 2016 y 2020, se encontraron 2,198 resultados, incluyendo publicaciones académicas, profesionales, revistas, noticias y materiales de conferencias. Posteriormente se agregaron filtros específicos por materia, arrojando la búsqueda lo siguiente; *artificial intelligence* + *surveillance* + *development* (inteligencia artificial

+ vigilancia + desarrollo): 393 resultados; *artificial intelligence* + *surveillance* + *health* (inteligencia artificial + vigilancia + salud): 548 resultados; *artificial intelligence* + *surveillance* + *ethics* (inteligencia artificial + vigilancia + ética): 85 resultados; *artificial intelligence* + *surveillance* + *human rights* (inteligencia artificial + vigilancia + derechos humanos): 39 resultados; artificial intelligence + surveillance + law (inteligencia artificial + vigilancia + derecho): 147 resultados; *artificial intelligence* + *surveillance* + *criminal law* (inteligencia artificial + vigilancia + derecho penal): 3 resultados; y *artificial intelligence* + *surveillance* + *victims* (inteligencia artificial + vigilancia + victimas): 2 resultados.

Gráfica 2.




Fuente: Elaboración propia.

De esta búsqueda preliminar puede apreciarse que los rubros con más investigación son el desarrollo de tecnologías y la salud, en comparación con los derechos humanos, el derecho penal y las víctimas. Cabe destacar que, por efectos de la pandemia del virus SARS-CoV-2 (COVID-19) (fines epidemiológicos), la vigilancia de la salud se ha incrementado considerablemente. Este balance lleva a pensar en lo siguiente: ¿cuáles son los sistemas de vigilancia por inteligencia artificial y el *big data* más desarrollados? ¿Están impactando a los derechos humanos de los usuarios? Ante la búsqueda de respuestas, es alarmante que los derechos humanos, las ciencias penales y la victimología sean un terreno olvidado en el mundo de la inteligencia artificial; de ahí el interés en desarrollar temas relacionados con estas materias, con el fin de prevenir violaciones a los derechos de los usuarios.

## III. SISTEMAS DE VIGILANCIA A TRAVÉS DE IA MÁS DESARROLLADOS EN LA INVESTIGACIÓN

Sin duda, a partir del desarrollo de la inteligencia artificial se han detonado mecanismos de vigilancia con diversos fines y propósitos, y en este apartado se mencionarán, de acuerdo con los artículos seleccionados, cuáles son los sistemas de vigilancia más estudiados a partir del desarrollo de la IA.

Como se puede apreciar en la gráfica 2, en los últimos cinco años el 45% de la investigación ha girado en torno al desarrollo de la tecnología de vigilancia a través de la inteligencia artificial y, a su vez, ha sido primordial el segmento respectivo a la vigilancia por video, para distintos fines. La vigilancia a través de video, o *videovigilancia*, puede dividirse en dos segmentos: 1) la que se encarga de identificar y recolectar *imágenes de personas*, que involucra los sistemas de reconocimiento facial; y 2) la que recae en *objetos*.

El desarrollo de este tipo de investigación se ha encargado, en su mayoría, de crear técnicas cada vez más precisas para la recolección de datos: almacenamiento, distribución y análisis comparativos de los resultados que arroja la videovigilancia a través de la inteligencia artificial. El debate gira en torno a los servidores capaces de almacenar el *big data*, el procesamiento eficaz de esa información y, en casos mínimos, investigaciones que tratan de incrementar la seguridad de las personas. Llama la atención que, con el desarrollo de ciudades inteligentes, emergen nuevos conceptos de identificación, como el tránsito en puertos marítimos, carreteras, control de tráfico, control de estacionamientos y, en algunos casos, control de personas. Algunas investigaciones también desarrollan, con enfoque tecnológico, las detecciones de personas armadas en fracciones de segundo, a través de la combinación de cámaras de alta definición, algoritmos y bases de datos; sin embargo, a pesar de que el objetivo de dichas investigaciones sea mejorar la efectividad de la detención y, por tanto, inhibir el crimen, el desarrollo de esa tecnología carece de un enfoque garantista dirigido a los usuarios.

Otro tipo de vigilancia es la implementada por las redes sociales, a través de las cuales se recolecta todo tipo de información: páginas *web* visitadas; frecuencia, horarios y fines de la visita, por mencionar algunos ejemplos. Más allá de lo anterior, también existe la recolección de datos respecto de formularios a los que el usuario accede en la red, y que obtiene desde un registro para proporcionar información a cambio de datos personales, hasta el registro de datos en el comercio electrónico, pudiendo establecerse,

con ello, criterios de compra, de perfil y hasta pronósticos de necesidades en el futuro:

> …para predecir las tendencias, el Big Data emplea algoritmos que combinan información de las redes sociales y de la búsqueda en la web para identificar las preferencias de los consumidores. También se emplea en la fijación de los precios mediante un seguimiento de los competidores, el coste de los productos y otras variables; las empresas son capaces de analizar cómo varía la demanda ante subidas y bajadas de precio en tiempo real y finalmente, el Big Data potencia las ventas al ofrecer una experiencia personalizada y prevenir el abandono de la compra mediante un proceso de compra ajustado a las preferencias del consumidor. (Álvarez, 2018)

No menos aventurado es que, entre más datos personales recolectados, la inteligencia artificial puede crear un perfil más preciso y, por tanto, de control de las personas, no solo de sus compras, sino también de creencias políticas, sociales o religiosas, información que puede usarse con fines políticos o comerciales, entre otros. El desarrollo de este tipo de vigilancia pretende, sobre todo, generar mejores *softwares* de recolección de datos, mejores servidores de almacenamiento y procesadores más rápidos, que den respuesta inmediata a quien pudiera hacer uso de esa información; sin embargo, es limitado o nulo el enfoque que se da a la protección del usuario.

Es importante destacar que, con motivo de la pandemia de la COVID-19, se ha incrementado el desarrollo de investigación en el segmento vigilancia de la salud por IA y, si bien es cierto se han aplicado mecanismos muy eficaces de detección temprana de contagio, también es cierto que la investigación a partir de la limitación de libertades y el respeto a los derechos humanos ha pasado a un segundo plano. El debate de hoy se centra en qué país crea la tecnología más eficaz para la detección temprana del virus, con variables de mayor precisión en menor tiempo, lo que incluye también vigilancia por redes sociales, entre otros aspectos.

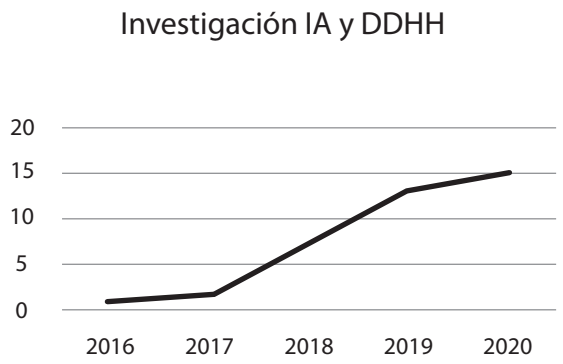
Entonces, en materia de sistemas de vigilancia más populares para la investigación, puede concluirse que el segmento más avanzado es el desarrollo tecnológico, pero solo con enfoque técnico y no necesariamente humanista.

## IV. LOS DERECHOS HUMANOS COMO LA ASIGNATURA MENOS DESARROLLADA EN LA INVESTIGACIÓN SOBRE VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL

Como se apuntó, una de las disciplinas relevantes para la investigación del fenómeno de vigilancia a través de la inteligencia artificial son los derechos humanos. Es fundamental que el tema de los derechos humanos se investigue a la par del crecimiento del fenómeno de la IA; al momento de elaborarse este trabajo, se observa mucha disparidad: mientras que el desarrollo tecnológico ocupa el 45% de la investigación, cuestiones tan relevantes como la salud, la ética, la ley y los derechos humanos, alcanzan el 55% restante. Más grave aún es que, de acuerdo con estas variables seleccionadas, la investigación entre el fenómeno de vigilancia por inteligencia artificial y su relación con los derechos humanos apenas alcance el 3% de la búsqueda realizada.

En los últimos años, el desarrollo de la inteligencia artificial ha alcanzado límites exponenciales, mientras que el de su relación con los derechos humanos es el siguiente:

Gráfica 3.




Fuente: Elaboración propia.

Tan solo en el cuatrienio 2016-2020, la publicación de artículos en el rubro *artificial intelligence* + *surveillance* + *human rights* fue de 39, mientras que en el rubro *artificial intelligence* + *surveillance* + *development* se elaboraron 393 publicaciones.

Por tanto, es evidente que existe una brecha en la investigación entre el desarrollo de la IA y el impacto de esta en los derechos humanos, sobre todo en cuanto a los tipos de vigilancia que se han mencionado.

## V. EL DERECHO HUMANO A LA PRIVACIDAD: EL IMPACTO DE LA VIGILANCIA Y EL *BIG DATA*

La privacidad "es un elemento consustancial a la dignidad humana y, por esa misma razón, debe ser protegido por el derecho. En cambio, el derecho a la privacidad sí podría definirse cómo aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público". (García Ricci, 2013)

El derecho a la privacidad es uno de los principales que giran en torno al uso de la inteligencia artificial y la recolección de datos. A nivel internacional, "la privacidad, consagrada en el derecho internacional de los derechos humanos y reforzada por una red sólida de las leyes y jurisprudencia de protección de datos nacionales y regionales, se ve significativamente afectada por la Inteligencia Artificial" (Fjeld, Achten, Hilligoss, Nagy y Srikumar, 2020). A modo de ejemplo: la videovigilancia es una de las tecnologías más desarrolladas en la investigación; en sociedades poco democráticas, se utiliza para restringir todo tipo de libertades de los ciudadanos, empezando por la de tránsito; los tiempos de los recorridos deambulatorios son procesados por la inteligencia artificial y recolectados por el *big data*, y terminan en análisis de identidad (racial, de género, por edad, situación familiar, laboral, etc.). Posteriormente, estos datos son procesados de la mejor manera que convenga al Estado para mantener el control, y que trastoca otros derechos humanos, como el de no discriminación. A partir de la selección programada por estos algoritmos, se pueden vulnerar los derechos que el Estado tendría que garantizar, no condicionar. Los algoritmos pueden estar sesgados (puesto que son programados por humanos), y ahí se encuentra la falla de inicio por lo que hace a los procesos objetivos de selección y de limitación; por ejemplo: ¿por qué se determina que una persona afroamericana tiene mayor probabilidad de delinquir que una caucásica? La respuesta es simple: porque un patrón humano dominante a partir de una construcción social determina esta discriminación, borrando toda posibilidad de garantizar el respeto a la dignidad de una persona y el libre albedrío. Estas víctimas de discriminación pueden terminar, con motivo de

la programación de algún algoritmo, como víctimas en un proceso penal donde también puedan ser condenadas a partir de patrones erróneos. El *big data* y los algoritmos pueden heredar o reflejar perjuicios y patrones de exclusión, o ser resultado de quienes han tomado decisiones anteriores más allá de la intencionalidad; se trata de un peligro objetivo que hay que prevenir (Barocas, 2016).

En el caso de las redes sociales, la inteligencia artificial, de acuerdo con el perfil del usuario y haciendo uso de algoritmos y procesos de *deep learning* a través del *big data*, puede compartir los datos de aquel para efectos comerciales, vulnerando así el derecho a la privacidad; por ejemplo, puede vender sus patrones de búsqueda, el tipo de perfiles que sigue para sugerirle compras por correo electrónico, mensajes de texto, *cookies* (archivos que crean los sitios visitados en internet, para que dichos sitios consulten la actividad previa del navegador), etcétera. ¿No tendría el usuario derecho a resguardar estos datos, a pesar de que existan corrientes que aseguran que, una vez publicada información en redes sociales, pasa al terreno de lo público? Esta violación al derecho a la privacidad, ¿convierte en víctima a los usuarios de redes sociales y puede llegar al extremo de originar un procedimiento penal? La respuesta parecería afirmativa, ya que la información compartida puede provocar, como se ha demostrado, linchamientos sociales por odio racial, cuestiones de género, etcétera. Basta que la información, de acuerdo con algoritmos programados, se "viralice" y llegue a antagonistas que generen un daño irreversible.

Los mecanismos de geolocalización, otro tipo de vigilancia, presuponen una violación al derecho a la privacidad; basta con tener un teléfono móvil y desplazarse por cualquier lugar. Inmediatamente, de acuerdo con la posición geográfica del usuario, pueden comenzar las sugerencias de compras, rutas o, peor aún, que esa información se comparta con el Estado o corporaciones de cualquier tipo para fines no comerciales, lo cual vulneraría, por ejemplo, el derecho humano a la seguridad; en México, en virtud del confinamiento debido a la COVID-19, se implementó, a la par de la geolocalización, el registro de lugares de asistencia a partir de un código QR (del inglés *Quick Response code*, "código de respuesta rápida").

De ello, el usuario no conoce, a pesar del acuerdo de confidencialidad y la protección de datos, cómo se usa su información y cómo se gestiona la base de datos en la cual se almacena aquella. "Se trata de tener localizados o geolocalizados a los contagiados (e incluso a los sanos, para que no se salten el confinamiento), y tener preparados recursos sanitarios para

asistirlos." (Cascón, 2020) ¿Solo para fines de control de la pandemia? Este ejemplo se relaciona con el derecho humano a la salud, y podría decirse que, si el tratamiento de estos datos fuere utilizado de buena manera, no solo evitaría actores del procedimiento penal que por alguna circunstancia pudieran terminar como víctimas o imputados, sino, ante la situación actual de salubridad en el mundo, como víctimas mortales. La vigilancia epidemiológica por inteligencia artificial y *big data*, lejos de generar víctimas por violación al derecho a la privacidad, debe ser un parteaguas positivo para demostrar que el uso de esta tecnología puede colaborar con la humanidad no solo para mejorar procesos, sino para salvar vidas. Hay que normar estos mecanismos de protección sin restringir derechos humanos.

## VI. RETOS Y DESAFÍOS DE LA VIGILANCIA A TRAVÉS DE LA INTELIGENCIA ARTIFICIAL Y EL RESPETO A LOS DERECHOS HUMANOS

Cuestiones como transparencia, ética y legalidad se han desarrollado en la academia, pero no al ritmo de la investigación técnica que mejora constantemente a la vigilancia a través de la inteligencia artificial. De la consulta del material referido en esta investigación, se advierte que el uso de la vigilancia a través de inteligencia artificial pretende optimizar la vida diaria de los usuarios, y que aplicar esta tecnología supone muchos beneficios; la automatización de procesos con motivo del reconocimiento facial; el orden y la seguridad en las ciudades inteligentes; la vigilancia vehicular para disminuir el tráfico; las sugerencias de compras cuando existen ofertas; la interactuación a distancia con muchas personas a la vez; o la realización de trámites mediante un sistema de reconocimiento dactilar.

El avance tecnológico que ha logrado la IA es cada vez mayor, y sus beneficios son evidentes. Un ejemplo se observa en la vigilancia que se realiza actualmente en materia de salud; en regímenes autoritarios se controló la pandemia eficientemente gracias a esta tecnología. En Estados cuyas democracias son incipientes, se ha intentado implementar con algo de éxito; entonces, la pregunta que surge, partir del desarrollo de la investigación transversal para proteger los derechos humanos de los usuarios, es la siguiente: ¿puede lograrse un equilibrio entre la evolución de la vigilancia y la vigilancia de su uso? La respuesta sería afirmativa; si se logra esta armonía y se avanza conjuntamente en la investigación, tanto tecnológica como

humanística, se podría generar un círculo virtuoso que mejoraría los procesos y daría certeza a los usuarios para el uso de esta tecnología, amén de impedir los abusos por cualquiera que tenga en sus manos la información que recolectan esos medios de vigilancia.

Como se ha presentado en este artículo, existen escasas investigaciones con muchas preocupaciones acerca del impacto en los derechos humanos del uso de la vigilancia a través de la inteligencia artificial, y pocas respuestas que la ciencia que desarrolla estos conceptos pueda responder. Con la motivación de la investigación bajo este rubro (derechos humanos), se podrían generar numerosos beneficios a un espectro muy amplio de usuarios, que no solo entran en el rubro de vigilancia por IA, sino que se relacionan con otros aspectos, como la seguridad pública, la prevención del delito y la victimología. Por tanto, existe una gran brecha que llenar en lo referente al enfoque garantista que debería desarrollarse a la par de la inteligencia artificial, sobre todo en cuanto a cualquier tipo de vigilancia.

En conclusión, a partir del análisis de la investigación cuantitativa del fenómeno de vigilancia a través de la inteligencia artificial, se encuentra una disparidad entre desarrollo tecnológico y derechos humanos, que, de continuar, podría ocasionar graves consecuencias en las libertades de los individuos, y podría generar víctimas que tendrían que ser atendidas bajo la óptica del derecho penal y la victimología.

Por ello, con esta investigación se ha pretendido coadyuvar a eliminar esa brecha y generar, a la par del desarrollo tecnológico, mecanismos de protección a los derechos humanos de los usuarios que son, o pudieran ser, vigilados por la inteligencia artificial y, con ello, no solo protegerlos, sino también crear un ambiente de confianza, donde se pueda seguir utilizando la inteligencia artificial de manera beneficiosa.

## VII. FUENTES DE CONSULTA

Álvarez Torre, L. (2018). *El Big data y el cambio en el modelo de negocio de las empresas de e-commerce: el caso de Amazon y Alibaba*. Madrid: Universidad Pontificia Comillas. Disponible en: https://repositorio.comillas.edu/xmlui/handle/11531/18640

Barocas, S. y Selbst, A.D. (2016). "Big Data's Disparate Impact". *California Law Review*, vol. 104, No. 3, June 2016.

Bathaee, Y. (2018). "The artificial Intelligence black box and the failure of intent and causation". *Harvard Journal of Law & Technology*, Vol. 31, No. 2, Spring 2018. 890-938.

Cascón-Katchadourian, J. (2020). "Tecnologías para luchar contra la pandemia Covid 19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad". Disponible en: https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/79450

Casas Roma, J., Nin Guerrero, J., y Julbe López, F. (2019). "*Big Data*: Análisis de datos en entornos masivos". Barcelona: Universitat Oberta de Catalunya.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., y Srikumar, M. (2020). "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights - based Approaches to Principles for AI". Disponible en: https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y

García Ricci, D. (2013). "Artículo 16 constitucional. Derecho a la privacidad". En Ferrer Mac-Gregor Poisot, E. *et al.* (coords.), *Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana*. Tomo I. México: Suprema Corte de Justicia de la Nación, Universidad Nacional Autónoma de México, Fundación Konrad Adenauer.

Gómez Gil, M. (2015). "Aprendizaje profundo. El poder del aprendizaje automático unido al poder de cálculo de las computadoras actuales". Disponible en: https://ccc.inaoep.mx/~pgomez/conferences/PggTSys16.pdf

Niño, M., e Illarramendi, A. (2015). "Entendiendo el Big Data: antecedentes, origen y desarrollo posterior". Disponible en: https://www.dyna-newtech.com/busqueda-NT/entendiendo-big-data-antecedentes-origen-y-desarrollo-posterior

# CIRCUNSTANCIAS EN LA PROCURACIÓN E IMPARTICIÓN DE JUSTICIA

# PANORAMA GENERAL DE LA *E-JUSTICE* EN MÉXICO Y SU UTILIZACIÓN EN EL PROCEDIMIENTO PENAL ACUSATORIO: AVANCES Y RETOS PARA SU CONSOLIDACIÓN

Hugo Oscar Granja Pérez*

* Abogado penalista, Doctorando en Derecho por la Universidad Nacional Autónoma de México, Maestro en Política Criminal y Máster en Derecho Penal Internacional. Contacto: hugo@hgranja.com (www.hgranja.com)

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Justicia digital** | *E-Justice* |
| **Brecha digital** | *Digital inequality* |
| **Tecnología de la información** | *Information technology* |
| **Acceso a la justicia** | *Access to justice* |
| **Justicia penal** | *Criminal justice* |



**Resumen.** La *e-justic*e en México avanza lentamente, porque, además de enfocar los esfuerzos para la creación de una infraestructura digital que la soporte, no se deben dejar de atender situaciones y circunstancias que son determinantes para el funcionamiento eficaz y eficiente de la justicia digital, como la brecha digital, los altos índices de impunidad, el porcentaje elevado de cifra negra y la poca utilización de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) para interactuar con el gobierno.

**Abstract.** E-justice in Mexico advances slowly, because, in addition to focusing the efforts for the creation of a digital infrastructure that supports it, situations and circumstances that are decisive for the effective and efficient functioning of digital justice should not be neglected, such as the digital divide, the high rates of impunity, the high percentage of black numbers and the little use of information, communication, knowledge and digital learning technologies to interact with the government.


Fecha de recepción: 15 de enero de 2021
Fecha de aceptación: 9 de febrero de 2021

SUMARIO:







## I. INTRODUCCIÓN

La utilización de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en la administración de justicia es una cuestión improrrogable en México y el mundo, situación que ha sido confirmada por la emergencia sanitaria por el virus SARS-CoV-2 (COVID-19), que de un momento a otro paralizó numerosas actividades de las personas alrededor del mundo. Para mantener el orden social y los bienes comunes, fue necesario continuar con ciertas actividades, sobre todo las económicas, las de salud, la distribución de alimento y la administración de justicia.

Algunos países, principalmente los que pertenecen a la Unión Europea, ya tenían por lo menos 17 años desarrollando un *e-government* y una *e-justice*, que fueron puestos a prueba y, aun así, tuvieron que enfrentar complicaciones para su desarrollo adecuado. En otros casos, en países con menor desarrollo y acceso a las TICCAD, la emergencia sanitaria evidenció no solo la falta de infraestructura digital en los gobiernos, sino también el problema del acceso a las personas y la realidad de la brecha digital que enfrentan.

México, además de los bajos índices de acceso a las TICCAD que presenta, enfrenta problemas que podrían retardar la implementación y consolidación de la *e-justice*, a pesar de los cuatro casos significativos que tiene en la actualidad (Sala especializada en juicio en línea del Tribunal Federal de Justicia Administrativa, Portal de servicios en línea del Poder Judicial de la Federación, el Tribunal virtual del Estado de Nuevo León y el Tribunal electrónico del Estado de México). La poca infraestructura digital, la brecha digital, los altos índices de impunidad, el porcentaje elevado de cifra negra[1] y la poca utilización de las TICCAD para interactuar con el gobierno, representan un obstáculo serio que el país debe resolver de manera urgente.

[1] Número de delitos y delincuentes que no han sido descubiertos o condenados. (N. del E.)

La reforma constitucional de 2008 en materia de justicia penal y seguridad pública introdujo la oralidad en el procedimiento penal, como la forma predominante de su desarrollo, pero además propició las condiciones para la modernización de la justicia penal a través de las TICCAD. La implementación de la reforma no ha cumplido las expectativas de los expertos ni de los justiciables, que siguen padeciendo las inclemencias que siempre han caracterizado a la justicia penal en México.

## II. TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIÓN, CONOCIMIENTO Y APRENDIZAJE DIGITALES (TICCAD) Y BRECHA DIGITAL EN MÉXICO

Desde su aparición, las Tecnologías de la Información y la Comunicación (TIC) han contribuido al beneficio de las personas, facilitando la vida cotidiana, reduciendo los tiempos y permitiendo el acceso prácticamente a todo tipo de información desde cualquier parte del mundo. Las TIC fueron evolucionando e incluyendo otros aspectos como resultado de su utilización en la vida diaria de los gobiernos, las instituciones y las personas, hasta aparecer las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD).

El acceso a las TICCAD en México, según información de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares de 2019, arroja tres datos importantes: 1. El 70.1% de la población de seis años o más en México es usuaria de internet; 2. 20.1 millones de hogares (56.4% del total nacional) disponen de conexión a internet; y, 3. De la población con estudios universitarios, el 96.4% se conecta a la red, mientras que, del grupo de personas con estudios de educación básica, se conecta el 59.1 % (INEGI, 2020).

De la población en México que tuvo acceso a las TICCAD en 2019, el 76.6% reside en zonas urbanas, mientras que el 47.7% en zonas rurales; por nivel de escolaridad, de la población con educación superior tuvo acceso a internet el 96.4%, con educación media el 91.8%, y, con educación básica, el 59.1%; del total de población con acceso a internet, el 91.5% fue para entretenimiento; el 90.7% para información; el 90.6% para comunicarse; el 83.8% para educación y capacitación; y el 35.6% para interactuar con el gobierno (INEGI, 2020).

La distribución de los usuarios de internet por grupos de edad en 2019 en México, indica que los usuarios entre 18 y 24 años representan el 91.2%; entre 25 y 34 años, el 86.9%; entre 35 y 44 años, el 79.3%; entre 45 y 54 años, el 66.2%; y de 55 años y más, el 34.7% (INEGI, 2020).

Las estadísticas en México no solo reflejan un acceso precario a las TICCAD, además de que quienes las tienen las utilizan predominantemente para entretenimiento, lo cual muestra que la cultura del *e-gobierno* se encuentra por debajo de la media del porcentaje del 70.1% de la población.

En comparación con países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), entre 2005 y 2019 los países que tuvieron más acceso a internet fueron Corea del Sur en 2019, con 99.7% de los hogares, seguida por Noruega, con 98.4% en el mismo año. En el caso de México, el acceso a internet alcanzo el 56.4% de hogares (OCDE, 2020). Los países que tuvieron mayor porcentaje en el acceso a una computadora en casa fueron Países Bajos, con 97.6% en 2017, y Noruega, con 94.9 % en el mismo año, mientras que en México representó un 44.3% en 2019 (OCDE, 2020).

De la mano del acceso a las TICCAD se encuentra la brecha digital, concepto que en principio se limitaba a la falta de acceso físico a aquellas, y que luego incluyó a la de habilidades necesarias para el empleo adecuado de las tecnologías (Gómez, 2018). La OCDE definió a la brecha digital en estos términos: "La distancia existente entre individuos, áreas residenciales, áreas de negocios y geográficas en los diferentes niveles socio-económicos en relación a sus oportunidades para acceder a las nuevas tecnologías de la información y la comunicación, así como al uso de Internet, lo que acaba reflejando diferencias tanto entre países como dentro de los mismos." (OCDE, 2001)

Para México, la brecha digital representa el nuevo reto del milenio. El objetivo es que nadie quede excluido del uso correcto de las tecnologías (Senado de la República, 2018). El acceso a las TICCAD no es garantía de la inexistencia de la brecha digital, porque esta se encuentra incluso en población con estudios universitarios. En este sentido, el acceso a las TICCAD y la alfabetización y el aprendizaje digital representan un derecho humano de última generación, que permite a las personas acceder a mejores condiciones de vida; si bien en el caso de personas en edad de formación educativa (5-25 años) existen opciones como el Programa de Red Escolar (1997), el Programa de Inclusión y Alfabetización Digital (PIAD, 2013-2015), el Programa de Inclusión Digital (2016-2017) y la Nueva Escuela Mexicana

(2018-2024), en el caso de personas adultas y/o sin formación educativa la situación del acceso a las TICCAD y la brecha digital se complica.

La Asociación de Internet MX, en la decimoquinta edición del *Estudio sobre los Hábitos de los Usuarios de Internet en México 2019*, destacó: "No saber utilizar la herramienta es una barrera que se encuentra presente en el segmento de más de 34 años, por otro lado, el segmento de 17 años o menos percibe que una de sus principales barreras es el costo elevado del servicio." (AIMX, 2019)

En el caso de los adultos mayores, la brecha digital se ha convertido en una nueva forma de exclusión social, situación que se agudiza con la emergencia sanitaria por la COVID-19 (Fuerte, 2020); ante esta situación, la alfabetización y el aprendizaje digital en personas adultas y adultos mayores contribuirán a la inclusión social en todos sus aspectos (Paz, 2008). En sociedades del conocimiento en transición, es fundamental atender, de manera integral, el problema que representa la brecha digital en todos los rangos de edad, porque, en esa medida, el acceso pleno a las condiciones de las nuevas sociedades determinará el bienestar de vida de todas las personas.

## III. LA E-JUSTICE EN MÉXICO Y EN EL MUNDO

La *e-justice* se puede definir como "el recurso a las tecnologías de la información y la comunicación para mejorar el acceso de los ciudadanos a la justicia y para la eficacia de la acción judicial entendida como toda actividad consistente en resolver un litigio o en sancionar penalmente una conducta" (CCE, 2008:3), de modo que el aprovechamiento de las TICCAD en la labor judicial crea y consolida a la *e-justice*, que en muchos países, incluyendo a la Unión Europea, aún se encuentra en desarrollo. En México no termina de consolidarse; es algo relativamente nuevo en los órganos jurisdiccionales, y se ha limitado al acceso de la autoridad judicial y de los abogados postulantes.

En el ciclo de conferencias "Justicia Digital", que tuvo lugar en el Senado de la República el 10 de septiembre de 2020, se llegó al acuerdo sobre la necesidad de modernizar el sistema de justicia (Canal del Congreso, 2020). En México sobresalen la Sala especializada en juicio en línea del Tribunal Federal de Justicia Administrativa y el sistema electrónico del Poder Judicial de la Federación, a través del cual se pueden realizar varios trámites jurisdiccionales por medio de la Firma Electrónica. En los diversos Poderes

Judiciales locales de la República, se han ido implementado las TICCAD para varios trámites y actuaciones, principalmente la presentación de demandas, la revisión del expediente y la recepción de notificaciones. El Estado de Nuevo León cuenta con un Tribunal virtual que data de 2005, a través del cual se presta el servicio en línea para la consulta y el seguimiento de expedientes y notificaciones, así como la realización de trámites en línea, como el de promociones electrónicas (PJENL, 2020). Asimismo, desde 2018, en el Estado de México figura el Tribunal electrónico, el cual registra avances significativos en la implementación y desarrollo de la *e-justice*, y en donde se dictó la primera sentencia penal virtual el 12 de mayo de 2020, y donde se consumaron el primer divorcio en línea y la primera adopción de un niño vía remota, junto con una cantidad considerable de audiencias penales (u-GOB, 2020).

Recientemente, la organización México Evalúa presentó la *Guía de buenas prácticas en el uso de nuevas tecnologías para la impartición de justicia*, recopilando las mejores prácticas nacionales e internacionales para implementar nuevas tecnologías en la impartición de justicia (México Evalúa, 2020). La organización considera que la digitalización de la justicia es deseable por dos razones: por una parte, porque mejora la eficiencia de la impartición de justicia y, por otra, porque amplía los servicios judiciales durante la pandemia. En el documento se identifica una serie de propuestas para el caso mexicano, así como dificultades que podrían enfrentar los ciudadanos al momento de hacer uso de las TICCAD para acceder a la justicia en línea: "En cuanto a los usuarios, la implementación de este tipo de herramientas es continuamente acompañada de advertencias relacionadas con los riesgos potenciales de excluir o dejar en estado de indefensión a aquellos ciudadanos que no cuentan con los medios necesarios para interactuar virtualmente con la autoridad." (Guía, 2020:41)

Ante las posibles dificultades que tengan los justiciables para acceder a la *e-justice*, es importante introducirlos de manera directa, no solo al empleo de las TICCAD, sino también a las alternativas de justicia en línea con las que cuenta el poder judicial, en una labor de inclusión y tutela efectiva judicial, como propietario del problema legal que encomienda al profesional del derecho, para tratar de resolverlo. Sin embargo, las malas prácticas en el foro impiden que el justiciable acceda, en igualdad de condiciones, a los archivos que contienen el procedimiento jurisdiccional que enfrenta. En este sentido, el abogado postulante se convierte en un garante de ese acceso efectivo a favor de su representado, el cual en ninguna circunstancia puede

omitir o evitar, porque es él, precisamente, un equilibrio entre la autoridad y el justiciable; pero, para eso, el ejercicio de la abogacía debe adoptar herramientas informáticas y de comunicación que le permitan construir los puentes tecnológicos que faciliten la *e-justice* de su cliente.

Con todo, desde la praxis, la falta de inversión en recursos informáticos de innovación y capacitación para su aprovechamiento, por parte de abogados postulantes (despachos y oficinas jurídicos), más allá de la página web y las redes sociales gratuitas, es un factor que impide al justiciable hacer efectivo el derecho de acceso a la justicia.

El gran reto en México, más allá de la infraestructura para materializar la *e-justice*, es la educación tecnológica de los ciudadanos, que finalmente posibilitará que el acceso a la justicia pueda suceder las 24 horas de los 365 días del año, pero sin dejar de prestar atención a las limitaciones que existen en el país respecto al acceso universal a las TICCAD.

La *e-justice* será efectiva cuando cualquier justiciable tenga acceso de manera directa e irrestricta para resolver un problema o situación legales, sin la necesidad de un abogado, más allá de lo que sea necesario para su representación legal; esto le permitirá conocer, de manera íntegra, el contenido del procedimiento, la etapa procesal en la que se encuentra, las partes y autoridades que intervienen y el turno que tiene en el órgano jurisdiccional, lo cual, sin duda, no solo garantizará el acceso a la justicia de manera pronta y expedita, sino que contribuirá a una práctica profesional vigilada y supervisada de la autoridad judicial y de los abogados, reduciendo la mala praxis y privilegiando la ética judicial.

Lo cierto es que la *e-justice* no es una responsabilidad únicamente del poder judicial, sino que debe ser una red colaborativa que involucre a las instancias gubernamentales que guarden relación directa e indirecta con la actividad judicial y al sector privado.

Los beneficios que proporcionan las TICCAD en la administración de justicia no solamente tienen que ver con garantizar el derecho humano al acceso a la justicia; además, generan una repercusión directa en todas las personas que intervienen y también en el medio ambiente. Lo anterior significa que reducen los tiempos de traslado y espera, impactan en la disposición de recursos económicos, permiten conocer en tiempo real la situación de los procedimientos jurisdiccionales, acceder a los registros desde cualquier parte del mundo, y reducir el empleo de papel y tinta, entre otras cuestiones; sin embargo, del universo de personas que tienen acceso a internet en México, solo el 35.6% lo utiliza para interactuar con el gobierno, lo cual representa un reto significativo de cultura digital.

México enfrenta dos situaciones que es importante atender de manera simultánea. Primero, el acceso a la justicia es un problema grave y vigente, que refleja cifras que rozan el 99.7% de impunidad; con 49.67 puntos, ocupa el lugar 60 de 69 países (IGI, 2020)[2] en dicho rubro, y del 93.7% de cifra negra (ENVIPE, 2019); segundo, el problema, también grave y vigente, del acceso a las TICCAD y la brecha digital. Lo anterior complica de manera considerable la consolidación de una *e-justice*.

Existen aspectos y circunstancias que deben ser tomados en cuenta para definir un camino serio hacia la construcción de una *e-justice* eficaz y eficiente en el país, que se muestran en el siguiente cuadro:

| **SITUACIONES Y CIRCUNSTANCIAS PARA TOMAR EN CUENTA EN LA IMPLEMENTACIÓN Y DESARROLLO DE LA *E-JUSTICE* EN MÉXICO** | |
|---|---|
| Personas que interactúan con el gobierno a través de las tecnologías de la información | 35.6% del universo de personas que tienen acceso a internet en México |
| Personas que no saber utilizar la herramienta digital | 34 años y más (Rango de edad) |
| Impunidad | 99.7%<br>49.67 pts.<br>País 60 de 69 en impunidad (mundial)<br>Cuarto país más corrupto en América |
| Cifra negra | 93.7% |
| Brecha digital | Se amplía considerablemente a partir de los 35 años y más |
| Infraestructura digital en el poder judicial relevante | Sala especializada en juicio en línea del TFJA<br>Poder Judicial de la Federación<br>Tribunal virtual (Nuevo León)<br>Tribunal electrónico (Edo. de México) |

Fuente: Elaboración propia.

[2] Los países con impunidad muy alta son: 59) Guatemala (49.66 puntos); 60) México (49.67 puntos); 61) Kirguistán (51.80 puntos); 62) Nepal (51.94 puntos); 63) Guyana (52.07 puntos); 64) Paraguay (53.15 puntos); 65) Azerbaiyán (54.56 puntos); 66) Argelia (57.63 puntos); 67) Marruecos (58.04 puntos); 68) Honduras (59.69 puntos); y 69) Tailandia (62.82 puntos).

En el caso de la Unión Europea, la Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo "Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)" de 30 de mayo de 2008, estableció la importancia de dar prioridad a proyectos operativos; favorecer las arquitecturas descentralizadas sin descuidar la necesidad de una coordinación europea; y ajustarse con preferencia al marco jurídico existente, utilizando las herramientas informáticas para mejorar la eficacia de los instrumentos jurídicos adoptados.

Posteriormente, en el Plan de Acción E-justicia 2009-2013, se establecieron las directrices de la utilización de las TICCAD para la modernización de la administración de justicia (Bueno, 2011). El Plan de Acción señaló tres funciones de la *e-justice* europea: a) Acceso a la información correspondiente al ámbito de la justicia; b) Desmaterialización de los procedimientos; y c) Comunicaciones entre autoridades judiciales (DOUE, 2009).

En la actualidad, la Unión Europea, a través del Consejo, ha realizado una serie de conclusiones relativas al acceso a la justicia: aprovechar las oportunidades de la digitalización (CUE, 2020), en las cuales se destaca que "la transformación digital ha cambiado profundamente la vida de las personas en las últimas décadas y que seguirá haciéndolo", reconociendo que los sistemas judiciales son pilares fundamentales del Estado de derecho, y que "la realización de procedimientos judiciales digitales, la comunicación electrónica entre las partes, los tribunales y las autoridades, la transmisión electrónica de documentos y la celebración de audiencias y conferencias en línea, ya se han convertido en elementos importantes de una administración judicial eficiente en numerosos Estados miembros" (CUE, 2020:6).

Por su parte, el cuadro de indicadores de la justicia en la Unión Europea 2020, publicado por la Comisión Europea, en el que se muestran los avances significativos que ha tenido la *e-justice* desde 2003 hasta 2020, en temas como accesibilidad a información sobre el sistema judicial, presentación de demandas, la posibilidad de supervisar y hacer avanzar un procedimiento en línea, acceso a las sentencias en línea (partes y público en general), aspectos financieros de los órganos judiciales, educación sobre derechos a través de las TICCAD, disponibilidad de conexión a internet en tribunales, asistencia jurídica gratuita en línea, información disponible para hablantes no nativos, así como información dirigida a las personas con discapacidad visual o auditiva (CE, 2020).

Por lo que hace a América Latina, Chile expidió en 2016 la Ley de Tramitación Electrónica, por la que se crea una oficina virtual judicial, permitiendo a los abogados y ciudadanos gestionar en línea sus causas, audiencias, notificaciones y otros procedimientos legales, facilitando la diligencia de exhortos, cartas rogatorias, oficios y comunicaciones judiciales a través del sistema de tramitación electrónica del poder judicial (red de tribunales nacionales). Además, con la expedición del instructivo de transformación digital en 2019, se han establecido políticas para gestionar la modernización del gobierno en todas sus instancias, entre las que sobresalen: a) Política de identidad digital única: gestionar una identidad digital única (clave única) para que cada ciudadano se encuentre identificado de la misma manera en todas las plataformas digitales del Estado; b) Política de cero fila: digitalizar los trámites públicos para que los ciudadanos no tengan que hacer fila en las instituciones; y c) Política de cero papel: optimizar la gestión documental y el control de expedientes para eliminar de forma gradual el uso de papel.

A nivel global, la pandemia de la COVID-19 no solamente ha paralizado, en algunos casos por completo, a las principales economías mundiales y locales, sino también los servicios gubernamentales, entre ellos la administración de justicia, lo cual ha producido su inevitable digitalización, haciendo necesaria la utilización cotidiana de las TICCAD, con lo que se crea una nueva forma de administrar justicia y servicios legales, que ya venía en desarrollo desde 2003, por lo menos.[3]

## IV. EL DERECHO HUMANO DE ACCESO A LA JUSTICIA FRENTE A LAS TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIÓN, CONOCIMIENTO Y APRENDIZAJE DIGITALES (TICCAD)

A partir de 2013, el Consejo de la Judicatura Federal, actuando coordinadamente con la Suprema Corte de Justicia de la Nación y el Tribunal Electoral del Poder Judicial de la Federación (Acuerdo General Conjunto 1/2013; Acuerdo General Conjunto 1/2014 y Acuerdo General Conjunto 1/2015), ha destacado la importancia de la utilización de las TIC, creando

[3] Desde el año 2003, la Comisión de las Comunidades Europeas, ha desarrollado el Portal de la Red Judicial Europea en materia civil y mercantil, y ha apoyado la realización de los Atlas judiciales penales y civiles que permiten a los especialistas identificar a las autoridades judiciales competentes en los distintos puntos del territorio.

incluso Direcciones Generales de Tecnologías de la Información en cada órgano del Poder Judicial de la Federación, así como destacando la importancia de la eficacia y eficiencia en su uso, reconociendo que constituyen un elemento fundamental para garantizar el derecho humano de acceso a la justicia, reconocido por el artículo 17 de la Constitución Política de los Estados Unidos Mexicanos, recalcando la importancia del juicio de amparo penal y los procedimientos penales.

La Suprema Corte de Justicia de la Nación, en criterios aislados y de jurisprudencia, se ha referido a las TIC como una herramienta que favorece el acceso a la justicia de las personas en diversos procedimientos jurisdiccionales, especialmente el juicio de amparo y los procedimientos penales.

Recientemente, el Pleno de la Suprema Corte, al resolver la contradicción de tesis 28/2019,[4] concluyó que las tecnologías de la información han representado un cambio importante en el ámbito judicial, que necesariamente requerirá de reglas claras y de fácil acceso que permitan, sobre todo al justiciable, acceder de forma más expedita a la impartición de justicia, situación que el propio Pleno dejó clara en la contradicción de tesis 45/2018, que originó la tesis de título y subtítulo: "DEMANDA DE AMPARO INDIRECTO PRESENTADA A TRAVÉS DEL PORTAL DE SERVICIOS EN LÍNEA DEL PODER JUDICIAL DE LA FEDERACIÓN. PROCEDE DESECHARLA DE PLANO CUANDO CARECE DE LA FIRMA ELECTRÓNICA DEL QUEJOSO."[5] En la ejecutoria[6] se justifica el sentido de la jurisprudencia, atendiendo a que:

> …la falta de firma constituye un obstáculo para considerar que es el agraviado quien inicia la actividad jurisdiccional, sin que al respecto sea relevante el hecho de que el quejoso contara con nombre de usuario y firma electrónica, que se requieren para ingresar al Portal de Servicios en Línea (…) pues ese ingreso no produce los efectos de validación de la evidencia criptográfica, porque son cosas distintas. (…) La firma electrónica es el conjunto de

[4] *Cfr.* Tesis P./J. 18/2020 (10a.), de título y subtítulo: "INCIDENTE DE SUSPENSIÓN. LAS VIDEOGRABACIONES CONTENIDAS EN MEDIOS ELECTRÓNICOS TIENEN EL CARÁCTER DE PRUEBA DOCUMENTAL Y, POR TANTO, PUEDEN SER OFRECIDAS POR LAS PARTES EN AQUÉL." *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 82, enero de 2021, t. I, p. 5. Esta tesis se publicó el viernes 08 de enero de 2021 a las 10:09 horas en el *Semanario Judicial de la Federación* y, por ende, se considera de aplicación obligatoria a partir del lunes 11 de enero de 2021, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 16/2019. Registro digital: 2022595. (N. del E.)

[5] *Cfr.* Tesis P./J. 8/2019 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 65, abril de 2019, t. I, p. 79. Esta tesis se publicó el viernes 26 de abril de 2019 a las 10:30 horas en el *Semanario Judicial de la Federación* y, por ende, se considera de aplicación obligatoria a partir del lunes 29 de abril de 2019, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 19/2013. Registro digital: 2019715 (N. del E.)

[6] *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 67, junio de 2019, t. I, p. 37. Registro digital: 28811 (N. del E.)

> datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control.

Podría considerarse que el sentido estricto y formalista del Pleno de la Corte no garantiza y pone en riesgo el derecho humano de acceso a la justicia, porque, con independencia de las justificaciones técnicas sobre la necesaria utilización de la firma electrónica al momento de ingresar una demanda a través del portal de servicios en línea, debe permear el hecho de que la finalidad de las TICCAD en la administración de justicia es facilitar el acceso a cualquier ciudadano, y no representar un obstáculo en el que solamente el 70.1% de la población en México tenga acceso a internet, y que, de ese porcentaje, el 91.5% lo haga para buscar entretenimiento, y solamente el 35.6% para interactuar con el gobierno. A lo anterior se agrega que, para la tramitación de la firma electrónica ante el Poder Judicial de la Federación, aunque los requisitos sean mínimos, el proceso de registro sin asistencia u orientación es complicado, además de la falta de campañas sociales por parte del poder judicial para concientizar a la población sobre su tramitación y la importancia que tiene para la presentación de demandas y prosecución del juicio de amparo.

El Máximo Tribunal no debe desatender la finalidad ni la naturaleza del juicio de amparo, que se describieron de forma excepcional en el siguiente criterio jurisprudencial:[7]

> El juicio de amparo es el instrumento procesal creado por nuestra Constitución Federal para que los gobernados puedan hacer proteger sus garantías constitucionales de las violaciones que al respecto cometan las autoridades. Y ese instrumento no sólo debe ser motivo académico de satisfacción, sino que también en la vida real y concreta debe otorgar a los ciudadanos una protección fácil y accesible para sus derechos más fundamentales, independientemente del nivel de educación de esos ciudadanos, e independientemente de que tengan o no, abundantes recursos económicos, así como del nivel de su asesoría legal. Esto es importante, porque la protección que el Poder Judicial Federal hace de las garantías constitucionales de los gobernados debe funcionar como un amortiguador entre el poder del Estado y los intereses legales de los individuos, y en la medida en que ese amortiguador funcione, en vez de sentirse un poder opresivo, se respirará un clima de derecho. Luego los Jueces de amparo no deben hacer de la técnica de ese juicio un monstruo del cual se pueda hablar académicamente, pero que resulte muy limitado en la práctica para la protección real y concreta de los derechos constitucionales real y concretamente conculcados. De donde se desprende que las normas que regulan el procedimiento constitucional deben

[7] *Cfr.* Tesis de rubro: "AMPARO, FINALIDAD Y NATURALEZA DEL." *Semanario Judicial de la Federación*, Séptima Época, vol. 103-108, Sexta Parte, p. 285. Registro digital: 252943 (N. del E.)

> interpretarse con espíritu generoso, que facilite el acceso del amparo al pueblo gobernado. En un régimen de derecho, lo importante no es desechar las demandas de amparo que no están perfectamente estructuradas, sino obtener la composición de los conflictos que surgen entre gobernados y gobernantes, y resolver judicialmente sobre el fondo de las pretensiones de éstos.





La transición hacia una era digital de la justicia debe contemplar las áreas de oportunidad del país en diversos sectores y contribuir a mejorarlos. El Poder Judicial de la Federación, en especial la Suprema Corte, debe reconocer que el país se encuentra en un proceso de transición hacia la *e-justice*, y que el principal objetivo es garantizar y potenciar el acceso a la justicia; en estos momentos, la empatía de sus criterios se debe ajustar a la realidad de la vida social en el país.

En general, el poder judicial en México avanza hacia una *e-justice* completa, eficaz, eficiente y, sobre todo, de uso fácil y rápido para toda la ciudadanía, para garantizar y potenciar el derecho de acceso de la justicia en cualquier materia y ante cualquier autoridad; pero no debe olvidar atender los problemas pendientes de la administración de justicia, lo que será determinante para el éxito de la justicia digital; de otra manera, esta no constituirá una herramienta diferenciadora que mejore la calidad de vida de los justiciables.

## V. LA *E-JUSTIC*E PENAL EN MÉXICO

La Reforma Constitucional en Materia de Justicia Penal y Seguridad Pública de 2008, introdujo la oralidad en el procedimiento penal como la forma predominante de su desarrollo; pero, además, propició las condiciones para la modernización de la justicia penal a través de las TICCAD.

En materia de justicia penal, el procedimiento cuenta con limitaciones considerables frente a la sociedad del conocimiento y las TICCAD. La implementación de la reforma no ha satisfecho las expectativas de los expertos ni mucho menos de los justiciables. Las TICCAD se han convertido en un aliado importante de la nueva forma de tramitación de los procedimientos penales en México a partir de 2008, sobre todo por las grabaciones de audio y video, que en buena medida han suplido al expediente en papel, así como el seguimiento del procedimiento a través de la información que se publica en las páginas web del poder judicial de las diferentes entidades federativas, principalmente acuerdos (resumen) y, en el mejor de los casos,

el acceso a la causa penal digitalizada a través de un usuario y contraseña. En el caso de la investigación (inicial y complementaria), el uso de las TICCAD se encuentra orientada a las diversas técnicas de investigación, hasta donde lo permitan la infraestructura y el presupuesto de las fiscalías en el país, manteniéndose la carpeta de investigación en papel, sobre la cual las partes (acusadora y defensa) deberán estudiar sus intervenciones, y que siempre es la principal herramienta que se utiliza en las audiencias penales.

En varios de sus artículos, el Código Nacional de Procedimientos Penales establece disposiciones relativas al uso de las tecnologías: a) Cuando una persona con algún tipo de discapacidad los requiera para que le permitan obtener, de forma comprensible, la información que involucre sus intereses dentro del procedimiento (art. 45, segundo párrafo); b) La presentación de denuncias o querellas, la transmisión de medios de prueba y actos procesales (art. 51); c) Para el registro de todas las audiencias en los diferentes procedimientos penales (art. 61, primer párrafo); d) Las notificaciones a través de medios tecnológicos [art. 82, fracción I, inciso b)]; y e) Para reproducir datos de prueba o prueba (art. 381). En materia de justicia penal, la Federación y las entidades federativas proveerán los recursos tecnológicos que requiera la implementación del procedimiento penal acusatorio.

La implementación y el desarrollo de la *e-justice* deberá nutrir, en igualdad de condiciones, al procedimiento penal acusatorio en las diferentes entidades federativas; la propuesta de su utilización deberá estar orientada más allá de las tecnologías disponibles de uso general por la población, creando una infraestructura única que garantice la imparcialidad, la protección de los datos personales y la garantía del respeto a los derechos de todos los involucrados.

## VI. FUENTES DE CONSULTA

Baena. L. (2020). "La #JusticiaDigital del futuro llega con el Tribunal Electrónico del PJEdomex: u-gob." Recuperado de: https://u-gob.com/la-justiciadigital-del-futuro-llega-con-el-tribunal-electronico-del-pjedomex/

Bueno, F. (2011). "Justicia online y ciudadanía: el portal europeo e-justicia como medio de información y apoyo a los ciudadanos para solventar sus litigios transfronterizos." *Revista Europea de Derechos Fundamentales*. Núm.

18, julio-diciembre. Recuperado de: file:///C:/Users/Usuario/Downloads/Dialnet-JusticiaOnlineYCiudadania-3906387.pdf

Comisión de las Comunidades Europeas (2008). Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo "Hacia una estrategia europea en materia de E-justicia (Justicia en línea)". Bruselas: Comisión de las Comunidades Europeas.

Comisión Europea (2020). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. Cuadro de Indicadores de la Justicia en la EU de 2020*. Bruselas: Comisión Europea.

Consejo de la Unión Europea (2020). *Conclusiones "Acceso a la justicia: aprovechar las oportunidades de la digitalización"*. Bruselas: Consejo de la Unión Europea.

Diario Oficial de la Unión Europea (2009). *Informaciones Procedentes de Instituciones y Órganos de la Unión Europea, Consejo. Plan de Acción Plurianual 2009-2013 Relativo a la Justicia en Red Europea*. Bruselas: Consejo de la Unión Europea.

Estudios antiguos (2020). *Hábitos de internet*: Asociación de Internet MX. Recuperado de: https://www.asociaciondeinternet.mx/estudios/habitos-de-internet

Fuerte. K. (2020). "¿Cómo afecta la brecha digital a los adultos mayores?" Observatorio de innovación educativa, Instituto Tecnológico de Estudios Superiores de Monterrey. Recuperado de: https://observatorio.tec.mx/edu-news/brecha-digital-adultos-mayores-exclusion-social

H. Congreso de la Unión (2020). Código Nacional de Procedimientos Penales. Ciudad de México: H. Congreso de la Unión.

H. Congreso Nacional de Chile (2016). *Nueva Ley de Tramitación Electrónica 20.886*. Santiago de Chile: H. Congreso Nacional de Chile.

H. Congreso Nacional de Chile (2019). *Instructivo de transformación digital*. Santiago de Chile: H. Congreso Nacional de Chile.

Información; Boletines (2018). Senado de la Republica. Recuperado de: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/41122-abatir-el-analfabetismo-tecnologico-el-nuevo-reto-del-milenio.html

Instituto Nacional de Estadística y Geografía (2019). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2019 (ENVIPE)*. Recuperado de: https://www.inegi.org.mx/programas/envipe/2019/

Instituto Nacional de Estadística y Geografía (2020). *Estadísticas a propósito del día Mundial del internet. Datos Nacionales*. Recuperado de: https://

www.inegi.org.mx/contenidos/saladeprensa/aproposito/2020/eap_internet20.pdf

México Evalúa (2020). *Guía de buenas prácticas en el uso de nuevas tecnologías para la impartición de justicia*. Recuperado de: https://u-gob.com/la-justicia-digital-del-futuro-llega-con-el-tribunal-electronico-del-pjedomex/#google_vignette

Organización para la Cooperación y el Desarrollo Económicos (2020). *Acceso a computadoras desde casa*. Recuperado de: https://data.oecd.org/ict/access-to-computers-from-home.htm#indicator-chart

Organización para la Cooperación y el Desarrollo Económicos (2020). *Acceso a Internet*. Recuperado de: https://data.oecd.org/ict/internet-access.htm#indicator-chart

Paz, L. (2008). "Alfabetización digital en el Adulto Maduro. Una estrategia para la inclusión social." XVI Congreso Internacional sobre Educación Electrónica, Móvil, Virtual y a distancia, Bogotá, Colombia. Recuperado de: http://sired.udenar.edu.co/3620/

Secretaria de Educación Pública (2020). *Agenda digital educativa*. Recuperado de: https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2020-02-05-1/assets/documentos/Agenda_Digital_Educacion.pdf

*Semanario Judicial de la Federación* (2020). Suprema Corte de Justicia de la Nación. Recuperado de: https://sjf2.scjn.gob.mx/busqueda-principal-tesis

Universidad de las Américas de Puebla (2020). *Índice Global de Impunidad México 2020*. Recuperado de: https://www.udlap.mx/cesij/files/indices-globales/0-IGI-2020-UDLAP.pdf

Video en Demanda (2020). Comisión de Justicia. "Ciclo de conferencias: Justicia Digital." Parte 2. Canal del Congreso, el Canal de la Unión. Recuperado de: https://www.canaldelcongreso.gob.mx/voda/reproducir/1_styiay74/Comision_de_Justicia_Ciclo_de_conferencias_Justicia_Digital_Parte_2

# SENTENCIA Y PREDICCIÓN ALGORÍTMICA PENAL. HERRAMIENTA O SUPLENCIA HUMANA

Juliana Vivar Vera*

* Profesora del Departamento de Derecho de la Escuela de Ciencias Sociales y Gobierno. Región Centro-Sur del Tecnológico de Monterrey. Contacto: jvivarv@tec.mx

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Sentencia penal** | *Criminal sentence* |
| **Procesador predictivo** | *Predictive processor* |
| **Jueces** | *Judges* |
| **Función judicial** | *Judicial function* |
| **Inteligencia artificial** | *Artificial intelligence* |



**Resumen.** Este artículo pretende mostrar la complejidad de la sentencia penal en México, junto con un panorama de inclusión de los *softwares* predictivos de aquella. Se resaltan las características que identifican al juez humano y al procesador para un trabajo conjunto o, incluso, advirtiendo la sustitución del humano en el dictado de sentencias penales.

**Abstract.** This article aims to show the complexity of the criminal sentence in Mexico, together with an overview of the inclusion of predictive software. The characteristics that identify the human judge and the processor are highlighted for a joint work or, even, considering the substitution of the human in the issuance of criminal sentences.



Fecha de recepción: 13 de enero de 2021
Fecha de aceptación: 16 de marzo de 2021

SUMARIO:







## I. INTRODUCCIÓN

La principal función jurisdiccional es la decisión. Una decisión judicial penal representa una responsabilidad no solo jurídica, sino de vida para el destinatario y para el propio juez; se trata, además, de un elemento simbólico poderoso del Estado para mantener el monopolio del control social. Así, la complejidad en su diseño no solo es formal, sino material.

Los *softwares* predictivos están a la vanguardia en otros países en las decisiones jurídicas en materias distintas de la penal. En México, el proyecto de reforma judicial con y para el Poder Judicial, propuesto por este último el 12 febrero de 2020, se refiere, entre otros temas, a agilizar la tramitología del acceso a la justicia; sin embargo, el avance acelerado de la tecnología a nivel mundial experimenta la combinación algorítmica que emula el lenguaje comprensivo humano para acercarse a la aplicación teórica argumentativa que justifica la decisión judicial con motivación y fundamentación de derechos humanos, aplicada al caso concreto para auxiliar al juez en su función de sentenciar.

La complejidad de que el *software* predictivo sea auxiliar del juez o, incluso, en el futuro, lo sustituya en la labor de sentenciar penalmente, debe analizarse conforme a las características que distinguen al humano de la máquina, y a aquellas que les son comunes, como el error judicial y el sesgo algorítmico. El cambio de paradigma de la función judicial ante la inminente incidencia de la tecnología es necesario, a fin de que el trabajo mecánico y la capacidad creativa humana se distingan y la esperada justicia penal, sensible a la realidad humana, sea un hecho.

El objetivo de la presente contribución es mostrar la complejidad que representa la función de sentenciar penalmente por el juez humano y con el auxilio de los *softwares* predictivos; para lograrlo, se enfatizarán de forma general, en un primer punto, los elementos que complican la función de

sentenciar en materia penal; posteriormente, se mostrará el impacto del funcionamiento de los *softwares* predictivos, siguiendo con la descripción coincidente del juez humano y el robot, que radica en el error judicial y el sesgo algorítmico, para concluir resaltando las características de la función del juez penal humano y del *software* predictivo.

## II. LA COMPLEJIDAD EN LA CONSTRUCCIÓN DE LA SENTENCIA PENAL

La sentencia penal tiene sesgos, tanto en su construcción como en su ejecución. La motivación para declarar la responsabilidad penal tiene sesgos valorativos desde que las partes presentan su teoría del caso; así, el abogado utiliza técnicas y estrategias para dar la dirección intencional propia al caso y convencer al juez; luego, en la individualización de la pena, si bien existen parámetros legales, estos dan lugar también a la discrecionalidad judicial para imponer una pena exacta. En este primer acercamiento, vale preguntar si tres historias distintas —la que acusa, la que defiende y la que vela por la víctima— ayudan a que el juez tenga certeza de que su decisión final es justa.

Por supuesto que la simpleza que representa el protocolo de un juicio tiene una profunda justificación teórica. El derecho penal se va ajustando a los avances teóricos que ahora se ven indefinidos; la teoría de Robert Alexy, tomada como modelo de optimización de principios para la interpretación de los derechos humanos (Alexy, 1993), ha sido ya criticada[1] y, por tanto, provoca incertidumbre en la conceptualización general del derecho. El sistema de justicia penal mexicano, a partir de la reforma constitucional en materia penal publicada el 18 de junio de 2008 en el *Diario Oficial de la Federación*, ofreció una metamorfosis en el indeseable, pero vital, sistema de justicia penal, y este fue fortalecido con la reforma constitucional de 2011, con lo cual se constituyó y consolidó con base garantista y de aplicación mínima punitiva —en armonía con la teoría penal minimalista de Luigi Ferrajoli—.

Sin embargo, el derecho penal mínimo sigue siendo aspiracional; se encuentra plasmado en las leyes penales, pero sin alcance a la realidad de las sociedades desiguales, lo cual dificulta su interpretación con el principio de la exacta aplicación de la ley penal y acorde al seguimiento metodológico

[1] Por autores como Juan Antonio García Amado, Manuel Atienza y Jan Sieckman, entre otros.

de la teoría del delito, que tiene por resultado la contradicción entre la violencia y los derechos humanos.

La costumbre en el control social formal del sistema mixto penal que se aplicaba antes de esta reforma,[2] siguió arraigada en el nuevo sistema, con la clásica estructura lógica positivista de la norma jurídica. La imposición de límites a la conducta de los integrantes de la sociedad, en forma de descripciones normativas jurídicas, conduce a una consecuente sanción por el juez, quien tiene el *ius puniendi* en un aparente respeto al principio de legalidad por la exacta aplicación de la ley penal (*nullum crimen nulla poena sine lege*), puesto que, para que una conducta sea considerada como delito, debe contener los elementos del particular tipo penal (la existencia de tipicidad) y, al establecerse la culpabilidad, se aplica una sanción dentro del parámetro establecido en la punibilidad.

La aplicación técnica es apreciada en la ley; sin embargo, con el principio de convencionalidad es posible lograr el objetivo ambicioso de la reforma al sistema de justicia penal:

> Mejorar la impartición de justicia penal en nuestro país, a través de un procedimiento acusatorio y oral, más transparente, dinámico y garantista, tanto para los imputados como para las víctimas, en el que se cumpla con el objetivo de esclarecer los hechos, proteger a los inocentes, procurar que los culpables no queden impunes y que se reparen los daños causados por el delito. En el Nuevo Sistema de Justicia Penal los operadores jurídicos tienen un rol más participativo, transparente y con pleno respeto a los derechos fundamentales del imputado y de la víctima. (Consejo de la Judicatura Federal)

El juez se ajusta a la tipicidad del delito con base en el código sustantivo penal, y a las reglas procedimentales marcadas por el Código Nacional de Procedimientos Penales. Sin duda, esta legislación es la que identifica la disciplina jurídica del caso, pero no es suficiente; las leyes alternas y la jurisprudencia nacional e internacional, de aplicación transversal y específica en cada caso, dificultan la función de sentenciar y el resultado evidencia que el sistema penal acusatorio actual no ha garantizado el principio de convencionalidad en el ejercicio de ponderación y fundamentación razonada del sinnúmero de leyes existentes.

Por otra parte, el marco legal muestra que el derecho aún se esfuerza por lograr su pretensión de ocuparse de conductas cuando, probablemente, no están reservadas a él, como sucede con el delito de aborto, cuando el sujeto

[2] A pesar de que el sistema mixto combina elementos del inquisitivo y del acusatorio, la costumbre positivista y punitiva seguía arraigada en los jueces.

activo es la madre, y se atenúa la pena con circunstancias discriminadoras para la mujer: que el producto de la gestación sea fruto de unión ilegitima, que la mujer no tenga mala fama y haya logrado ocultar su embarazo; o la descripción de la Norma Oficial Mexicana 046-SSA2-2005. Violencia familiar, sexual y contra las mujeres. Criterios para la prevención y atención,[3] que alude a la posibilidad de aborto en niñas mayores de 12 años en caso de violación. De este modo, se observa que la regulación legal, como herramienta, puede ser letal contra la sociedad desde su redacción, y contraponerse a la garantía de los derechos humanos.

Ante este panorama complejo, la aplicación del sistema de justicia penal refleja una notable vulneración al artículo 30 de la Declaración Universal de los Derechos Humanos. Esto es así, puesto que la estructura legal e institucional refleja la función declarada de respeto a los derechos humanos; pero la función latente, que es la que corresponde a la sociedad sufriente, se refleja en las violaciones claras y constantes a los derechos de las personas. La reforma estructural en materia penal aun no muestra una valoración internacional positiva,[4] pero sí constituye el elemento simbólico de muerte en vida. El juez es el verdugo por el cual se daña la existencia de forma irreparable a través de la pena impuesta, y la satisfacción de justicia sigue siendo la esperanza de los justiciables.

## III. EL IMPACTO DEL *SOFTWARE* PREDICTIVO EN LA DECISIÓN PENAL

La normalización de los diversos usos tecnológicos ha sido bien recibida por las instituciones, porque auxilian a los servidores públicos a volver eficientes los procesos burocrático-técnicos. Las instituciones de justicia no fueron la excepción y los programas de "tramitología" sirvieron para el efectivo acceso a la justicia y la transparencia del proceso; primero, en la publicación de resoluciones en línea, el estado del expediente, etc.,[5] y después los juicios en línea y la tecnología avanzada para las audiencias orales.

[3] Disponible en: https://www.cndh.org.mx/DocTR/2016/JUR/A70/01/JUR-20170331-NOR19.pdf (N. del E.)

[4] El World Justice Project ubica a México en el lugar 108 de 128 en cuanto a adherencia al Estado de derecho, y en el lugar 119 en cuanto a justicia penal. *World Justicie Project* (2020). Índice de Estado de Derecho 2020. Disponible en: https://bit.ly/3ntgqj

[5] La exposición de motivos de la reforma al Sistema de Justicia Penal contempla aún el uso de la tecnología como auxiliar de trámite en la administración de justicia, como en la recepción y transmisión de medios de prueba y actos procesales, interpretación de idioma y el registro de audio y video de las audiencias. Ver: https://www.senado.gob.mx/comisiones/justicia/docs/Iniciativa/Iniciativa_Conjunta_unica.pdf

La experiencia exitosa de la evolución algorítmica del caso "Watson",[6] utilizada posteriormente para el procesamiento de bibliografía en medicina y luego en lo legal, llevó a dar mayor oportunidad de adaptar la llamada "inteligencia artificial" al conocimiento legal para la razonabilidad lógico-formal predictiva en las sentencias.

De esta forma, los algoritmos predictivos se fueron introduciendo en el sistema de justicia penal con pretensión de ayuda a la actividad jurisdiccional. En materia penal, la reserva a la utilización de *softwares* predictivos resultaba obvia, en virtud de que el resultado final consiste en una sentencia que, en caso de ser condenatoria, necesariamente viola derechos humanos para el destinatario; entonces, la relación entre juzgador y justiciable sería interrumpida mecánicamente en la valoración libre y lógica que se encuentra destinada a los jueces humanos. El derecho penal es la disciplina indeseable más cercana a la sociedad por la fractura de las relaciones humanas, y es necesario que las decisiones penales tengan un papel simbólico en su interpretación; pero, al mismo tiempo, que sea representativa de acciones para mejorar tales relaciones sociales, con objeto de reducir la violencia.

La complejidad en el tecnicismo del *software* predictivo radica en la alimentación de los datos y en su procesamiento, así como en la funcionalidad del documento. La creación previa de derecho por las resoluciones es útil para que la máquina ocupe palabras clave precargadas para hacer la búsqueda y predecir la solución. Tal es el caso del *software* "Prometea", el cual sigue los siguientes pasos: en primer lugar, lee todas las actuaciones previas del caso disponibles y puestas en línea en la página de consulta pública de expedientes, donde hay más de 300,000 documentos; luego, el sistema hace un paneo de las palabras clave (preconfiguradas) del expediente con los patrones de los precedentes judiciales de la base de datos y, en menos de 15 segundos en promedio, predice cuál es la solución que debería adoptarse; acto seguido, ofrece al usuario el modelo que debería utilizar y le hace unas breves preguntas, para adecuar el modelo al expediente en concreto (Corvalan, 2018).

Puede observarse en este procedimiento que la intervención humana es mínima y, en algunos casos, la intención de los programadores es que llegue a ser innecesaria (Sourdin, 2018: 62); es por ello que algunos desarrolladores siguen trabajando en el perfeccionamiento de las combinaciones

[6] IBM revolucionó la tecnología con la plataforma Watson. El avance innovador del *machine learning* permitió que compitiera en argumentos y en juegos, y ahora crea modelos potentes a partir de cero. IBM, *Watson Anywhere*. Disponible en: https://ibm.co/3orvwqy

algorítmicas del aprendizaje profundo (*deep learning*) (Chollet, 2018: 8), subcampo específico del aprendizaje automático o aprendizaje de capas sucesivas, de cada vez más representaciones significativas mediante técnicas como la retropropagación *(backpropagation*) (Chollet, 2018: 332), de tal manera que se tenga la capacidad del razonamiento formal y abstracto a partir de la intuición, para lograr una argumentación lógica que parta de una "minería" (exploración) y análisis de textos legales, que tome modelos de razonamiento y representación del conocimiento legal conforme a la teoría jurídica, la interpretación legal y la incidencia de la dimensión epistémica de la política. Los modelos de razonamiento *Assertions on individuals* (A-BOX) y *Assertions on concepts* (T-BOX) están desarrollando esta tecnología para el análisis sintético y semántico, a fin de crear un corpus de normas multilingües.[7] Mientras tanto, hoy en día el aprendizaje profundo sigue siendo utilizado para reducir la carga cognitiva técnica, como lo ofrece el desarrollador "Keras".[8]

Al no ser el derecho ostensivo (Tamayo, 2011), el verbo "decir" representa una gran responsabilidad para quien realizará la función judicial, puesto que la complejidad del concepto lo hace indefinible y, por tanto, las palabras puestas en formato correcto al comunicarlo son el objetivo de segundo plano, pues lo esencial son el sentido y la intención con que se producen. El fondo de la sentencia penal es la que impacta y transforma vidas; el formato de las palabras con que esta es producida solo son la herramienta con que aquella intención se visibiliza.

La forma de comunicar el sentido de la decisión penal debe considerar la relación entre quien la produce y quien la recibe. El error, sin duda, es que esta sencilla forma de comunicación es sustituida por la relación entre el juez y la ley. Las diversas teorías argumentativas han basado sus postulados en el convencimiento a través de la comunicación entre personas, donde las palabras representan un significado. En comparativo, la forma de comunicación que ofrece el procesador es puramente racional, formal y matemática, con lenguaje natural puesto por programadores humanos, no especializados en la complejidad de la justificación interna y externa que implica la sentencia; por ello, los esfuerzos de emulación del lenguaje también están a la vanguardia, como en el caso de Python (un lenguaje de

[7] Puede encontrarse mayor referencia y detalle de los proyectos en: Mirel. "Mining and reasoning with legal text". Disponible en: https://www.mirelproject.eu/ y "Laboratorio de Investigación y desarrollo de la Inteligencia Artificial-LIDIA". Disponible en: thttp://lidia.cs.uns.edu.ar/home/

[8] Puede consultarse más sobre ello en: Keras, K. "Simple. Flexible. Powerful". Disponible en: https://keras.io/

programación multiparadigma). El lenguaje, entonces, provendrá siempre de una persona, ya sea directa o indirectamente; por tanto, podrá haber fallas en el sentido de la decisión penal.

Por eso, las intersecciones valorativas de la justicia diferenciada son esenciales para la interpretación material y no violatoria de derechos humanos que dificulta la función judicial en materia penal, como son la perspectiva de género, la justicia para adolescentes, la justicia restaurativa y los usos y costumbres en comunidades indígenas, por ejemplo, donde impera la necesidad interdisciplinaria de modelos teóricos o epistémicos como la decolonialidad, las teorías de violencias y de paz, el feminismo, etc., que convivan con los correspondientes al derecho penal, porque la traducción de las desigualdades particulares deriva de fenómenos amplios, como sería un caso de feminicidio que necesariamente derivó de una violencia previa de género, término que, a su vez, es interpretable socialmente y diferenciado entre comunidades por genealogías antropológicas.

A pesar de que el algoritmo matemático hiciera cálculos de entendimiento del contexto, solo el juez humano podría alcanzar la comprensión, en nuestro ejemplo, de la cadena de sucesos cuyo resultado es una mujer muerta por un sujeto; más aún, si se trata de un caso nuevo, el *software* no tendría elementos para predecir, por no tener ejemplos anteriores con los cuales relacionarlo o, si los hay y son suficientes, que todos estos hayan sido resoluciones con perspectiva de género, tomando los elementos anteriores que den sentido a la ley que aplicó; de lo contrario, la máquina tomará este sesgo omisivo y lo perpetuará.

Otra cuestión en el impacto de la decisión penal es la reparación del daño a la víctima, tema que, en el sistema de justicia penal actual de México, es referente internacional. A diferencia de otros países, la reparación es integral y extiende su aplicación a una persona que ha sufrido un daño, no solo a consecuencia de un delito sino, de forma transversal, a quien le han sido violentados sus derechos humanos. Por tal motivo, la reparación integral del daño tiene un significado más profundo y ambicioso, detallado en la Ley General de Víctimas, que hace imprescindible la interdisciplinariedad e interseccionalidad y es también una función judicial el determinarlo a pesar del control horizontal, haciendo una correspondencia entre el impacto del daño y la posibilidad de cubrirlo en corresponsabilidad con el Estado, de manera que sean satisfechas las cinco grandes medidas que contempla la ley: restitución, rehabilitación, compensación, satisfacción y garantía de no repetición; todas ellas aplicadas con enfoque diferenciado

en sus dimensiones individual, colectiva, material, moral y simbólica (Ley General de Víctimas, 2016). Esta complejidad, obligada por el juez y representada por el asesor jurídico victimal en el proceso penal, evidenciaría la expectativa de justicia a la víctima, que aún es utópica y que tampoco está siendo contemplada por procesadores predictivos como *Prometea, Xiao Fa* y *Northpointe Suite Risk Need Assessments*, probablemente porque no sea un tema mundial y en México sea incipiente tanto el conocimiento práctico del significado de víctima como parte en el proceso, como la introducción de procesadores algorítmicos en la justicia penal.

En general, los países y las asambleas internacionales en el mundo, principalmente en Europa y Latinoamérica, trabajan para lograr un avance tecnológico de la inteligencia artificial con ética y respeto a los derechos humanos, para mantener la confianza gubernamental, así como la integridad y la privacidad, la responsabilidad y el uso confiable. La Asamblea Parlamentaria del Consejo de Europa hace esfuerzos para examinar el papel de los algoritmos y la inteligencia artificial en los sistemas de justicia penal desde la perspectiva de las normas del Consejo de Europa sobre derechos humanos y Estado de derecho, con miras a hacer posibles recomendaciones de nuevas medidas a los Estados miembros y al Comité de Ministros (Parliamentary Assembly, 2018); propugna, además, la regulación a las empresas para que transparenten el código fuente de sus sistemas y, así, evitar el sesgo discriminatorio que se va acumulando con datos que están contaminados de prejuicios (Parliamentary Assembly, 2020).

Por su parte, la Organización de Naciones Unidas (ONU) hace un llamado al "bienestar digital" para advertir el estado de mercado que hasta hoy tiene la inteligencia artificial (IA), y no trabaja para el combate a la desigualdad social que exacerba los sesgos y reproduce la selección de aquellos que crean y utilizan dicha inteligencia, es decir, hombres blancos y con recursos económicos, que reflejan su propia perspectiva de la vida y la jerarquización de valores. Por eso, es menester la garantía de los derechos humanos desde las prácticas en las que se basan la creación, la auditoría y el mantenimiento de los datos (Asamblea General de las Naciones Unidas, 2019).

Así, el reto para los desarrolladores de *softwares* es que los adapten al enfoque teórico complejo de aplicación de justicia respetuosa de derechos humanos acorde al Estado constitucional, puesto que los términos "dignidad", "libertad" y "transparencia" son valores que tendrán una medición en los algoritmos, así como el uso del término "autodeterminación algorítmica" para asegurar el libre desarrollo de la personalidad (Corvalán, 2017)

en los antecedentes fácticos. Esta línea, ya trabajada en los estudios experimentales tanto en el Tribunal Europeo de Derechos Humanos como en la Corte Interamericana de Derechos Humanos, encontró que los factores fácticos son de gran relevancia, así como los pesos que ciertas frases otorgan al algoritmo de aprendizaje automático (Medvedeva, Vols y Wieling, 2020). El reto, también, es que existan algoritmos que tomen en cuenta las nuevas relaciones entre humanos y máquinas, que sean de verificación independiente y que puedan cuantificar y certificar, de alguna manera, esta capacidad de intuición, inteligibilidad, adaptabilidad y adecuación de los objetivos del robot (Benanti, s.f.).

Ante este panorama alentador, es necesario advertir que, independientemente de las regulaciones legales y políticas, la tecnología sigue su curso, así que no es suficiente la mención positivizada del término "dignidad humana", sino que debe alcanzar la comprensión de los desarrolladores, quienes no deben ser exclusivos del sector privado, puesto que los derechos humanos se anteponen al Estado y no a las empresas; en todo caso, deben participar personas de los diversos sectores sociales, preferentemente que sean y estén siendo sujetas a proceso penal, que hayan cometido un delito o que lo hayan sufrido, todo bajo la comprensión del significado del tipo penal desde la cosmovisión de los destinatarios; es decir, una participación plural que logre la realidad que, sin algoritmos, no se ha alcanzado en México.

En general, el avance tecnológico tiene objetivos distintos de la justicia y se le relaciona con el capitalismo. Las empresas tecnológicas, con base en su capacidad económica, están diseñando y creando tecnología para hacerse cargo de las responsabilidades del Estado, incluyendo el monopolio del control de la violencia, donde las desigualdades muestran a las personas vulnerables como las principales comisoras de delitos. El riesgo es que el algoritmo se sesgue desde los datos de entrada solo con unos delitos y solo contra algunas personas para el resultado final, que es la sentencia: el algoritmo contra la sociedad.

La pretensión debe consistir en que la amenaza de la extinción del *Ser* retome el fundamento humano para el control tecnológico, no por la ley, sino por reencontrar lo humano en el humano. La IA debe transformar el sentido actual de la violencia y su normalización:

> ...no es la ideología la que tiene la capacidad de materializar la violencia, sino que la necesidad de sostener escenarios permanentes de conflicto violento gestionados mercantilmente es la que se aprovecha de las ideologías para sostener estos escenarios y con ello enormes mercados (...) Cualquier ideología declarada para justificar el conflicto en turno

> será finalmente irrelevante (...) Hoy se ejerce una violencia bélica sin que sea necesario identificar un enemigo. Los enemigos se identifican de manera meramente contingente. (Lefranc Weegan, 2015)





Así, para lograr la efectiva garantía de los derechos humanos, la IA debe, primero, analizar el reconocimiento de la persona en su dignidad y, luego, la situación contextual del conflicto.

En esta complejidad, y como una opción de mejoramiento de la justicia penal, la cibernética se asoma al seductor trabajo de toma de decisiones judiciales (como China, Estonia, Noruega, Argentina, Colombia, España, entre otros). El avance es tal, que el *machine learning* y el *deep learning* (Darlington, 2019), como ramas de la IA, representan el aprendizaje automático y complejo, y se ven como oportunidad de ayuda o sustitución del juez humano para una decisión correcta y justa.

Las complejidades que presenta el *software* predictivo actualmente, y por lo cual se generan discusiones éticas como las llamadas "cajas negras", siguen teniendo avances de optimizaciones con el análisis posterior de las relaciones de los datos de inicio y salida, que permite hacer interpretaciones orientadas a la combinación de texto y contexto (Nay, 2017), lo cual ayuda para la tecnicidad de identificación de la ley aplicable a un caso concreto.

Esta tecnología predictiva se presenta con características de objetividad, neutralidad e infalibilidad. Parecería que, finalmente, el "Juez Hércules" humano del que hablaba Dworkin se vuelve realidad con el auxilio de la tecnología, pero con el riesgo de ser sustituido por el "juez omniartificial", con sabiduría e inteligencia inigualables, cuya razón supera el error y el atavismo humanos, perfecto y perfectible, con datos lógicos y objetivos que combinan algoritmos matemáticos para acercarse a la combinación neuronal, lejano a preconcepciones y contaminaciones de experiencias vividas: la esperanza de una justicia tecnificada con ejercicios a base de prueba y error constantes.

## IV. ERROR HUMANO Y SESGO ALGORÍTMICO

El error judicial provoca un impacto negativo y muestra el riesgo de la subjetividad humana. La causa se analiza por la decisión primaria del juez cuando, a pesar de la ley, la intención preconcebida del delito, de la persona y del contexto del caso, le representa un significado. A fin de evitar

y controlar el resultado errático en la sentencia, el juez humano tiene dos vías que guían su proceder: legalismo y pragmatismo, aristas entre las que existe una gran brecha (Posner, 2011: 52). Desde luego que la teoría legalista es la que fundamenta, en forma "oficial", la actuación del juez. Se trata de un juez que no corre riesgos ni abre puertas a la crítica, a diferencia del juez pragmatista, que sí lo hace, defendiendo su posición y evitando el sentimiento de subordinación al documento legal que le impone una decisión ajena a su postura (*Idem*).

La aplicación jurídica a la que aluden los abogados penalistas en la actualidad, insta al juez a que se guíe por el mismo criterio bajo un espectro legal más amplio (nacional e internacional), pero resulta imposible atender al gran bagaje legislativo identificando reglas y principios, y luego interpretarlo de acuerdo con el caso, alejándose en lo posible de su propia esencia subjetiva humana y de sus características idiosincrásicas, lo cual implica no atender a la ideología, personalidad y trayectoria, para evitar la parcialidad o la arbitrariedad: "La ratio de la independencia judicial es la imparcialidad, una imparcialidad que constituye una garantía constitucional implícita en la norma *normarum* española y que se mide, actualmente, por el sometimiento del operador jurídico a las pautas jurídicas previamente establecidas para la resolución del conflicto jurídico." (Martínez Alarcón, 2004: 68)

A pesar de ser formal, el legalismo sin duda ofrece un panorama cerrado a la aplicación jurídica y, por tanto, de seguridad y certeza para recurrir la resolución. Uno de los ejemplos más mediáticos en esta vía fue con el que se inauguró el Sistema de Justicia Penal en Chihuahua el 29 de agosto de 2008, último día en que Rubí Marisol Frayre Escobedo, de 16 años, fue vista por sus amistades.[9] Ante el error evidenciado, y con la intención de resarcir el daño irreversible, se imputó la responsabilidad a los tres jueces, quienes, a su vez, responsabilizaron a la investigación realizada por el Ministerio Público:

> Los jueces destacaron que desecharon esas pruebas porque no eran contundentes y el artículo 331 del Código Procesal Penal de Chihuahua dispone que los elementos de prueba no tendrán valor si han sido obtenidos por un medio ilícito. Establece además que la declaración del imputado sólo tendrá validez si es prestada voluntariamente ante el Ministerio Público o un juez y asistido por un defensor; esto, subrayaron, no ocurrió... Nosotros no

[9] Un trágico caso de proceso por el delito de feminicidio que evidencia la discordancia en la valoración de las pruebas entre el tribunal de primera instancia y el tribunal de casación; el primero con una sentencia absolutoria y, el segundo, con una condena de cincuenta años de prisión. Carlos (2012); Carmona (2012, 22 noviembre).

> declaramos inocente o culpable a Barraza, sólo lo absolvimos por insuficiencia de pruebas; el Ministerio Público no hizo bien su trabajo. (Ballinas, V., 2011, 19 enero)





Con el argumento legal, se aseguran de que ni una pizca de humanidad quede en la resolución del caso.

La contrafigura del legalismo se encuentra en el pragmatismo. Las resoluciones judiciales en esta vía no son formales, ni su aplicación depende de un silogismo de caso y normas; es más visible la creación de nuevo derecho por el derecho previo aplicable e interpretable —principalmente en los casos difíciles—; es decir, donde la regla no ofrece una aplicación literal.

La labor jurisdiccional penal pragmatista debe contemplar las consecuencias de las decisiones no solo en el plano legal, sino también personal, de los justiciables; es decir, se considera que el juzgador debe estar capacitado para determinar cuáles son las mejores consecuencias para la víctima y el victimario, así como para la comunidad. Sensibilizarse y responsabilizarse por las personas implica, necesariamente, el sentido subjetivo de ser juez.

Esta segunda vertiente es correspondiente al llamado neoconstitucionalismo, acorde a un modelo garantista del sistema de justicia penal, donde las decisiones judiciales implican un raciocinio humano más allá de lo legal, que aún no se evidencia en la realidad. A pesar de que el propio ordenamiento legal indica que la sentencia debe ser conforme a la libre valoración de pruebas, aún falta en la costumbre jurídica una interpretación ponderativa entre reglas y principios. Pareciera que la mención de artículos legales cumple con la fundamentación exigida, pese a que la ductilidad del derecho signifique que la legislación es la herramienta para el juzgador, que juega un papel principal en el posmodernismo a partir del derecho de la posguerra (Zagrebelsky, 2013: 34). Ejemplos de esto se encuentran, principalmente, en las sentencias de la Corte Interamericana de Derechos Humanos.

Paralelamente a esta discordancia aplicativa del derecho por los jueces humanos se encuentra la tecnificación de los *softwares* que han basado su esfuerzo en prueba y error con el objetivo de perfeccionamiento; es decir, libre de sesgos subjetivos humanos (Sourdin, 2018); sin embargo, el llamado "sesgo algorítmico" es comparable con el "error judicial".

Uno de los ejemplos más conocidos que mueve al debate sobre la objetividad de los procesadores por el resultado de supuestos sesgos raciales y de género, es el procesador "Compas" (*Correctional Offender Management Profiling for Alternative Sanctions)*, que calificaba a las personas con un número

de riesgo correspondiente a la pena que debía imponerse, y que fue puesto en evidencia el 23 de mayo de 2016 por ProPublica, organización sin fines de lucro, en el artículo "Machine Bias", que trató el sesgo racial del *software* con referencia a algunos casos, sobre todo el de Brisha Borden y Vernon Prater, en el cual se evidenció que en la sentencia de apelación se impuso una pena incorrecta por recomendación del algoritmo (Angwin, Larson y Mattu, 2016). Por supuesto que la empresa Northpointe Suite, dueña del sistema informático COMPAS, justificó estas acusaciones, centrándose en la validez científica del *software* con el argumento de que solo podría ser interpretado con conocimiento sólido de las técnicas y matices metodológicos comunes a él (Equivant, 2018).

La empresa aceptó el error en el procesador, aunque no el sesgo discriminatorio, pues afirmó que los datos fueron objetivos, según porcentajes de entrada en la población destinataria. Los acusados afroamericanos que fueron predichos como reincidentes, realmente reincidieron en una tasa más alta (63%) que las personas blancas (59%). El análisis de Northpointe encontró que las personas blancas que reincidieron, dentro de los siguientes dos años, fueron clasificadas erróneamente como de bajo riesgo casi dos veces, tan a menudo como los reincidentes afroamericanos (48% y 28%, respectivamente). Asimismo, los acusados blancos que se predijo que no reincidirían, en realidad no reincidieron a una tasa más alta (71%) que las personas afroamericanas (65%). Esto evidencia paridad predictiva para el *General Reoffending Risk Scale* (GRRS) para afroamericanos y personas blancas en la población objetivo (Dieterich, Mendoza y Brennan, 2016).

No hubo mayores detalles de la metodología de combinación de datos por justificación del secreto empresarial, aunque una razón más, pero sin ser mencionada, es que quedó fuera del control humano de la empresa por el aprendizaje automático, lo que comúnmente se llama "cajas negras".

Ante esta evidencia de funcionamiento del procesador, puede afirmarse que:

1. La simple sospecha de sesgo algorítmico discriminatorio genera duda sobre los procesadores predictivos en las decisiones judiciales penales, ya sea como auxiliares o como sustitutos del juez, pues la complejidad de comprensión de la teoría jurídico-penal y su interpretación legal no parecerían resolver el error judicial;
2. Existe también el riesgo de retornar al etiquetamiento social y la selección de la población vulnerable como los clientes favoritos del sistema

penal (Zaffaroni, 2006:11), lo cual implica un derecho penal de autor y no de acto, clasificado para el estudio clínico pero potenciado con lenguaje de programación avanzado, que limita y se contrapone a un derecho por y para la sociedad, entendible, entendido y reconocido, aun como auxiliar para el conocimiento del juez, lo cual cuestiona el binomio perfecto judicial: humano-máquina; y

3. El error del algoritmo es una oportunidad para alejar la responsabilidad profesional y humana del juez de las decisiones penales, como ocurrió en el caso *State v. Loomis* (Supreme Court of Wisconsin, 2016), en el que Eric Loomis fue sentenciado a seis años de prisión debido a la evaluación de riesgos que hizo el *software* Compas, con un sistema no del todo transparente debido al secreto comercial; en apelación, los jueces de la Corte Suprema se negaron a conocer del caso.

La reforma al sistema de justicia penal trajo consigo la definición de responsabilidades de los servidores públicos y, aunque una buena decisión judicial depende de una carpeta de investigación completa; es decir, con todos los elementos del contexto del caso, los jueces tienen la responsabilidad de interpretar y armonizar lo que les sea presentado, y vincularlo a la selección de leyes y artículos nacionales e internacionales para resolver el caso conforme a reglas y principios, además de valorar las pruebas desahogadas de forma libre y lógica. Aun si el juez humano analizara el caso en este contexto, el error deriva de su preconcepción; por otro lado, si es que es auxiliado por el procesador, depende de la responsabilidad profesional, puesto que la confianza en la exactitud matemática de la programación algorítmica y la carga de trabajo resulta en que un escrito pre-hecho sea "pulido" por el juez humano, pero como cumplimiento de su labor de empleado, ajeno a la impartición de justicia y conformándose con "pulir" el documento, que no contiene su convicción plena. Ante este panorama, valdría más la sustitución total que eliminara del juez esa responsabilidad simulada.

Debe advertirse que la mano humana está presente en la alimentación inicial del procesador, así es que, si la información está sesgada, incompleta o sin situaciones delictivas innovadoras, el proceso de combinación algorítmica no tendrá otro resultado que una injusticia.

La transparencia que los sistemas penales intentan hacer valer se ve mermada por los sistemas de cajas negras que, por protección comercial, o porque se pierda el control del procesamiento de datos, esconden la razón

y el punto exacto del error o el sesgo generador de la injusticia y, por tanto, dan información insuficiente para una apelación correcta, que pueda evidenciar el error. Entonces, con ello se perdería para el justiciable la debida indemnización, como derecho establecido en la Convención Americana de Derechos Humanos (SCJN, 2020).

Así, tanto el juez humano como la máquina incurren en error, son selectivos y estigmatizantes, lo cual es el resultado, en gran medida, de los datos que el humano tiene a su alcance sobre una realidad parcial, desigual y vulnerada, y de leyes incompletas en cuanto a conductas dañosas. Falta, pues, un proceder que potencie el valor subjetivo de la responsabilidad a partir de la subjetividad del juzgador penal, conforme las partes le muestran las piezas en juicio. Si se trata de un *software* que ayude con esa tarea, o que sustituya al juez humano, el riesgo aumenta en virtud de que la máquina depende de una realidad construida y preseleccionada por programadores lejanos a los conceptos sociales.

Para evitar el error y el sesgo, el enfoque de interpretación para la garantía de derechos humanos, tanto de la víctima como del probable responsable del delito, debe partir de la sensibilidad hacia el otro, donde la valoración de los hechos no se ciña a lo presentado por las partes en el juicio, sino que ese espacio sea trasladado a lo ocurrido, utilizando la imaginación como herramienta humana. De esta forma, la optimización de principios será casi innata y, por tanto, un acercamiento a la justicia, diverso del cumplimiento forzado de la imposición legal de parámetros para la imposición de sanciones que limitan este proceder y que, incluso, contemplan elementos discriminatorios de los sujetos, suponiendo una discriminación positiva, como es el caso de la justicia penal indígena.

Con esta diferencia inicial, parecería que la subjetividad humana es la razón por la que el error judicial y, por tanto, la violación injustificada de derechos a cargo del Estado, tiene sentido. Entonces, la diferencia entre hombre y máquina es que el primero pone su ser en el caso, mientras que la segunda combina algoritmos para obtener una mejor respuesta; sin embargo, lo coincidente es que la esencia de estos es la mano humana, bajo una razón técnica diseñada con base en percepciones sociales con patrones de criminalización social.

## V. EL JUEZ HUMANO Y EL ALGORITMO PENAL. CARACTERÍSTICAS IDENTITARIAS

A pesar del proyecto de reforma al poder judicial, que se comenta en líneas posteriores, muchos jueces penales no gozan de una buena reputación; se les identifica con corrupción, exceso de subjetividad, parcialidad, conveniencia política y relación con el crimen organizado. La reforma en materia penal fue una reconfiguración de la viciada costumbre legalista que servía de velo a las prácticas discriminatorias y corruptas en el sistema penal mixto, y parecería que la implementación del *software* predictivo, como auxiliar o sustituto del juez humano, serviría para el control de la reforma judicial. Sin embargo, con ello solo se reafirma la desconfianza al juez humano como aplicador de justicia, y al procesador como un medio de control más a la discrecionalidad judicial. Por ello es necesario el análisis del humano como sujeto en la función judicial y en su persona, porque tiene relación con los seres a los que juzga.

Los límites impuestos por el Estado y la ley han mecanizado la labor judicial, impidiendo redescubrir y valorar el significado de la justicia penal como potenciadora de bienestar y como medio para la resiliencia ante el dolor causado por el daño delictivo que requiere sensibilidad y empatía; es decir, sentir, entender y comprender al otro en la audiencia, más allá de observar con morbo los momentos procesales. La dignidad que el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos reconoce, y que el proceso penal debe garantizar, no entraña seguir protocolos y técnicas procesales de actuación, sino asumir la dignidad propia y la de los justiciables, descubrir la capacidad de sentir y sentir al otro, imaginar su dolor a través del relato de los hechos y comprender el hecho delictivo en el contexto que le es ajeno; en suma, romper la faceta de empleado del Estado que cumple con un trabajo rutinario y mecanizado.

Para prevenir el desdén al ser humano ante el avance tecnológico, es importante acentuar las características coincidentes y divergentes entre el humano y la máquina y, luego, entre estos y la sociedad. Ni el humano ni la máquina fueron creados con el propósito único de toma de decisiones, sino que esta función les fue delegada. El algoritmo predictivo para tomar decisiones penales es una muestra de la capacidad de tecnificación humana con pretensión de exactitud y rapidez; por el contrario, el juez humano tiene múltiples roles sociales, que convergen de forma integral en la decisión penal.

La tecnología fue diseñada y construida a partir de las posibilidades científicas infinitas de humanos expertos en ciencias exactas. Los múltiples usos de la tecnología son los que derivaron en la opción de ayudar al humano a facilitar su cotidianeidad y, por ello, las tareas técnicas se delegan cada vez más a las máquinas. Asimismo, el humano aún se esfuerza por dar explicación al origen de la vida. El objetivo de su vida no fue cumplir una sola función, ni que su existencia compitiera con una creación propia. El diseño humano en su conjunto —mente-cuerpo y alma— es perfecto *per se*, al grado de ser inexplicable en su totalidad. A partir de los esfuerzos de la multiplicidad de tareas que realiza, se entienden los motivos de sus acciones. Por ello, en principio, la toma de decisiones penales es facultad del ser humano, quien, a su vez, otorga funciones auxiliares a la máquina.

El ser humano puede interpretar conductas en su interacción con sus congéneres, lo cual representa una gran responsabilidad para con otras personas e, incluso, el Estado. Los diversos sentidos e impactos de las decisiones judiciales, en los momentos procesales, son justificados técnicamente para una declaración estatal de justicia, pero conforme a una realidad humana subjetiva que convive con la interacción social y política. Se requieren características específicas para una labor especial profunda, que impacta en quien la ejecuta, más allá de un documento físico o electrónico.

En la actualidad, el juez penal toma decisiones durante el proceso penal con el objetivo de ayudar al Estado a cumplir el suyo: legitimar el monopolio del control social punitivo; materializar el control formal de la violencia con que ejerce la venganza pública. El juez humano no legitima, en lo material, el monopolio del control de la violencia, además de que está sujeto constantemente a condena social.[10] Por otro lado, la oferta de los procesadores predictivos es sorprendente: ayudan al juez a vincular los datos de las personas con los resultados de las evaluaciones individuales, y hacen planes de tratamiento e informes de progreso a largo plazo, al tiempo que ofrecen una funcionalidad crítica para la creación de informes de investigación previa a la decisión (Equivant, s.f.); asimismo, logran una productividad notable de mejora y seleccionan los casos urgentes con eficacia (Estevez, Fillottrani y Linares, 2020: 63, 69). La oferta de la IA resulta más atractiva

[10] En México causó revuelo la libertad de 77 implicados en el caso de la desaparición, en 2014, de 43 estudiantes de la Normal de Ayotzinapa, en Iguala. *El Financiero* (septiembre,2019). Disponible en: https://bit.ly/3igKOuv; También el caso llamado "Los porkys", donde el juez concedió amparo contra una orden de aprensión a uno de los involucrados en el abuso sexual de una menor. *El Universal* (Septiembre, 2019). Disponible en: https://bit.ly/3jk3CdK

si el juez solo ofrece conocimientos especializados, si bien a la larga aquella requiera dichos conocimientos cada vez menos.

En términos institucionales, el proceso también es de aprendizaje: el juez humano ha demostrado comportamiento institucional que pone en duda la comprensión que tiene de su función, puesto que la ha asumido como deidad que juzga cualquier acto humano, protegido por una burocracia administrativa y organizativa que ha aprovechado para un constante "abuso de poder". En primer término, se cuestiona aún a la llamada "familia judicial",[11] las resoluciones con sesgo político y las sospechas de corrupción.

El citado Proyecto de Reforma con y para el Poder Judicial[12] aborda, entre otros temas, el nombramiento del personal para eliminar la exacerbada discrecionalidad en la contratación, así como el nepotismo; también tiene como objetivo acabar con la corrupción que dirige el sentido de las sentencias; impulsar la perspectiva de género para acabar con el hostigamiento sexual y fortalecer el sistema de carrera para que los defensores públicos se conviertan en verdaderos abogados de los pobres; promete un nuevo perfil de juez que tenga carrera judicial, capacitado sobre los avances de la ciencia jurídica, impulsando el pensamiento crítico que, con *herramientas argumentativas sofisticadas,* permita dar soluciones sencillas, claras y justas, de acuerdo con el objetivo de la Reforma Integral al Sistema de Justicia Penal.

Sin duda, lo que resalta en la reforma al poder judicial es que prevé que la IA apoye la función judicial, especialmente en la transformación de la jurisprudencia por reiteración, en el caso exclusivo de la Suprema Corte,[13] en un *sistema de precedentes,* lo cual facilitaría el trabajo de la IA para identificar casos análogos al que se esté resolviendo.

Sin duda, el procesador de IA no solo es una herramienta para el juez, sino que representa un símbolo adicional del sistema de justicia penal para imponerse al destinatario e intentar legitimar el poder de violar derechos humanos (Barrera, 2012). Se trata de un ritual extraño, ajeno al deber moral de juzgar y a la interacción entre personas; ahora el caso puede ser resuelto por la tecnología: un tribunal digital (The Technolawgist, 2020) cuyo

[11] Hace referencia al nepotismo dentro del poder judicial, donde obtienen prestaciones y sueldos superiores en promedio a la media nacional.

[12] Para mayor detalle de cada tema del proyecto de reforma judicial, consultar el "Proyecto de Reformas con y para el Poder Judicial de la Federación" (12 de febrero de 2020). Disponible en: https://www.scjn.gob.mx/sites/default/files/carrusel_usos_multiples/documento/2020-02/Proyecto%20de%20Reforma%20Judicial_1%20%283%29.pdf

[13] El sistema de integración de jurisprudencia por reiteración prevalecerá en el caso de los tribunales colegiados de circuito. (N. del E.)

uso está reservado para quienes tienen acceso a la tecnología y, por supuesto, para los grupos que la controlan; una justicia favorable a minorías que simbolizan el poder económico de un país.

El poder económico, representado en el monopolio de la violencia, se consolida con el procesador como símbolo de superioridad ante los "súbditos" y de desprecio a la cuestión criminal; una despersonalización que invite al justiciable a conformarse con la decisión, puesto que la "perfecta" abstracción de su caso no la hizo un humano "imperfecto" ni intervino en ella. Si los tecnicismos jurídicos resultan complejos, la programación y la traducción algorítmica los volverán intimidatorios.

Con todo, la característica que será decisiva para que la máquina "ayude" al humano o lo sustituya es la *subjetividad*, característica innata del ser humano y debida al aprendizaje experiencial. El conocimiento es alimentado y estructurado por interiorización de cánones éticos que sesgan necesariamente el caso a una visión propia, y que, por tanto, en una aplicación positivista del ordenamiento jurídico, lo adecuan a la decisión previamente formada.

Lo contrapuesto a la subjetividad es la objetividad, y esta es la apuesta perversa del *software*, que se abstrae de cualquier identificación con quienes esperan un fallo y utiliza datos precisos, fuera de toda preconcepción del caso. Sin embargo, intenta imitar los procesos inductivos y deductivos del cerebro humano a partir de circuitos electrónicos y programas de cómputo que simulan las redes neuronales humanas (como la prueba de Turing, *Deep blue, Watson*, *Project Debater* y *DeepMind)*.

La argumentación sobre situaciones sociales es una realidad para la máquina, capaz de analizar oraciones y procesar principios de cómo los humanos construyen el argumento para construir la narrativa lógica del debate; así, intenta "borrar" la subjetividad humana imperfecta con un sistema de motivación judicial técnico que asegure justicia; pero, al mismo tiempo, la copia cerebral imperfecta y limitada contiene necesariamente datos humanos y, por tanto, subjetivos.

Aun así, la objetividad no es legalmente exigible al juez; el Código Nacional de Procedimientos Penales advierte que la convicción del juez debe estar presente al momento de resolver, y que el razonamiento libre, el criterio y el humanismo serán la esencia de la sentencia, que tendrá una estructura metodológica con la aplicación del principio de convencionalidad e interpretación extensiva de la ley. Se espera, pues, que el juez se involucre en el caso más allá del formalismo y la compostura en una sala de

audiencia, recordando que la convocatoria a esta deriva de un evento dañoso. El juez tiene la oportunidad de observar y escuchar a los justiciables. Solo el humano es capaz de "ver el rostro del otro" —su alma, a decir de Levinas—, y esta humanidad sensible es lo que aclama la justicia penal.

Por otra parte, a pesar de que el aprendizaje automático pueda "pulir" matemáticamente la subjetividad humana con la selección de casos "correctos" que servirán como patrón para la decisión del nuevo caso, la esencia de este aprendizaje por capas trata de experiencias exclusivamente humanas. El *deep learning*, a pesar de lo simple que es (Chollet, 2018), requiere un espacio dimensional muy amplio que capture el alcance de los datos originales, es decir, que alcance a ver la realidad tal como la interpreta el ser humano. Las "redes neuronales" no tienen nada que ver con el cerebro humano, y el término correcto debería ser "layered representations learning or hierarchical representations learning, or maybe even deep differentiable models or chained geometric transforms, to emphasize the fact that continuous geometric space manipulation is at their core"[14] (Chollet, 2018).

El *deep learning* corre el riesgo de ser sobreestimado a partir de los intentos de antropomorfizar, malinterpretando las técnicas, al punto de creer que la máquina predictora entiende y comprende sus propias decisiones, igual que el humano lo hace con experiencias sensoriomotoras. No obstante, en el intento de emular las interacciones humanas, el desarrollador *Faception*[15] asegura analizar, con aprendizaje automático de la biometría, la personalidad facial de una persona, a partir de lo cual realiza una detección predictiva y habilita acciones preventivas. Con solo analizar la imagen facial de una persona, revela automáticamente su personalidad, para hacer diagnósticos basados en imágenes de género y edad precisos, todo para mejorar la interacción personal con su propietario; puede calificar a las personas como introvertidas o extrovertidas, con tendencia a ser compasivas y cooperativas, y permite enfocar a los posibles terroristas y criminales antes de que hagan daño. Este modelo lombrosiano supera el intento de la morfopsicología, que ha sido criticada como pseudociencia, pero que es atractiva como alternativa de seguridad pública (Torregrosa y Payá, 2017).

[14] "[A]prendizaje de representaciones en capas o aprendizaje de representaciones jerárquicas, o tal vez incluso modelos diferenciables profundos o transformaciones geométricas encadenadas, para enfatizar el hecho de que la manipulación continua del espacio geométrico está en su núcleo." [Trad. E.]

[15] Para mayor detalle del desarrollador de IA, consultar su página. Disponible en: https://www.faception.com/

Se comprueba, entonces, que el juez humano y la máquina comparten subjetividad. El procesador filtra y convierte el dolor en datos, mientras que el humano lo percibe, lo siente y lucha contra él para no sesgar su decisión. Al juez humano le toca redescubrirse en su maravillosa subjetividad, que aleje los atavismos legales y contemple el valor de la justicia, entendiendo, antes de juzgar, las causas generadoras del proceder dañoso; y luego, si es acompañado por un auxiliar tecnológico, revisa con cautela los datos arrojados y, con la experiencia en sus roles, detecta posibles fallas o datos incompletos, para complementarla con un panorama muy cercano a la realidad del caso.

Sin embargo, y a pesar de la existencia de la interpretación extensiva, libre y lógica al dictar una sentencia penal, la propia ley se contrapone, puesto que contiene restricciones legales y parámetros de decisión que limitan la discrecionalidad. Entonces, si bien el juez debe actuar con convicción legal, esta se encuentra en riesgo de revisión por un superior, como control de subjetividad. Se comprende ahora la conveniencia del acompañamiento judicial por la herramienta tecnológica que "limpie" las experiencias derivadas de la multiplicidad de roles sociales, más aquellas, directas e indirectas, referentes a la violencia, que tendrán interpretaciones distintas de acuerdo con las características individuales y las conveniencias políticas y sociales.

La institución judicial es resultado de un desarrollo social y profesional que se tradujo en experiencia (Berger y Luckmann, 2001: 87), y esto previene del peligro de suponer que todas nuestras preferencias están basadas en algún criterio racional absoluto, llevándonos a decir que "los valores constituyen una elección individual y son el motor de la personalidad del ser" (Sanabria, 2009: 909), pues cada individuo decide en función de su contexto y sus necesidades propias; así, no se puede decidir sobre algo que se desconoce, que es extraño para su realidad y, por tanto, incomprensible. Sin embargo, es esperable que la sensibilidad y el sentimiento de compasión subsanen lo anterior y que se juzgue correctamente.

La libertad y la autonomía de la voluntad también son innatas en el ser humano, y las comparte con quien juzgará; por ello, el Estado propende a coartar la libertad del juez, para evitar que dicte una sentencia condenatoria anteponiendo su subjetividad, libertad y autonomía al merecimiento de la pena por el destinatario, evitando así la venganza privada "legal". Aun así, el juez no puede evitar romper esta regla; su subjetividad le impone reconocer lo que ha interiorizado como bueno y malo, ya sea por convicción

o por conveniencia. La libertad y la autonomía de la voluntad no se advierten en un procesador, porque es un humano quien introduce los datos de inicio para que ocurra el proceso de combinación algorítmica; sin embargo, el aprendizaje llega a ser autónomo cuando el procesador ejerce su libertad técnica y "decide" sin intervención humana. Sin embargo, si se trata de delitos, la infinita creatividad natural del humano diariamente actualiza nuevos supuestos dañosos y, por tanto, la legislación es modificada, contrariamente a la capacidad del procesador, que es finita. El cerebro y la mente humana comprenden e imaginan la acción de otro semejante que daña, de ahí que para los programadores represente un reto lograr lo mismo en programadores. En el juez humano, la capacidad es natural y, por ello, crea decisiones de manera inconsciente (Posner, 2011: 77).

En el *Deep Learning*, la fuente de realidad indirecta para la interpretación logra un significado de justicia distinto del que el humano obtiene de forma directa de la realidad, logrando así una interpretación abstracta imposible de definir matemáticamente, puesto que tiene que ver con la esencia del ser y su relación en la sociedad: "El derecho no es revelado por Dios ni descubierto por la ciencia, es una obra plenamente humana en la que participan quienes se dedican a estudiarlo y que no pueden interpretarlo sin tomar en cuenta los valores que transmite: compartir un mismo deber ser con la sociedad." (Supiot, 2007: 28)

La IA, lejos de ser autónoma y objetiva, está impregnada de datos estadísticos, preconcepciones humanas, contextos comunitarios e individuales, grupos vulnerados combinados con las decisiones judiciales, correctas o no, pero fuera de toda comprensión, entendimiento y sensibilización, con riesgo de errores de traducción algorítmica. Por el contrario, el humano tiene experiencias de vida, está envuelto en una cultura y procesos de resiliencia que ponen a la vista del juez contextos ajenos a su propia realidad, y que pueden despertar su sensibilización, benevolencia y compasión, para llevar su pensamiento crítico más allá del mandato legal.

El ser humano es autónomo y subjetivo y, por tanto, libre, y ello ratifica su dignidad. La dignidad es la diferencia sustancial entre el humano y el *software*. La actividad de sentenciar significa la promesa de una vida mejor, más allá de la punición; sirve para comprender las causas y el significado del delito, así como el dolor de quien lo sufrió.

## VI. CONCLUSIONES

El análisis de la complejidad de la sentencia penal como la principal función de los jueces, extiende el panorama de discusión de los *softwares* predictivos en materia penal; obliga a construir vías de reconfiguración de la función técnica de la justicia penal, viciada por la costumbre legalista y formalista.

El avance tecnológico no atiende a leyes y políticas de Estado; su esencia de mercado arrasa con todo indicio de bienestar social, más aún si este se contrapone a su dinámica capitalista. Esto es conveniente para el Estado, pues el procesador algorítmico será una herramienta simbólica, no solo de poder económico, sino de intimidación con su control punitivo, con el que se afianzaría como monopolizador de la violencia, capaz de criminalizar a quienes estorben su avance económico.

No hay duda de que algunas de las recomendaciones a las empresas creadoras de *softwares* han tenido efecto, así como en la investigación experimental, pero sigue siendo insuficiente para detener el imperativo tecnológico irreflexivo del significado de justicia penal. La subjetividad humana es la característica que aquella necesita. La costumbre positivista, que traducía la objetividad en aplicación mecánica de la ley, ahora convive con la interpretación ponderativa de principios para garantizar derechos humanos; para esto es necesario el raciocinio del juez y, por tanto, la comprensión profunda del caso, más allá de la formalidad que implica una audiencia. Por ello, el juez debe transformar su función técnica actual en una función humanizada, y verificar que los valores de justicia y responsabilidad se evidencien con el resultado de transformación positiva de los justiciables, a partir de la sentencia penal. Entonces, la justicia penal tendrá un significado regenerador.

## VII. FUENTES DE CONSULTA

Alexy, R. (1993). *Teoría de los derechos fundamentales*. Madrid, Centro de Estudios Constitucionales.

Asamblea General de las Naciones Unidas (2019). *La extrema pobreza y los derechos humanos*. Disponible en: https://bit.ly/3jp1Dog

Ballinas, V. (2011, 19 enero). "Defienden jueces de Chihuahua sentencia absolutoria en favor de Sergio Barraza". *La Jornada*. Disponible en: https://bit.ly/35oi8fF

Barrera, L. (2012). *La Corte Suprema en escena, Una etnografía del mundo judicial*. Madrid, Siglo XXl Editores.

Benanti, Paolo (s.f.). *La dignidad de la persona en la era de Máquina Sapiens*. Disponible en: https://bit.ly/36cau9j

Berger, P. y Luckmann, T. (2001). *La construcción social de la realidad*. Argentina, Amorrortu Editores.

Carmona, B.E. (2012, 22 noviembre). "Marisela, Rubí, Sergio... Historia trágica que dio la vuelta al mundo". *El Diario mx*. Disponible en: https://bit.ly/3s3Izkt

Carlos, R.E. (2012). "El Proceso Acusatorio en el estado de Chihuahua y el caso del homicidio de Rubí Fraire". En Cienfuegos Salgado, D. y Froto Mandariaga, G. (Eds.), *Los Derechos Humanos en el momento actual*. México: UNAM.

Consejo de la Judicatura Federal (2016). Consejo de la Judicatura Federal. Disponible en: https://www.cjf.gob.mx/sjpa/

Corvalán, J. (2017). "Inteligencia Artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia". *Journal of Constitutional Research*. Disponible en: https://bit.ly/36sUQ9R

Chollet, F. (2018). *Deep Learning with Python*. Nueva York: Manning Publications Co. Disponible en: https://bit.ly/33dFX9k

Darlington, K. (2019). "¿Pueden las tecnologías actuales emular la inteligencia humana?" Open Mind BBVA. Disponible en: https://bit.ly/347eqFx

Dieterich, W., Mendoza, C. y Brennan, T. (2016). "COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity". Northpointe Inc. Disponible en: https://bit.ly/2S4HRCC

Diputados. (2014). Código Nacional de Procedimientos Penales. Disponible en: https://bit.ly/3l3pjiI

Diputados. (2016). Ley General de Víctimas. Disponible en: https://bit.ly/2K8z0j4

Equivant (2018). "Official Response to Science Advances". Disponible en: https://bit.ly/3cEmNwh

Equivant (s.f.). "Northpointe Suite case manager". Disponible en: https://bit.ly/3cGMZX0

Estevez, E., Fillottrani, P. y Linares, S. (2020). "PROMETEA: Transformando la administración de justicia con herramientas de inteligencia

artificial". Nueva York: Banco Interamericano de Desarrollo. Disponible en: https://bit.ly/36grqvm

Lefranc Weegan, F.C. (2015). "Poder de fuego. Acerca de una violencia sin odio". En F. Tenorio Tagle (Ed.), *El sistema de justicia penal y las nuevas formas de observar la cuestión criminal* (pp. 259-287). INACIPE.

Martínez Alarcón, M.L. (2004). *La independencia judicial*. Centro de Estudios Políticos y Constitucionales.

Medvedeva, M., Vols, M. y Wieling, M. (2020). "Using machine learning to predict decisions of the European Court of Human Rights". *Artif Intell Law*. Disponible en: https://bit.ly/36eG2vh

Nay, J.J. (2017) "Predicting and understanding law-making with word vectors and an ensemble model". *PLoS ONE* 12(5): e0176999. Disponible en: https://doi.org/10.1371/journal.pone.0176999

Parliamentary Assembly (2020). "Justice by algorithm? A committee urges smart regulation of AI in criminal justice to avoid unfairness". Disponible en: https://bit.ly/338cjCe

Posner, R.A. (2011). *Cómo deciden los jueces*. Madrid, Marcial Pons.

Secretaría de Gobernación (2008). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. Disponible en: https://bit.ly/399dGSZ

ProPublica. (2016, 23 mayo). *Machine Bias*. Disponible en: https://bit.ly/2LDKjQA

Sourdin, T. (2018). "Judge v Robot? Artificial Intelligence and Judicial Decision-making". *UNSW Law Journal*. Disponible en: https://bit.ly/38E3e77

Supiot, A. (2007). *Homo juridicus. Un ensayo sobre la función antropológica del derecho*. España, Siglo XXI.

Suprema Corte de Justicia de la Nación (2020). "Reformas con y para el Poder Judicial". Disponible en: https://www.scjn.gob.mx/sites/default/files/carrusel_usos_multiples/documento/2020-02/Proyecto%20de%20Reforma%20Judicial_1%20(3).pdf

Supreme Court of the United States. (2016, 16 octubre). *Eric L. Loomis, Petitioner v. Wisconsin*. Disponible en: https://bit.ly/3ifc8et

Torregrosa, J. y Payá, R. (2017). "Así es el rostro de un criminal". España: Noverbal, Comunicación no verbal científica. Disponible en: https://bit.ly/2GeAczp

The Technolawgist (2020). "Los jueces de fase: tribunales digitales y blockchain". Disponible en: https://bit.ly/3jtuMz3

World Justice Project (2020). Índice de Estado de Derecho 2020. Disponible en: https://bit.ly/38l9ekN

Zaffaroni, E.R. (2006). *Manual de Derecho Penal. Parte General*. Buenos Aires, Ediar.

Zagrebelsky, G. (2013). *El derecho dúctil,* Trad. Marina Gascón, 10a. ed., Madrid, Trotta.

# LA POSIBILIDAD DE LA POLICÍA PREDICTIVA

Víctor Shaí Nóhpal Rodríguez*

* Agente de la Policía de Investigación de la Fiscalía General de Justicia de la Ciudad de México. Contacto: vistaelite95@hotmail.com

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Predicción** | *Prediction* |
| **Delito** | *Crime* |
| **Conducta** | *Behavior* |
| **Inteligencia artificial** | *Artificial intelligence* |
| **Policía** | *Police* |



**Resumen.** Las políticas públicas de seguridad actuales tienden a velar por la estabilidad social, apoyándose de una constante actualización en la política criminal para mitigar el delito. Adecuar esta política a una sociedad que cambia constantemente puede ser difícil, por los múltiples factores que propician la comisión de un delito. Cuando se delinque, se genera un sinfín de información jurídica y criminológica, mal recabada en ocasiones, y que suele utilizarse para diseñar medidas vagas de prevención del delito. Debido a lo anterior, es necesario apoyarse de nuevas tecnologías que procesen datos precisos y concisos para auxiliar a las policías con informes certeros que ayuden a predecir conductas antisociales, así como a establecer medidas proactivas de prevención *ad hoc*.

**Abstract.** Current public security policies tend to ensure social stability, relying on constant updating of criminal policy to mitigate crime. Adapting this policy to a constantly changing society can be difficult, due to the multiple factors that lead to the commission of a crime. When a crime is committed, endless legal and criminological information is generated, sometimes poorly collected, and which is often used to design vague crime prevention measures. Due to the above, it is necessary to rely on new technologies that process precise and concise data to assist the police with accurate reports that help predict antisocial behaviors, as well as establish proactive ad hoc prevention measures.



Fecha de recepción: 15 de enero de 2021
Fecha de aceptación: 22 de febrero de 2021

SUMARIO:







## I. INTRODUCCIÓN

Escuchar la palabra *predicción* invita a pensar en películas de ciencia ficción o en un gitano ante una bola de cristal, tratando de predecir el futuro; sin embargo, en países como Estados Unidos, Francia, España (NOBBOT, 2019) e, incluso, hasta hace dos años, Uruguay (Luna, 2019), se han desarrollado técnicas analíticas basadas en análisis matemáticos para identificar nuevas medidas aplicables a las funciones policiales, con el objetivo de prevenir y resolver delitos, así como identificar a posibles víctimas y victimarios. El modelo de policía predictiva se define como el uso de distintas técnicas de análisis de información para predecir un delito y, a partir de ello, diseñar una intervención policial inteligente, eficaz y proactiva (RAND, 2019).

RAND Corporation es una institución con sede en Santa Mónica, California, que ayuda a mejorar las políticas y la toma de decisiones a través de la investigación y el análisis. Ha sido uno de los pioneros y máximos desarrolladores de la policía predictiva, a la cual define de la siguiente manera: "La Policía Predictiva es la aplicación de técnicas analíticas, particularmente cuantitativas, para identificar los posibles objetivos de la intervención policial y prevenir el crimen o resolver crímenes pasados haciendo predicciones estadísticas." (J. Perry, RAND, 2013) Estas predicciones son creadas por ordenadores con información de delitos ya cometidos, y que generan algoritmos al realizar un análisis masivo de datos y de patrones de comportamiento, para, finalmente, predecir lugares y momentos de riesgo, así como señalar la naturaleza de una conducta criminal. De esta forma, los cuerpos de policía encargados de la prevención del delito pueden sacar más partido a sus recursos, concentrando esfuerzos, sobre todo, en los lugares criminógenos ya localizados, donde el riesgo y el peligro son inminentes.

De modo primordial para los policías encargados de la prevención del delito, el deber de la aplicación del estatuto requiere que este sea proactivo, y es ahí donde radica el éxito de la policía predictiva. En los últimos años se le ha dado una mayor importancia a las estrategias policiales proactivas que a las reactivas (UNODC, 2010), conceptualizando a las primeras como las estrategias policiales dirigidas a la reducción del perjuicio de nuevos delitos, inmediatamente después de haberse identificado a la amenaza.

Dicho lo anterior, se puede inferir que la policía predictiva, muy lejos de ser un gitano clarividente ante una bola de cristal, es un método de trabajo que utiliza herramientas tecnológicas avanzadas y análisis de datos basados en técnicas matemático-predictivas, con el propósito de tomar medidas preventivas ante la inminencia de una conducta delictiva. En pocas palabras, *seguridad proactiva.* Pero, ¿qué tan exacta puede ser la predicción de un delito?, ¿cómo se puede convertir en un algoritmo la información obtenida de un delito?, ¿puede llegar a ser eficiente la policía predictiva?, ¿los policías con funciones de prevención o investigación tendrán que realizar funciones de predicción?

El equipo de trabajo de la policía predictiva debe estar integrado por distintos especialistas, como victimólogos, criminólogos, criminalistas, psicólogos, sociólogos, antropólogos, matemáticos, ingenieros, programadores, desarrolladores y todo aquel profesionista que ayude a utilizar la información que se tiene, para tratar de prever la comisión de un delito; pero, sobre todo, policías con amplia experiencia en reacción inmediata al delito, debido a que la antigua escuela de la policía será pieza clave para la recolección de información, pues la precisión de los programas de la policía predictiva dependerá, en gran medida, de los datos útiles que se ingresen en el sistema. Como puede verse, la policía predictiva requiere bastantes especialistas para su correcta funcionalidad, por lo que no es fútil hacer mención de que supone el diseño de distintas etapas, en donde se desarrollará, de manera organizada, la pericia de cada especialista para que la intuición aduzca evidencia científica.

Para efectos de este artículo, surgido de aportaciones de distintas ciencias y disciplinas en torno a la materia, se utilizan indistintamente los términos crimen y delito, criminal y delincuente, criminalidad y delincuencia, así como criminógeno y delincuencial.

## II. ¿PROBABILIDAD, PREDICCIÓN O PREVENCIÓN?

La Real Academia Española define a la probabilidad como la razón entre el número de casos favorables y el número de casos posibles; por otro lado, a la predicción como la acción y el efecto de anunciar por revelación, conocimiento fundado, intuición o conjetura, algo que ha de suceder; y, finalmente, a la prevención como acción y efecto de prever, ver, conocer de antemano o con anticipación un daño o perjuicio, precaver, evitar, estorbar o impedir algo. Es decir, debemos hacer estadística para poder calcular la probabilidad de un caso concreto, así como para predecirlo y prevenirlo. Trasladando esto a las definiciones consultadas, *hacer estadística para tener datos útiles que ayuden a calcular un posible delito, anunciar por conocimiento fundado que ha de suceder en un tiempo y lugar específico, anticiparlo e impedir que se cometa.*

La prevención no se diferencia de la preparación y disposición que previamente se haga para evitar que algo acontezca. ¿Cómo podemos prevenir la muerte por inundación o, actualmente, el contagio de la COVID-19? Pues teniendo un previo conocimiento, experiencias que vayan suministrando datos, factores que permitan facilitar la acción o decisión oportuna y correcta. Así se pueden pronosticar las causas de por qué se delinque; con tal conocimiento se aplicará el correctivo y, en consecuencia, se podrá controlar el problema (Alabares, 2018).

## III. INGREDIENTES INDISPENSABLES PARA LA COMISIÓN DE UN DELITO

Antes de intentar predecir un delito, es indispensable conocer las diferentes conceptualizaciones legales, sociológicas, psicológicas y criminológicas que giran en torno a él, así como los factores que lo constituyen, debido a que dichos factores serán los datos útiles que se utilizarán en este método predictivo.

El Código Penal Federal, es su artículo 7o., define al delito como el acto u omisión que sancionan las leyes penales, por lo que el delito es un comportamiento típico, antijurídico y culpable, cuyos elementos son la conducta, la tipicidad, la antijuridicidad y la culpabilidad (Quintino, 2013: 1). Partiendo de lo expuesto, se puede inferir que únicamente una conducta, cualquiera que esta sea, puede ser considerada delito cuando esté descrita

en una ley penal, no exista una causa de justificación y no medie una causa de inculpabilidad.

Para la psicología, el delito es una actitud interior inconforme con las exigencias de la norma (Soto, 2014: 29); debido a ello, los psicólogos advertirán esa manifestación externa, organizarán sistemáticamente los factores que la componen y elaborarán teorías que traten de explicarla. Debido a que la policía predictiva centra su atención, principalmente, en delitos dolosos, es decir, cometidos por quienes, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quieren o aceptan la realización del hecho descrito por la ley; la psicología criminal estudia al delincuente que fue consciente de que era un acto injusto el que tenía en mente y, aun así, quiso cometerlo (Soto, 2014: 29). Siendo lacónicos, para la psicología es indispensable la voluntad para que un delito se pueda cometer. Para los psicólogos y psiquiatras, el estudio del sujeto tiende a ser individual. Si se trabaja para el sistema penal, suele solicitarse el estudio individual de sujetos dentro de un proceso penal previo (Pérez, 2018).

Por otro lado, la sociología considera el acto criminal como una respuesta de ciertos individuos a los estímulos modulados por la organización social (Pérez, 2011); por ende, no puede existir una conducta delictiva cuando una persona se encuentra separada de una sociedad; un individuo no puede cometer un delito perjudicándose a sí mismo, por lo que necesita del conjunto social para vulnerar el derecho ajeno.

Para la criminología, el estudio del delito es más amplio, debido a su autonomía científica lícita; la propia determinación de su objeto puede estudiar críticamente por qué a determinada conducta se le considera delito o por qué no (Pérez, 2018). El delito es producto de un comportamiento causado por determinados factores internos o externos; es una elección racional de un individuo egoísta y aislado que busca satisfacer de inmediato su deseo (Becker, 1974). Determinar con exactitud los factores externos e internos que originan un comportamiento es la misión que debe acometerse para obtener datos objetivos que realizarán predicciones precisas. Stanley Becker teorizaba que una persona comete un delito si la utilidad esperada para él excede la utilidad que podría obtener usando su tiempo y otros recursos en otras actividades, punto de suma importancia para el desarrollo y la construcción de una predicción. Aunado a lo anterior, el delito no se manifiesta de forma aleatoria en el espacio o en el tiempo, sino que en él inciden la oportunidad y el criterio de selectividad: ocurre en lugares

y períodos específicos y busca a la víctima propicia, variables que mutan de acuerdo con la importancia del contexto y de los factores ambientales (Larrauri, 2003).

En suma, hay tres elementos que deben darse simultáneamente, en el mismo lugar y al mismo tiempo, para que se produzcan las conductas delictivas: un delincuente motivado, un objetivo apropiado y ausencia de vigilancia, elementos que están constituidos por variables como la edad, el sexo, la condición socioeconómica, las creencias, la complexión física, el nivel sociocultural, el grado académico y la experiencia, entre otras (Santos, 2019).

Este conjunto de variables, en las que los sujetos activos tienen mayor o menor coincidencia, aportan de manera significativa patrones rutinarios tanto del perpetrador como de la víctima, que interactúan con el contexto situacional de aquel y deciden el éxito de la actividad delictiva. Se diría que estos patrones rutinarios son claves en una sociedad como la actual, en la cual los criminales tienen muchas más oportunidades para delinquir, y en la que los estilos de vida de la gente llevan, por ejemplo, a dejar las casas solas durante la jornada de trabajo y las vacaciones; salir de sus sectores a lugares de alta concentración de personas y realizar una serie de actividades en lugares públicos. Una sociedad donde, además, se han diversificado profesiones y negocios, y donde se corren riesgos y se puede ser víctima de delitos (Santos, 2019).

## IV. ¿CÓMO SE PUEDE OBTENER, INTERPRETAR Y UTILIZAR LA INFORMACIÓN OBTENIDA DE UN DELITO?

Es cierto que el éxito de la policía predictiva radica en la veracidad de la información recabada, así como que, en ocasiones, la información obtenida es errónea, incompleta o se tergiversa de una persona a otra. Dicha problemática no debe ser óbice para una correcta implementación, pues es aquí donde entra la importancia de la policía de primer contacto, especializada en recabar información precisa y concisa, y obligada a hacer llegar, a través de medios de comunicación electrónicos, dicha información de manera inmediata y directa al personal que se encargará de analizarla. Desafortunadamente, en estos tiempos la información va de un lado a otro, y se pierden o modifican sus detalles más esenciales, situación que debe ser solucionada para obtener mejores resultados.

Un punto clave para obtener más información de un criminal, no radica necesariamente en observar al criminal, sino a la víctima. En la mayor parte de las ocasiones, los policías, al momento de estar investigando un delito, suponen rasgos y características del sujeto activo, dejando a un lado a la víctima, la mayor fuente de información de evidencia anecdótica. La víctima, en específico la directa, es la persona física que ha sufrido algún daño o menoscabo a sus bienes jurídicos por la comisión de un delito, por lo que, si se la entrevista adecuadamente, se pueden conocer el tiempo y el lugar del hecho, la media filiación del agresor (en caso de que la recordara), el *modus operandi*, así como características de la propia víctima que motivaran la agresión. La entrevista a una víctima es muy diferente de cualquier otra, en la que se esperan ciertas respuestas, como lo puede ser una entrevista de trabajo, donde hay preguntas determinadas que se contestan de modo específico. Cuando se trata de un delito, las preguntas deben ir cambiando constantemente, adecuándose a las respuestas obtenidas, profundizando en detalles (en caso de que la condición del delito o la victima lo permita), moldeándose a un caso concreto, único y especifico, obteniendo información que permita alimentar cabalmente una estadística criminal. Si en una primera intervención no se logra obtener la información requerida, difícilmente se hará en una segunda intervención. Para esta fase se requiere que, como autoridades con funciones de seguridad pública, se desarrollen habilidades victimológicas.

Interpretar la información es un trabajo esencial para los criminólogos, sociólogos y psicólogos, que tendrán la importante labor de comprender y explicar los factores que propiciaron la ocurrencia de un hecho delictivo, los cuales serán variables de sus especialidades determinadas. Posteriormente, las variables obtenidas se utilizarán para crear patrones de comportamiento en un lugar y tiempo específicos. Se dice fácil, pero resulta un trabajo extenso y laborioso; actualmente existen numerosas profesiones dedicadas a la perfilación criminal con teorías interesantes, hechos sencillos y, lo que es más importante, de verdadera utilidad para el investigador. Tejeiro *et al.* (2016) señalan:

1. Los criminales no viajan lejos (de hecho, los más violentos viajan incluso menos que los menos violentos).
2. Los criminales no "cagan en su portal" (o sea, suelen dejar una pequeña distancia entre su propia base de operaciones y el lugar de los hechos).

3. Los criminales suelen cometer sus series de crímenes a 3 o 5 kilómetros de su domicilio, alejándose a medida que progresan en la serie.
4. Comparada con la victimología o la conducta violenta o sexual, la geografía aporta un mejor marco del que derivar inferencias sobre un crimen, está menos sujeta a interpretaciones y es más fácil de clasificar.





Desde hace décadas, en Estados Unidos, el desarrollo de los ordenadores permitió el diseño y la puesta en práctica de diversos programas computacionales, como Dragnet, Rigel, CrimeStat y Predator, para el apoyo automatizado de la policía, a fin de complementar el desarrollo de sus investigaciones en los casos criminales en serie (Tejeiro, 2016).

En el caso de CrimeStat III, es un programa de estadísticas espaciales para el análisis de ubicaciones de incidentes delictivos, desarrollado por Ned Levine & Associates bajo la dirección de Ned Levine, que fue financiado con subvenciones del Instituto Nacional de Justicia. El programa está basado en Windows e interactúa con la mayoría de los programas GIS (Geographic Information System) de escritorio. El propósito es proporcionar herramientas estadísticas complementarias para ayudar a las agencias de aplicación de la ley y a los investigadores de justicia penal en sus esfuerzos de mapeo del crimen. CrimeStat está siendo utilizado por muchos departamentos de policía de todo el país, así como por la justicia penal y otros investigadores. La última versión es la 3.3. (CrimeStat, 2010).

## V. CONCLUSIONES

Hablar de nuevos cambios para la mejora en la investigación y persecución del delito suele sonar paradójico, más aún cuando lo que se intenta implementar es un método predictivo. Cierto es que los policías de antaño refieren que el método de la policía predictiva no les resulta ajeno, debido a que, con las limitaciones en sus recursos, usaban métodos con similitudes tiempo atrás. Sin embargo, se debe formalizar y dar nombre a las actividades policiacas diarias, convertir la intuición en evidencia científica.

En suma, el método de la policía científica consiste en la utilización de información obtenida por las distintas áreas especializadas, procurando mantener su autenticidad, para prever la ocurrencia de un crimen, utilizando herramientas tecnológicas y análisis de datos para tomar decisiones encaminadas a la prevención del delito.

## VI. FUENTES DE CONSULTA


Álvarez, D.L.G., Montenegro, N.M.C., Martínez, J.M. (2012). *Apuntes acerca de dos escuelas criminológicas: Clásica y Positivista*. México: Facultad de Psicología. UNAM.

Becker, G. S. (1974). *Crimen y castigo: un enfoque económico*. Essay in the economics of Crime and Punishment, Becker, G. and Lands, W. eds. NBER.

CrimeStat. (2010). "About CrimeStat". Consultado en: https://www.icpsr.umich.edu/CrimeStat/about.html

L. Perry, Walter., McInnis, Brian., C. Price, Carter. (2013). *Predictive Policing*. E.UA.: RAND.

Larrauri, P.E. (2003). *Teorías criminológicas: explicación y prevención de la delincuencia*. España: Bosch.

Luna, D. (2019). *Policía predictiva*. Bogotá: Editorial La República. Recuperado de: https://www.larepublica.co/analisis/david-luna-400682/policia-predictiva-2848252

NOBBOT. Tecnología para las personas. (NOBBOT). (2019). "La policía predictiva: así ayuda un algoritmo a combatir los delitos". Recuperado de: https://www.nobbot.com/pantallas/algoritmos-policia-predictiva/.

Pérez, G.E., Rodríguez, J.R.R., Loy, V.B. (2018). *La aplicación de la criminología clínica en las investigaciones forenses actuales*. Cuba: Universidad de Ciencias Médicas de Villa Clara.

Pérez, L.J.A. (2011). *Explicación sociológica de la criminalidad*. Perú: Universidad de San Martín de Porres.

Quintino, Z.R. (2013). *La legítima defensa del policía*. México: Flores.

RAND. (2019). OBJECTIVE ANALYSIS EFECTIVE SOLUTION. Recuperado de: https://www.rand.org/pubs/research_reports/RR233.html#:~:text=Predictive%20policing%20is%20the%20use,problems%20more%20effectively%20and%20efficiently.

Santos, A.T., Jiménez A.M.A. (2019). *El miedo de las víctimas: diseccionando la criminología del control*. Chile: Universidad del Zulia.

Soto, C.J.E. (2014). *Manual de investigación psicológica del delito*. España: Ediciones Pirámide.

Tejeiro, R., Soria, M.A., Gallardo, C. (2016) *Perfilación geográfica en la investigación criminal*. México: Pirámide.

UNODC. Organización de las Naciones Unidas Contra la Droga y el Delito. (2010). *Manual de instrucciones para la evaluación de justicia penal*. E.U.A.: Naciones Unidas.

# VISIONES PARA EL FUTURO

# LA EVOLUCIÓN DEL RETRATO HABLADO: DEL LÁPIZ Y EL PAPEL A LOS ALGORITMOS GENÉTICOS*

Luis Fernando Cuevas Remigio**, Katya Rodríguez Vázquez***, Arodi Farrera****, Sergio Padilla Renaud***** y Germán Palafox Palafox******

* Los autores agradecen el apoyo otorgado por el proyecto PAPIIT IN-101620, UNAM.
** Universidad Nacional Autónoma de México
*** Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas, Universidad Nacional Autónoma de México.
**** Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas, Universidad Nacional Autónoma de México.
***** Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas, Universidad Nacional Autónoma de México.
****** Facultad de Psicología, Universidad Nacional Autónoma de México.

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Retrato hablado** | *Facial composite* |
| **Rostro** | *Face* |
| **Programación evolutiva** | *Evolutionary programming* |
| **Algoritmos genéticos** | *Genetic algorithms* |
| **Identificación** | *Identification* |



**Resumen.** El retrato hablado es una técnica frecuentemente utilizada en la investigación policial. Sin embargo, la investigación de laboratorio indica que el nivel de identificación de un rostro, a partir de un retrato hablado, es bajo. Una de las razones de esto es que el retrato hablado tradicional no se aproxima a los procesos de reconocimiento facial humano. En las últimas dos décadas se han creado sistemas de cuarta generación, basados en programación evolutiva con algoritmos genéticos, cuya principal característica es la combinación y evolución de rostros completos que gradualmente pueden converger en un rostro objetivo. El sistema Caramex II, basado en las características antropométricas del rostro de la población mexicana, pretende utilizar una aproximación evolutiva para construir retratos hablados.

**Abstract.** Facial composite is a technique frequently used in police investigation. However, laboratory research indicates that the level of identification of a face, from a facial composite, is low. One reason for this is that the traditional sketch does not approximate human facial recognition processes. In the last two decades there have been fourth generation systems, based on evolutionary programming with genetic algorithms, whose main characteristic is the combination and evolution of complete faces that gradually can converge on an objective face. The Caramex II system, based on the anthropometric characteristics of the face of the Mexican population, intends to use an evolutionary approach to construct facial composites.



Fecha de recepción: 30 de octubre de 2020
Fecha de aceptación: 11 de noviembre de 2020

SUMARIO:







## I. INTRODUCCIÓN

El retrato compuesto forense, comúnmente conocido como retrato hablado, es la técnica por medio de la cual una víctima o testigo de un evento delictivo proporciona la descripción verbal de los rasgos faciales de un sospechoso a un experto en arte forense, quien intenta recrear el rostro de dicho sospechoso a través de un dibujo. Desde que se introdujo esta técnica como parte de la investigación policial, ha existido una serie de cambios o generaciones en la forma de realizar el retrato hablado. La primera generación comenzó a finales de siglo XIX, cuando diferentes departamentos de policía en Europa y en Estados Unidos solicitaron a retratistas o caricaturistas de periódicos su colaboración para dibujar los rostros de sospechosos de algún delito (Taylor, 2001). Esta primera etapa se extendió hasta la década de los cincuenta del siglo XX, en la cual se va profesionalizando y especializando la labor de los artistas forenses.

La segunda generación comenzó con la introducción de técnicas mecánicas para la construcción del retrato hablado, como los sistemas Identikit y Photofit (Davies y Valentine, 2007). Estos sistemas contaban con un catálogo de imágenes de diferentes rasgos faciales (ojos, narices, bocas, etc.), con el objetivo de que las víctimas o testigos de un delito seleccionaran estos rasgos, tomando como criterio su grado de semejanza con el de un sospechoso, y construir su rostro (Davies y Valentine, 2007). En el caso de Identikit, estos rasgos eran dibujos impresos en acetatos transparentes que se podían sobreponer para formar el rostro. Este sistema contaba con un lápiz especial de cera, con el cual se podían añadir elementos a la composición final, como marcas, lunares, arrugas o cicatrices para mejorar el parecido. En el caso de Photofit, eran imágenes de fotografías de rasgos faciales impresas en cartón con un recorte especial para que encajaran, a manera de un rompecabezas, y poder formar el rostro del sospechoso (Taylor,

2001). Esta segunda generación se extendió hasta la década de 1980, cuando aparecieron los primeros sistemas informáticos.

En la tercera generación destacan programas como Mac-Mug-Pro y E-Fit (Davies y Valentine, 2007), muy similares a los sistemas mecánicos, debido a que contaban con un catálogo de rasgos faciales que debían ser seleccionados por las víctimas o testigos, pero que contaban con la ventaja de poder utilizar algunas herramientas de edición de imágenes que permitían aumentar o disminuir el tamaño de los rasgos, aclarar u oscurecer la piel o agregar elementos, como arrugas o bigotes (Davies y Valentine, 2007). Esta tercera generación se extendió hasta el final del siglo XX.

Con el cambio de siglo y con el avance en la capacidad de las computadoras para procesar imágenes y el desarrollo de la inteligencia artificial, se diseñaron nuevas técnicas de construcción de retratos hablados. La característica principal de esta nueva generación se fundamenta en una aproximación *holística* o global de construir los retratos hablados, es decir, se deja de lado la descripción verbal de las víctimas o testigos y se prioriza una manera más natural o cercana a la percepción facial humana. Esto se realiza a través de la selección y combinación de rostros completos. Las víctimas o testigos que utilizan estos nuevos sistemas deben seleccionar rostros que, *grosso modo*, se asemejen al rostro de un sospechoso. Estos sistemas utilizan una programación con algoritmos genéticos (Holland, 1975; Goldberg, 1989), que les permiten combinar y evolucionar estos rostros hasta converger en un rostro objetivo.

## II. LOS PROBLEMAS DEL RETRATO HABLADO

A pesar de ser una de las técnicas periciales más empleadas en la investigación policial, el retrato hablado presenta una serie de problemas que poca atención ha recibido por parte de la autoridad (Davies y Valentine, 2007). Por ejemplo, la organización no gubernamental *Innocence Project* informó en un estudio que, de 367 casos de identificación incorrecta en Estados Unidos, el 69% implicó la declaración de un solo testigo, y el 27% de estos casos involucró el uso de un retrato hablado (Innocence Project, 2016). Además, la investigación psicológica de laboratorio sobre reconocimiento de retratos hablados muestra un desempeño pobre por parte de los participantes en diversos experimentos, para identificar un rostro conocido a partir de un retrato hablado. Por ejemplo, en su investigación, Davies (1986)

confrontó el desempeño de dos grupos de participantes para construir, con ayuda de expertos en arte forense o con Photofit, un grupo de rostros desconocidos para ellos. Los rostros fueron una serie de fotografías mostradas durante un minuto a los participantes. Los retratos hablados elaborados por los artistas forenses y con Photofit, fueron luego mostrados a otro grupo de participantes que sí conocían los rostros, a partir de los cuales se elaboraron los retratos hablados para que intentaran reconocerlos. Sus resultados mostraron que los retratos hablados hechos con arte forense fueron mejor identificados que aquellos elaborados con Photofit. Sin embargo, los retratos hablados hechos por artistas forenses, que mayor calificación de identificación obtuvieron, fueron aquellos elaborados en presencia del rostro, es decir, observándolo en todo momento, que aquellos hechos a partir de la memoria de los participantes.

En otra investigación parecida, pero utilizando esta vez Identikit, Laughery y Fowler (1980) hallaron nuevamente que los retratos hablados hechos con arte forense fueron mejor identificados que aquellos hechos con Identikit. Sin embargo, otra vez los retratos hablados que mayores puntajes de identificación obtuvieron fueron los hechos en presencia del rostro, en lugar de a partir de la memoria de los participantes. Por otro lado, Davies, van der Willick y Morrison (2000) compararon el sistema mecánico Photofit con el sistema informático E-fit para construir retratos hablados de rostros conocidos y desconocidos para sus participantes. Los retratos hablados fueron también realizados en presencia del rostro y a partir de la memoria de los participantes. Sus resultados indicaron que los retratos hablados elaborados en presencia del rostro y elaborados con E-fit fueron mejor identificados que aquellos hechos con Photofit. Por su parte, aquellos retratos elaborados de memoria obtuvieron bajos puntajes de identificación, independientemente del sistema utilizado, además de que no hubo diferencias significativas para los rostros conocidos o desconocidos. Otras investigaciones han reportado resultados similares (Brace, Pike, Allen y Kemp, 2006; Brace, Pike y Kemp, 2000; Davies y Oldman, 1999). De manera general, la tendencia que se encuentra en esta clase de investigaciones muestra que los niveles de identificación de un rostro a partir de un retrato hablado en condiciones ideales, es decir, construido en presencia del rostro, oscilan en alrededor del 20%, mientras que aquellos elaborados simulando situaciones forenses reales alcanzan menos del 5% (Zahradnikova, Duchovicova y Schreiber, 2016).

Existen dos principales factores que explicarían el bajo nivel de identificación de esta técnica. El primero de ellos es la forma en la que se construyen los retratos hablados a partir de rasgos individuales. La mayoría de los sistemas de construcción de retratos hablados requiere que las víctimas o testigos de un delito proporcionen una descripción verbal de un rostro o que seleccione, de entre un catálogo, aquellos rasgos faciales que más se asemejen al de un sospechoso. Sin embargo, existe abundante investigación psicológica que indica que la percepción de un rostro es *holística* o global; es decir, como una sola unidad perceptual, más que como un conjunto de rasgos individuales agrupados (Behrmann, Richler, Avidan y Kimchi, 2015; Tanaka y Farah, 1993; Tanaka y Simonyi, 2016). Algunas investigaciones que apoyan esta idea son las que han acuñado el término *efecto de inversión del rostro* (Boutsen y Humphreys, 2003; Carbon y Leder, 2005; Thompson, 1988; Valentine, 1988), el cual se refiere a la tendencia de las personas a no percibir grandes alteraciones en la imagen de un rostro (como los ojos y la boca volteados), cuando este se presenta de manera invertida. Solo hasta que se coloca en posición vertical, con la cabeza hacia arriba, es cuando las personas pueden percibir lo grotesco de la apariencia de este rostro.

La explicación que proporcionan los investigadores para este efecto indica que, cuando un rostro se muestra de forma invertida, se interrumpe la capacidad de percepción holística y se utiliza un procesamiento individual de cada rasgo facial. Sin embargo, este procesamiento por rasgos no es del todo eficiente, por lo cual no permite detectar los rasgos alterados de un rostro en forma invertida. Otra evidencia del procesamiento holístico proviene del denominado "efecto de composición del rostro" (Young, Hellawell y Hay, 2013), que se refiere a la tendencia de las personas a percibir como un solo rostro a la imagen compuesta por dos mitades, una superior y otra inferior, de dos rostros distintos. En algunos experimentos de tiempo de reacción se ha encontrado que, cuando se utilizan rostros de celebridades que se combinan entre sí para formar rostros compuestos, los participantes tienen una mayor latencia para identificar a las celebridades a partir de la mitad superior, cuando estas mitades están completamente alineadas. Sin embargo, cuando las mitades se muestran desalineadas, el tiempo de respuesta disminuye (Hole, 1994; Rossion, 2008; Young, Hellawell y Hay, 2013). Además, este efecto desaparece cuando los rostros compuestos se muestran de manera invertida (Hole, 1994, Rossion, 2008).

Otro de los efectos que apoya el procesamiento holístico es el denominado "efecto del todo sobre sus partes" (Tanaka y Farah, 1993), que se refiere

a la tendencia a reconocer, de manera más precisa, un rasgo facial, como una nariz, cuando esta se encuentra en el contexto de un rostro completo que cuando se muestra de manera aislada, como en los catálogos de rasgos faciales de los sistemas mecánicos de retrato hablado. Por ejemplo, Tanaka y Farah (1993) le solicitaron a un grupo de participantes que intentaran memorizar una serie de rostros. Luego, evaluaron la memoria de sus participantes para determinar si podían reconocer tres rasgos faciales de los rostros aprendidos (nariz, boca y ojos) en dos condiciones distintas: rostro completo y rasgo aislado. En la condición de rostro completo se presentaba un par de rostros iguales, a excepción de un rasgo distinto, por ejemplo, la nariz, mientras que, en la condición de rasgo aislado, solo se presentaban dos rasgos, por ejemplo, dos narices. La tarea de los participantes era identificar, en ambas condiciones, el rasgo de los rostros aprendidos. Sus resultados mostraron que los participantes fueron más precisos para reconocer un rasgo cuando este se presentaba en el contexto de un rostro completo que de manera aislada.

El segundo factor relacionado con el bajo nivel de identificación de un retrato hablado es el componente verbal de aquel. Muchas investigaciones (Dodson, Johnson y Schooler, 1997; Fallshore y Schooler, 1995; Ryan y Schooler, 1998; Schooler y Engstler-Schooler, 1990; Sporer, 2007) sugieren que describir un rostro desconocido que se ha observado brevemente puede afectar su posterior reconocimiento. Por ejemplo, Schooler y Engstler-Schooler (1990), en uno de sus experimentos, mostraron a un grupo de participantes un video de 30 segundos, en el cual aparecía una persona asaltando un banco. Luego de observar este video, la mitad de sus participantes llevó a cabo una tarea de lectura durante cinco minutos. A la otra mitad se le pidió que proporcionara una descripción por escrito, lo más detallada posible, del rostro del asaltante durante cinco minutos. Al término de ambas tareas, los dos grupos fueron sometidos a una tarea de reconocimiento, en la cual tenían que tratar de identificar el rostro del asaltante del video de entre otros ocho rostros distractores. Sus resultados mostraron que los participantes que proporcionaron la descripción detallada del rostro del asaltante pudieron identificarlo correctamente en un 38%, mientras que los participantes de la actividad de lectura pudieron reconocerlo en un 64%. Los investigadores denominaron a este efecto "ensombrecimiento verbal", y consideraron que se presenta debido a que la memoria verbal de un rostro interfiere con la memoria visual de este; como no existen las palabras lo suficientemente precisas para describir la forma y el tamaño de

los rasgos faciales, esta descripción puede alterar la representación visual original del rostro por otra sesgada y menos precisa. Por su parte, Wells, Charman y Olson (2005) demostraron un efecto similar durante la construcción de retratos hablados.





## III. RETRATO HABLADO DE CUARTA GENERACIÓN

En las últimas dos décadas se ha desarrollado una serie de *softwares* de cuarta generación que intentan abatir las limitaciones de los métodos tradicionales de construcción de retratos hablados (Frowd *et al.,* 2015a; Frowd, Erickson, Lampinen *et al.,* 2015b; Davies y Valentine, 2007). Estos sistemas, principalmente Evo-Fit y EFIT-V (Frowd *et al.*, 2015; Valentine, 2010; Zahradnikova, Duchovicova y Schreiber, 2018), utilizan rostros completos para la construcción de los retratos y una programación con algoritmos genéticos (Holland, 1975; Goldberg, 1989). Estas características permiten, en primer lugar, que los testigos seleccionen rostros completos, tomando en cuentan si presentan rasgos similares a los del rostro de un sospechoso. Por otro lado, y a través de su programación con algoritmos genéticos, estos *softwares* combinan los rostros seleccionados por los testigos para gradualmente converger en un retrato, en teoría, mucho más perecido al rostro del sospechoso. De acuerdo con los investigadores (Frowd *et al.,* 2015a; Frowd, Erickson, Lampinen *et al.,* 2015b; Davies y Valentine, 2007; Valentine *et al.,* 2010; Zahradnikova, Duchovicova y Schreiber, 2016), la metodología que emplean estos *softwares* hace que la descripción verbal de un rostro sea innecesaria durante la construcción del retrato y la selección y combinación de rostros completos sea más cercana al reconocimiento facial humano.

La teoría psicológica de la que parten estos *softwares* se basa en la percepción holística o global del rostro, y que la representación mental de cada uno de estos, que se guarda en la memoria, está organizada en un *espacio facial multidimensional* (Valentine, 1991, 2002; Valentine, *et al.*, 2010). De acuerdo con esta teoría, cada rostro es almacenado en términos de sus valores (o vectores) en un amplio rango de dimensiones faciales. Por ejemplo, una persona ha observado una cantidad considerable de rostros a lo largo de su vida y ha podido percatarse que existen narices que son muy cortas o largas, además de otras que estarían entre esos extremos. Según la teoría del espacio facial, esta característica de las narices podría representarse en la memoria como un continuo o una dimensión. Si además se considera

otro rasgo facial, como la separación entre los ojos, se podría establecer otra dimensión; es decir, hay rostros cuyos ojos parecen estar muy juntos o separados, además de rostros con valores entre estos extremos. De esta manera, se podrían agregar más valores o dimensiones de rasgos faciales, como el tamaño de las orejas, la anchura de la boca, lo largo de la cara, la edad aparente, etc. Según esta teoría, todos estos valores faciales estarían almacenados en la memoria en un espacio multidimensional. De esta manera, cuando una persona considera que dos rostros son muy parecidos entre sí, sería porque sus vectores dimensionales son muy similares.

## IV. ANÁLISIS DE COMPONENTES PRINCIPALES

La teoría del espacio facial puede ser modelada matemáticamente a través de un método denominado "análisis de componentes principales" (PCA, por sus siglas en inglés), que es la base para los *softwares* de cuarta generación. Un rostro está compuesto por una gran cantidad de rasgos faciales (ojos, nariz, boca, lunares, etc.). La variabilidad que existe en cada uno de estos rasgos agrega una dimensión al espacio facial multidimensional. Entre más rasgos consideremos, mayor será el número de combinaciones posibles que podríamos tener para formar un rostro y, por tanto, más se complica el análisis. Cuando se trabaja con imágenes, esta dimensionalidad es aún mayor, pues, en lugar de tener una serie de rasgos, estamos trabajando con miles de píxeles, y cada uno de ellos cuenta como una dimensión; por lo que un conjunto cualquiera de imágenes (no es la cantidad de imágenes, sino la cantidad de variables lo que incrementa la dimensionalidad) representa un espacio multidimensional de información que requiere grandes demandas de memoria.

El PCA se utiliza para reducir la variación de dicho espacio de información a unas cuantas variables nuevas, conocidas como componentes principales. Cada una de estas nuevas variables es una combinación lineal de las variables originales; es decir, cada componente principal toma en cuenta todas las variables originales a la vez. Por ello, se les podría considerar como una representación holística del rostro (es decir, en lugar de centrarnos en las variables por separado, las concentramos todas en un componente principal). Este análisis se utiliza entonces para reducir a unos cuantos componentes o conjunto de dimensiones, conocidos como *eigenvalues* (o *eigenfaces* en este contexto), una serie de imágenes de rostros (Sirovich

y Kirby, 1987; Turk y Pentland, 1991). Cada *eigenface* es holístico, es decir, contiene una representación "resumida" de la imagen facial a partir de la cual se generó. Cuando se toma una muestra amplia de rostros y se les aplica un PCA, algunos de estos componentes principales pueden interpretarse como si codificaran alguna característica particular, como el sexo, la textura de la piel, el color del cabello, la edad, entre otros. Además, cuando se realiza un PCA, los *eigenfaces* resultantes se codifican como una serie de pesos o valores (*weights*), los cuales pueden ser recombinados para generar rostros nuevos (Craw y Cameron, 1991, 1992). Sin embargo, cuando se recombinan tales pesos para formar rostros nuevos, estos pueden parecer desproporcionados, amorfos o difuminados (Troje y Vetter, 1996). Para evitar esta situación, Craw y Cameron (1991) propusieron el análisis separado para la forma y la textura de los rostros.

Primero, la forma se obtiene a través de una serie de *landmarks* o marcadores de referencia que se colocan sobre el rostro, para indicarle al programa la posición de los rasgos faciales. Estos *landmarks* están codificados en valores de coordenadas *x* e *y*. Este método genera que el análisis de los rostros que lleva a cabo el PCA se estandarice a una forma facial única (denominada *shape-free*), donde los *landmarks* se localizan en la misma posición en cada una de las imágenes de la muestra de rostros. Generalmente, esta forma facial única es el promedio de la forma del conjunto de los diferentes rostros que constituyen la muestra (es decir, *morph*). Por su parte, la textura está representada por la escala de grises o la información de color de la imagen de los rostros. Cada *landmark* proporciona información de la textura dependiendo de su posición. De esta manera, diferentes rostros presentarán una variación distinta en la información de textura. Posteriormente, textura y forma pueden ser combinados con la aplicación de otro PCA como parte de un algoritmo denominado *active appearance model*, que proporciona un solo conjunto de parámetros compactados de modo óptimo para esta información (Cootes, Edwards y Taylor, 1998; Cootes y Taylor, 2001). Uno de los problemas con esta metodología es que no es posible reconstruir adecuadamente el tipo de cabello. Para ese fin, algunos sistemas recurren a un catálogo de imágenes con diferentes estilos y cortes de cabello, que pueden ser colocados al término de la construcción del retrato.

## V. EVOLUCIÓN DE ROSTROS

El PCA se puede combinar con algoritmos evolutivos para converger en la imagen de un rostro objetivo (*target face*). Los algoritmos evolutivos son llamados así porque emplean dos conceptos fundamentales de la evolución: variación aleatoria (mutación) y selección. La construcción de retratos compuestos comienza con la generación de un conjunto aleatorio de imágenes faciales (artificiales) dentro del espacio facial del PCA. Posteriormente, el usuario selecciona los rostros que considera más similares a los de un rostro objetivo. En el primer conjunto de rostros que muestra el espacio facial habrá un amplio rango de rostros, y ninguno necesariamente se parecerá al rostro objetivo. Sin embargo, las selecciones de rostros que haga el usuario servirán para "engendrar" un nuevo conjunto de rostros, introduciendo mutaciones del rostro o rostros "padre". El proceso se repite hasta que las siguientes "generaciones" de rostros comiencen a parecerse entre sí, y termina cuando el usuario considera que ya no puede elegir entre las nuevas generaciones de imágenes, porque todos reproducen igual de bien el rostro objetivo, o bien, porque el proceso fracasó en reproducirlo.

Gibson, Pallares-Bejarano y Solomon (2003) identifican tres tipos de algoritmos evolutivos indispensables para la construcción de retratos hablados:

1. *Scale rating*. En este algoritmo, todas las imágenes, en cada generación, son calificadas en una escala de similitud respecto del rostro objetivo. Los rostros mejor calificados son seleccionados para engendrar la siguiente selección, habilitando tanto el cruce (*crossover*) como la mutación (Hancock, *et al.*, 2000).
2. *Select Multiple Mutate*. En este algoritmo, el testigo selecciona el rostro más parecido, el cual es reproducido con mutaciones aleatorias en todos los rostros de la siguiente generación, excepto en uno (Tredoux *et al.*, 1999).
3. *Follow the leader.* Este algoritmo muestra una serie de rostros nuevos con el mejor parecido posible, alcanzado por el sistema respecto al rostro objetivo. El testigo debe, entonces, simplemente elegir aquellos rostros que, a su juicio, reproducen de mejor manera el rostro objetivo. Este proceso se repite para alimentar a las siguientes generaciones y obtener un registro histórico de evolución, que sirve de guía para el proceso.

La ventaja de este procedimiento para construir retratos forenses es que permite hacer modificaciones globales u holísticas de un rostro, el cual se aproxima mucho más al proceso de reconocimiento facial humano, además de prescindir por completo de la descripción verbal. Sin embargo, algunos testigos señalan que ciertos rasgos del rostro, en su etapa de evolución final, requieren la modificación de un rasgo específico. Esto no es posible a través de esta metodología. Para ello, se utilizan programas de edición de imágenes, como Photoshop, pero trabajando con la configuración global del rostro, y no con partes aisladas.

## VI. *SOFTWARES* DE CUARTA GENERACIÓN

Existen hasta el momento cuatro sistemas de construcción de retratos hablados de cuarta generación. Estos *softwares* utilizan, de manera general, el procedimiento descrito en la sección anterior, pero difieren en el empleo de algunos algoritmos para optimizar su tarea. El primero de ellos fue desarrollado en la Universidad de Ciudad del Cabo (Tredoux *et al.*, 2006) y se denomina ID. Este *software* utiliza un algoritmo denominado PBIL (*population based incremental learning*), el cual guía la búsqueda de un rostro objetivo dentro de su espacio facial de la siguiente manera:

1. El sistema genera una pequeña muestra aleatoria de rostros, los cuales son mostrados al usuario.
2. El usuario selecciona el rostro que más se asemeje a un rostro objetivo.
3. El sistema usa los coeficientes del rostro seleccionado como una nueva *semilla* o punto de partida para generar nuevos rostros que mostrar al usuario.

Sin embargo, el sistema requiere de 100 a 150 generaciones para producir un rostro aproximado al rostro objetivo. Por esta razón, y considerando que en un contexto real este número de generaciones es proclive a la fatiga y a terminar la búsqueda del rostro objetivo antes de converger en una aproximación adecuada, los investigadores introdujeron un nuevo algoritmo denominado *M-choice*, que optimiza y reduce el tiempo de búsqueda. Este algoritmo opera de la siguiente forma:

1. El sistema genera una pequeña muestra aleatoria de rostros, los cuales son mostrados al usuario.
2. El usuario selecciona una serie de rostros que son similares al rostro objetivo en un orden de similitud; es decir, la primera selección es el rostro más similar, la segunda es la segunda mejor similitud, etc. El número de rostros seleccionados puede variar de generación en generación.
3. El sistema calcula la media y la varianza de estas selecciones y las utiliza como base para crear nuevas generaciones de rostros para mostrar al usuario.

Tredoux *et al.* (2006) evaluaron este sistema en dos experimentos para determinar su eficiencia. En el primero se comparó el desempeño de los algoritmos PBIL y M-choice, utilizando la información de solo la textura o textura y forma para construir los retratos. En este experimento, un grupo de 30 participantes observó dos rostros durante 30 segundos. Posteriormente, se les explicó el funcionamiento de ID y cómo se construían los retratos con este sistema. Una vez comprendida esta parte, los participantes debieron construir los rostros observados de memoria. La mitad de los participantes utilizó el algoritmo PBIL, y la otra mitad M-choice. Una vez construidos los retratos, otro grupo de participantes tuvo que evaluar su parecido con el rostro a partir del cual se elaboraron. Para ello, se diseñó una tarea en la computadora, en la que se mostraban a la derecha los rostros originales y, a la izquierda, una serie de cuatro retratos (distractores) y un retrato construido con el sistema ID. Debajo de cada retrato se mostraba una escala de similitud de 7 puntos, donde 1 representó *nada parecido* y 7, *muy parecido*. La tarea de los participantes fue observar las imágenes y determinar el grado de similitud utilizando la escala mostrada. Sus resultados arrojaron que, en todas las condiciones, excepto aquellas que utilizaban el algoritmo M-choice, con solo la información de textura, se obtuvieron puntuaciones de reconocimiento superior a las esperadas por azar. Además, se encontró que el algoritmo de M-Choice fue superior a PBIL cuando este podía utilizar la información de textura y forma para construir los retratos. En su segundo experimento, compararon el sistema ID con otro *software* de construcción de retratos hablados de tercera generación, basado en la selección de rasgos llamado FACES (IQ Biometrix). Sus resultados mostraron un desempeño superior de ID sobre FACES; sin embargo, los retratos construidos con ID no obtuvieron calificaciones muy altas de similitud por los participantes del experimento.

El otro sistema fue desarrollado por la Universidad Técnica de Estambul (Kurt *et al.,* 2006) y se llama INIH (*Interactive Nature-Inspired Heuristics*). Este *software* utiliza cinco diferentes algoritmos evolutivos para construir los retratos compuestos. El primero de ellos, *Interactive Generational Genetic Algorithm* (IGGA), emplea la siguiente estrategia:

1. Las nuevas generaciones de rostros son creadas a través de la selección que hace el usuario de los rostros mostrados por el sistema. Luego, estos se combinan y mutan.
2. El valor de ajuste (similitud) es obtenido directamente del usuario; es decir, cada rostro mostrado por el sistema es calificado por aquel con base en el grado de similitud de este con respecto a un rostro objetivo.
3. A través de una "competición" binaria basada en las calificaciones de similitud, se establecen los rostros "padres".
4. Luego se aplica una *mutación gaussiana*; es decir, la asignación de un valor aleatorio basado en una distribución normal o de Gauss, para crear la nueva generación de rostros (*offsprings*).

*Interactive Steady-State Genetic Algorithm (ISSGA)*:

1. La población ahora consiste en 3 rostros (dos padres y un descendiente).
2. El usuario debe entonces elegir el peor individuo, es decir, el rostro que menos se asemeje al rostro objetivo.
3. Entonces se genera un "hijo" como resultado de la recombinación de los genes de los rostros "padre", y aplicando una mutación gaussiana.

*Interactive Evolutionary Strategy (*IES):

1. Las nuevas generaciones de rostros se crean a partir de las operaciones de cruza (*crossover*) y mutación.
2. Se eligen pares de padres para recombinación de manera aleatoria.
3. Se aplica una mutación gaussiana.
4. En cada etapa se selecciona un número de rostros de la población mostrada.

*Interactive Differential Strategy* (IDS)*:*

1. En este caso, las mutaciones preceden a las operaciones de cruza.

2. La diferencia de los valores de pesos (*weights*) entre dos rostros candidatos se agrega a un tercero, para obtener otro rostro padre para una nueva recombinación genética.
3. En cada etapa se selecciona un número de rostros de la población mostrada.





*Interactive Particle Swarm Optimization* (IPSO):

1. La nueva población de soluciones potenciales se genera en cada iteración.
2. El usuario debe seleccionar, en cada etapa, la mejor opción de esta población.
3. En la etapa final, se muestran al usuario las mejores opciones de rostros seleccionadas, para elegir la mejor solución global.

Para evaluar este sistema, los investigadores desarrollaron un experimento, en el cual, a un grupo de participantes le mostraron una serie de rostros para luego construirlos de memoria, utilizando uno de los cinco algoritmos mencionados anteriormente. Una vez construidos estos retratos, se mostraron a otro grupo de participantes que conocían los rostros, a partir de los cuales se elaboraron, para que intentaran reconocerlos a través de proporcionar su nombre. Los resultados mostraron que los algoritmos ISSGA e IES fueron los que mayor porcentaje de reconocimiento obtuvieron. Sin embargo, el algoritmo ISSGA requirió de un mayor número de generaciones para llegar a una buena aproximación. Los investigadores reconocen que el sistema debe mejorarse para que sea competitivo con otros (Kurt *et al.,* 2006; Zahradnikova, Duchovicova y Schreiber, 2016).

El otro sistema, denominado inicialmente EigenFIT y luego E-FIT V, fue desarrollado en la Universidad de Kent (Gibson *et al.*, 2009; Solomon *et al.*, 2005), y se trató del primer *software* comercial de cuarta generación para construir retratos hablados. Este sistema estuvo originalmente basado en el algoritmo *Full Scale Rating Algorithm* (FSR), el cual operaba de la siguiente manera:

1. Cada individuo o rostro del espacio facial se calificaba con una escala del 1 al 10, con base en el grado de semejanza con respecto a un rostro objetivo.

2. Se utilizaban operaciones de cruza y mutación, basadas en las calificaciones proporcionadas por el usurario para engendrar a la siguiente generación.



Debido a la lenta velocidad de convergencia para alcanzar un retrato que se asemejara al rostro objetivo, se decidió implementar el algoritmo *Follow the leader* (FTL), el cual opera de la siguiente manera:

1. Se muestran al usuario dos rostros, con la indicación de que seleccione el mejor.
2. Se genera un descendiente (*offspring*) en cada iteración, como resultado de la selección de mejor semejanza por parte del usuario, además de un nuevo rostro de las iteraciones previas.
3. En esta implementación no existe una función de ajuste ni se preservan los mejores individuos para la siguiente generación.

Por último, los investigadores propusieron el algoritmo *Select Multiply and Mutate* como una estrategia que combinaba el porcentaje satisfactorio de convergencia y su simplicidad cognitiva. Este algoritmo opera de la siguiente manera:

1. Se muestran al usuario nueve rostros para que elija al mejor individuo.
2. Para evitar perder el mejor rostro o individuo una vez que se aplican los procesos evolutivos, este se copia a la siguiente generación sin cambios.
3. Luego, la nueva generación se compone de ocho individuos adicionales, clones del rostro mejor calificado.

En modificaciones posteriores (Solomon *et al.,* 2013), los investigadores lograron producir retratos de apariencia aceptable al rostro objetivo en 42 generaciones. Sin embargo, como el sistema cuenta con diferentes herramientas para modificar directamente los rostros, se puede alcanzar un retrato de apariencia aceptable en 25 iteraciones, en los cuales se muestran y se evalúan 225 rostros. Sin embargo, y a pesar de que muchos departamentos de policía en Europa y Estados Unidos utilizan este *software*, no existe mucha información pública de su desempeño. Solamente un estudio (Valentine *et al.,* 2010) reportó un 20% de identificación correcta en una tarea que implicaba proporcionar los nombres de los actores de una serie

conocidos por sus participantes, y cuyos retratos habían sido elaborados con este *software*. Sin embargo, cuando a los participantes no se les proporcionaba ninguna pista de a quiénes pertenecían los retratos, el porcentaje de identificación disminuyó hasta 0.8 %, a pesar de que los participantes conocían a los actores de la serie. Por el contrario, evaluaciones del desempeño de este *software* en contextos de testigos reales, llevados a cabo por la policía del oeste de Yorkshire en Reino Unido, entre 2010 y 2011, mostraron un 55% de identificación correcta de sospechosos (Solomon *et al.*, 2013).

Finalmente, está el sistema llamado Evo-Fit (Frowd *et al.*, 2015), el cual fue desarrollado en la Universidad de Stirling y la Universidad Central de Lancashire. Este *software* requiere que se establezca el rango de edad aproximado de un rostro objetivo. Posteriormente, el sistema le mostrará al usuario una serie de rostros al azar dentro del rango de edad seleccionado; enseguida, el usuario debe seleccionar el tipo de cabello del rostro objetivo entre un catálogo con diferentes estilos. La forma en que este sistema construye los retratos es a través de la selección de la forma del rostro y, luego, la textura de la piel, para finalmente combinar ambas. Este sistema utiliza un algoritmo llamado *Interactive Evolutionary Algorithm*, el cual opera de la siguiente manera:

1. Al inicio, se le muestra al usuario una serie de 10 a 32 rostros generados al azar. Luego, el usuario debe seleccionar aquellos rostros que por su forma se asemejen lo más posible al rostro objetivo, y luego por la textura. Finalmente, el usuario debe seleccionar aquellos rostros que mejor combinen forma y textura para obtener un solo individuo.
2. Para evitar que el mejor individuo o rostro se pierdan durante el proceso de evolución, este se copia y se transmite a la siguiente generación.
3. Los rostros de las diferentes generaciones son creados como resultado de los procesos evolutivos de cruza y mutación. Entonces, los nuevos rostros se obtienen de la combinación de los genes (coeficientes) de los rostros seleccionados por el usuario.

La investigación llevada a cabo por Frowd *et al.* (2001) indica que se requieren 10 generaciones para obtener un retrato aproximado de un rostro objetivo, si la población se fija en 160 rostros a evaluar por el usuario. Este *software* se emplea en diferentes departamentos de policía de Reino Unido y, a diferencia de los otros sistemas, existe una gran cantidad de investigación

sobre su desempeño (Frowd *et al.,* 2015). Para evaluar este sistema y otros similares, Frowd *et al*. (2005b) propusieron un protocolo de referencia (*gold standard*), el cual implica dos grupos de participantes en dos tareas distintas. El primer grupo participa en la construcción de los retratos a través de observar un rostro desconocido durante 1 minuto. Luego de un intervalo de 48 horas, los participantes son entrevistados sobre los rostros que observaron con una *entrevista cognitiva* (Fisher y Geiselman, 1992; Frowd *et al.,* 2008), la cual ha mostrado ser efectiva para ayudar a víctimas y testigos a recordar más detalles de un evento delictivo que hayan presenciado. Posteriormente, cada participante construirá de memoria el rostro que observó con Evo-Fit (o con el sistema disponible). Los rostros construidos con este sistema serán luego evaluados para su reconocimiento por el segundo grupo de participantes.

Este segundo grupo debe conocer los rostros a partir de los cuales se elaboraron los retratos, ya sea porque son profesores, celebridades, compañeros de escuela o trabajo, que solo este grupo conoce. Para determinar que un retrato ha sido correctamente identificado, los participantes de este segundo grupo deberán proporcionar el nombre de la persona que está representada en esos retratos. En las primeras versiones de Evo-Fit (Frowd *et al.*, 2004), este sistema alcanzó una tasa de identificación correcta de apenas 9.46%. En una versión posterior (Frowd *et al*., 2007a), y siguiendo su protocolo de referencia propuesto, se incrementó la identificación a 11%. Este incremento se debió, de acuerdo con los investigadores, a una serie de agregados o manipulaciones de las "dimensiones holísticas" de los retratos (Frowd *et al.,* 2006). Estas dimensiones holísticas implicaban la posibilidad de modificar el retrato final, de tal manera que se pudiera aumentar o disminuir la edad aparente del rostro, el peso, y aclarar u oscurecer la piel, además de otras dimensiones psicológicas, como atractivo, introversión, amenaza o masculinidad del rostro. Esto último se conseguía agregando ciertas sobras o cambios sutiles en la expresión facial, como el ceño fruncido o una ligera sonrisa. En las primeras versiones de Evo-Fit, se podía comenzar la construcción de un retrato eligiendo una serie de opciones, como el tipo de cabello, cuello u orejas; es decir, comenzando por lo que se consideran los rasgos externos del rostro. Sin embargo, estos rasgos externos son, en general, bien recordados por las personas que han observado un rostro desconocido brevemente. En cambio, los rasgos internos (cejas, ojos, nariz y boca) presentan mayor dificultad para ser recordados (Ellis, Shepherd, Davies, 1979). Para fomentar la atención en los rasgos internos

durante los procesos evolutivos de construcción de un retrato, Frowd *et al.* (2008) modificaron este procedimiento, de tal manera que, en su nueva versión, la construcción del retrato comenzaba eligiendo un tipo de cabello particular, para luego mostrarse difuminado durante todo el proceso de evolución del rostro, destacando solo los rasgos internos. Hasta el final de la construcción del retrato se mostraba el rostro de forma completa. Con estas modificaciones al inicio, además de los agregados de las dimensiones holísticas al final de la construcción del retrato, se incrementó la identificación correcta hasta un 24.5% (Frowd *et al*., 2011b).

Investigaciones posteriores mostraron que, si se omitían completamente los rasgos externos hasta el final de la construcción del retrato, se podía incrementar la identificación hasta un 42% (Frowd *et al.*, 2012d). Un porcentaje similar de incremento se obtuvo cuando se introdujeron cambios en la forma de presentar al público el retrato, y en la manera de entrevistar a los participantes. Por ejemplo, para la presentación pública del retrato se utilizaba una versión en la que se exageraban ciertos rasgos (caricaturización), o se presentaba con movimiento. Además, se introdujo una modificación a la entrevista cognitiva, llamada entrevista cognitiva holística, que enfatizaba los aspectos globales para recordar de un rostro (Frowd *et al.,* 2007b; Frowd *et al.,* 2012a). En los últimos años, este sistema se ha ido modificando y mejorando hasta alcanzar tasas de identificación correcta del 74% (Fondarella *et al.*, 2015; Frowd *et al.*, 2013; Frowd *et al.*, 2014a).

En una revisión de su efectividad con testigos reales, el departamento de policía de Humberside, en el norte de Inglaterra, reportó un 60% de arrestos de sospechosos utilizando este sistema, en un periodo de 12 meses en 2010 (Frowd *et al.*, 2012b).

## VII. CARAMEX

En México se ha desarrollado un acervo de imágenes de rasgos faciales para la generación de retratos hablados de sospechosos basado en las características antropométricas del rostro de esta población (Serrano, Villanueva, Luy y Link, 1997; Serrano, 2013; Villanueva, 2010). Este proyecto se denominó "La cara del mexicano" (Villanueva, 2010) y es, hasta el momento, una aproximación única a la construcción de retratos hablados en el mundo. Dada la gran variabilidad genética que representa el mestizaje

de la población mexicana, era importante, de acuerdo con los investigadores, contar con un acervo de imágenes que tomara en cuenta esta situación.

Este proyecto involucró la colaboración del Instituto de Investigaciones Antropológicas (IIA) de la Universidad Nacional Autónoma de México (UNAM) y la entonces Procuraduría General de Justicia del Distrito Federal (PGJDF). La investigación fue llevada a cabo entre 1993 y 1997, e implicó la obtención de un registro fotográfico del rostro de 2,890 individuos de diferentes regiones de México. Cada una de estas fotos fue tomada de frente y de perfil izquierdo con iguales condiciones de iluminación y distancia lente-rostro. En total, se recopilaron 5,780 imágenes. A partir de estas, se obtuvieron 21 mediciones antropométricas del rostro, de las que derivaron diferentes índices morfológicos y valoraciones morfoscópicas, como la forma de la inserción del cabello, el tipo de calvicie, la distribución del vello facial, la forma del dorso de la nariz, entre otras. Posteriormente, todos estos índices fueron sometidos a un análisis estadístico multivariado con el objetivo de establecer los factores tipológicos más representativos del rostro, y obtener imágenes prototípicas de cada uno de los rasgos faciales para hombres y mujeres. El resultado fue un acervo fotográfico, denominado Caramex, el cual contiene 586 archivos, de los cuales 405 están distribuidos en 26 directorios con rasgos faciales, que abarcan desde la forma general de la cara hasta arrugas o lunares (Villanueva, 2010).

La manera de construir los retratos hablados con este acervo implica la utilización del programa PhotoShop para la manipulación y edición de cada imagen. El proceso requiere que los participantes-testigos observen, primero, las diferentes formas del rostro y seleccionen la que consideran más parecida a la de la persona que observaron, para, posteriormente, ir seleccionando el resto de los rasgos faciales y colocarlos sobre esta forma facial. Este acervo, listo para usarse, fue entregado a la PGJ en 1996, y en los años subsecuentes a otros departamentos de policía de México. Según Santiago (2004, en Serrano, 2013: 9), en 2004, solo en la Ciudad de México, "cada mes, medio centenar de peritos recurrían, en casi mil casos, a Caramex para tratar de ubicar a una persona".

## VIII. CARAMEX-II

Actualmente, en el Instituto de Investigación en Matemáticas Aplicadas y en Sistemas de la Universidad Nacional Autónoma de México se desarrolla

un *software* para la construcción de retratos. Al igual que otros *softwares* de cuarta generación, este se apoya en algoritmos de reconocimiento facial y creación de redes neuronales, a través de bibliotecas como Dlib, OpenCV y TensorFlow. Este procedimiento sigue los siguientes pasos:

1. Gracias al conjunto de imágenes de Caramex, es posible contar con una colección de rasgos "típicos" de la cara del mexicano y sus *landmarks* o marcadores de referencia asociados y, a su vez, por medio del *toolkit* de detección de Dlib, se reconocen los rasgos faciales principales (ojos, nariz, boca, contorno facial) dentro del catálogo de imágenes de rostros de Caramex. Los rasgos detectados se recortan y ajustan para formar combinaciones en diferentes formas de cara, para obtener una vasta colección de rostros posibles.
2. Una vez obtenida esta galería de imágenes, se introduce a una red neuronal convolucional generada en la biblioteca de código abierto para aprendizaje automático TensorFlow, donde las imágenes son transformadas en matrices de píxeles con valores que van del 0 al 1, tras una normalización de los valores originales de 0 a 255. Por medio de varias convoluciones, se toman conjuntos de píxeles relativamente cercanos de la imagen, y se van multiplicando escalarmente por una pequeña matriz llamada *kernel*, la cual, aunada a otros *kernels*, funciona como filtro. En las primeras convoluciones es posible detectar características primitivas, como líneas o curvas. Al paso de más capas en las convoluciones, será capaz de reconocer formas más complejas. Al final, este conjunto de imágenes sirve para entrenar y probar el funcionamiento de la red neuronal artificial.
3. Un grupo de estos retratos es presentado para que el usuario seleccione los más parecidos al rostro que se busca identificar. Esta selección es analizada por la red neuronal.
4. Cuando la red convolucional ya está entrenada, es capaz de distinguir y clasificar rostros generados automáticamente a través de una técnica de "morphing" implementada con algoritmos en la biblioteca OpenCV, convirtiendo las imágenes en arreglos de números flotantes y tomando *landmarks* de referencia para encontrar puntos dentro de triángulos de Delaunay (Borut 2005; Mohammadzade *et al.*, 2018), para encontrar transformaciones afines que puedan generar y ajustar a una nueva imagen del promedio de las 2 o más imágenes seleccionadas con anterioridad, logrando así mezclar los rostros.

5. Ya que el sistema clasifica los rostros escogidos, es posible saber con qué clase de rasgos fue formado dicho rostro, y sugerir una nueva combinación de rasgos para obtener rostros semejantes a los escogidos previamente. Este paso se repite hasta que el *morphing* de imágenes sea lo más parecido al retrato buscado.

## IX. CONCLUSIONES

El retrato hablado es una técnica ampliamente utilizada en la investigación policial. Sin embargo, se ha evaluado muy poco su eficacia en escenarios reales de la comisión de un delito. En México, se siguen utilizando el arte forense y el catálogo de imágenes Caramex, que desde una perspectiva cognitiva siguen siendo métodos tradicionales que muy poco tienen que ver con los procesos de percepción facial humana. Es en este sentido que las nuevas metodologías de los sistemas de cuarta generación ofrecen una alternativa a los métodos tradicionales. Su principal ventaja radica en la utilización de rostros completos que permiten que la carga de trabajo recaiga sobre la memoria visual de una víctima o testigo, y no sobre su capacidad de descripción verbal susceptible de error, o de contaminar su memoria visual del rostro de un sospechoso.

La investigación que lleva a cabo el grupo del IIMAS presenta, en este mismo sentido, una ventaja extra. Para construir sus retratos hablados, la mayoría de los sistemas de cuarta generación utilizan como base de datos una serie de rostros relativamente pequeños, sin un criterio claro de inclusión. Por su parte, Caramex II cuenta con una sólida investigación estadística de los rasgos faciales más representativos de la población mexicana. La utilización de técnicas de inteligencia artificial, programación evolutiva, algoritmos genéticos, procesamiento de imágenes y el conocimiento sobre percepción facial humana, puede proporcionar un salto enorme en el desarrollo de nuevas estrategias de construcción de retratos hablados. Pero aún se requiere mayor investigación.

## X. FUENTES DE CONSULTA

Behrmann, M., Richler, J.J., Avidan, G., y Kimchi, R. (2015). "Holistic face perception". *Oxford handbook of perceptual organization*, 758-774.

Boutsen, L., y Humphreys, G.W. (2003). "The effect of inversion on the encoding of normal and 'Thatcherized' faces". *The Quarterly Journal of Experimental Psychology*, *56*(6), 955-975.

Brace, N.A., Pike, G.E., Allen, P., y Kemp, R.I. (2006). "Identifying composites of famous faces: Investigating memory, language, and system issues". *Psychology, Crime & Law*, *12*(4), 351-366.

Brace, N., Pike, G., y Kemp, R. (2000). "Investigating E-FIT using famous faces". *Forensic psychology and law*, 272-276.

Carbon, C.C., y Leder, H. (2005). "When feature information comes first! Early processing of inverted faces". *Perception*, *34*(9), 1117-1134.

Cootes, T.F., y Taylor, C.J. (2001, July). "Statistical models of appearance for medical image analysis and computer vision". *Medical Imaging 2001: Image Processing* (Vol. 4322, pp. 236-248). International Society for Optics and Photonics.

Cootes, T.F., Edwards, G.J., y Taylor, C.J. (1998, June). "Active appearance models". *European conference on computer vision* (pp. 484-498). Springer, Berlin, Heidelberg.

Craw, I., y Cameron, P. (1991). "Parameterising images for recognition and reconstruction". In *BMVC91* (pp. 367-370). Springer, London.

Craw, I., y Cameron, P. (1992). "Face recognition by computer". In *BMVC92* (pp. 498-507). Springer, London.

Davies, G. (1986). "Capturing likeness in eyewitness composites: The police artist and his rivals". *Medicine, Science, and the Law*, *26*(4), 283-290.

Davies, G., y Oldman, H. (1999). "The impact of character attribution on composite production: A real world effect?" *Current Psychology*, *18*(1), 128-139.

Davies, G., y Valentine, T. (2007). "Facial composites: Forensic utility and psychological research". *The Handbook of Eyewitness Psychology: Volume II* (pp. 73-98). Psychology Press.

Davies, G., Van der Willik, P., y Morrison, L.J. (2000). "Facial composite production: A comparison of mechanical and computer-driven systems". *Journal of Applied Psychology*, *85*(1), 119.

Dodson, C.S., Johnson, M.K., y Schooler, J.W. (1997). "The verbal overshadowing effect: Why descriptions impair face recognition". *Memory & Cognition*, *25*(2), 129-139.

Ellis, H.D. (1986). "Introduction to aspects of face processing: Ten questions in need of answers". *Aspects of face processing* (pp. 3-13). Springer, Dordrecht.

Ellis, H.D., Shepherd, J.W., y Davies, G.M. (1979). "Identification of familiar and unfamiliar faces from internal and external features: Some implications for theories of face recognition". *Perception*, *8*(4), 431-439.

Fallshore, M. y Schooler, J.W. (1995). "Verbal vulnerability of perceptual expertise". *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *21*(6), 1608.

Fisher, R.P., y Geiselman, R.E. (1992). *Memory enhancing techniques for investigative interviewing: The cognitive interview*. Charles C Thomas Publisher.

Fodarella, C., Kuivaniemi-Smith, H., Gawrylowicz, J., y Frowd, C. (2015). "Forensic procedures for facial-composite construction". *Journal of Forensic Practice*, *17*(4), 259-270.

Frowd C.D. (2001). "EvoFIT: a holistic, evolutionary facial imaging system". PhD thesis, University of Stirling.

Frowd, C.D., Valentine, T. y Davis, J. (2015a). "Facial composites and techniques to improve image recognizability". *Forensic facial identification: Theory and practice of identification from eyewitnesses, composites, and CCTV*, 43-70.

Frowd, C.D., Erickson, W.B., Lampinen, J.M., Skelton, F.C., McIntyre, A.H. y Hancock, P.J. (2015b). "A decade of evolving composites: regression and meta-analysis". *Journal of Forensic Practice*.

Frowd, C.D., Skelton, F., Hepton, G., Holden, L., Minahil, S., Pitchford, M. y Hancock, P.J. (2013). "Whole-face procedures for recovering facial images from memory". *Science & Justice*, *53*(2), 89-97.

Frowd, C.D., Carson, D., Ness, H., Richardson, J., Morrison, L., Mclanaghan, S. y Hancock, P. (2005b). "A forensically valid comparison of facial composite systems". *Psychology, Crime & Law*, *11*(1), 33-52

Frowd, C.D., Hancock, P.J. y Carson, D. (2004). "EvoFIT: A holistic, evolutionary facial imaging technique for creating composites". *ACM Transactions on applied perception (TAP)*, *1*(1), 19-39.

Frowd, C.D., Bruce, V., Ness, H., Bowie, L., Paterson, J., Thomson-Bogner, C. & Hancock, P.J. (2007a). "Parallel approaches to composite production: interfaces that behave contrary to expectation". *Ergonomics*, *50*(4), 562-585.

Frowd, C., Bruce, V., Ross, D., McIntyre, A., y Hancock, P.J. (2007b). "An application of caricature: how to improve the recognition of facial composites". *Visual Cognition*, *15*(8), 954-984.

Frowd, C., Park, J., McIntyre, A., Bruce, V., Pitchford, M., Fields, S. y Hancock, P.J. (2008, August). "Effecting an improvement to the fitness

function. How to evolve a more identifiable face". *2008 Bio-inspired, Learning and Intelligent Systems for Security* (pp. 3-10). IEEE.

Frowd, C.D., Pitchford, M., Bruce, V., Jackson, S., Hepton, G., Greenall, M. y Hancock, P.J. (2011b). "The psychology of face construction: giving evolution a helping hand". *Applied Cognitive Psychology*, *25*(2), 195-203.

Frowd, C., Nelson, L., Skelton, F., Noyce, R., Atkins, R., Heard, P. y Hancock, P.J. (2012a). "Interviewing techniques for Darwinian facial-composite systems". *Applied Cognitive Psychology*, *26*(4), 576-584.

Frowd, C.D., Pitchford, M., Skelton, F., Petkovic, A., Prosser, C. y Coates, B. (2012b, September). "Catching even more offenders with EvoFIT facial composites". *2012 Third International Conference on Emerging Security Technologies* (pp. 20-26). IEEE.

Frowd, C.D., Skelton, F., Atherton, C., Pitchford, M., Hepton, G., Holden, L. y Hancock, P.J. (2012d). "Recovering faces from memory: The distracting influence of external facial features". *Journal of Experimental Psychology: Applied*, *18*(2), 224.

Frowd, C.D., Jones, S., Fodarella, C., Skelton, F., Fields, S., Williams, A. y Date, L. (2014). "Configural and featural information in facial-composite images". *Science & Justice*, *54*(3), 215-227.

Frowd, C.D., Bruce, V., McIntyre, A.H., Ross, D., Fields, S., Plenderleith, Y. y Hancock, P.J. (2006). "Implementing holistic dimensions for a facial composite system". *Journal of Multimedia*, *1*(3), 42-51.

Gibson, S.J., Solomon, C.J., Maylin, M.I. y Clark, C. (2009). "New methodology in facial composite construction: From theory to practice". *International Journal of Electronic Security and Digital Forensics*, *2*(2), 156-168.

Hancock, P.J., Bruce, V. y Burton, A.M. (2000). "Recognition of unfamiliar faces". *Trends in cognitive sciences*, *4*(9), 330-337.

Hole, G.J. (1994). "Configurational factors in the perception of unfamiliar faces". *Perception*, *23*(1), 65-74.

Innocence Project (2016): *Reevaluating lineups: why witness make mistakes and how to reduce the chance of a misidentification.* Recuperado de: https://www.innocenceproject.org/reevaluating-lineups-why-witnesses-make-mistakes-and-how-to-reduce-the-chance-of-a-misidentification/

Kurt, B., Etaner-Uyar, A.S., Akbal, T., Demir, N., Kanlikilicer, A.E., Kus, M.C. y Ulu, F.H. (2006, September). "Active appearance model-based facial composite generation with interactive nature-inspired heuristics". *International Workshop on Multimedia Content Representation, Classification and Security* (pp. 183-190). Springer, Berlin, Heidelberg.

Laughery, K.R. y Fowler, R.H. (1980). "Sketch artist and Identi-kit procedures for recalling faces". *Journal of Applied Psychology*, *65*(3), 307.

Mohammadzade, H., Sayyafan, A. y Ghojogh, B. (2018). "Pixel-Level Alignment of Facial Images for High Accuracy Recognition Using Ensemble of Patches". *Journal of the Optical Society of America* A. 35. 10.1364/JOSAA.35.001149.

Rossion, B. (2008). "Picture-plane inversion leads to qualitative changes of face perception". *Acta psychologica*, *128*(2), 274-289.

Ryan, R.S., y Schooler, J.W. (1998). "Whom do words hurt? Individual differences in susceptibility to verbal overshadowing". *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *12*(7), S105-S125.

Schooler, J.W., y Engstler-Schooler, T.Y. (1990). "Verbal overshadowing of visual memories: Some things are better left unsaid". *Cognitive psychology*, *22*(1), 36-71.

Serrano, S.C. (2013). "Un sistema automatizado de identificación de rasgos faciales (retrato hablado) para la población mexicana". *La bibliotecología y la documentación en el contexto de la internacionalización y el acceso abierto*. (Coord.) Jaime Ríos Ortega y César Augusto Ramírez Velázquez. México, UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información.

Serrano, C., Villanueva, M., Luy, J. y Link, K.F. (1997). "El proyecto 'La cara del mexicano'. Un sistema de retrato hablado asistido por computadora para la población mexicana." *Boletín de Enlaces*: 26-28, Coordinación de Humanidades, UNAM, México.

Sirovich, L. y Kirby, M. (1987). "Low-dimensional procedure for the characterization of human faces". *Josa a*, *4*(3), 519-524.

Solomon, C.J., Gibson, S.J. y Pallares-Bejarano, A. (2005). "Eigenfit–the generation of photographic-quality facial composites". *The Journal of Forensic Science*.

Solomon, C.J., Gibson, S.J. y Mist, J.J. (2013). "Interactive evolutionary generation of facial composites for locating suspects in criminal investigations". *Applied Soft Computing*, *13*(7), 3298-3306.

Sporer, S.L. (2007). "Person descriptions as retrieval cues: Do they really help?" *Psychology, Crime & Law*, *13*(6), 591-609.

Tanaka, J.W. y Farah, M.J. (1993). "Parts and wholes in face recognition". *The Quarterly journal of experimental psychology*, *46*(2), 225-245.

Tanaka, J.W. y Simonyi, D. (2016). "The 'parts and wholes' of face recognition: A review of the literature". *Quarterly Journal of Experimental Psychology*, *69*(10), 1876-1889.

Taylor, K.T. (2000). *Forensic art and illustration*. CRC Press.

Thompson, P. (1980). "Margaret Thatcher: a new illusion". *Perception*.

Tredoux, C. (1999). "Statistical considerations when determining measures of lineup size and lineup bias". *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *13*(S1), S9-S26.

Tredoux, C., Nunez, D., Oxtoby, O. y Prag, B. (2006). "An evaluation of ID: an eigenface based construction system: reviewed article." *South African Computer Journal*, *2006*(37), 90-97.

Troje, N.F. y Vetter, T. (1996). *Representations of human faces*. Max-Planck-Institut Tubingen

Turk, M. y Pentland, A. (1991). "Eigenfaces for recognition". *Journal of cognitive neuroscience*, *3*(1), 71-86.

Valentine, T. (1988). "Upside-down faces: A review of the effect of inversion upon face recognition". *British journal of psychology*, *79*(4), 471-491.

Valentine, T. (1991). "A unified account of the effects of distinctiveness, inversion, and race in face recognition". *The Quarterly Journal of Experimental Psychology Section A*, *43*(2), 161-204.

Valentine, T. (Ed.). (2002). *Cognitive and computational aspects of face recognition: Explorations in face space*. Routledge.

Valentine, T., Davis, J.P., Thorner, K., Solomon, C. y Gibson, S. (2010). "Evolving and combining facial composites: Between-witness and within-witness morphs compared". *Journal of Experimental Psychology: Applied*, *16*(1), 72.

Villanueva, S.G. (2010). *Morfología facial. Estudios en población mexicana a través de fotografías digitales*. México, UNAM, Instituto de Investigaciones Antropológicas.

Wells, G.L., Charman, S.D., y Olson, E.A. (2005). "Building face composites can harm lineup identification performance". *Journal of experimental psychology: Applied*, *11*(3), 147.

Zahradnikova, B., Duchovicova, S. y Schreiber, P. (2018). "Facial composite systems". *Artificial Intelligence Review*, *49*(1), 131-152.

Žalik, Borut (2005). "An efficient sweep-line Delaunay triangulation algorithm". *Computer-Aided Design*, *37* (10), pp. 1027-1038.

# LA INTELIGENCIA ARTIFICIAL Y LA LEY ANTILAVADO EN MÉXICO

Fernando Lascurain Farell*

* Candidato a Doctor en Derecho por la Universidad Panamericana y profesor en esta última. Contacto: flascurain@up.edu.mx

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Lavado de dinero** | *Money laundering* |
| **Inteligencia artificial** | *Artificial intelligence* |
| **Sistema financiero** | *Finance system* |
| **Factura electrónica** | *Electronic bill* |
| **Inteligencia financiera** | *Financial intelligence* |



**Resumen.** Ante la problemática mundial del lavado de dinero, es fundamental reforzar las herramientas de prevención contra dicho delito; el uso de la inteligencia artificial podría ser la respuesta ante ese reto.

En relación con la venta de vehículos nuevos, debería incorporarse la obligación de recabar la información que origina el análisis de una forma segura y confiable.

En México se cuenta con la factura electrónica como fuente para que la autoridad inicie de forma precisa su labor, con la certeza de que la información contenida en ella es cierta.

La propuesta contenida en este artículo no requiere adecuación alguna a la ley de la materia, sino que solo implica modificar formas de operar que se reconocen en diversas materias, además de combatir la omisión del envío de información en tiempo y forma.

**Abstract.** Given the global problem of money laundering, it is essential to strengthen the prevention tools against this crime; the use of artificial intelligence could be the answer to this challenge.

Regarding the sale of new vehicles, the obligation to collect the information that originates the analysis in a safe and reliable way should be incorporated.

In Mexico, the electronic bill is used as a source for the authority to precisely do its work, with the certainty that the information contained in it is true.

The proposal contained in this article does not require any legal changes, but only implies modifying ways of operating that are recognized in various matters, in addition to prevent the omission of sending information in a timely manner.


Fecha de recepción: 6 de octubre de 2020
Fecha de aceptación: 23 de octubre de 2020

SUMARIO:







## I. INTRODUCCIÓN

Sundar Pichai, director ejecutivo de Google, afirmó que la revolución de la inteligencia artificial es "más profunda que la electricidad o el fuego" (Barrio, 2020). En una era que se ha visto impactada de forma brutal por un acontecimiento mundial vinculado a la salud (COVID-19), han quedado al descubierto dos grandes grupos de personas: 1) aquellos que han tenido la capacidad de adaptarse a la utilización exacerbada de las tecnologías de la información para desarrollar sus obligaciones y actividades personales; y 2) aquellos que siguen negándose, de forma sistemática, a habituarse a las demandas de los tiempos de la inmediatez y la conectividad.

Lo anterior obliga a mirar hacia el ámbito legal, en particular con relación a la prevención del delito y, más aún, de uno que se ha convertido en noticia común: el lavado de dinero, que se caracteriza por el alto grado de complejidad para su realización exitosa, y por lo difícil que resulta su prevención adecuada.

Uno de los mayores reclamos legítimos de la sociedad es que los resultados de la lucha contra este delito sean visibles. La comisión de este ilícito se ha incrementado de forma vertiginosa, al tiempo que se ha evidenciado lo complicado de su prevención. Es imperioso echar mano de herramientas que permitan tener información en tiempo real, sin margen de error y, sobre todo, que facilite el cruce de bases de datos igualmente confiables y precisas en sus resultados.

## II. INTELIGENCIA ARTIFICIAL

En 1956, John McCarthy acuñó el término "inteligencia artificial", a la cual definió como "la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes" (Barrio, 2020: 111). Santiago Gómez Sancha (*Idem*) la conceptúa así: "Las tecnologías que permiten

hacer a las máquinas labores que hasta hoy solo pueden realizar los seres humanos." Es a todas luces entendible que esta herramienta permite realizar operaciones de forma mucho más rápida, sobre todo si uno se basa en la minería de datos: "Es un proceso iterativo de búsqueda de información no trivial en grandes volúmenes de datos que busca generar información similar a la que podría generar un experto humano: asociaciones, cambios, anomalías y estructuras significativas." (Gallegos, 2019) Entonces, es evidente que no puede soslayarse la utilización de esta tecnología para prevenir ilícitos violentos, como ya se hace en otras latitudes de forma exitosa.

Por ejemplo, PredPol (*predictive policing*) [2018], desarrollado por la UCLA y la policía de Los Ángeles, se dedica a la vigilancia policial predictiva; consiste en identificar los horarios y lugares donde es más probable que ocurran delitos específicos, para acto seguido patrullar esas áreas y, en la medida de lo posible, evitar que esos delitos ocurran. La herramienta de operaciones diarias identifica dónde y cuándo es más probable que suceda un delito. Las predicciones se hacen con base solo en información sobre victimización; es decir, delitos que se han denunciado a la policía. Esta información es anónima; nunca se recopila ni utiliza información personal.

Por otra parte, la Solución Nacional de Análisis de Datos (NDAS) [Baraniuk, 2018] utiliza una combinación de inteligencia artificial y estadísticas para tratar de evaluar el riesgo de que alguien cometa o se convierta en víctima de un crimen con arma o cuchillo, así como la probabilidad de que alguien sea víctima de delitos como la trata de personas. NDAS se está diseñando para que todas las fuerzas policiales del Reino Unido puedan usarla eventualmente.

Asimismo, White Collar Crime Risk Zones[1] es una iniciativa vinculada a la utilización de tecnología para prevenir delitos patrimoniales no violentos, como el lavado de dinero. El Sistema de Alerta Temprana de Delitos de Cuello Blanco (WCCEWS, por sus siglas en inglés) es un modelo predictivo de delitos de cuello blanco que utiliza clasificadores aleatorios para identificar zonas de alto riesgo para incidentes de delitos financieros. El sistema es capaz de lograr una precisión predictiva considerable.

El modelo actual se basa en información georreferenciada. No se consideran otros factores que pueden proporcionar información adicional sobre la probabilidad de actividad delictiva financiera. Fundamentalmente, el modelo proporciona una estimación de los delitos de cuello blanco para una región particular. No llega al grado de identificar a los individuos que

[1] *White Collar Crime Risk Zones*. En: https://whitecollar.thenewinquiry.com/ Recuperado el 6 de octubre de 2020.

podrían cometer un delito financiero dentro de una región específica. Es decir, todas las entidades dentro de las zonas de alto riesgo son tratadas uniformemente como sospechosas.

Recientemente, algunos investigadores han demostrado la efectividad de aplicar técnicas de aprendizaje automático a los rasgos faciales para cuantificar la "criminalidad" de un individuo; por tanto, se planea aumentar el modelo con análisis facial y psicometría para identificar posibles delitos financieros a nivel individual. Como prueba, se descargaron las imágenes de 7,000 ejecutivos corporativos cuyos perfiles de LinkedIn sugieren que trabajan para organizaciones financieras, y luego se promediaron sus caras para producir sujetos criminales de cuello blanco generalizados para cada zona de alto riesgo. Es probable que, en el futuro, estos esfuerzos permitan predecir la criminalidad a través del análisis facial en tiempo real.

## III. LA INTELIGENCIA ARTIFICIAL EN MÉXICO

En 2017, el Servicio de Administración Tributaria (SAT) de México hizo público que utiliza la inteligencia artificial:

> El SAT utiliza técnicas de Machine Learning, un subconjunto de Inteligencia Artificial, que permite la recopilación de un gran volumen de datos de facturas electrónicas para formular expectativas y tendencias con respecto a los resultados de su análisis que permiten el reconocimiento de patrones y el aprendizaje automático al agrupar los datos de facturación electrónica en algoritmos formados matemáticamente, mismos que cuando se ejecutan, desarrollan una serie de reglas que se utilizan para analizar los datos en detalle.
>
> El SAT también trabaja en el ajuste de un modelo de algoritmos de inteligencia artificial en una plataforma tecnológica, a través de la integración de diversas fuentes de información, con el fin de detectar con un alto grado de certeza a las empresas que simulan operaciones o evaden sus obligaciones, para fortalecer los mecanismos que aseguren el cumplimiento de las obligaciones tributarias por parte de los contribuyentes (Redacción, 2017).

Lo anterior permite al SAT cuidar que los contribuyentes cumplan sus obligaciones fiscales, por medio de la utilización del Comprobante Fiscal Digital por Internet (CFDI), con fundamento en el artículo 29 del Código Fiscal de la Federación, como una potente herramienta capaz de identificar y georreferenciar un sinnúmero de información de personas físicas y morales, tocantes al tipo de productos y servicios que demandan —por ejemplo,

autos, camiones, boletos de avión, computadoras, inmuebles, estados de cuenta bancarios, servicios profesionales, etc.—, y con qué frecuencia.

El CFDI ha ido ganando terreno en la vida cotidiana, a grado tal que el Primer Tribunal Colegiado en Materias Penal y Administrativa del Vigésimo Primer Circuito se refirió a la eficacia probatoria de aquel en la tesis XXI.1o.P.A.11 K (10a.),[2] que establece:

> DOCUMENTO ELECTRÓNICO. SI CUENTA CON CADENA ORIGINAL, SELLO O FIRMA DIGITAL QUE GENERE CONVICCIÓN EN CUANTO A SU AUTENTICIDAD, SU EFICACIA PROBATORIA ES PLENA. De conformidad con el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, constituye un medio de prueba que debe valorarse conforme a las reglas específicas contenidas en el propio precepto y no con base en las reglas generales aplicables a las copias simples de documentos públicos o privados impresos. Así, para establecer la fuerza probatoria de aquella información, conocida como documento electrónico, debe atenderse a la fiabilidad del método en que se generó, comunicó, recibió o archivó y, en su caso, si es posible atribuir su contenido a las personas obligadas e, igualmente, si es accesible para su ulterior consulta. En congruencia con ello, si el documento electrónico, por ejemplo, una factura, cuenta con cadena original, sello o firma digital que genere convicción en cuanto a su autenticidad, su eficacia probatoria es plena y, por ende, queda a cargo de quien lo objete aportar las pruebas necesarias o agotar los medios pertinentes para desvirtuarla.

## IV. PREVENCIÓN DEL LAVADO DE DINERO

Por lo anterior, resulta difícil de entender por qué la autoridad, en este caso la Unidad de Inteligencia Financiera (UIF), se niega a utilizar la inteligencia artificial para el cumplimiento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (en lo sucesivo Ley Antilavado), publicada el 17 de octubre de 2012 en el *Diario Oficial de la Federación*, que marcó un cambio radical en la forma de operar de muchas empresas, sobre todo en las agencias distribuidoras de vehículos automotores nuevos, teniendo como base de información al CFDI.

Si bien es cierto que contar con este cuerpo normativo deriva de compromisos internacionales asumidos con anterioridad, es evidente, también, que se llega a este puerto de forma tardía y deficiente. Ha sido una

[2] *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 47, octubre de 2017, t. IV, p. 2434. Esta tesis se publicó el viernes 27 de octubre de 2017 a las 10:37 horas en el *Semanario Judicial de la Federación*. Registro digital: 2015428. (N. del E.)

exigencia del Grupo de Acción Financiera Internacional (GAFI) el que los países cuenten con legislación para prevenir el lavado de dinero (que en el sistema jurídico mexicano se denomina "operaciones con recursos de procedencia ilícita" en el artículo 400 bis del Código Penal Federal), no solo para el sector financiero (México ya contaba con una regulación robusta en este aspecto desde hace varios años), sino también para lo que se conoce como actividades y profesiones no financieras designadas; es decir, el sector comercial.

Y es en el marco del sector comercial en donde se ubica el nacimiento de la Ley Antilavado, que utiliza el término "actividades vulnerables", a diferencia de los "sujetos obligados" a que se refiere la regulación financiera, aun cuando el SAT se empeñe en llamarlos sujetos obligados.

## V. LA VENTA DE VEHÍCULOS NUEVOS

Dentro de las actividades vulnerables se encuentran más de 15, pero este texto remite únicamente a la fracción VIII del artículo 17 de la citada ley; es decir: "La comercialización o distribución habitual profesional de vehículos, nuevos o usados, ya sean aéreos, marítimos o terrestres con un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal." Según la Evaluación Nacional de Riesgos 2020, dada a conocer el 21 de septiembre de dicho año, dicha actividad ocupa el segundo lugar en lo que se refiere al riesgo alto.

Los distribuidores de vehículos automotores, al vender unidades nuevas, son los que actualizan la hipótesis prevista anteriormente, lo que los lleva a cumplir un número importante de obligaciones; pero las que mayor impacto generan son, sin duda, las de identificar al cliente para efectos de la Ley Antilavado y, en su caso, presentar el aviso correspondiente, siempre y cuando la operación haya sido por un importe superior a las 6,420 unidades de medida y actualización ($86.88 pesos para 2020) [INEGI].

No es nuevo el que deba identificarse al cliente para comprar un vehículo, lo cual se logra, por ejemplo, a través del Registro Público Vehicular, el Aviso de Privacidad, un Contrato de Adhesión, el Comprobante Fiscal Digital y diversas disposiciones del sistema financiero, en caso de que la unidad sea adquirida con un financiamiento; asimismo, para efectos del seguro, expedición de láminas, tarjeta de circulación y un engomado para poder circular. Sin embargo, a diferencia de la Ley Antilavado, se requiere

un proceso particular y muy detallado para integrar un expediente, así como la presentación de un aviso o, en su defecto, un informe (opera cuando no se realizó operación alguna por arriba del umbral durante ese mes, o por una acumulación respecto al mismo cliente, pero de igual forma hay que hacérselo saber al SAT, que, a su vez, se lo hace llegar a la UIF). Es decir, quien realice la actividad vulnerable debe hacer el proceso de envío de la información mediante el acceso a un portal especifico (SPPLD), y después capturar la información necesaria del tipo de vehículo, datos del comprador, forma de pago, etc., con el riesgo de que haya un error en la información allí requerida y su puntual envío). Pero no es un asunto menor que la hipótesis que actualiza el envío de la información se produce hasta que se liquide el precio de la unidad, tal como lo establece la UIF en un criterio (AMDA).

Al mes de agosto de 2020, el 62.8%[3] de las ventas de vehículos nuevos se produjo con un financiamiento (AMDA), lo cual significa que, por medio de instituciones del sistema financiero, se cumplió cabalmente con el proceso de identificación y conocimiento del cliente, por lo que resulta ocioso hacer de nueva cuenta, al amparo de la Ley Antilavado, el cumplimiento de la obligación de identificar y, en su caso, presentar el aviso, con el subsecuente riesgo que eso implica: en primer lugar, que la autoridad no reciba de forma oportuna (por ejemplo, si el vehículo no se ha liquidado aún) y precisa la información, y que la actividad vulnerable omita el cumplimiento de su obligación, lo que genera un doble efecto: carecer de la información en tiempo y forma para la autoridad, así como una contingencia económica para la agencia, y se deja de lado la oportunidad de usar el CFDI, que básicamente contiene casi toda la información que requiere la UIF y no depende de la liquidación de la unidad; en caso de necesitarse mayores datos, estos pueden implementarse mediante un complemento al CFDI.

Sin embargo, los datos verdaderamente reveladores de todo lo anterior pueden encontrarse en las siguientes cifras:

- El 20 de enero de 2020, el autor de estas líneas presentó, a través de la Plataforma Nacional de Transparencia, la solicitud número 0000600026320 a la Unidad de Inteligencia Financiera (UIF), en la cual se le pidió informar cuántos avisos de venta de vehículos nuevos había

[3] FINANCIAMIENTO AUTOMOTRIZ. (s. f.). AMDA. Recuperado el 6 de octubre de 2020, de: https://www.amda.mx/financiamiento-automotriz/

recibido desde la entrada en vigor de la ley y, en consecuencia, cuántas denuncias se habían presentado.

- El 17 de febrero de 2020, la UIF respondió que había recibido, de 2013 al 20 de enero de 2020, 8,863,630 avisos de vehículos aéreos, marítimos o terrestres, negándose a precisar cuántos de esos avisos eran de vehículos terrestres nuevos; tampoco respondió cuántas denuncias se habían presentado.

- El 20 de febrero de 2020 se interpuso un recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que se registró bajo el expediente RRA02383/20.

- El 27 de mayo de 2020, el INAI instruyó al sujeto obligado (UIF) para que diera la información.

- El 19 de junio de 2020, la UIF notificó, mediante oficio número D.E. UIF/110/202/2020, que en total se habían presentado las siguientes denuncias por año:

| AÑO | DENUNCIAS |
|---|---|
| 2013 | 0 |
| 2014 | 6 |
| 2015 | 5 |
| 2016 | 17 |
| 2017 | 10 |
| 2018 | 8 |
| 2019 | 48 |
| Junio 2020 | 28 |

Del cuadro anterior se desprende que, a junio de 2020, se presentó un total de 122 denuncias, derivadas de la información que recibe la UIF al amparo de la multicitada ley. Si se toma en consideración que ese total abarca unidades nuevas y usadas aéreas, marítimas y terrestres comercializadas en

ese periodo, es evidente que el número mayor lo abarcan las unidades terrestres nuevas, de acuerdo con los siguientes datos:

| Año | Ventas de vehículos nuevos |
|---|---|
| 2013 | 1,065,098 |
| 2014 | 1,136,965 |
| 2015 | 1,354,444 |
| 2016 | 1,607,165 |
| 2017 | 1,534,827 |
| 2018 | 1,426,926 |
| 2019 | 1,317,727 |
| Junio 2020 | 436,445 |

Es claro que el número de unidades nuevas vendidas (9,879,597) es mucho mayor que el número de avisos recibidos (8,863,630). Ahora bien, es preciso puntualizar lo siguiente: las unidades vendidas comprenden vehículos nuevos terrestres, sin incluir motocicletas ni triciclos motorizados; aunque pocas de estas unidades podrían ser objeto de aviso, es necesario precisar que hay un número no identificado de aviones, barcos, lanchas y demás vehículos en la misma situación.

Es innegable que la autoridad está recibiendo mucha —por no decir demasiada— información que le genera poca utilidad; si se compara el número de avisos con las denuncias presentadas, resulta que el 0.001% de los avisos termina en un proceso de denuncia, y aún falta por analizar cuántas de esas denuncias culminan en una sentencia condenatoria.

Para el distribuidor de autos, cumplir con la Ley Antilavado ha representado gastos muy altos, que van desde la implementación de procesos, sistemas, capacitación y, en muchos casos, la imposición de multas altísimas (por ejemplo, la omisión de presentar un aviso es de $868,800.00 pesos) que deben atenderse, previa contratación de abogados. Y todo esto ¿para qué? Como se pudo apreciar, la autoridad recibe demasiada información que no le representa valor agregado alguno, y lo único que genera es gran

[4] VENTAS DE VEHÍCULOS LIGEROS. (s. f.). AMDA. Recuperado el 6 de octubre de 2020 de: https://www.amda.mx/ventas-de-vehiculos-ligeros/

carga operativa y una mayor posibilidad de contingencias no menores para el distribuidor.

Lo que la autoridad debería hacer es recabar la información que necesita, mediante medidas precisas y objetivas, de otras autoridades que ya cuentan con ella en mecanismos mucho más ágiles, como la extracción directa del documento de la operación (el CFDI), y cruzarla, en su caso, con lo que el sistema financiero reciba, e inclusive también con el Registro Público Vehicular, para estar en posibilidad de realizar sus análisis correspondientes, pero sin imponerle al distribuidor trabajo y responsabilidad.

Esto ya está previsto en el artículo 19 de la Ley Antilavado, que la UIF se ha negado a implementar:

> ...el Reglamento deberá considerar como medio de cumplimiento alternativo de las obligaciones señaladas en los artículos anteriores, el cumplimiento, en tiempo y forma, que los particulares realicen de otras obligaciones a su cargo, establecidas en leyes especiales, que impliquen proporcionar la misma información materia de los Avisos establecidos por esta Ley; para ello la Secretaría tomará en consideración la información proporcionada en formatos, registros, sistemas y cualquier otro medio al que tenga acceso.

## VI. REFLEXIONES FINALES

La puesta en marcha del cumplimiento alternativo previsto en la Ley Antilavado permitiría la utilización del CFDI con la correspondiente implementación de la inteligencia artificial, que tendría el efecto de beneficiar a la autoridad, la cual recibiría de forma automática la información sin desfase ni errores, y los distribuidores disminuirían ostensiblemente la carga operativa y el riesgo de incumplimiento ante la realidad de ser sancionados con multas que, en muchos casos, acaban siendo ruinosas, y que pareciera denotar un espíritu recaudatorio de la legislación, en lugar de evitar la comisión de ilícitos.

## VII. FUENTES DE CONSULTA

AMDA. "Prevención lavado de dinero". Disponible en: https://www.amda.mx/prevencion-lavado-de-dinero-criterios/, consultado el 6 de octubre de 2020.

AMDA. "Financiamiento automotriz". Disponible en: https://www.amda.mx/financiamiento-automotriz/, consultado el 6 de octubre de 2020.

Baraniuk, C. (26 de noviembre de 2018). "Exclusive: UK Police Wants AI to Stop Violent Crime Before It Happens". En *New Scientist*. Disponible en: https://www.newscientist.com/article/2186512-exclusive-uk-police-wants-ai-to-stop-violent-crime-before-it-happens/, consultado el 6 de octubre de 2020.

Barrio, A.M. (2020). *Legal Tech. La transformación digital de la abogacía*. España: Wolters Kluwer.

Campuzano Gallegos, A. (2019). *Inteligencia artificial para abogados Ya es tiempo…* México: Thomson Reuters.

Cámara de Diputados. Código Fiscal de la Federación (1981). *Diario Oficial de la Federación.*

INEGI. "UMA". Disponible en: https://www.inegi.org.mx/temas/uma/

Redacción Innova MX (19 de octubre de 2017). "Inteligencia artificial". En Innova mx. Disponible en: https://www.gob.mx/innovamx/articulos/inteligencia-artificial-131287, consultado el 6 de octubre de 2020.

*PredPol*. "Overview". Disponible en: https://www.predpol.com/about/, consultado el 6 de octubre de 2020.

Secretaría de Hacienda. *Portal de Prevención de Lavado de Dinero*. (s. f.). Portal antilavado. Disponible en: https://sppld.sat.gob.mx/pld/interiores/sppld.html, consultado el 6 de octubre de 2020.

*White Collar Crime Risk Zones*. (s.f.). *The New Inquiry*. Disponible en: https://whitecollar.thenewinquiry.com/, consultado el 6 de octubre de 2020.