

# El Mundo de la Criminalística

Vol. 1 Núm.1 (2026)



## CIBERCRIMINALIDAD

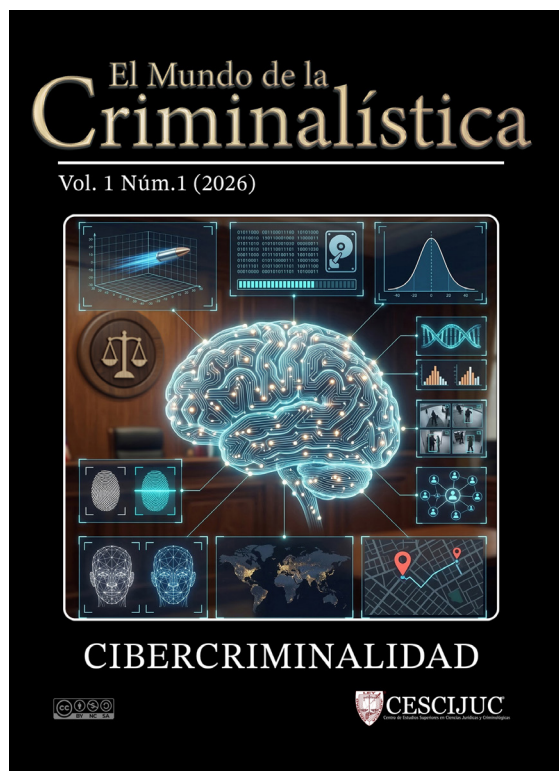




# CESCIJUC<sup>®</sup>

Centro de Estudios Superiores en  
Ciencias Jurídicas y Criminológicas





**El Mundo de la Criminalística**, vol. 1, núm. 1, julio-diciembre de 2026, es una publicación semestral editada por el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas (CECACIJUC), A.C., Balderas 138, Col. Centro, Delegación Cuauhtémoc, CP. 06070, Ciudad de México, Tel. 55 55059348.

Página electrónica de la revista:  
<https://revista.cescijuc.edu.mx/files>

Correo electrónico:

[investigacion.nacional@cescijuc.edu.mx](mailto:investigacion.nacional@cescijuc.edu.mx)

Editor responsable: Néstor Daniel Martínez Domínguez, Certificado de Reserva de Derechos al Uso Exclusivo No. 04-2025-061712385200-102, ISSN: en trámite, —ambos otorgados por el Instituto Nacional de Derechos de Autor.

Responsable de la última actualización de este Número, Néstor Daniel Martínez Domínguez, Balderas 138, Col. Centro, Delegación Cuauhtémoc, CP. 06070, Ciudad de México, fecha de última modificación, 15 de julio de 2026. Tamaño del archivo: 35646 KB

El contenido de los artículos publicados es responsabilidad de las personas autoras y no refleja la postura del Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas.

## Director

Dr. Francisco Javier García Ramírez

## Comité Editorial

Dr. Teófilo Benítez Granados

Dra. Margarita Montaña Soriano

Dr. Roberto Izquierdo Plata

Dra. Blanca Briseño Patlanis

Mtra. Cynthia Cruz Herrera

Mtro. Gabriel Mauricio Flores

## Editor

Dr. Néstor Daniel Martínez Domínguez

## Diseño y Formación

Lic. Isaac Tapia López

## Ilustración

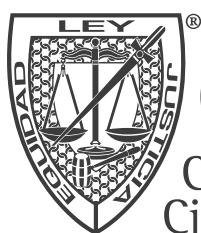
Lic. Isaac Tapia López

Imágenes generadas a través de Nano

Banana 2, GPT Image 2 y edición digital.

**Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas**  
Balderas 138, Col. Centro, Delegación Cuauhtémoc, CP. 06070, Ciudad de México.





**CESCIJUC**<sup>®</sup>  
Centro de Estudios Superiores en  
Ciencias Jurídicas y Criminológicas

## **Directorio Institucional**

*Dr. Teófilo Benítez Granados*  
Rector

*Dr. Teófilo Benítez Estrada*  
Director Académico

*Dr. Francisco Javier García Ramírez*  
Director del Instituto de  
Investigación del Cescijuc

*Dra. Joanna Cristal Gómez Olivera*  
Dirección Administrativa

*Lic. José Gabriel Aranda Mondragón*  
Contralor

*Lic. Teófilo Benítez Arrona*  
Presidente de la Fundación Cescijuc

*Sra. María Elena Granados Enciso*  
Vicepresidenta de la Fundación Cescijuc



# CESCIJUC®

Centro de Estudios Superiores en  
Ciencias Jurídicas y Criminológicas

## Plantel Balderas

Calle Balderas, núm. 138, casi esq.  
Chapultepec, Col. Centro, Deleg.  
Cuauhtémoc, CDMX, C.P. 06070.

## Plantel Niños Héroes 188

Av. Niños Héroes, núm. 188, Col.  
Doctores, Deleg. Cuauhtémoc,  
CDMX, C.P. 06720

## Plantel Chapultepec 27

Av. Chapultepec 27, Colonia Centro,  
Centro, Cuauhtémoc, CDMX.  
C.P. 06000

## Plantel Chapultepec 29

Av. Chapultepec, núm. 29, Col.  
Centro, Cuauhtémoc, CDMX,  
C.P. 06010.

## Plantel Niños Héroes 222

Av. Niños Héroes 222, Col. Doctores,  
Cuauhtémoc, CDMX,  
C.P. 06720

## Plantel Dr. Erazo

C. Dr. Erazo 122, Doctores,  
Cuauhtémoc, CDMX,  
C.P. 06720

## Plantel Dr. Lucio

Doctor Rafal Lucio 9, Despachos  
301-302, Doctores, Cuauhtémoc,  
CDMX, C.P. 06720

## Plantel Ecatepec

Av. Insurgentes 9, San Cristóbal  
Centro, Ecatepec de Morelos, Méx. C.  
P. 55000

## Plantel Tlalnepantla

C. Dr. Av. Dr. Gustavo Baz 220,  
Lomas, Tlalnemex, Tlalnepantla,  
Méx. C.P. 54070

## Plantel Nezahualcóyotl

Calle Monumento a La Revolución  
187, Metropolitana 2da Secc, Cdad.  
Nezahualcóyotl, Méx. C.P. 57740

## Plantel Toluca

Av. Baja Velocidad 519, Pílares,  
San Jerónimo Chicahualco, Méx.  
C.P. 52175

## Plantel Guadalajara

C. Jesús 12, Centro, Guadalajara,  
Jalisco, C. P. 44200

## Plantel Monterrey

Ruperto Martínez 926, Centro,  
Monterrey, N.L., C.P. 64000

## Plantel Sonora

Calle Gral. José María Yáñez 136,  
Centro, Hermosillo, Sonora,  
C.P. 83000

## Plantel Puebla

Av. 5 Pte. 1710, Barrio de San  
Sebastián, Heroica Puebla de  
Zaragoza, Puebla, C.P. 72090

## Plantel Morelia

C. La Corregidora 680, Centro  
histórico de Morelia, Morelia,  
Michoacán, C.P. 58000

## Plantel Chihuahua

C. Juan Aldama 3900-3908,  
Obrera, Chihuahua, Chihuahua,  
C.P. 31350

## CESCIJUC Virtual

55 5505 9498/ 55 5505 9348  
contacto@cescijuc.com.mx

[www.cescijuc.edu.mx](http://www.cescijuc.edu.mx)





**El Mundo de la Criminalística** es una publicación de Acceso Abierto bajo la licencia Licencia Creative Commons Atribución/ Reconocimiento-NoComercial 4.0 Internacional (CC BY-NC 4.0)





# Contenido

- | 12 **Presentación**  
*Teófilo Benítez Granados*
- | 14 **Editorial**  
*Francisco Javier García Ramírez*
- | 16 **¿Puede un algoritmo ser perito?**  
**Inteligencia artificial y los nuevos retos de la prueba pericial en México**  
*Jesús Ángel Arreola Gayosso*
- | 26 **El perito en el proceso penal:**  
**La importancia del conocimiento especializado en la justicia penal**  
*Juan Manuel Herrera Moreno*
- | 40 **Cuando la tecnología aprende de nosotros... y nos vigila**  
*Oswaldo Aguilar Rivera*

- | 56    Entre fraudes, datos, pantallas e internet:  
Un acercamiento a la cibercriminalidad en México**  
*José María Salazar García*
- | 72    ¿Quién tiene tus datos? La vulneración de datos  
personales en Guatemala**  
*Yarely Elizabeth Gómez Gómez*
- | 84    Cuando el delito transita de escenarios análogos al  
espacio digital**  
Una conversación con el Dr. Francisco Rodríguez  
Almirón  
*Cynthia Cruz Herrera*
- | 92    ¿Qué ocurre cuando un ciberataque afecta la vida  
cotidiana?**  
Entrevista con el Dr. Miguel Olmedo Cardenete  
*Néstor Daniel Martínez Domínguez*



# | Presentación

La educación superior enfrenta el desafío permanente de generar conocimiento pertinente y de contribuir a que este participe activamente en la comprensión y atención de los problemas que experimenta la sociedad. La investigación constituye una de las funciones esenciales de las instituciones universitarias; sin embargo, su alcance se fortalece cuando sus resultados trascienden los espacios académicos y se incorporan al diálogo con los distintos sectores sociales y profesionales.

Con esta convicción, el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas (CESCIJUC) presenta *El Mundo de la Criminalística*, una revista de divulgación concebida como un espacio para compartir conocimientos, experiencias y reflexiones sobre la criminalística, la criminología, el derecho, las ciencias forenses y otras disciplinas afines que contribuyen al estudio del fenómeno delictivo y de la procuración de justicia.

Este proyecto editorial forma parte del compromiso institucional del CESCIJUC con la investigación, la formación de profesionales y la difusión del conocimiento. La generación de evidencia científica representa un componente indispensable para fortalecer la enseñanza, enriquecer la práctica profesional y favorecer la construcción de respuestas frente a los desafíos que plantean las transformaciones sociales y tecnológicas de nuestro tiempo.

Las páginas de esta revista buscan reunir aportaciones provenientes de distintas perspectivas disciplinarias, convencidos de que la complejidad de los fenómenos contemporáneos requiere enfoques cada vez más integrales. La criminalística dialoga hoy con disciplinas como el derecho, la informática, la medicina, la psicología, la ingeniería, la biología y las ciencias sociales, entre muchas otras, configurando un campo de conocimiento dinámico y en constante evolución.

La primera edición se dedica a la cibercriminalidad, uno de los fenómenos que mejor refleja la velocidad con la que evolucionan las formas de delinquir y los retos que enfrentan las instituciones responsables de investigar estos hechos. Comprender estos procesos exige fortalecer la investigación científica, promover la actualización permanente de quienes participan en el sistema de justicia y consolidar espacios que favorezcan la difusión responsable del conocimiento.

Con *El Mundo de la Criminalística*, nuestra institución reafirma su compromiso con un proyecto educativo que articula docencia, investigación y vinculación con la sociedad. Aspiramos a que esta revista se consolide como un referente de divulgación en el ámbito de las ciencias jurídicas y criminológicas, así como un punto de encuentro para estudiantes, docentes, investigadores y profesionales interesados en comprender los problemas contemporáneos desde una perspectiva científica, crítica e interdisciplinaria.

Agradezco a quienes hicieron posible este proyecto editorial y extendiendo una cordial invitación a nuestras y nuestros lectores para que encuentren en estas páginas un espacio de reflexión que contribuya a fortalecer el conocimiento, el pensamiento crítico y el compromiso con la justicia.



### **Dr. Teófilo Benítez Granados**

Rector del Centro de Estudios Superiores en  
Ciencias Jurídicas y Criminológicas (CESCIJUC)



## | Editorial

Las sociedades contemporáneas enfrentan formas de criminalidad cuya evolución ocurre al mismo ritmo que los cambios tecnológicos, económicos y culturales. La digitalización de la vida cotidiana, el desarrollo de nuevas herramientas tecnológicas y la creciente complejidad de las relaciones sociales han modificado tanto las modalidades delictivas como los procedimientos destinados a su investigación. En este contexto, la criminalística y las ciencias forenses ocupan un lugar estratégico para comprender estos fenómenos y aportar conocimientos que fortalezcan la procuración y administración de justicia.

Desde esta perspectiva surge *El Mundo de la Criminalística*, una revista de divulgación impulsada por el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas (CESCIJUC). Este proyecto editorial nace con el propósito de contribuir a la circulación social del conocimiento generado en la investigación sobre criminalística, criminología, derecho y ciencias forenses, favoreciendo el intercambio de ideas entre la comunidad académica, las personas dedicadas al ejercicio profesional y todos aquellos interesados en comprender los desafíos contemporáneos de la investigación criminal.

La investigación constituye una de las funciones sustantivas de las instituciones de educación superior. Sin embargo, su impacto no depende únicamente de la producción de nuevos conocimientos, sino también de su capacidad para incorporarse a la discusión pública y enriquecer la comprensión de problemas que afectan a la sociedad. La divulgación científica representa, en este sentido, un espacio de encuentro entre la generación de conocimiento y su apropiación social, permitiendo que los resultados de la investigación dialoguen con los distintos sectores involucrados en la prevención del delito, la investigación criminal y la construcción de una cultura de legalidad.

El número inaugural de la revista está dedicado a la cibercriminalidad, un fenómeno que evidencia cómo las transformaciones tecnológicas modifican de manera constante los escenarios en los que se desarrollan las conductas delictivas. Con esta primera edición inicia un proyecto que aspira a consolidarse como un espacio permanente para la difusión del conocimiento en materia de criminalística y ciencias forenses. Cada número buscará acercar investigaciones, experiencias y reflexiones sobre los problemas que enfrentan la seguridad, la justicia y la investigación criminal, promoviendo el diálogo entre distintas disciplinas y contribuyendo a fortalecer la relación entre la producción científica y las necesidades de la sociedad.

El Centro de Investigación del CESCIJUC refrenda así su compromiso con la generación, difusión y aprovechamiento social del conocimiento, convencido de que la investigación científica adquiere mayor relevancia cuando trasciende los espacios académicos y participa activamente en la comprensión de los desafíos que caracterizan a nuestro tiempo.



### **Francisco Javier García Ramírez**

Director del Instituto de Investigación del  
Centro de Estudios Superiores en Ciencias  
Jurídicas y Criminológicas (CESCIJUC)



# ¿Puede un algoritmo ser perito?

Inteligencia artificial y los nuevos retos de la prueba pericial en México

Jesús Ángel Arreola Gayosso

Durante las últimas décadas, la investigación criminal ha experimentado transformaciones profundas derivadas del avance tecnológico. La digitalización de la información, el uso de bases de datos biométricos, la mejora en los sistemas de análisis de imágenes y el desarrollo de herramientas computacionales han modificado la forma en que se investigan los delitos. En este contexto, la inteligencia artificial (IA) comienza a ocupar un lugar cada vez más visible dentro de las ciencias forenses. Hoy es posible encontrar sistemas que ayudan a comparar dactilogramas, identificar rostros en grabaciones de cámaras de vigilancia, analizar grandes volúmenes de información criminal o incluso reconstruir escenarios mediante simulaciones digitales. Estas herramientas prometen aumentar la rapidez y precisión de los análisis periciales. Sin embargo, su incorporación también plantea preguntas relevantes para el ámbito jurídico, como por ejemplo:

¿Hasta qué punto puede confiarse en las decisiones de un algoritmo?, ¿puede un sistema de inteligencia artificial sustituir el juicio de un perito?, ¿cómo se presenta una prueba generada por un sistema automatizado ante un tribunal?

Estas interrogantes adquieren especial relevancia en el contexto mexicano, donde el sistema de justicia penal ha experimentado importantes reformas en las últimas décadas, particularmente con la implementación del sistema acusatorio. En este modelo, la prueba pericial juega un papel fundamental para esclarecer hechos y sustentar decisiones judiciales. Por ello, la integración de herramientas basadas en inteligencia artificial en los procesos periciales exige una reflexión cuidadosa sobre sus implicaciones técnicas, jurídicas y éticas.

Este artículo aborda, los principales desafíos que plantea la inteligencia artificial en la producción y valoración de la prueba pericial en México.





## ANÁLISIS

01770

|      |     |       |                  |
|------|-----|-------|------------------|
| 0269 | 068 | 00508 | 9101100HC0101000 |
| 0201 | 800 | 93001 | 0001100000000000 |
| 0100 | 800 | 45000 | 0000000000000000 |
| 0269 | 001 | 88000 | 0001110000000000 |
| 0100 | 800 | 00000 | 0001110000000000 |
| 0000 | 001 | 90000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |
| 0000 | 001 | 00000 | 0001110000000000 |

## ANÁLISIS DE DATOS DIGITALES

## COINCIDENCIA BIOMÉTRICA



## ANÁLISIS ALGORÍTMICO

|        |        |        |
|--------|--------|--------|
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |
| 000000 | 000000 | 000000 |

## DIGITAL FORENSIC



21  
281  
T0001.0  
T001T11 00  
OTP CIT1  
TO 1 T12121  
P T80881  
1 17e3126831072  
EVIDENCE\_ID:  
DNA\_SEQ: 300020  
CASE\_LOG:  
TIMESTAMP: 182500





## La prueba pericial en el sistema de justicia mexicano

En los procesos judiciales, la prueba pericial tiene como objetivo aportar conocimientos técnicos o científicos que permitan aclarar aspectos del caso que escapen al conocimiento común del juez o de las partes. El perito actúa como un especialista que interpreta indicios, aplica metodologías científicas y presenta sus conclusiones de manera comprensible ante el tribunal.

En México, los dictámenes periciales pueden abarcar diversas especialidades: balística, genética, medicina legal, grafoscopia, informática, análisis de documentos, entre muchas otras. Cada una de estas disciplinas se basa en procedimientos técnicos específicos y requiere profesionales capacitados para interpretar correctamente los resultados.



En el actual sistema acusatorio, el perito puede ser interrogado y contrainterrogado por las partes, lo que permite evaluar la solidez de su dictamen. La introducción de sistemas de inteligencia artificial en estas áreas plantea una cuestión central: si parte del análisis es realizado por un algoritmo:



¿quién es realmente el autor del dictamen pericial? ¿El perito que opera la herramienta o el sistema que produce el resultado?

## Inteligencia artificial (IA) en las ciencias forenses

La inteligencia artificial puede definirse, de manera general, como el conjunto de técnicas computacionales que permiten a las máquinas realizar tareas que normalmente requieren inteligencia humana, como reconocer patrones, clasificar información o aprender a partir de datos.

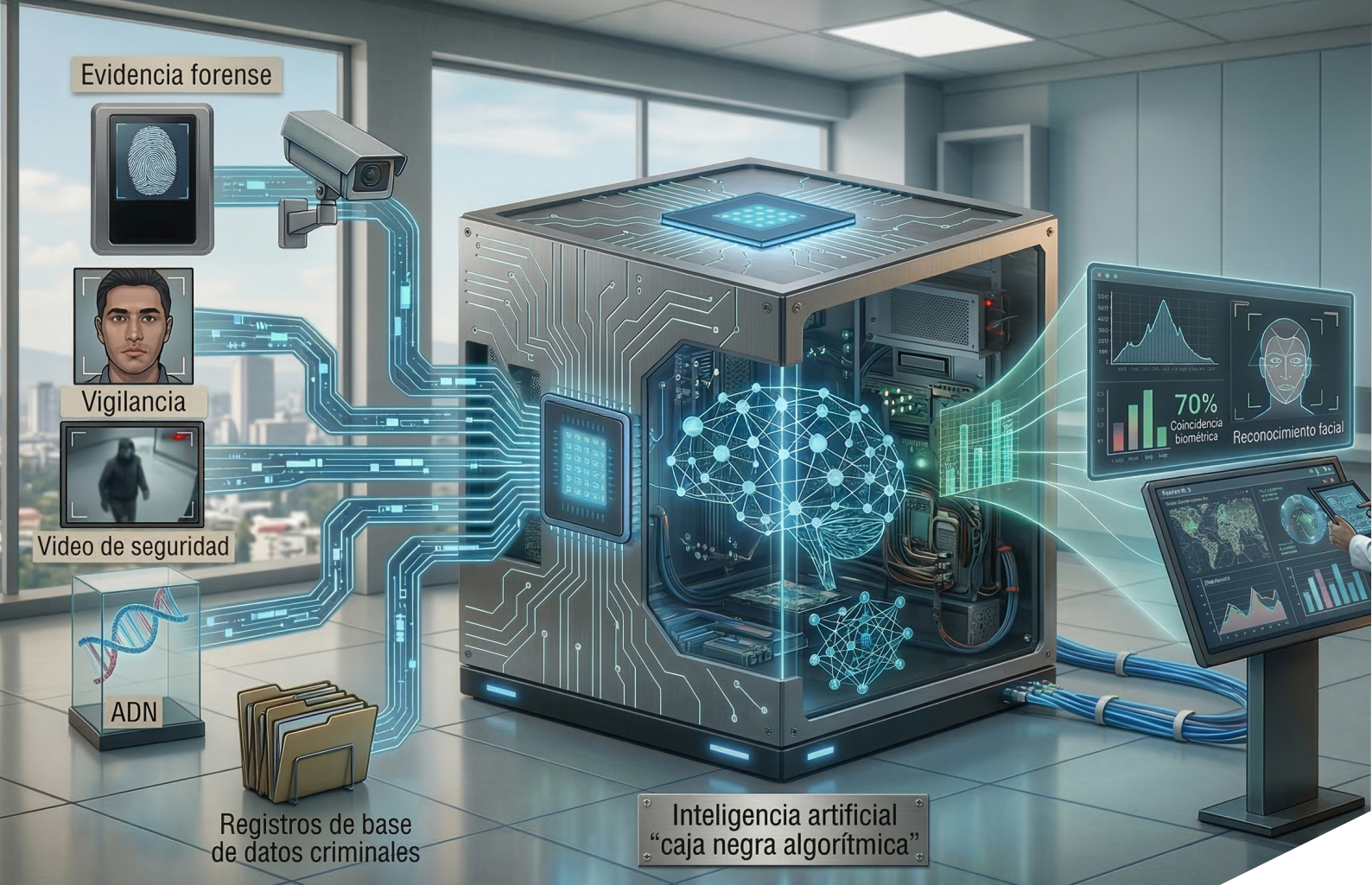
En el ámbito forense, la IA ya se utiliza en diversas aplicaciones:

- Reconocimiento facial: algoritmos capaces de comparar imágenes de rostros con bases de datos para identificar posibles coincidencias.
- Análisis de dactilogramas: sistemas automatizados que comparan miles o millones de registros en cuestión de segundos.
- Procesamiento de imágenes y video: herramientas que permiten mejorar la calidad de grabaciones, detectar objetos o rastrear movimientos.
- Análisis de grandes bases de datos criminales: algoritmos que identifican patrones o conexiones entre eventos delictivos.
- Simulaciones y reconstrucciones digitales: modelos computacionales que ayudan a recrear dinámicas de accidentes o trayectorias balísticas.



Estas aplicaciones no necesariamente sustituyen al perito, pero sí modifican su función. En muchos casos, el especialista pasa de realizar directamente el análisis a interpretar los resultados generados por sistemas automatizados.





## El problema de la “caja negra”

Uno de los principales desafíos asociados con la inteligencia artificial es lo que algunos especialistas denominan el problema de la “caja negra”. Muchos algoritmos, especialmente aquellos basados en aprendizaje automático, generan resultados a partir de procesos internos que no siempre son fácilmente comprensibles para los usuarios. En otras palabras, el sistema puede ofrecer una respuesta —por ejemplo, una coincidencia entre dos dactilogramas o una probabilidad de identificación facial— sin que el usuario tenga plena claridad sobre cómo llegó a esa conclusión.

Desde el punto de vista científico y jurídico, esto plantea varias dificultades. En el ámbito pericial, es fundamental poder explicar qué metodología se utilizó, qué datos se analizaron y cómo se llegó a la conclusión final. Si el funcionamiento del algoritmo es opaco, la capacidad de justificar el dictamen estará limitado. En el contexto de un juicio, donde la publicidad y la posibilidad de refutar la prueba son principios fundamentales (Art 20 CPEUM)<sup>1</sup>, la opacidad algorítmica puede convertirse en un problema significativo.

<sup>1</sup>El Artículo 20 de la Constitución Política de los Estados Unidos Mexicanos establece el marco del sistema penal acusatorio y oral. Se divide en tres apartados que garantizan un proceso penal rápido, transparente y justo, protegiendo los derechos tanto de la víctima como del imputado, basado en principios de contradicción e inmediación.

## ¿Puede un algoritmo ser considerado perito?

Desde una perspectiva estrictamente jurídica, la figura del perito está asociada a una persona con conocimientos especializados que interviene en el proceso judicial. En este sentido, un algoritmo no puede ser considerado perito en sí mismo.

Sin embargo, la cuestión no es tan simple. Si un sistema automatizado realiza una parte sustancial del análisis técnico, su influencia en el resultado del dictamen puede ser considerable.

El perito podría convertirse en un intermediario entre el algoritmo y el tribunal.

Esto genera unos debates relevantes como:

- ¿Debe el perito comprender plenamente el funcionamiento del sistema que utiliza?
- ¿Es suficiente confiar en herramientas desarrolladas por empresas o instituciones especializadas?

En muchos campos científicos, el uso de instrumentos complejos es común. Un médico puede utilizar un equipo de resonancia magnética sin conocer todos los detalles de su ingeniería. Sin embargo, en el ámbito judicial la exigencia de explicabilidad suele ser mayor, ya que las conclusiones pueden influir directamente en decisiones que afectan derechos fundamentales.

## Sesgos algorítmicos y riesgos de error

Otro tema central en el debate sobre inteligencia artificial es el de los sesgos algorítmicos. Los sistemas de aprendizaje automático dependen de los datos con los que fueron entrenados. Si esos datos contienen sesgos o limitaciones, el algoritmo puede reproducirlos o amplificarlos. En el caso del reconocimiento facial, por ejemplo, diversos estudios internacionales han mostrado que algunos sistemas presentan mayores tasas de error al analizar rostros de ciertos grupos poblacionales. Esto puede generar identificaciones incorrectas o resultados poco confiables.

En el contexto de la investigación criminal, un error de este tipo puede tener consecuencias graves. La identificación equivocada de una persona puede influir en decisiones de investigación, detenciones o incluso procesos judiciales. Por ello, diversos especialistas insisten en que los sistemas de inteligencia artificial utilizados en ámbitos forenses deben someterse a evaluaciones rigurosas de precisión, confiabilidad y posibles sesgos.







## El marco jurídico mexicano frente a la evidencia tecnológica

El sistema de justicia mexicano reconoce diversas formas de prueba científica y tecnológica. Sin embargo, la regulación específica sobre inteligencia artificial aún es incipiente.

Las normas procesales establecen criterios generales sobre la valoración de la prueba pericial, pero no siempre contemplan las particularidades de los sistemas algorítmicos. Esto plantea la necesidad de desarrollar lineamientos que permitan garantizar:

- Transparencia en el uso de tecnologías,
- Posibilidad de revisión por parte de las partes,
- Documentación de los métodos utilizados,
- Control sobre la calidad de los sistemas empleados.

Algunos especialistas sugieren que los tribunales deberán familiarizarse cada vez más con conceptos relacionados con algoritmos, bases de datos y análisis automatizado. En este sentido, la formación interdisciplinaria de jueces, fiscales, defensores y peritos podría convertirse en un elemento clave para el futuro del sistema de justicia.

## El papel del perito en la era de la inteligencia artificial

Lejos de desaparecer, el papel del perito podría volverse aún más importante en un contexto donde las herramientas tecnológicas son cada vez más complejas. El especialista no solo deberá interpretar evidencias, sino también evaluar la confiabilidad de los sistemas que utiliza. Esto implica comprender aspectos como:

- Calidad de los datos analizados.
- Límites del algoritmo utilizado.
- Margen de error del sistema.
- Condiciones en las que se generó el resultado.



El perito se convierte así en un mediador entre la tecnología y el proceso judicial, capaz de traducir resultados técnicos en explicaciones comprensibles para el tribunal.

Además, la presencia del experto humano sigue siendo fundamental para contextualizar los indicios de evidencia. Un algoritmo puede detectar patrones, pero no necesariamente interpretar el significado jurídico o investigativo de esos resultados.



## Como primeras conclusiones

La incorporación de la inteligencia artificial en las ciencias forenses representa uno de los cambios más significativos en la investigación criminal contemporánea. Sus aplicaciones prometen mejorar la eficiencia de los análisis y ampliar las capacidades de los laboratorios y equipos periciales.

No obstante, estos avances también plantean desafíos importantes para el sistema de justicia. La opacidad de algunos algoritmos, la posibilidad de sesgos en los datos y la dificultad para explicar ciertos procesos automatizados obligan a reflexionar sobre la forma en que se producen y valoran las pruebas periciales.

En el contexto mexicano, donde la prueba científica tiene un papel cada vez más relevante dentro del sistema penal acusatorio, resulta fundamental desarrollar marcos normativos, metodológicos y éticos que orienten el uso de estas tecnologías.

La pregunta que da título a este artículo —si un algoritmo puede ser perito— probablemente tenga una respuesta clara desde el punto de vista jurídico: no. Sin embargo, la influencia de los sistemas automatizados en el análisis de evidencias seguirá creciendo en los próximos años.

Por ello, el verdadero desafío no consiste en decidir si la inteligencia artificial debe utilizarse en las ciencias forenses, sino en cómo integrarla de manera responsable, transparente y crítica dentro de los procesos de investigación y justicia.

## Referencias bibliográficas

- García-Bernalt, I. Y. (2024). La inteligencia artificial en el proceso penal: Eficiencia versus garantías. *IUS ET SCIENTIA*, 10(2), 80-100.  
<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.04>
- Granja Pérez, H. O. (2023). Utilización de la inteligencia artificial de sistema experto en la investigación del delito. *Revista Mexicana De Ciencias Penales*, 7(21), 3-20.  
<https://doi.org/10.57042/rmcp.v7i21.674>
- Gutiérrez, J. D. (2024). Documento de consulta pública: Directrices de la UNESCO para el uso de sistemas de inteligencia artificial en juzgados y tribunales (p. 30). UNESCO.  
[https://unesdoc.unesco.org/ark:/48223/pf0000390781\\_spa](https://unesdoc.unesco.org/ark:/48223/pf0000390781_spa)
- Pérez Estrada, M. J. (2021). La inteligencia artificial como prueba científica en el proceso penal español. *Revista Brasileira de Direito Processual Penal*, 7(2), 1385-1410.

### ¿Puede un algoritmo ser perito?

Inteligencia artificial y los nuevos retos de la prueba pericial en México

### Can an Algorithm Act as an Expert Witness?

Artificial Intelligence and the Emerging Challenges of Expert Evidence in Mexico

**Jesús Ángel Arreola Gayosso\***

*Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas, México*

jesus.arreolag@gmail.com

**Resumen:** El artículo analiza el impacto de la inteligencia artificial en la prueba pericial dentro del sistema de justicia mexicano. En este texto, se abordan sus principales aplicaciones en las ciencias forenses, como el reconocimiento facial y el análisis automatizado de datos. Asimismo, se examinan los retos que plantea su uso, incluyendo la opacidad algorítmica, los posibles sesgos y las dificultades para garantizar transparencia y contradicción en juicio. Se sostiene que, aunque la inteligencia artificial no puede sustituir al perito, sí transforma su papel, exigiendo nuevas competencias y criterios para asegurar la validez y confiabilidad de la evidencia científica.

**Palabras clave:** inteligencia artificial; prueba pericial: Ciencias forenses.

**Abstract:** This article explores the impact of artificial intelligence on expert evidence within the Mexican justice system. It outlines its main applications in forensic science, including facial recognition and automated data analysis, and discusses the challenges associated with its use, such as algorithmic opacity, potential biases, and the need to ensure transparency in court. The article suggests that, while artificial intelligence cannot replace the expert witness, it is reshaping their role and raising new questions about the reliability and evaluation of scientific evidence.

**Keywords:** Artificial intelligence; Expert evidence; Forensic science

\*Doctorante en ciencias forenses por el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas (CESCIJUC). Maestro en ciencias Penales y Criminalística, licenciado en criminología y Criminalística. CEO de AG servicios Periciales.

## Cómo citar:

Arreola Gayosso, J. Á. (2026). ¿Puede un algoritmo ser perito? *El Mundo de la Criminalística*, 1, 16-24.



# El perito en el proceso penal:

## La importancia del conocimiento especializado en la justicia penal

Juan Manuel Herrera Moreno

Una huella dactilar localizada en el lugar de los hechos, un casquillo percutido, un documento cuya autenticidad se pone en duda o una muestra biológica recuperada durante una investigación pueden convertirse en elementos relevantes dentro de un proceso penal. Sin embargo, ninguno de estos indicios posee un significado por sí mismo.

Es precisamente en este punto donde la criminalística y las ciencias forenses encuentran uno de sus principales espacios de actuación. A través de métodos científicos y procedimientos técnicos, estas disciplinas contribuyen al estudio de los indicios relacionados con un hecho probablemente delictivo, permitiendo reconstruir los acontecimientos e identificar a las personas, objetos o circunstancias vinculadas con una investigación (Guzmán, 1997; Rodríguez Regalado, 2006).

Dentro de este proceso, la figura del perito ocupa un lugar central. Su intervención permite incorporar al proceso penal conocimientos provenientes de disciplinas como la medicina forense, la balística, la genética, la química, la informática o la psicología mediante dictámenes sustentados en principios científicos y técnicos. Más que emitir una opinión, el perito explica, interpreta y comunica los resultados de un análisis especializado para contribuir al esclarecimiento de los hechos.

Aunque en el lenguaje cotidiano suele asociarse la palabra perito con la idea de un experto, desde el punto de vista jurídico su significado es más preciso. Se trata de la persona que posee conocimientos especializados en una ciencia, técnica, arte u oficio y que auxilia a la autoridad judicial cuando la resolución de un asunto requiere conocimientos que exceden el ámbito estrictamente jurídico (RAE, 2025).

La participación de las y los peritos no implica sustituir la función del juzgador ni determinar el resultado de un proceso. Su responsabilidad consiste en aportar elementos objetivos derivados de la aplicación de métodos científicos o técnicos que permitan comprender mejor la evidencia disponible. En otras palabras, el conocimiento especializado no reemplaza la decisión judicial, sino que proporciona información que contribuye a una valoración más completa de los hechos.





En la actualidad, la investigación criminal exige cada vez mayor especialización. La complejidad de los delitos, el desarrollo de nuevas tecnologías y las exigencias del sistema penal acusatorio han incrementado la necesidad de contar con profesionales capaces de analizar evidencia científica con rigor metodológico. Como consecuencia, el trabajo pericial se ha convertido en un componente indispensable para la administración de justicia.

No obstante, el desarrollo de esta actividad también enfrenta desafíos. La formación especializada, la actualización permanente, la aplicación de metodologías confiables y la capacidad para comunicar los resultados durante el juicio oral constituyen algunos de los factores que determinan la calidad de un dictamen pericial. Un error técnico, una interpretación insuficientemente fundamentada o una deficiente explicación de los hallazgos pueden afectar la valoración de la prueba e, incluso, influir en el resultado de un proceso judicial.

Comprender el papel del perito implica reconocer que la administración de justicia no depende únicamente de la correcta aplicación del derecho. También requiere la participación de especialistas capaces de traducir el conocimiento científico en información útil para esclarecer los hechos y apoyar la toma de decisiones dentro del proceso penal.



## *La prueba pericial: del conocimiento científico a la evidencia judicial*

La investigación de un hecho probablemente delictivo no termina cuando se localizan indicios en el lugar de los hechos. Huellas, documentos, armas, muestras biológicas o dispositivos electrónicos constituyen únicamente fuentes potenciales de información. Para que esos elementos puedan adquirir valor dentro del proceso penal es necesario analizarlos mediante procedimientos especializados y explicar qué información aportan a la investigación. Ese proceso da origen a la prueba pericial.

La prueba pericial constituye uno de los medios mediante los cuales el conocimiento científico o técnico se incorpora al proceso judicial. Su objeto son los hechos controvertidos y su finalidad consiste en auxiliar a la autoridad para comprender aspectos cuya interpretación requiere conocimientos especializados (Schiattino Machado, 1999). A diferencia de otros medios de prueba, el dictamen pericial no crea hechos nuevos ni sustituye la función del juez; proporciona elementos técnicos que permiten interpretar la evidencia y facilitar su valoración jurídica.





Esta característica distingue a la prueba pericial del testimonio. Mientras el testigo declara sobre hechos que percibió directamente, el perito comparece para explicar los resultados de un estudio especializado. Su aportación no consiste en narrar acontecimientos, sino en interpretar información obtenida mediante la aplicación de conocimientos científicos, técnicos o artísticos. De ahí que el dictamen represente una explicación fundamentada y no una decisión sobre la responsabilidad jurídica de las personas involucradas.

La utilidad de una prueba pericial depende tanto del rigor con el que fue elaborada como de la posibilidad de comprender el procedimiento seguido para obtener sus conclusiones. Por esta razón, un dictamen debe describir el objeto de estudio, las técnicas empleadas, la metodología aplicada, los análisis realizados y las conclusiones alcanzadas. Esta estructura permite que las partes conozcan el proceso seguido por el especialista y facilita que la autoridad judicial valore la consistencia técnica del estudio.

En consecuencia, el valor de la prueba pericial no depende exclusivamente del documento que integra el expediente. Durante el juicio oral, el especialista debe explicar el procedimiento seguido, justificar la metodología empleada y responder a los cuestionamientos formulados por las partes. Es precisamente en ese espacio donde el conocimiento científico se somete al debate jurídico y donde la claridad de la exposición resulta tan importante como la calidad técnica del análisis realizado.

Desde esta perspectiva, la prueba pericial representa el punto de encuentro entre la ciencia y el derecho. Su finalidad no consiste en reemplazar la decisión judicial, sino en aportar elementos objetivos que permitan comprender mejor la evidencia disponible y contribuir a una resolución sustentada en información técnicamente fundada.





## Del indicio al dictamen pericial

La labor pericial forma parte de un proceso de investigación en el que intervienen diversas autoridades y especialistas. Desde que ocurre un hecho probablemente delictivo, cada actuación relacionada con los indicios debe desarrollarse bajo procedimientos que permitan conservar su integridad y asegurar que la información obtenida pueda ser utilizada durante el proceso penal.

La investigación criminal comienza con la definición de una estrategia orientada al esclarecimiento de los hechos, comúnmente conocida como teoría del caso. A partir de ella se determina qué información debe obtenerse, cuáles son los indicios relevantes y qué disciplinas especializadas deberán intervenir. Se trata de un trabajo necesariamente multidisciplinario, sustentado en la observación, la descripción sistemática y la aplicación del método científico (Ruiz, 2015).

En este proceso, el lugar de los hechos representa una de las principales fuentes de información. La identificación, preservación y análisis de los indicios permiten reconstruir acontecimientos que, en muchas ocasiones, no pueden conocerse mediante otros medios de prueba. Para ello, la criminalística se apoya en principios como el intercambio, la correspondencia de características, la reconstrucción de los hechos y la probabilidad, los cuales orientan el análisis de la evidencia y contribuyen a formular explicaciones técnicamente sustentadas.

La obtención de resultados confiables también depende de la coordinación entre quienes participan en la investigación. Policías, ministerios públicos, peritos y demás servidores públicos desarrollan funciones específicas que se complementan entre sí. Mientras unos preservan el lugar de intervención y aseguran los indicios, otros realizan los estudios especializados, documentan los hallazgos y elaboran los informes correspondientes. Esta responsabilidad compartida busca mantener la integridad de la evidencia durante todo el procedimiento y reducir el riesgo de alteraciones que puedan afectar su valoración posterior.

El resultado de ese trabajo se refleja en el dictamen pericial. Este documento no consiste únicamente en presentar conclusiones, sino en explicar el procedimiento seguido para alcanzarlas. Un dictamen debe describir el material de estudio, las técnicas empleadas, la metodología utilizada, los resultados obtenidos y el razonamiento que permite sostener las conclusiones. De igual manera, puede acompañarse de informes técnicos o ejecutivos elaborados con distintos niveles de especialización, según las necesidades de la investigación o de la autoridad que los solicita.

Sin embargo, el trabajo del perito no concluye con la entrega del informe. En el sistema penal acusatorio, el dictamen constituye el punto de partida para la participación del especialista durante el juicio oral. Será en la audiencia donde deba explicar su metodología, justificar sus conclusiones y responder a las preguntas formuladas por las partes. En consecuencia, la solidez de una pericia depende tanto del rigor científico con que fue elaborada como de la capacidad del especialista para comunicar con claridad el conocimiento que sustenta sus conclusiones.





## Los desafíos del ejercicio pericial

El ejercicio pericial exige una combinación de conocimientos científicos, experiencia profesional y responsabilidad ética. Sin embargo, la calidad de un dictamen no depende únicamente de la formación académica del especialista. También intervienen factores relacionados con la manera en que se desarrolla la investigación, la aplicación de metodologías apropiadas y la capacidad para defender técnicamente las conclusiones durante el juicio.

La experiencia profesional muestra que algunos errores pueden comprometer la utilidad de un peritaje. Entre los más frecuentes se encuentran trabajar con un número insuficiente de indicios cuando existen más elementos disponibles; realizar análisis limitados; omitir la explicación de la metodología empleada; incorporar información técnica irrelevante o formular conclusiones que exceden el alcance de la evidencia analizada. Del mismo modo, prácticas como modificar muestras, dañar documentos originales, emitir dictámenes orientados por los intereses de alguna de las partes o presentar afirmaciones absolutas sin el debido respaldo científico afectan la confiabilidad del trabajo pericial.

Estos aspectos permiten comprender que un buen dictamen no depende únicamente del conocimiento técnico. La claridad metodológica y la transparencia con la que se presentan los resultados constituyen condiciones indispensables para que las conclusiones puedan ser evaluadas y, en su caso, contrastadas durante el proceso judicial.





Desde esta perspectiva, el sistema penal acusatorio exige que el especialista reúna tres condiciones fundamentales: acreditación, confiabilidad y credibilidad. La acreditación se relaciona con la formación profesional y la documentación que respalda los conocimientos del perito; la confiabilidad hace referencia al empleo de metodologías aceptadas y técnicamente válidas; mientras que la credibilidad se construye cuando el especialista demuestra, durante el juicio, que puede sostener científicamente sus conclusiones frente al interrogatorio y al contrainterrogatorio (Hernández López, 2022; Sánchez Marín, 2024).

En este punto resulta especialmente valiosa la reflexión que plantea el autor del manuscrito. Desde su experiencia profesional, sostiene que la acreditación puede obtenerse mediante la formación y la actualización constante, y que la confiabilidad depende del seguimiento de metodologías aceptadas por la comunidad especializada. Sin embargo, considera que el mayor reto consiste en construir credibilidad, ya que ésta se demuestra únicamente cuando el perito comparece ante un tribunal, explica con claridad su trabajo y responde con solvencia a los cuestionamientos que surgen durante el juicio.

La experiencia también muestra que la formación del perito no concluye con la obtención de un título profesional. La actualización permanente, el desarrollo de habilidades de comunicación, el control emocional y la preparación para la audiencia forman parte del ejercicio cotidiano de quienes participan como especialistas en la administración de justicia. El conocimiento científico constituye la base del trabajo pericial, pero es la práctica profesional la que permite consolidar la experiencia necesaria para enfrentar los desafíos que plantea cada caso.





## La prueba pericial en la administración de justicia

La incorporación del conocimiento especializado al proceso penal representa una de las características distintivas del sistema de justicia contemporáneo. A través de la prueba pericial, disciplinas como la criminalística y las ciencias forenses contribuyen a esclarecer hechos que difícilmente podrían comprenderse únicamente mediante la aplicación del derecho.

No obstante, el valor de un dictamen no depende exclusivamente del empleo de técnicas o instrumentos especializados. Su utilidad radica en la posibilidad de demostrar que las conclusiones derivan de procedimientos verificables, metodologías aceptadas y razonamientos que puedan explicarse de manera clara durante el juicio oral. Por ello, la prueba pericial constituye un medio de apoyo para la autoridad judicial y no un mecanismo destinado a sustituir su función decisoria (Schiattino Machado, 1999).

En este contexto, el perito asume una responsabilidad que trasciende la elaboración de un informe técnico. Su trabajo implica analizar la evidencia con objetividad, comunicar sus resultados con precisión y sostener sus conclusiones mediante argumentos científicos cuando sea requerido por la autoridad. La calidad de la administración de justicia depende, en buena medida, de que ese conocimiento especializado sea incorporado al proceso con rigor metodológico, transparencia y responsabilidad profesional.



La creciente complejidad de los fenómenos delictivos plantea nuevos desafíos para las ciencias forenses y para quienes participan en ellas. La incorporación de tecnologías, el desarrollo de nuevas metodologías y la necesidad de fortalecer la capacitación de los especialistas exigen procesos permanentes de actualización. En este escenario, la preparación técnica continúa siendo indispensable, pero también lo son la ética profesional, la capacidad de comunicar el conocimiento científico y el compromiso con la búsqueda de la verdad procesal.

En definitiva, la función del perito no consiste únicamente en elaborar un dictamen. Su principal contribución radica en hacer comprensible el conocimiento especializado para que pueda ser valorado dentro del proceso penal y contribuya a una administración de justicia sustentada en evidencia científicamente fundada.





## Reflexiones finales

Hablar del trabajo pericial implica reconocer que la administración de justicia no depende únicamente de la aplicación de las normas jurídicas. En numerosos casos, la comprensión de los hechos exige recurrir a conocimientos científicos y técnicos que permitan interpretar indicios, explicar fenómenos complejos y aportar elementos objetivos para la valoración de la prueba.

En este contexto, la prueba pericial constituye uno de los principales vínculos entre la ciencia y el derecho. Su relevancia no radica exclusivamente en la utilización de tecnologías o metodologías especializadas, sino en la posibilidad de transformar la evidencia en información comprensible, verificable y útil para quienes tienen la responsabilidad de impartir justicia. Cada dictamen representa el resultado de un proceso de análisis que debe sostenerse tanto en el rigor metodológico como en la capacidad del especialista para explicar y defender sus conclusiones.

El sistema penal acusatorio también ha redefinido el papel de las y los peritos. Actualmente, ya no basta con poseer conocimientos especializados; resulta indispensable demostrar que estos se aplican mediante procedimientos técnicamente válidos, con objetividad, transparencia y apego a principios éticos. De igual manera, la participación del especialista durante el juicio oral exige habilidades de comunicación que permitan traducir conceptos científicos a un lenguaje accesible para los operadores jurídicos, sin perder precisión técnica.



La creciente complejidad de los fenómenos delictivos plantea nuevos retos para la práctica pericial. La incorporación de tecnologías digitales, el desarrollo de nuevas disciplinas forenses y la evolución constante de los métodos de investigación hacen necesaria una actualización permanente de quienes desempeñan esta función. En este escenario, la formación profesional, la experiencia y la mejora continua representan condiciones indispensables para fortalecer la calidad de los dictámenes y la confianza en la prueba pericial.

Finalmente, conviene recordar que el trabajo del perito no tiene como propósito determinar la responsabilidad de una persona ni sustituir las decisiones de la autoridad jurisdiccional. Su verdadera aportación consiste en proporcionar conocimiento especializado que contribuya al esclarecimiento de los hechos y permita que las resoluciones judiciales se sustenten en evidencia científicamente analizada. En esa medida, la labor pericial continúa siendo uno de los pilares que articulan el diálogo entre la criminalística, las ciencias forenses y la administración de justicia.

## Referencias bibliográficas

Guzmán, C. (1997). *Manual de Criminalística* (1.a ed.). Ediciones la Rocca.

Rodríguez Regalado, P. (2006). Aportes en materia Criminalística. Compendio de Ponencias *Desarrolladas del I Congreso Internacional de Ciencias Forenses y Criminalística, I*.

Ruiz Jaramillo, L. B. (2015). La prueba pericial y su valoración en el proceso penal colombiano, hacia un régimen procesal holístico. *Revista de la Facultad de Derecho y Ciencias Políticas*, 45(123), 481-511.

Schiattino Machado C. (1999), *Vademécum pericial* (1.a ed.). Buenos aires, Ediciones La Roca.



### **El perito en el proceso penal:**

Cuando el conocimiento especializado contribuye a la administración de justicia

### **The Expert Witness in Criminal Proceedings:**

Why Specialized Knowledge Matters in Criminal Justice

**Juan Manuel Herrera Moreno\***

juanmahm2000@gmail.com

*Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas, México*

**Resumen:** La prueba pericial constituye uno de los principales mecanismos mediante los cuales el conocimiento especializado se incorpora al sistema de justicia penal. A través de ella, disciplinas como la criminalística y las ciencias forenses aportan elementos técnicos y científicos que contribuyen al esclarecimiento de los hechos y a la valoración de la prueba. El presente artículo tiene como propósito explicar el papel que desempeña la prueba pericial dentro del proceso penal mexicano, describiendo la intervención del perito desde el análisis de los indicios hasta la elaboración y defensa del dictamen durante el juicio oral. Asimismo, se reflexiona sobre algunos de los desafíos que enfrenta actualmente el ejercicio pericial, particularmente en relación con la acreditación profesional, la confiabilidad metodológica y la credibilidad del especialista. Se concluye que la aportación del perito trasciende la elaboración de un informe técnico, al constituirse como un vínculo entre el conocimiento científico y la administración de justicia.

**Palabras clave:** Prueba pericial; perito; criminalística; ciencias forenses; sistema penal acusatorio.

**Abstract:** Expert evidence is one of the primary mechanisms through which specialized knowledge is incorporated into the criminal justice system. Through expert testimony, disciplines such as criminalistics and forensic sciences provide scientific and technical evidence that contributes to fact-finding and the evaluation of evidence in criminal proceedings. This article examines the role of expert evidence within the Mexican criminal justice system, describing the work of expert witnesses from the examination of physical evidence to the preparation and presentation of expert reports during oral trials. It also discusses some of the current challenges faced by forensic practitioners, particularly those related to professional accreditation, methodological reliability, and expert credibility. The article concludes that the contribution of expert witnesses extends beyond the preparation of technical reports, serving as a bridge between scientific knowledge and the administration of justice.

**Keywords:** Expert evidence; expert witness; criminalistics; forensic sciences; accusatorial criminal justice system.

\*Doctorante y docente investigador del Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas

## **Cómo citar:**

Herrera Moreno, J. M. (2026). El perito en el proceso penal: La importancia del conocimiento especializado en la justicia penal. *El Mundo de la Criminalística*, 1, 26-38.





# 8 CONGRESO IBEROAMERICANO DEL SISTEMA PROCESAL PENAL ACUSATORIO Y DOGMÁTICA PENAL

[www.cescijuc.edu.mx](http://www.cescijuc.edu.mx)

19<sub>y</sub>20 | 2026  
SEPTIEMBRE

📍 CASINO CAMPO MARTE  
POLANCO, CHAPULTEPEC, 11580 CIUDAD DE MÉXICO

● COSTO POR DÍA: \$1,200.00 MXN



# Cuando la tecnología aprende de nosotros...

y nos vigila

**Oswaldo Aguilar Rivera**

oswaldoaguilarrivera@gmail.com

Todos dejamos huellas. Algunas permanecen sobre los objetos que tocamos; otras quedan registradas en documentos, fotografías o grabaciones. Muchas más se producen sin que las percibamos, como ocurre cada vez que utilizamos un teléfono celular, consultamos una aplicación de navegación, realizamos una compra electrónica, compartimos una fotografía en redes sociales o simplemente llevamos un reloj inteligente durante nuestras actividades cotidianas. En criminalística, estas huellas —junto con otros rastros y vestigios— forman parte de lo que técnicamente se conoce como indicios, es decir, elementos que, analizados dentro de una investigación, pueden aportar información para reconstruir un hecho.

Durante mucho tiempo, las huellas que interesaban a la investigación criminal eran principalmente materiales: una huella dactilar sobre un objeto, una fibra textil, una gota de sangre, un casquillo percutido o un documento. Hoy ese panorama se ha ampliado. Las tecnologías digitales también producen huellas. Cada búsqueda en internet, cada recorrido registrado por un sistema de geolocalización, cada acceso a una plataforma digital o cada interacción con un dispositivo conectado genera información que puede convertirse en una pieza más para comprender cómo ocurrieron determinados acontecimientos.

Vista de manera aislada, gran parte de esa información parece carecer de importancia. Sin embargo, cuando millones de registros se integran y se analizan de manera conjunta, comienzan a revelar patrones. Es posible identificar recorridos habituales, horarios, lugares frecuentados, formas de movilidad, vínculos entre personas o cambios en las rutinas cotidianas. Las huellas digitales no solo registran acciones; también permiten reconstruir contextos, establecer relaciones y comprender comportamientos que antes resultaban mucho más difíciles de identificar.

Esta transformación también ha modificado el trabajo de la criminalística. La investigación ya no depende exclusivamente del análisis de evidencias obtenidas en una escena del crimen. En muchos casos incorpora información generada por teléfonos inteligentes, cámaras de videovigilancia, sistemas de posicionamiento global, plataformas digitales y otros dispositivos que acompañan buena parte de nuestra vida cotidiana. A ello se suma la inteligencia artificial, cuya capacidad para procesar grandes volúmenes de información permite reconocer relaciones y patrones que hace apenas algunos años habrían requerido largos procesos de análisis.



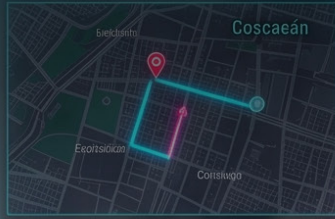


CCTV ACTIVE  
SYSTEM STATUS: SECURE  
USER TRACKING

CCTV ACTIVE  
SYSTNG · SECURE  
USER TRACKING  
NETWORK ANOMALIES



### Rastreo GPS



Ruta actual: Parque Coyoacán →  
Mercado  
Ubizaciones: COMX, Aochímico

### Actividad Digital

- Publicación: "Tarde perfecta en Coyoacán!"
- Publicación: "Tarde perfecta en Coyoacán!"

### Compras Recientes

- Tacas de canasía - \$60
- Spotify Premium - \$129
- Café de Coyoacán - \$85
- Uber - \$150

### Redes Sociales

- 14k Seguidores
- 1k Mo Ouzta en la publicación de ayer
- 1.2m Vistas en TiTTok



**Valeria Méndez**  
Portil de Usuario



Al mismo tiempo, estos cambios invitan a reflexionar sobre la manera en que entendemos la vigilancia. Anteriormente, vigilar significó observar. Hoy también implica registrar, almacenar, relacionar e interpretar la información que producimos mientras interactuamos con tecnologías digitales. En este proceso participan algoritmos capaces de identificar regularidades, generar inferencias y aprender continuamente a partir de los datos que dejamos en nuestra vida cotidiana. Comprender cómo funciona esta nueva forma de vigilancia resulta indispensable para entender muchos de los desafíos que actualmente enfrentan la investigación criminal, el cibercrimen y la protección de los derechos humanos.

Sin embargo, la incorporación de estas capacidades también plantea una pregunta fundamental para la investigación criminal: ¿hasta dónde puede llegar el uso de tecnologías capaces de reconstruir buena parte de la vida cotidiana de una persona? La respuesta no depende únicamente de los avances de la inteligencia artificial. También exige considerar el marco jurídico que regula la obtención y el tratamiento de la información, así como principios indispensables para un Estado de derecho, entre ellos el respeto a la privacidad, la protección de los datos personales, el debido proceso y los derechos humanos. En este sentido, el desafío no consiste solamente en desarrollar mejores herramientas para investigar, sino en garantizar que su utilización fortalezca la justicia sin comprometer las libertades que busca proteger.

La criminalística siempre ha buscado comprender lo que las huellas pueden revelar sobre un hecho. Hoy muchas de esas huellas se producen en entornos digitales y requieren nuevas formas de interpretación. El propósito de este artículo es ofrecer una mirada sobre esa transformación, explicar cómo las tecnologías actuales han modificado las formas de observar, registrar y analizar la información, y reflexionar sobre lo que estos cambios significan para la investigación criminal y la protección de los derechos humanos.

## *Las huellas cambian con las sociedades*

Las huellas siempre han acompañado la vida social. Mucho antes de que existieran los teléfonos inteligentes, internet o la inteligencia artificial, las personas dejaban rastros de su presencia y de sus actividades. Un documento firmado, una fotografía, un registro civil, una licencia de conducir o una llamada telefónica podían convertirse en fuentes de información para identificar personas, reconstruir acontecimientos o apoyar una investigación. Lo que ha cambiado no es la existencia de esas huellas, sino la forma en que se producen, se registra y se interpretan. Cada época ha desarrollado sus propios mecanismos para observar, documentar y conservar información sobre las personas. En algunos momentos predominó la observación directa; posteriormente aparecieron archivos documentales, sistemas de identificación, fotografías, cámaras de videovigilancia y bases de datos.

Comprender esta transformación requiere mirar la vigilancia como un proceso histórico. Con frecuencia se piensa que la vigilancia surgió con internet o con las redes sociales. En realidad, las sociedades siempre han desarrollado mecanismos para observar, controlar o



registrar determinadas conductas. Lo que caracteriza al momento actual no es la existencia de la vigilancia, sino la capacidad tecnológica para producir, almacenar y procesar cantidades de información que hace apenas unas décadas habrían sido difíciles de imaginar.

Por ello, es importante analizar este proceso desde una perspectiva histórica. A este recorrido, se le puede denominar como genealogía de la vigilancia (Aguilar, 2025), porque permite comprender que las formas contemporáneas de observar no aparecieron de manera espontánea. Son el resultado de una evolución en la que cada innovación tecnológica amplió las posibilidades para registrar información, conservarla durante más tiempo y utilizarla en distintos ámbitos de la vida social, entre ellos la seguridad, la administración pública, el comercio y la investigación criminal.

Al mismo tiempo, esta evolución también ha dado lugar a nuevas formas de regulación. Conforme aumentó la capacidad para observar y registrar información sobre las personas, también se hizo necesario desarrollar mecanismos jurídicos destinados a proteger su intimidad, limitar el ejercicio del poder y garantizar que las herramientas de vigilancia se utilizaran únicamente bajo criterios de legalidad, necesidad y proporcionalidad. La historia de la vigilancia es, por ello, también la historia de la construcción de derechos frente al desarrollo tecnológico.

Pensemos en una situación cotidiana. Hace algunos años, conocer los desplazamientos habituales de una persona requería seguirla físicamente durante varios días. Hoy, un teléfono inteligente, un sistema de navegación, una aplicación de transporte o un reloj inteligente pueden registrar buena parte de esos recorridos mientras la persona realiza actividades completamente ordinarias. La diferencia no radica únicamente en la cantidad de información disponible, sino en la manera en que esa información puede integrarse para comprender comportamientos, reconstruir trayectorias o apoyar una investigación.

Esta perspectiva histórica también permite evitar una idea frecuente: pensar que las tecnologías digitales sustituyeron las formas tradicionales de investigación. En realidad, ambas conviven. Las huellas físicas continúan siendo fundamentales para la criminalística, pero ahora dialogan con nuevas fuentes de información que amplían las posibilidades para comprender un hecho. Observar esta continuidad resulta indispensable para entender cómo la investigación criminal ha incorporado herramientas digitales sin abandonar los principios básicos que históricamente han orientado el estudio de los indicios.

## ***Cuando la vigilancia comenzó a aprender***

Durante mucho tiempo, la función principal de los sistemas de vigilancia consistía en registrar información. Una cámara captaba imágenes, un archivo almacenaba documentos y una base de datos conservaba registros para ser consultados cuando fuera necesario. Aunque estas herramientas facilitaban el trabajo de distintas instituciones, su capacidad dependía, en gran medida, de la intervención humana. Eran las personas quienes observaban las imágenes, revisaban los documentos, comparaban fotografías o buscaban coincidencias entre distintos registros.







DENSIDAD GLOBAL: ALTA (EST. 312 INDIVIDUOS).



EMERGENCIA

COLEGA  
(14%)

COLEGA

FAMILIAR

DATO CONEXIÓN (14%)

SUJETO 1235:  
ANA RAMÍREZ.  
EDAD: 24.  
ID: MX-55-133.  
RIESGO: BAJO.  
DESTINO: INDIOS VERDES.

FEMENINO  
165cm  
BFSÉHO est.  
165cm

SUJETO 1234:  
ANA RAMÍREZ.  
EDAD: 35.  
ID: MX-55-133.  
RIESGO: BAJO.  
DESTINO: INDIOS VERDES.

SUJETO 1235:  
CARMEN DÍAZ.  
EDAD: 31.  
ID: MX-55-124.  
RIESGO: BAJO.  
CONEXIÓN: COLEGA (ANA R.)

SUJETO 1234:  
ANA RAMÍREZ.  
EDAD: 26.  
ID: MX-55-123.  
RIESGO: BAJO.  
DESTINO: INDIOS VERDES.

FEMENINO  
ALT est.  
165cm  
CAMINANDO

3-365-135] ANNO AGAIRES RESOSTEEOY YHQA DATA DDL EIO DEANDED CANA ST...  
3-536-178] BEMTARJ BR&E4 DVED TENG...  
3-535-326] DUCO A20 CIDEVI TESPVESEHENG DUEZSNIDOCOL EIO DEANDED CANA RT...  
3-585-326] ANA AABEADUICA (ENT: 313 INDIVIDUOS)  
3-536-328] BDCO NANIRES RESOSTEEOY YADA DATA DUE EIO DEANDED CANA BT...  
3-533-333] AKIA W3OHIEGA (ENT: 313 INDIVIDUOS)  
3-533-330] SBFRINA JADHAILIA AUA (ENT: 313 INDIVIDUOS)  
3-661-350] AGTO FONGUE SAI DEDUIES DESGEUTION CASI CKVITACOOV IMBRIRES...

En la actualidad, ese escenario ha comenzado a cambiar. La incorporación de sistemas de inteligencia artificial ha permitido desarrollar herramientas capaces de procesar enormes cantidades de información en tiempos muy reducidos. Más que sustituir a quienes investigan, estas tecnologías amplían la capacidad para identificar relaciones, reconocer patrones y encontrar conexiones que difícilmente podrían advertirse mediante una revisión convencional.

Pensemos en un ejemplo sencillo. Una cámara instalada en una estación del transporte público registra miles de personas todos los días. Durante años, revisar ese material implicaba observar horas de grabación para localizar a una persona o reconstruir un recorrido. Hoy existen sistemas capaces de reconocer determinadas características físicas, comparar imágenes obtenidas en distintos momentos e identificar coincidencias entre millones de registros en cuestión de segundos. La cámara continúa registrando imágenes, pero ahora el sistema también puede analizarlas.

Lo mismo ocurre con la información que producimos mientras utilizamos tecnologías digitales. Los teléfonos inteligentes registran desplazamientos, las aplicaciones almacenan búsquedas, los dispositivos conectados generan información sobre nuestros hábitos y muchas plataformas conservan un historial de nuestras interacciones. Cuando estos registros se analizan de manera conjunta, dejan de ser simples datos aislados para convertirse en una fuente de información capaz de mostrar tendencias, relaciones y comportamientos. Para explicar esta transformación, podemos pensar en el término genética de la vigilancia (Aguilar, 2025). Éste no refiere únicamente a la incorporación de nuevas tecnologías, sino a la manera en que la propia vigilancia ha modificado sus capacidades. Si durante buena parte de su historia consistió en observar y registrar, hoy también aprende. Es capaz de reconocer regularidades, establecer asociaciones entre datos y generar inferencias sobre determinadas conductas a partir de la información disponible.

La idea de una genética de la vigilancia permite comprender que no estamos frente a una ruptura absoluta con las formas tradicionales de observación, sino ante un proceso de evolución. Así como las sociedades incorporan nuevas tecnologías para comunicarse, trabajar o desplazarse, también desarrollan nuevas formas de producir conocimiento a partir de las huellas que generan las personas en su vida cotidiana. La inteligencia artificial forma parte de esa transformación porque incrementa la capacidad para procesar información y aprender de ella.

Este cambio tiene implicaciones importantes para la criminalística. La evidencia digital ya no se limita a proporcionar información sobre un hecho específico; también puede contribuir a reconstruir contextos, identificar patrones de comportamiento y fortalecer distintas líneas de investigación. Al mismo tiempo, esta capacidad obliga a reflexionar sobre la calidad de los datos, los posibles sesgos de los algoritmos, la transparencia de los sistemas utilizados y los límites que deben establecerse para proteger los derechos fundamentales de las personas.

Por ello, la inteligencia artificial debe entenderse como una herramienta cuyo valor depende del contexto en el que se utiliza. Puede contribuir al esclarecimiento de un delito, facilitar la búsqueda de personas desaparecidas, apoyar el análisis de evidencia digital o



fortalecer tareas de prevención. Sin embargo, también puede utilizarse para ampliar mecanismos de vigilancia desproporcionada, generar perfiles sin control suficiente o reproducir sesgos presentes en los datos con los que estos sistemas han sido entrenados.

Precisamente por ello, la incorporación de inteligencia artificial a la investigación criminal no puede entenderse únicamente como un desafío tecnológico. También representa un desafío jurídico y ético. Las decisiones que apoyan una investigación no deberían descansar exclusivamente en sistemas automatizados ni en inferencias producidas por algoritmos cuya lógica resulta difícil de conocer o verificar. La supervisión humana, la transparencia en los procedimientos y la posibilidad de revisar críticamente los resultados constituyen condiciones indispensables para garantizar el debido proceso y proteger los derechos fundamentales de las personas involucradas en una investigación.

Desde esta perspectiva, la inteligencia artificial debe fortalecer la capacidad de análisis de quienes investigan, no sustituir su criterio profesional. La responsabilidad sobre las decisiones continúa siendo humana. Son las personas quienes valoran la evidencia, construyen hipótesis, verifican la información y determinan el alcance jurídico de los resultados obtenidos mediante estas tecnologías.

## ***Cuando las huellas comienzan a contar una historia***

Imaginemos una situación sencilla. Una persona sale todos los días de su casa a las siete de la mañana. Su teléfono celular registra el recorrido hasta el trabajo. Antes de llegar se detiene unos minutos en una cafetería. Los martes y jueves visita un gimnasio; los viernes pasa por la casa de sus padres y los fines de semana suele viajar a otra ciudad. Ninguna de estas actividades tiene, por sí misma, un significado especial. Son acciones que forman parte de la vida cotidiana y que millones de personas realizan todos los días.

Ahora imaginemos que esa información se registra durante varios meses. Los recorridos dejan de ser desplazamientos aislados y comienzan a formar una secuencia. Es posible reconocer horarios, lugares frecuentes, cambios de rutina y patrones de movilidad. Incluso pueden identificarse relaciones entre personas que coinciden de manera constante en determinados espacios o reconstruirse trayectorias que ayudan a comprender cómo ocurrieron ciertos acontecimientos.

Este ejemplo permite comprender que la geolocalización ha dejado de ser una herramienta destinada únicamente a conocer la ubicación de un dispositivo. Hoy constituye una fuente de información que, analizada de manera conjunta con otros registros digitales, permite reconstruir aspectos importantes de la vida cotidiana. Cada desplazamiento deja una huella; la suma de esas huellas permite construir una historia.

Para explicar este fenómeno propongo el concepto de Vigilancia por Geolocalización Procesada por Inteligencia Artificial (VIPOGIA) (Aguilar, 2025). Se trata de una forma de comprender cómo la información espacial que producen los dispositivos digitales puede ser analizada mediante sistemas de inteligencia artificial para identificar patrones de comportamiento, establecer relaciones entre distintos eventos y generar inferencias sobre las actividades de una persona o de un grupo.





**PERFIL DEL SUJETO:**  
**Juan Pérez**  
(CONFIDENCIAL) | ID: JP38485

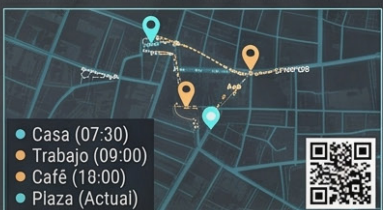


**COMPRAS RECIENTES** (En línea y Físicas)  
Amazon (Audifunca) 09:03 - 18:50  
Ouvo (Refresco) 09:03 - 18:30  
Oavo (Refresco) 09:03 - 13:50  
Merro Ticket 09:03 - 13:30  
Librería 08:03 - 18:40

**REDES SOCIALES** (Actividad)  
Likes en posts (12)  
Publicaciones nuevas (1)  
Fotos tomadas (3)



**HISTORIAL DE GEOLOCALIZACIÓN**



**PERFIL DEL SUJETO:**  
**Ana García**  
(CONFIDENCIAL) | ID: AG23845

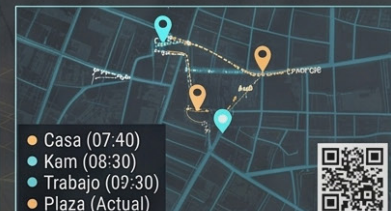


**COMPRAS RECIENTES**  
Zara (Blusa) 04:03 - 13:53  
Zara (Blusa) 03:03 - 13:38  
Uber Eats (Cena) 09:00 - 13:30  
Cine 09:00 - 18:34  
Uber Ride 08:00 - 18:30

**REDES SOCIALES**  
Likes en posts (13)  
Publicaciones (0)  
Fotos (3)



**HISTORIAL DE GEOLOCALIZACIÓN**





Lo relevante de este proceso no es únicamente la capacidad para conocer dónde se encuentra alguien en un momento determinado. Lo verdaderamente significativo es que la información acumulada permite comprender cómo se mueve, cuáles son sus rutinas, qué lugares frecuenta, cuánto tiempo permanece en ellos y qué cambios aparecen con el paso del tiempo. En otras palabras, la geolocalización deja de registrar posiciones aisladas para convertirse en una herramienta capaz de reconstruir dinámicas sociales.

Esta transformación tiene implicaciones importantes para la investigación criminal. Pensemos, por ejemplo, en la búsqueda de una persona desaparecida. La información de geolocalización puede contribuir a reconstruir sus últimos desplazamientos, identificar lugares donde permaneció durante más tiempo o establecer posibles rutas de movilidad. De manera similar, en una investigación relacionada con delincuencia organizada, fraude, extorsión o secuestro, los registros espaciales pueden aportar información útil para comprender la relación entre distintos hechos y orientar nuevas líneas de investigación.

Las mismas herramientas que fortalecen la investigación criminal también obligan a reflexionar sobre la forma en que se protegen los derechos humanos. La posibilidad de reconstruir trayectorias, identificar relaciones personales o anticipar determinados comportamientos representa una capacidad de enorme utilidad para localizar personas desaparecidas, esclarecer delitos complejos o fortalecer tareas de prevención. Sin embargo, esas mismas capacidades pueden resultar invasivas cuando se utilizan sin controles jurídicos claros o cuando la recolección y el procesamiento de datos exceden los fines para los cuales fueron obtenidos. La discusión, por lo tanto, no consiste en decidir si estas tecnologías deben utilizarse, sino en establecer bajo qué condiciones su empleo resulta compatible con la legalidad, la proporcionalidad y el respeto a la privacidad, la protección de los datos personales y los demás derechos fundamentales.

Por ello, VIPOGIA constituye una propuesta para reflexionar sobre la forma en que la inteligencia artificial modifica la producción y el análisis de la evidencia digital. La información espacial ya no representa únicamente un dato de ubicación; forma parte de un conjunto de huellas que, interpretadas dentro de un contexto específico, permiten comprender relaciones, reconstruir acontecimientos y generar conocimiento útil para la investigación criminal.

La criminalística ha trabajado históricamente con huellas capaces de explicar un hecho. Hoy esas huellas también se producen mientras caminamos por una ciudad con un teléfono celular en el bolsillo, utilizamos aplicaciones de transporte, consultamos mapas digitales o realizamos actividades tan cotidianas como comprar un café o asistir al trabajo. Comprender este nuevo escenario implica reconocer que las tecnologías digitales no solo registran nuestros movimientos; también producen información que, analizada de manera responsable, puede contribuir al esclarecimiento de los delitos y, al mismo tiempo, abrir nuevas discusiones sobre la protección de los derechos fundamentales.

## Las huellas que compartimos todos los días

Existe una idea que suele pasar inadvertida cuando hablamos de vigilancia tecnológica. Con frecuencia imaginamos que la información sobre las personas se obtiene mediante mecanismos sofisticados, sistemas ocultos o programas informáticos capaces de acceder a nuestros dispositivos sin autorización. Aunque estos escenarios pueden existir, una parte importante de la información que hoy circula en los entornos digitales la proporcionamos nosotros mismos.

Cada fotografía que compartimos, cada comentario en una red social, cada lugar que etiquetamos, cada compra que realizamos en una plataforma digital o cada aplicación a la que autorizamos acceder a nuestra ubicación contribuye a generar un volumen creciente de información sobre nuestras actividades cotidianas. En muchas ocasiones no somos plenamente conscientes de ello. Simplemente aceptamos las condiciones de uso de una aplicación, activamos los servicios de localización o compartimos información porque forma parte de la manera en que actualmente utilizamos las tecnologías.

En muchas ocasiones tampoco conocemos con claridad qué ocurre con esa información una vez que ha sido recopilada. Los permisos que aceptamos al instalar una aplicación o utilizar un dispositivo conectado pueden autorizar el acceso a datos de ubicación, contactos, imágenes, hábitos de navegación o patrones de consumo que posteriormente serán procesados mediante sistemas automatizados. Comprender estas dinámicas constituye una forma de prevención y también una manera de ejercer de forma más consciente derechos como la privacidad, la autodeterminación informativa y la protección de los datos personales.

Lo que hace algunos años podía entenderse como información aislada, hoy adquiere un significado distinto. La inteligencia artificial permite relacionar datos provenientes de múltiples fuentes, identificar regularidades y construir perfiles cada vez más precisos sobre las personas. No se trata únicamente de conocer dónde estuvo alguien o qué compró determinado día. El verdadero cambio consiste en la capacidad para inferir hábitos, anticipar comportamientos y establecer relaciones que difícilmente podrían advertirse observando un solo dato.

Este proceso también explica por qué la vigilancia contemporánea es diferente a la que conocieron generaciones anteriores. Al proponer el concepto de genética de la vigilancia, se ha buscado explicar esta transformación. Cada generación tecnológica incorpora capacidades desarrolladas anteriormente, las perfecciona y amplía su alcance. Esta evolución también plantea nuevos desafíos para la criminalística. Hoy prácticamente cualquier dispositivo conectado puede generar información útil para una investigación. Teléfonos celulares, relojes inteligentes, vehículos conectados, cámaras de videovigilancia, asistentes virtuales o dispositivos pertenecientes al denominado Internet de las Cosas producen datos que, analizados dentro de un contexto específico, pueden contribuir al esclarecimiento de un delito o a la reconstrucción de un hecho.



## Una mirada crítica sobre nuestras decisiones digitales

Las tecnologías digitales continuarán ampliando su presencia en prácticamente todos los ámbitos de la vida social. Cada nuevo dispositivo conectado, cada aplicación y cada sistema basado en inteligencia artificial incrementa las posibilidades para producir, almacenar y analizar información útil para la investigación criminal. Al mismo tiempo, también amplía la responsabilidad de comprender cómo funcionan estas herramientas y cuáles son sus implicaciones para la vida cotidiana.

Una parte importante de la información que hoy alimenta los sistemas de inteligencia artificial no proviene de mecanismos ocultos de vigilancia, sino de actividades que las propias personas realizan todos los días. Compartir una fotografía, autorizar el acceso a la ubicación de un teléfono celular, utilizar una aplicación de navegación, realizar una compra en línea o aceptar las condiciones de uso de una plataforma digital significa generar datos que posteriormente pueden ser recopilados, relacionados e interpretados. En la mayoría de los casos, estas decisiones se toman sin conocer con claridad qué información se está compartiendo, quién puede acceder a ella o con qué finalidad será utilizada.

Este escenario adquiere una dimensión todavía mayor con la expansión del Internet de las Cosas. Televisores inteligentes, asistentes virtuales, relojes, automóviles conectados, sistemas de videovigilancia doméstica, electrodomésticos y una gran variedad de dispositivos registran información de manera constante. Frente a esta realidad, el reto no consiste en rechazar la tecnología ni en asumir que todo desarrollo tecnológico representa una amenaza. El desafío consiste en comprenderla.

Desarrollar una cultura digital más consciente implica conocer qué información recopilan los dispositivos que utilizamos, revisar los permisos que concedemos al instalar aplicaciones, familiarizarse con las opciones de privacidad disponibles y comprender que cada decisión relacionada con los datos personales también tiene implicaciones para la seguridad y para el ejercicio de los derechos.

Esta responsabilidad no recae únicamente en la ciudadanía. También corresponde a las instituciones encargadas de la seguridad, la procuración y la administración de justicia garantizar que la inteligencia artificial y las tecnologías de vigilancia se utilicen dentro de un marco de legalidad y con pleno respeto a los derechos humanos. Herramientas como la geolocalización, el análisis automatizado de grandes volúmenes de información o los sistemas inteligentes de reconocimiento pueden contribuir a localizar personas desaparecidas, esclarecer delitos complejos, fortalecer las investigaciones y mejorar las capacidades institucionales. Sin embargo, su utilización solo resulta legítima cuando se encuentra sujeta a principios como la legalidad, la necesidad, la proporcionalidad, la transparencia, la rendición de cuentas, la protección de los datos personales y el debido proceso. La posibilidad técnica de obtener información nunca debe convertirse, por sí sola, en una justificación para ampliar de manera indiscriminada los mecanismos de vigilancia.



Uno de los grandes desafíos de nuestro tiempo consiste precisamente en lograr que el desarrollo tecnológico avance acompañado por el fortalecimiento de los marcos jurídicos y de la protección de los derechos humanos. La velocidad con la que evolucionan la inteligencia artificial y los sistemas digitales supera con frecuencia la capacidad de las normas para regularlos, lo que obliga a mantener una revisión permanente de los instrumentos legales, los criterios judiciales y las prácticas institucionales que orientan su utilización.

La criminalística ha incorporado históricamente nuevos conocimientos para responder a formas cambiantes de la delincuencia. La inteligencia artificial representa una etapa más de esa evolución y ofrece oportunidades importantes para fortalecer la investigación criminal. No obstante, el verdadero reto no consiste únicamente en desarrollar herramientas cada vez más sofisticadas, sino en garantizar que su utilización contribuya al acceso a la justicia, a la protección de las víctimas y al respeto irrestricto de los derechos humanos. Comprender cómo funcionan estas tecnologías, promover una ciudadanía digital informada y formar especialistas capaces de utilizarlas con responsabilidad constituye una condición indispensable para que la innovación tecnológica fortalezca la justicia sin perder de vista que, detrás de cada dato, cada algoritmo y cada sistema de vigilancia, siempre existen personas cuya dignidad y cuyos derechos deben permanecer en el centro de toda investigación.



## Referencias bibliográficas

Aguilar Rivera, O. (2025). *El impacto a los derechos humanos ante la vigilancia de la inteligencia artificial* [Doctorado, Universidad Nacional Autónoma de México].  
<https://ru.dgb.unam.mx/server/api/core/bitstreams/693e0966-eea1-4b3a-ad81-2119a136af5f/content>

**Cuando la tecnología aprende de nosotros...  
y nos vigila**

**When Technology Learns from Us...  
and Watches Us**

**Oswaldo Aguilar Rivera\***

*Instituto Nacional de Ciencias Penales, México*

oswaldoaguilarrivera@gmail.com

**Resumen:** La vida cotidiana deja una cantidad creciente de huellas digitales. Cada búsqueda en internet, cada recorrido registrado por un teléfono celular, cada fotografía compartida o cada dispositivo conectado genera información que, analizada de manera conjunta, puede revelar patrones sobre nuestras actividades, relaciones y formas de desplazarnos. Estas capacidades han transformado la manera en que la criminalística comprende la evidencia y han abierto nuevas posibilidades para investigar el cibercrimen mediante herramientas basadas en inteligencia artificial. A partir de ejemplos cercanos, este texto recorre la evolución de la vigilancia desde las formas tradicionales de observación hasta los sistemas actuales capaces de procesar grandes volúmenes de datos y generar inferencias sobre el comportamiento humano. En este recorrido se propone una mirada que permite comprender cómo la geolocalización, la inteligencia artificial y los dispositivos que utilizamos todos los días están modificando la producción de conocimiento útil para la investigación criminal. Finalmente, se invita a reflexionar sobre la importancia de desarrollar una cultura digital más consciente, capaz de aprovechar las posibilidades que ofrecen estas tecnologías sin perder de vista la protección de la privacidad, los derechos humanos y las libertades fundamentales.

**Palabras clave:** Inteligencia artificial; cibercriminalidad; vigilancia digital; geolocalización

**Abstract:** The expansion of artificial intelligence has transformed the ways in which the digital traces generated in everyday life are produced, recorded, and interpreted. Every internet search, geolocated movement, social media interaction, or connected device generates information that, when analyzed collectively, can reveal behavioral patterns and support criminal investigations. This article provides an accessible overview of these transformations from the perspective of criminalistics and surveillance studies. Drawing on everyday examples, it explains how technological developments have reshaped the ways information is observed, stored, and analyzed, creating new opportunities to reconstruct events and strengthen investigations related to cybercrime. It also introduces the concepts of the genealogy of surveillance, the genetics of surveillance, and Artificial Intelligence-Processed Geolocation Surveillance (VIPOGIA), proposed to better understand the evolution of surveillance systems and the role of artificial intelligence in processing spatial data. Finally, the article reflects on the importance of promoting informed and responsible uses of digital technologies, strengthening digital literacy regarding privacy, and developing institutional capacities that enable these technologies to contribute to criminal justice while safeguarding fundamental human rights.

**Keywords:** Artificial Intelligence; Cybercrime; Digital Surveillance; Geolocation

\*Doctor en Derecho por la Universidad Nacional Autónoma de México (UNAM). Es profesor del Instituto Nacional de Ciencias Penales (INACIPE) e integrante de la Línea de Investigación de Derecho e Inteligencia Artificial (LIDIA) del Instituto de Investigaciones Jurídicas de la UNAM. Sus investigaciones se centran en la inteligencia artificial, la vigilancia digital, el derecho penal y los derechos humanos.

## Cómo citar:

Aguilar Rivera, O. (2026). Cuando la tecnología aprende de nosotros... Y nos vigila. *El Mundo de la Criminalística*, 1, 40-55.



# Entre fraudes, datos, pantallas e internet:

## Un acercamiento a la cibercriminalidad en México

José María Salazar García

Una llamada que aparenta provenir del banco, un mensaje que solicita actualizar una contraseña, una cuenta de redes sociales que ha sido suplantada o la amenaza de publicar fotografías privadas son situaciones cada vez más frecuentes. Aunque suelen aparecer como hechos aislados, todos forman parte de un mismo fenómeno: la cibercriminalidad.

La expansión de las tecnologías digitales ha modificado profundamente la forma en que las personas trabajan, estudian, realizan operaciones financieras, se comunican e interactúan con instituciones públicas y privadas. Ese mismo proceso también ha transformado la manera en que se cometen diversos delitos. Hoy, una computadora, un teléfono inteligente o una plataforma digital pueden servir para obtener información personal, engañar a una víctima, difundir contenido íntimo sin autorización o incluso afectar el funcionamiento de servicios estratégicos.

Sin embargo, cuando se habla de estos casos suele pensarse únicamente en ataques informáticos o en personas que vulneran sistemas de cómputo. Esta imagen resulta limitada. La delincuencia en los entornos digitales comprende una variedad mucho mayor de conductas y plantea desafíos que no pueden entenderse únicamente desde la tecnología. También involucra la forma en que se construyen las leyes, la capacidad de las instituciones para investigar estos hechos y el equilibrio entre la seguridad y la protección de los derechos de las personas.

El propósito de este artículo es examinar cómo debe entenderse la cibercriminalidad en México, mostrando que se trata de un fenómeno que rebasa la comisión de delitos mediante tecnologías digitales e involucra desafíos relacionados con el marco jurídico, las capacidades institucionales, la cooperación internacional y la protección de los derechos humanos.







## Mismos delitos, entornos diferentes

Con frecuencia se afirma que internet creó nuevas formas de delincuencia. En realidad, muchas de las conductas que hoy asociamos con la cibercriminalidad existían mucho antes del desarrollo de las tecnologías digitales. El fraude, la extorsión, la falsificación documental, la intervención de comunicaciones privadas o la violación de la intimidad no surgieron con las computadoras. Lo que cambió fue el escenario donde pueden cometerse, la velocidad con la que se ejecutan, el número de personas que pueden resultar afectadas y la dificultad para investigar a quienes las realizan.

Este cambio también modificó la manera en que el derecho comenzó a describir estos fenómenos. Como señalan Alcalá y Meléndez (2023), una de las primeras aproximaciones fue la noción de delito informático. Los autores recuperan la definición propuesta por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que lo entiende como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático y/o transmisiones de datos” (p.3). Asimismo, retoman la propuesta de Téllez (2004), para quien estas conductas son aquellas en las que las computadoras constituyen el instrumento o el fin del delito. A partir de ambas definiciones, Alcalá y Meléndez observan que los dispositivos tecnológicos deben entenderse principalmente como el vehículo mediante el cual se desarrolla la conducta ilícita, más que como el bien jurídico que busca protegerse.

Conforme internet dejó de ser únicamente una herramienta para el procesamiento de información y se convirtió en un espacio donde se realizan actividades económicas, educativas, laborales y sociales, estas definiciones comenzaron a ampliarse. Por ello, vale la pena pensar en la propuesta de Romeo quien menciona a la cibercriminalidad como:

“el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (Romeo, 2006, en Alcalá & Meléndez, 2023, p.4).





La diferencia no es menor. Mientras las primeras definiciones concentraban su atención en las computadoras y los sistemas informáticos, ésta última propuesta de incorpora el entorno digital como espacio donde circula información que puede ser apropiada, modificada, difundida o utilizada de manera ilícita. En consecuencia, el problema deja de limitarse al funcionamiento de un equipo tecnológico y alcanza bienes jurídicos tan diversos como el patrimonio, la identidad, la privacidad, las comunicaciones o la intimidad.

Esta evolución conceptual ayuda a comprender por qué actualmente resulta más útil hablar de cibercriminalidad que de un único delito informático. La primera expresión permite reconocer que el fenómeno abarca un conjunto de conductas muy diversas, cuyas consecuencias trascienden el ámbito tecnológico y alcanzan múltiples derechos y bienes jurídicos. Esta diversidad también se refleja en la legislación mexicana, donde las conductas asociadas a la cibercriminalidad no se encuentran concentradas en una sola figura penal, sino distribuidas en distintos ordenamientos. En el cuadro 1, pueden verse algunas tipologías de este tipo de delitos.



## Cuadro 1. Características de los delitos informáticos

|                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Revelación de secretos</b>       | <ul style="list-style-type: none"> <li>• Difundir o revelar información confidencial o comunicación privada sin consentimiento y con perjuicio, y revelar información científica, industrial o comercial de la fuente que la generó</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|  <b>Violencia de correspondencia</b> | <ul style="list-style-type: none"> <li>• Abrir, interceptar o intervenir en forma dolosa comunicación privada (escrita, electrónica, magnética, óptica o informática).</li> <li>• Revelar, divulgar o utilizar indebidamente información o imágenes intervenidas sin consentimiento</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|  <b>Acceso informático indebido</b>  | <ul style="list-style-type: none"> <li>• Acceder a información en un aparato para el procesamiento o almacenamiento de datos o interferir el funcionamiento de un sistema, programa, base de datos o archivo informático, sin autorización</li> <li>• Acceder a imágenes o videos referentes a la genitalidad o actos sexuales, sin permiso del propietario</li> <li>• Acceder, modificar, destruir, copiar o provocar pérdida de información contenida en sistemas de videovigilancia que permiten la protección, visualización, transmisión, registro y almacenamiento de información. Ubicar, instalar, utilizar y operar sistemas de videovigilancia para grabar o captar imágenes en lugares, equipamiento, mobiliario, vía o espacio público, sin autorización, o aviso a las autoridades competentes</li> <li>• Atacar, destruir, robar, sabotear física e intencionalmente cualquier equipo de videovigilancia y su estructura que pertenezca a instituciones policiales, de seguridad pública y procuración de justicia</li> </ul> |
|  <b>Suplantación de identidad</b>  | <ul style="list-style-type: none"> <li>• Usurpar o sustituir a otra persona por cualquier medio, utilizando sin consentimiento sus datos personales con fines ilícitos o lucrativos</li> <li>• Asumir, apropiarse o utilizar la identidad de una persona física o jurídica</li> <li>• Transferir, poseer o utilizar datos identificativos de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita</li> <li>• Valerse de la homonimia, parecido físico o similitud de voz</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                                                                     |                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Violación a la intimidad</b> | <ul style="list-style-type: none"> <li>• Divulgar, compartir, distribuir, comercializar o amenazar con publicar información personal, privada o confidencial de una persona, imágenes, audios o videos, de contenido íntimo, erótico o sexual, impreso o digital</li> <li>• Condicionar el bloqueo de la difusión del contenido o se pretenda obtener un beneficio económico con la publicación o difusión del material</li> </ul>            |
|    | <b>Hostigamiento</b>            | <ul style="list-style-type: none"> <li>• Captar imágenes o registro audiovisual del cuerpo de otra persona o de alguna parte sin consentimiento y con carácter erótico sexual</li> </ul>                                                                                                                                                                                                                                                      |
|    | <b>Ciber acoso</b>              | <ul style="list-style-type: none"> <li>• Hostigar, amenazar o enviar contenido no requerido en una o más ocasiones por medio de cualquier espacio digital y cause un daño personal</li> </ul>                                                                                                                                                                                                                                                 |
|   | <b>Pornografía infantil</b>     | <ul style="list-style-type: none"> <li>• Fotografiar, videografiar, fijar, imprimir, exhibir, observar, comercializar, distribuir, difundir, almacenar, poseer u ofrecer actos de exhibicionismo corporal por una o varias personas menores de 18 años de edad, o personas que no tienen capacidad para comprender el hecho o resistirlo</li> </ul>                                                                                           |
|  | <b>Fraude informático</b>       | <ul style="list-style-type: none"> <li>• Obtener ilícitamente una cosa o alcanzar un lucro indebido, engañando o aprovechándose del error o la ignorancia; por cualquier medio digital</li> </ul>                                                                                                                                                                                                                                             |
|  | <b>Robo informático</b>         | <ul style="list-style-type: none"> <li>• Aprovechase de energía eléctrica, servicio telefónico, de Internet o de imagen televisiva, sin consentimiento. Adquirir, comercializar o poseer uno o más dispositivos electrónicos con capacidad de conectarse a internet de manera inalámbrica</li> </ul>                                                                                                                                          |
|  | <b>Extorsión</b>                | <ul style="list-style-type: none"> <li>• Obtener un lucro causando un perjuicio patrimonial a la víctima, al obligarlo, mediante uso de la fuerza física o moral, a hacer, tolerar o dejar de hacer algo</li> </ul>                                                                                                                                                                                                                           |
|  | <b>Falsificación</b>            | <ul style="list-style-type: none"> <li>• Suplantar, alterar, enajenar, destruir u ocultar cualquier clase de sellos, marcas, llaves, boletos, contraseñas, troqueles o cuños oficiales o particulares o uso no autorizado de los mismos</li> <li>• Alterar un documento público o privado, o cualquier dispositivo electrónico en forma de tarjeta plástica, o imitar los originales, obteniendo un beneficio o provocando un daño</li> </ul> |

Fuente: Alcalá y Meléndez, 2023, pp. 9 y 10.



La revisión realizada por Alcalá y Meléndez, muestra que bajo esta categoría conviven conductas tan distintas como la revelación de secretos, la intervención de comunicaciones privadas, el acceso indebido a sistemas informáticos, la suplantación de identidad, la violación de la intimidad, el ciberacoso, el fraude informático, la extorsión o la falsificación. Esta multiplicidad de conductas permite advertir que la cibercriminalidad no constituye un delito específico, sino un fenómeno que adopta múltiples formas y que afecta derechos igualmente diversos.

Por ello, se argumenta que más que un nuevo tipo de delito, la cibercriminalidad representa una nueva forma en que distintos delitos pueden manifestarse en una sociedad crecientemente digitalizada. Esta característica obliga a replantear la manera en que el derecho identifica, investiga y sanciona estas conductas. En consecuencia, el desafío ya no consiste únicamente en reconocer nuevas modalidades delictivas, sino en construir un marco normativo que permita responder de manera coherente a un fenómeno cuya complejidad rebasa las categorías jurídicas tradicionales.

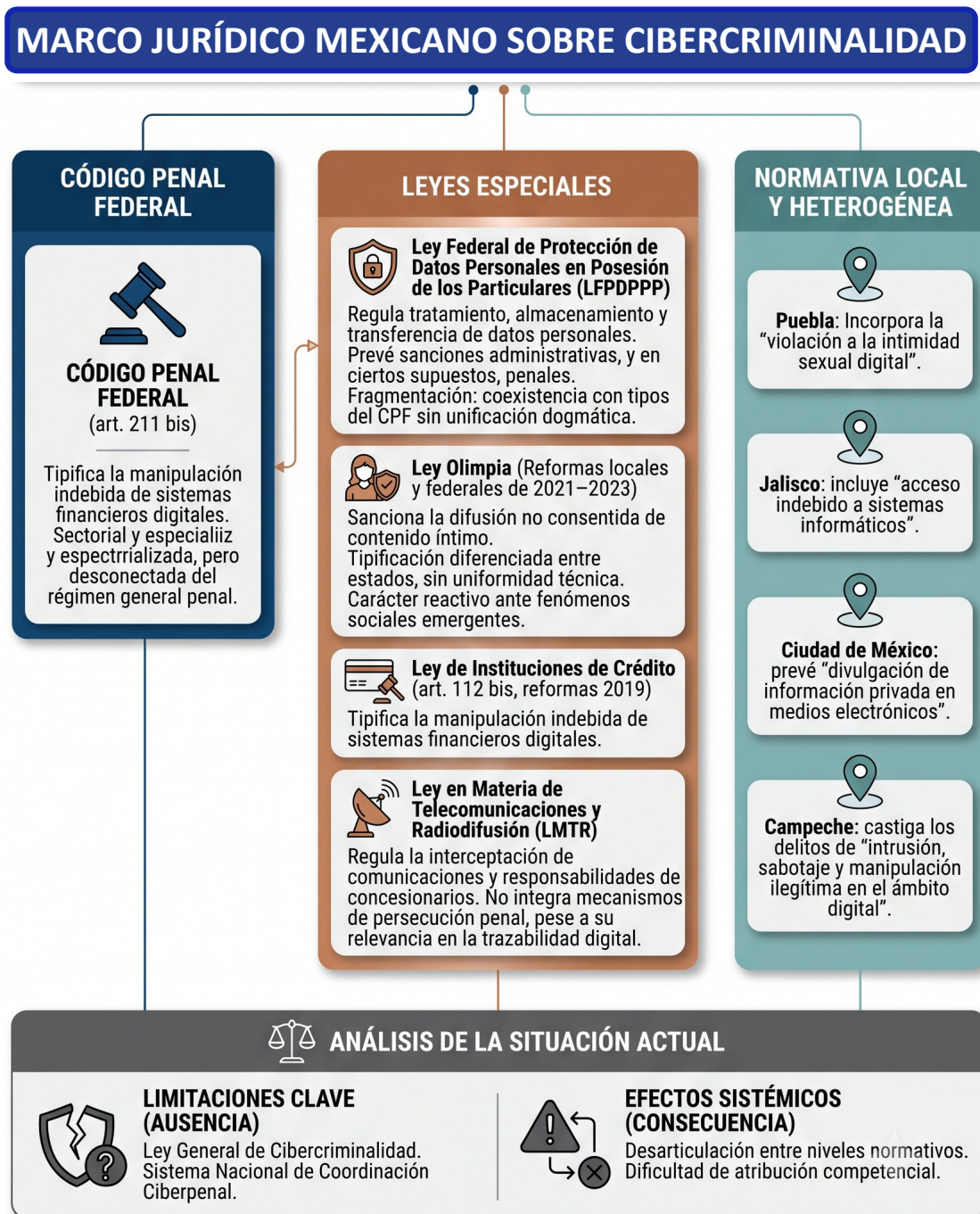
## *¿Está preparado el marco jurídico mexicano?*

Reconocer la diversidad de conductas que integran la cibercriminalidad conduce a una pregunta inevitable: ¿el marco jurídico mexicano cuenta con las herramientas necesarias para enfrentarlas? La respuesta no depende únicamente de la existencia de leyes que sancionen estos delitos, sino también de la forma en que dichas normas se articulan entre sí y de la capacidad de las instituciones para aplicarlas de manera coordinada.

En el ámbito internacional, el principal referente es el Convenio de Budapest sobre la Ciberdelincuencia, considerado el instrumento más importante para la cooperación penal frente a los delitos informáticos. Como explica Gala (2026), este tratado establece estándares mínimos para la tipificación de conductas relacionadas con la cibercriminalidad y mecanismos de colaboración entre los Estados, particularmente en investigaciones donde la evidencia digital o las personas involucradas se encuentran en distintos países. A este instrumento se suma el Segundo Protocolo Adicional, orientado a fortalecer la obtención de pruebas electrónicas y la cooperación internacional, así como la reciente Convención de las Naciones Unidas contra la Ciberdelincuencia, que amplía las obligaciones de los Estados en materia de investigación, intercambio de información y asistencia jurídica internacional (Gala, 2026).

En contraste con esta tendencia internacional, México aún no forma parte del Convenio de Budapest. Aunque el país ha desarrollado distintas disposiciones para atender conductas relacionadas con la cibercriminalidad, éstas se encuentran distribuidas entre leyes federales, códigos penales estatales y diversos ordenamientos especiales, lo que dificulta su aplicación como parte de una política integral. Esta relación, puede ejemplificarse en la Figura 1:

Figura 1. Marco jurídico mexicano en materia de cibercriminalidad



Fuente: Gala, 2026, p. 409.

A partir de este panorama, este autor sostiene que "el marco jurídico mexicano carece de una estructura sistemática unificada para abordar la cibercriminalidad" (Gala, 2026, p.409). En su análisis, la coexistencia de normas penales, administrativas y locales sin una articulación dogmática compromete tanto la aplicación del principio de legalidad como la eficacia de los procedimientos de investigación y persecución de estos delitos.





INFORME DE RED

EVIDENCIA DE CIBER CRIMINALIDAD

FISCALÍA DE CIBERCRIMEN

EVIDENCIA DIGITAL

ROBO DE IDENTIDAD

LIC. ARTURO RAMÍREZ  
COORDINADOR



Esta fragmentación tiene consecuencias prácticas. Una misma conducta puede involucrar la protección de datos personales, la intervención de comunicaciones privadas, delitos patrimoniales, violencia digital o acceso indebido a sistemas informáticos, materias que en México suelen encontrarse reguladas por disposiciones diferentes. En este contexto, la dificultad no radica únicamente en tipificar nuevas conductas, sino en coordinar un conjunto de normas e instituciones que fueron diseñadas para responder a problemas específicos y no necesariamente a un fenómeno transversal como la cibercriminalidad.

En este escenario, el desafío para México no consiste únicamente en incorporar nuevos delitos al marco legal o endurecer las sanciones existentes. La propia naturaleza de la cibercriminalidad exige respuestas coordinadas entre distintos órdenes de gobierno, instituciones y sectores que permitan prevenir, investigar y sancionar conductas cuya complejidad rebasa las fronteras territoriales y las categorías jurídicas tradicionales. Por ello, además de contar con un marco normativo coherente, resulta indispensable preguntarse cómo se están construyendo las políticas públicas y las capacidades institucionales necesarias para enfrentar este fenómeno.

## ¿Más leyes son suficientes?

La existencia de un marco jurídico constituye apenas uno de los componentes necesarios para enfrentar la cibercriminalidad. Contar con normas que tipifiquen determinadas conductas no garantiza, por sí mismo, que éstas puedan prevenirse, investigarse o sancionarse de manera efectiva. También es necesario definir quiénes participan en esa tarea, cómo se coordinan las instituciones y qué capacidades requieren para responder a un fenómeno que evoluciona al mismo ritmo que las tecnologías digitales.

Precisamente esta pregunta guía el trabajo de Aguilar y Quechol (2025), quienes analizaron dieciocho iniciativas legislativas presentadas en México entre 2019 y 2023 para identificar la manera en que el país ha concebido la ciberseguridad. Su investigación parte de señalar que las propuestas legislativas mexicanas han privilegiado una visión centrada en la seguridad nacional y la seguridad pública, dejando en segundo plano otros elementos indispensables para construir una política integral en la materia. Los resultados obtenidos respaldan esta hipótesis y muestran que la mayoría de las iniciativas se orientan a fortalecer las capacidades cibernéticas del Estado.

Sin embargo, los autores advierten que este enfoque presenta una limitación importante. Aunque reconoce el papel del Estado en la protección del ciberespacio, presta menor atención a la colaboración con otros actores que también participan en la prevención y atención de los riesgos digitales. De acuerdo con su análisis, las iniciativas revisadas muestran una ausencia de mecanismos claros de coordinación y gobernanza, a pesar de que organismos internacionales como la Unión Internacional de Telecomunicaciones (UIT), la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) han insistido en la necesidad de construir modelos de cooperación entre gobiernos, empresas, academia y sociedad civil.



Esta ausencia de una perspectiva colaborativa tiene implicaciones que van más allá de la organización administrativa del Estado. Como señalan Aguilar y Quechol (2025), aspectos como la protección de los derechos humanos, las asociaciones público-privadas, la protección de infraestructuras críticas, la cooperación regional e internacional, la formación de especialistas en ciberseguridad y la investigación sobre tecnologías emergentes aparecen de manera limitada o, en algunos casos, están ausentes de las iniciativas analizadas.

En otras palabras, la cibercriminalidad difícilmente puede enfrentarse únicamente desde una lógica punitiva o de seguridad nacional. Se trata de un fenómeno que involucra sistemas financieros, empresas tecnológicas, universidades, centros de investigación, organismos internacionales y millones de personas que utilizan diariamente servicios digitales. Esto significa que la eficacia de una política de ciberseguridad depende tanto de las leyes como de la capacidad para articular a estos actores alrededor de objetivos comunes.

## ***El reto también está en las capacidades institucionales***

La rapidez con la que evolucionan las tecnologías digitales plantea un desafío adicional para las instituciones encargadas de prevenir e investigar la cibercriminalidad. Las leyes constituyen un elemento indispensable, pero difícilmente pueden aplicarse de manera efectiva si no existen capacidades técnicas, recursos humanos especializados y mecanismos de cooperación que permitan responder a un fenómeno en constante transformación. En este sentido, Aguilar y Quechol (2025) advierten que las iniciativas legislativas analizadas concentran buena parte de sus esfuerzos en fortalecer las capacidades del Estado desde una perspectiva de seguridad pública y seguridad nacional. Sin embargo, los autores señalan que esta visión deja en segundo plano aspectos igualmente relevantes, como la formación de especialistas, la investigación científica, el desarrollo tecnológico, la cooperación entre instituciones y la participación de actores distintos al gobierno en la construcción de la ciberseguridad.

Esta preocupación adquiere mayor relevancia cuando se observan las capacidades disponibles en el país. De acuerdo con el estudio “Radiografía del talento digital: Especialización, brechas y oportunidades en ciberseguridad”, citado por Riquelme (2026), México requiere alrededor de 83 mil especialistas en ciberseguridad, pero dispone únicamente de cerca de seis mil profesionales con las competencias necesarias para atender esa demanda. La diferencia representa una brecha estimada de 77 mil especialistas, indispensable para proteger empresas, instituciones financieras, gobiernos e infraestructuras críticas.

Paradójicamente, el problema no parece estar únicamente en la cantidad de personas egresadas de carreras relacionadas con las tecnologías de la información. El mismo estudio señala que el país forma un número suficiente de profesionales para proyectar un superávit en este campo; sin embargo, sólo una parte logra incorporarse a funciones técnicas especializadas, mientras que muchos terminan desempeñándose en actividades administrativas, comerciales, educativas o de servicios.







A esta situación se suma otro fenómeno emergente. Gutiérrez (2026) indica que el conocimiento especializado en desarrollo de software, análisis de vulnerabilidades e infraestructura tecnológica se ha convertido en un recurso altamente disputado. Empresas, instituciones públicas y organizaciones dedicadas al cibercrimen compiten por atraer perfiles con habilidades avanzadas, lo que convierte al talento digital en un componente estratégico para la seguridad de un país. Aunque, también las redes criminales han comenzado a absorber a estos profesionales, derivado de la falta de oportunidades en el campo laboral de estos expertos en el país.

La necesidad de fortalecer estas capacidades resulta aún más evidente si se considera la magnitud de las amenazas digitales. De acuerdo con información difundida por IQSEC, durante el primer semestre de 2025 se registraron en México más de 40 mil millones de intentos de ciberataques, cifra que ubicó al país entre los más vulnerables de América Latina (Becerra, 2025). Aunque estos registros no equivalen al número de delitos consumados, sí ilustran la intensidad del entorno digital en el que operan diariamente instituciones públicas, empresas y personas usuarias de tecnologías.

Estos datos muestran que la cibercriminalidad no puede enfrentarse únicamente mediante reformas legales. También requiere inversión en formación especializada, investigación, innovación tecnológica y mecanismos permanentes de cooperación entre el sector público, la iniciativa privada y las instituciones académicas. En otras palabras, la seguridad en el entorno digital depende tanto de las normas como de las capacidades que una sociedad es capaz de construir para hacerlas efectivas.

## Conclusiones

La cibercriminalidad constituye un ejemplo de cómo las transformaciones tecnológicas modifican las dinámicas sociales a un ritmo que suele superar la capacidad de respuesta de las instituciones. Las formas de interacción, intercambio de información, comunicación y actividad económica han cambiado profundamente en las últimas décadas y, con ellas, también lo han hecho las modalidades mediante las cuales pueden cometerse distintas conductas delictivas. En este escenario, el derecho y la investigación criminal enfrentan el desafío permanente de adaptarse a realidades que evolucionan con mayor rapidez que los procesos legislativos, los diseños institucionales y, en ocasiones, las propias categorías jurídicas con las que tradicionalmente se ha comprendido el delito.

Esta situación no significa que el derecho se encuentre condenado a actuar siempre de manera reactiva. Por el contrario, pone de manifiesto la necesidad de que las respuestas jurídicas incorporen una comprensión más amplia de los procesos sociales y tecnológicos que configuran la vida contemporánea. La cibercriminalidad no representa únicamente un conjunto de nuevos riesgos asociados al uso de internet; también evidencia que los espacios donde se ejercen derechos, se desarrollan relaciones económicas y se construyen vínculos sociales se han desplazado, en buena medida, hacia entornos digitales.



En este contexto, fortalecer la respuesta frente a la cibercriminalidad implica mucho más que actualizar tipos penales o incorporar nuevas herramientas de investigación. También requiere desarrollar capacidades institucionales, formar especialistas, promover la cooperación entre los sectores público, privado y académico, e impulsar mecanismos de colaboración internacional acordes con un fenómeno que difícilmente reconoce fronteras. De igual manera, cualquier estrategia de ciberseguridad debe preservar el equilibrio entre la protección frente a las amenazas digitales y el respeto a los derechos humanos, particularmente aquellos relacionados con la privacidad, la protección de datos personales, la libertad de expresión, el acceso a la información y el debido proceso.

La experiencia de la cibercriminalidad muestra que el derecho no puede entenderse como un sistema aislado de los cambios sociales, sino como un campo en constante adaptación frente a nuevas formas de interacción humana. En la medida en que la vida cotidiana continúa desplazándose hacia espacios digitales, también lo harán los desafíos para la investigación criminal, la procuración de justicia y el diseño de políticas públicas. Comprender este fenómeno desde una perspectiva integral representa, por tanto, una condición necesaria para construir respuestas que no sólo resulten eficaces frente al delito, sino también compatibles con una sociedad cada vez más conectada y con los derechos que deben garantizarse en ella.



## Referencias bibliográficas

- Aguilar Antonio, J. M., & Quechol Maciel, K. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023). *PAAKAT: revista de tecnología y sociedad*, 15(28). <https://doi.org/10.32870/pk.a15n28.892>
- Alcalá Casillas, M. G., & Meléndez Ehrenzweig, M. Á. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: revista de tecnología y sociedad*, 13(24), 1-37. <https://doi.org/10.32870/pk.a13n24.759>
- Becerra, J. (2025, noviembre 25). *México registró 40 mil millones de intentos de ciberataques en primer semestre del 2025*.
- La Jornada. <https://www.jornada.com.mx/noticia/2025/11/25/economia/mexico-registro-40-mil-millones-de-intentos-de-ciberataques-en-primer-semester-del-2025>
- Gala Rodríguez, L. A. (2026). La cibercriminalidad en México: Entre la dispersión normativa y la impunidad digital. *Revista Multidisciplinar Epistemología de las Ciencias*, 3(1), 399-429. <https://doi.org/10.71112/d3625c91>
- Gutiérrez, F. (2026, junio 25). *Cibercrimen intensifica disputa por talento digital*. El Economista. <https://www.eleconomista.com.mx/capital-humano/cibercrimen-intensifica-disputa-talento-digital-20260525-814935.html>
- Riquelme, R. (2026, mayo 13). *México necesita 83,000 especialistas en ciberseguridad, pero solo tiene 6,000*. El Economista.
- <https://www.eleconomista.com.mx/tecnologia/mexico-necesita-83-000-especialistas-ciberseguridad-6-20260513-813373.html>

**Entre fraudes, datos, pantallas e internet:  
Un acercamiento a la cibercriminalidad en México**

**Between Fraud, Data, Screens, and the Internet:  
An Approach to Cybercrime in Mexico**

**José María Salazar García**  
*Investigador independiente*  
josemariasalazar1@hotmail.com

**Resumen:** La expansión de las tecnologías digitales ha transformado la manera en que las personas se comunican, realizan actividades económicas e interactúan con instituciones públicas y privadas. Este proceso también ha modificado las formas en que se desarrollan diversas conductas delictivas, dando lugar a un fenómeno que rebasa la idea tradicional de los delitos informáticos. El presente artículo examina cómo debe entenderse la cibercriminalidad en México, mostrando que comprende una amplia diversidad de conductas que afectan bienes jurídicos como el patrimonio, la identidad, la privacidad, las comunicaciones y la libertad sexual. A partir de una revisión de literatura especializada y de instrumentos normativos nacionales e internacionales, se analiza la evolución conceptual del fenómeno, la fragmentación del marco jurídico mexicano y los desafíos que enfrenta el país para construir una política integral de ciberseguridad. Asimismo, se discute la necesidad de fortalecer las capacidades institucionales, la formación de especialistas y los mecanismos de cooperación entre los sectores público, privado y académico, sin perder de vista la protección de los derechos humanos en los entornos digitales. Finalmente, se sostiene que la cibercriminalidad constituye un ejemplo de cómo las transformaciones sociales y tecnológicas avanzan con mayor rapidez que las respuestas jurídicas e institucionales, planteando nuevos retos para el derecho y la investigación criminal.

**Palabras clave:** Cibercriminalidad; ciberseguridad; delitos informáticos; derecho digital.

**Abstract:** The expansion of digital technologies has transformed the ways people communicate, conduct economic activities, and interact with public and private institutions. This process has also reshaped the ways in which criminal activities are carried out, giving rise to a phenomenon that extends beyond the traditional notion of computer-related crime. This article examines how cybercrime should be understood in Mexico, arguing that it encompasses a wide range of offenses affecting legal interests such as property, identity, privacy, communications, and sexual freedom. Drawing on specialized literature as well as national and international legal frameworks, the article discusses the conceptual evolution of cybercrime, the fragmentation of the Mexican legal framework, and the challenges involved in developing a comprehensive cybersecurity policy. It also highlights the importance of strengthening institutional capacities, training cybersecurity specialists, and fostering cooperation among government, the private sector, and academia while safeguarding human rights in digital environments. Finally, the article argues that cybercrime illustrates how social and technological transformations often evolve more rapidly than legal and institutional responses, posing new challenges for law, criminal investigation, and public policy.

**Keywords:** Cybercrime; cybersecurity; computer crime; digital law

\*Maestro en Derecho con amplia trayectoria en procuración de justicia y seguridad pública. Se desempeñó como Policía Federal de Investigación y Agente del Ministerio Público de la Federación, con experiencia especializada en investigación criminal, integración de carpetas de investigación y litigación en el sistema penal acusatorio.

## Cómo citar:

Salazar García, J. M. (2026). Entre fraudes, datos, pantallas e internet: Un acercamiento a la cibercriminalidad en México. *El Mundo de la Criminalística*, 1, 56-71.



# ¿Quién tiene tus datos?

## La vulneración de datos personales en Guatemala

Yarely Elizabeth Gómez Gómez

### Introducción

La protección de la información personal forma parte de los derechos que permiten salvaguardar la privacidad y la vida de las personas. Cada vez que un ciudadano proporciona su nombre, documento de identificación, domicilio, información bancaria o antecedentes médicos para realizar un trámite o acceder a un servicio, deposita en instituciones públicas o privadas la confianza de que esos datos serán utilizados únicamente para la finalidad con la que fueron recabados. Esa confianza resulta indispensable para el funcionamiento de numerosos servicios, pero también exige que la información permanezca protegida frente a accesos, usos o divulgaciones no autorizadas.

El desarrollo de las tecnologías de la información ha multiplicado las formas en que esos datos son almacenados, compartidos y procesados. Al mismo tiempo, han surgido nuevas modalidades para obtener información personal de manera ilícita, comercializar bases de datos o utilizar esos registros para cometer distintos delitos. Miró Llinares (2012) señala que el cibercrimen ha evolucionado al ritmo de los avances tecnológicos, incorporando conductas que aprovechan los sistemas informáticos para afectar bienes jurídicos que tradicionalmente habían permanecido fuera del entorno digital. En ese escenario, la información personal adquiere un valor que trasciende el ámbito administrativo y pasa a convertirse en un objetivo para distintas formas de delincuencia.

Guatemala, es un país que no está ajeno a esta realidad. El incremento en el uso de medios electrónicos para realizar actividades personales, comerciales y administrativas ha favorecido una mayor circulación de datos personales y, con ello, nuevas preocupaciones relacionadas con su protección. Aunque en los últimos años se han presentado iniciativas para regular esta materia y fortalecer el combate a los delitos informáticos, el país aún carece de una legislación integral que establezca principios, derechos y obligaciones específicos para el tratamiento de los datos personales.

El presente artículo analiza la vulneración de datos personales en Guatemala con el propósito de explicar por qué la protección de la información personal representa un componente esencial del derecho a la privacidad, identificar algunas de las formas en que estos datos pueden ser utilizados de manera indebida y reflexionar sobre la necesidad de fortalecer los mecanismos jurídicos destinados a garantizar este derecho frente a los riesgos que plantea el entorno digital.









## Datos personales y privacidad

La información personal acompaña a las personas a lo largo de prácticamente toda su vida. Registros civiles, expedientes escolares, historias clínicas, cuentas bancarias, contratos de telefonía, servicios de internet o plataformas digitales reúnen datos que permiten identificar a un individuo y conocer aspectos de su actividad cotidiana. En conjunto, esa información facilita el funcionamiento de instituciones y servicios, pero también hace visible la responsabilidad que implica su resguardo.

Desde el ámbito jurídico, los datos personales forman parte de la esfera privada de las personas y, por esa razón, su tratamiento debe responder a una finalidad legítima y respetar el derecho de cada individuo a decidir sobre el uso de la información que lo identifica. Osorio (2006) señala que la violación supone el quebrantamiento de un derecho reconocido por el ordenamiento jurídico. Trasladada al ámbito de la información personal, esta idea permite comprender que el acceso o utilización de datos sin autorización no representa únicamente una irregularidad administrativa, sino una posible afectación a derechos cuya protección corresponde garantizar al Estado.

La importancia de este derecho puede apreciarse en situaciones cotidianas. Al abrir una cuenta bancaria, solicitar una tarjeta de descuento, contratar un servicio telefónico o llenar un expediente médico, las personas proporcionan información con la expectativa de que será utilizada únicamente para los fines que justificaron su entrega. Esa expectativa forma parte de la relación de confianza que debe existir entre la ciudadanía y las instituciones responsables de administrar los datos personales.

El valor de esta información explica por qué su protección ha adquirido una importancia creciente. Además de permitir la identificación de las personas, los datos personales pueden revelar condiciones de salud, hábitos de consumo, actividades económicas, relaciones familiares o aspectos patrimoniales. Esa información resulta útil para la prestación de servicios, pero también puede generar beneficios económicos cuando se obtiene o comercializa de manera ilícita. De ahí que los datos personales hayan pasado a formar parte de los recursos más buscados por distintas modalidades de ciberdelincuencia.

La protección de la privacidad, por tanto, no depende únicamente de la existencia de sistemas informáticos seguros. También requiere que la información permanezca vinculada a la finalidad para la que fue recabada y que cualquier tratamiento distinto cuente con fundamento legal o con el consentimiento de su titular. Cuando estas condiciones dejan de cumplirse, la información personal comienza a circular fuera de los espacios para los que fue proporcionada y aparecen riesgos que trascienden la pérdida de confidencialidad para afectar otros derechos de las personas.



## Vulneración de datos personales

La protección de los datos personales parte de un principio sencillo: la información que una persona proporciona para un determinado fin no debe ser utilizada para otro distinto sin su conocimiento o consentimiento. Cuando ese principio se incumple, se produce una vulneración que puede afectar la privacidad, la intimidad y otros derechos relacionados con la vida personal.

Desde el punto de vista jurídico, la vulneración implica una transgresión a un derecho previamente reconocido. Ossorio (2006) explica que la violación supone el quebrantamiento de una disposición jurídica o de un derecho protegido por el ordenamiento legal. Aplicada al tratamiento de datos personales, esta idea permite comprender que el problema no radica únicamente en que la información sea conocida por terceros, sino en que sea obtenida, utilizada o difundida al margen de las condiciones bajo las cuales fue proporcionada.

En la práctica, la vulneración de datos personales puede presentarse de distintas maneras. Una de las más frecuentes consiste en el acceso ilícito a bases de datos mediante herramientas informáticas que permiten extraer información almacenada por instituciones públicas o privadas. También puede producirse cuando una organización comparte datos con terceros sin autorización, cuando la información es utilizada para fines diferentes a los originalmente previstos o cuando las medidas de seguridad resultan insuficientes para impedir el acceso de personas no autorizadas. En cualquiera de estas situaciones, la información pierde la protección que justificó su recopilación y queda expuesta a usos que escapen del control de su titular.

El desarrollo de las tecnologías digitales ha ampliado las posibilidades para que estas conductas ocurran. El uso del correo electrónico, las redes sociales, las aplicaciones móviles y los servicios financieros en línea ha facilitado nuevas formas de obtener información mediante engaños, suplantación de identidad o accesos indebidos a sistemas informáticos. Como señala Miró Llinares (2012), el cibercrimen comprende un conjunto de conductas que aprovechan las tecnologías digitales para afectar bienes jurídicos previamente protegidos por el derecho, entre ellos la privacidad y la información personal.

En Guatemala, esta problemática se manifiesta en diferentes espacios donde diariamente se recopilan datos personales. Instituciones financieras, empresas de telefonía, establecimientos comerciales, centros de salud y dependencias públicas administran grandes volúmenes de información necesarios para el desarrollo de sus actividades. Sin embargo, cuando esos registros son utilizados sin autorización o terminan circulando fuera de los fines para los que fueron obtenidos, las personas pierden el control sobre información que forma parte de su vida privada. Esta situación favorece prácticas como la comercialización ilegal de bases de datos, el contacto no autorizado con usuarios o el aprovechamiento de información personal para la comisión de distintos hechos delictivos.

La vulneración de datos personales no siempre produce un daño visible de manera inmediata. En muchas ocasiones sus efectos aparecen tiempo después, cuando la información comienza a utilizarse para fines distintos de aquellos que motivaron su recopilación. Por esa razón, comprender las consecuencias derivadas del uso indebido de los datos personales resulta indispensable para dimensionar la importancia de fortalecer su protección.







```
faces link addresses  
address> dev <dev> : change link address of device  
faces ip addresses  
y <dev> : add ip address to device  
es  
IPv6 routes  
CIDR> via <gateway> dev <dev> : add new route  
ame> mode <mode> local <ip> remote <ip> : create tunnel  
multicast memberships  
ache  
listening sockets  
l open network sockets on the system  
s/net/ipv4/ip_forward : activate packet forwarding  
ow file type  
ow all filesystem information about the file  
of previous word  
of previous WORD  
beginning of line ( column 1 ), enter insert mode  
acter in the middle of the screenline  
or line at top of window  
or line at middle of window  
or line at bottom of window  
te fold for <motion> text ( min 2 lines  
close fold  
create fold around tags  
 : split vertically and  
vertical split  
ove to window at rel  
l panel users in
```

```
filesystem:  
cat /etc/fstab : show mounted filesystems  
lsof <file> : show programs using <file>  
mkfs.ext4 <deviceFile> : make ext4 filesystem on device accessed by <  
mkfs.ntfs <deviceFile> : make ntfs filesystem on device accessed by <  
df <file> -h : show partition size, used space, free space, mounting  
the partition where <file> is  
System :  
/proc, /sys, /proc/sys : VFSs containing useful information on process  
memory and system, permits expert fine-tuning of the last.  
lshw : list all hardware  
lshw -C <class> : list all <class> hardware  
lspci : list all pci devices  
lsusb : list all usb devices  
dmesg : prints kernel logs, hardware and tech talk  
Keyboard :  
dumpkeys > keys.map : dump kernel keyboard map to file keys.map  
loadkeys keys.map : load keyboard map into kernel  
VTs, TTYS and X :  
openvt command : launch command on first VT available  
chvt N : change current foreground VT to N, created if not existent  
deallocvt : kill all unused VTs  
startx -- :2 : launch X server on display :2, with graphic environment  
xinit -- :2 : launch X server on display :2, with an xterm  
xauth : view/edit .Xauthority file  
xhost + : disable all X server, use with care ( or not at all  
Screen :  
C-a | : vertical split  
C-a <T> : switch  
C-a X : kill all  
C-a Q : kill all  
C-a N : show the  
C-a < : like way to move and
```



## Consecuencias del uso indebido de la información

La vulneración de datos personales trasciende la pérdida de confidencialidad de la información. Cuando los datos son utilizados sin autorización, las personas dejan de tener control sobre quién accede a ellos y con qué finalidad serán empleados. Esta situación puede derivar en fraudes, suplantación de identidad, extorsiones o en otras conductas que afectan tanto el patrimonio como la seguridad de la ciudadanía.

Las consecuencias también pueden manifestarse en otros ámbitos de la vida cotidiana. La utilización indebida de información financiera, laboral o relacionada con la salud puede generar prácticas discriminatorias, limitar el acceso a determinados servicios o facilitar decisiones basadas en información que debió permanecer bajo reserva. Por ello, la protección de los datos personales no solo busca resguardar la privacidad, sino evitar que la información sea utilizada para perjudicar a las personas.

En Guatemala, esta problemática también se refleja en la circulación no autorizada de bases de datos y en el uso de información personal para fines distintos de aquellos que motivaron su recopilación. Estas situaciones evidencian que la protección de los datos personales no depende únicamente de impedir accesos ilícitos a sistemas informáticos, sino también de garantizar un tratamiento responsable de la información por parte de quienes la administran.

La magnitud de estas consecuencias explica por qué la protección de los datos personales ocupa un lugar cada vez más importante dentro de la discusión jurídica. La necesidad de establecer reglas claras para el tratamiento de la información y mecanismos eficaces para prevenir su uso indebido forma parte de un debate que continúa abierto en Guatemala.

## Protección jurídica en Guatemala

La protección de los datos personales representa uno de los temas pendientes dentro del ordenamiento jurídico guatemalteco. Aunque la Constitución Política de la República reconoce derechos relacionados con la privacidad, la intimidad y la inviolabilidad de las comunicaciones, el país aún no cuenta con una legislación integral que regule el tratamiento de los datos personales y establezca obligaciones específicas para quienes los recopilan y administran.

La protección contra el ciberdelito en Guatemala no cuenta con una ley única y vigente, sino con una malla legal fragmentada que se apoya principalmente en reformas hechas al Código Penal en 1997, las cuales sancionan conductas básicas como la alteración de datos, destrucción de registros y piratería de software. Hace más de quince años, se presentaron distintas iniciativas legislativas orientadas a fortalecer la protección de la información personal y combatir los delitos informáticos. Entre ellas destaca, por ejemplo la Iniciativa de Ley 4055, presentada en 2009 ante el Congreso para crear la Ley de Delitos Informáticos, la iniciativa 4090-2009 donde se propone la Ley de Protección de Datos Personales; sin embargo, éstas aún se encuentran en espera. Aunque sobresalen normativas complementarias como la Ley de Firmas Electrónicas o la Ley de Acceso a la Información Pública, el



país carece de un marco moderno; de hecho, el Decreto 39-2022 (Ley contra la Ciberdelincuencia) quedó frenado en su aplicación práctica por temores de censura (Román, 2022). Actualmente, el debate jurídico se centra en actualizar el Código Penal para adherirse al Convenio de Budapest e impulsar nuevas iniciativas que castiguen delitos modernos como el fraude electrónico, el ransomware y el uso malicioso de deepfakes.

La ausencia de un marco jurídico integral plantea desafíos para las instituciones que diariamente recopilan información de la ciudadanía. Bancos, hospitales, centros educativos, empresas de telefonía y dependencias gubernamentales administran bases de datos que requieren medidas de seguridad, procedimientos claros para el tratamiento de la información y mecanismos que permitan responder de manera oportuna ante posibles vulneraciones.

El fortalecimiento de la protección jurídica no depende únicamente de la expedición de nuevas normas. También requiere políticas institucionales que promuevan el manejo responsable de la información, mecanismos eficaces de supervisión y una cultura de respeto hacia la privacidad como parte del ejercicio de los derechos de las personas. En un entorno donde el intercambio de información es cada vez más frecuente, la protección de los datos personales demanda la participación conjunta del Estado, las instituciones y la propia ciudadanía.

## Conclusiones

La información personal forma parte de la esfera privada de las personas y su protección constituye una condición indispensable para el ejercicio de derechos como la privacidad, la intimidad y la autodeterminación informativa. En un entorno donde el intercambio de datos es cada vez más frecuente, garantizar que esa información sea utilizada únicamente para los fines que justificaron su recopilación representa una responsabilidad compartida entre las instituciones que la administran, el Estado y la propia ciudadanía.

La vulneración de datos personales demuestra que las consecuencias del uso indebido de la información trascienden el ámbito tecnológico. La obtención, circulación o comercialización no autorizada de datos puede facilitar fraudes, suplantaciones de identidad, extorsiones y otras conductas delictivas que afectan tanto el patrimonio como la seguridad de las personas. Por ello, la protección de los datos personales también constituye una medida de prevención frente a diversas modalidades de ciberdelincuencia.

En Guatemala, el crecimiento de los servicios digitales y el aumento en la circulación de información personal han puesto de manifiesto la necesidad de fortalecer la respuesta jurídica frente a este fenómeno. Si bien existen propuestas orientadas a regular la protección de los datos personales y los delitos informáticos, todavía persiste el desafío de consolidar un marco normativo integral que establezca derechos, obligaciones y mecanismos eficaces para el tratamiento de la información personal.

Proteger los datos personales significa resguardar uno de los bienes más sensibles de las personas: su identidad y la información que forma parte de su vida privada. Fortalecer su protección jurídica, promover una gestión responsable de las bases de datos y fomentar una cultura de respeto hacia la privacidad contribuirá no solo a garantizar un derecho fundamental, sino también a reducir las oportunidades para que la información personal sea utilizada como instrumento para la comisión de otros delitos.







## Referencias bibliográficas

- Miró Llinares, F. (2012). Capítulo II. *Tipos de cibercrimen y clasificación de los mismos. En El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* (pp. 47-115). Marcial Pons.
- Ossorio, M. (2006). *Diccionario de Ciencias Jurídicas, Políticas y Sociales*. Buenos Aires, Argentina: Heliasta.
- Román, J. (2022, septiembre 1). Congreso oficializa que se archiva el decreto 39-2022 que contenía la Ley contra la ciberdelincuencia. Prensa Libre. <https://www.prensalibre.com/guatemala/politica/congreso-oficializa-que-se-archiva-el-decreto-39-2022-que-contentia-la-ley-contra-la-ciberdelincuencia-breaking/>

### ¿Quién tiene tus datos?

#### La vulneración de datos personales en Guatemala

### Who Has Your Data?

#### Personal Data Breaches in Guatemala

**Yarely Elizabeth Gómez Gómez\***

Investigadora independiente

bufetejuridico958@hotmail.com

**Resumen:** La protección de los datos personales ha adquirido una importancia creciente debido al aumento en la circulación de información mediante tecnologías digitales y al uso cotidiano de servicios que requieren el tratamiento de datos personales. En Guatemala, este escenario ha favorecido la aparición de distintas formas de vulneración de la información, así como nuevos riesgos para la privacidad y la seguridad de las personas. El artículo analiza la problemática de la vulneración de datos personales desde una perspectiva jurídica y criminalística, explicando el valor de la información personal, las principales formas en que puede ser obtenida o utilizada de manera indebida y las consecuencias derivadas de su uso no autorizado. Asimismo, examina la situación del marco jurídico guatemalteco, caracterizado por la existencia de iniciativas legislativas y disposiciones dispersas que aún no conforman un sistema integral de protección de datos personales. Finalmente, se reflexiona sobre la necesidad de fortalecer las capacidades institucionales para garantizar un tratamiento responsable de la información y promover una cultura de respeto hacia la privacidad. La protección de los datos personales representa no solo una garantía para el ejercicio de derechos fundamentales, sino también una herramienta para prevenir diversas modalidades de ciberdelincuencia y fortalecer la confianza de la ciudadanía en las instituciones que administran información personal.

**Palabras clave:** Protección de datos personales; privacidad; ciberdelincuencia; Guatemala

**Abstract:** The protection of personal data has become increasingly important due to the growing circulation of information through digital technologies and the widespread use of services that require the processing of personal information. In Guatemala, this context has encouraged different forms of data misuse while creating new risks for privacy and individual security. This article examines the issue of personal data breaches from both legal and criminalistic perspectives. It explains the value of personal information, the main ways in which it may be unlawfully obtained or misused, and the consequences arising from unauthorized access and disclosure. The paper also discusses the current legal framework in Guatemala, highlighting that existing legislative initiatives and scattered legal provisions have not yet resulted in a comprehensive personal data protection system. Finally, it reflects on the need to strengthen institutional capacities to ensure the responsible management of personal information and to promote a culture of respect for privacy. Protecting personal data not only safeguards fundamental rights but also contributes to preventing different forms of cybercrime and strengthening public trust in the institutions responsible for managing personal information.

**Keywords:** Personal data protection; Privacy; Cybercrime; Guatemala

\* Licenciada en Ciencias Jurídicas y Sociales, con Maestría en Derecho Penal y Derecho Procesal Penal. Es doctoranda en Derecho Penal y Ciencias Penales por la Universidad Mariano Gálvez de Guatemala y cursa estudios doctorales en el Instituto Universitario de Alta Formación (IUAF). Se desempeña como abogada litigante, asesora legal en el sector asegurador y docente en la Universidad Da Vinci de Guatemala.

## Cómo citar:

Gómez Gómez Y. E. (2026). ¿Quién tiene tus datos? La vulneración de datos personales en Guatemala *El Mundo de la Criminalística*, 1, 72-83.



# Cuando el delito transita de escenarios análogos al espacio digital



## Una conversación con el Dr. Francisco Rodríguez Almirón

Durante buena parte del siglo XX, la criminalística se asoció principalmente con el estudio de escenas del crimen, el análisis de huellas dactilares, la balística o el examen de indicios biológicos. Esa imagen, ampliamente difundida por la literatura, el cine y la televisión, continúa formando parte del imaginario colectivo sobre el trabajo forense. Sin embargo, el desarrollo de las tecnologías digitales ha incorporado nuevos espacios donde también se producen conductas delictivas y donde las evidencias adquieren características distintas a las que tradicionalmente han estudiado las ciencias forenses.

En la actualidad, una parte de estas conductas ocurre en entornos digitales. Dispositivos electrónicos, redes de comunicación, plataformas digitales, servicios en la nube, criptomonedas o sistemas basados en inteligencia artificial forman parte de escenarios donde pueden cometerse fraudes, robos de información, extorsiones o ataques dirigidos contra personas e instituciones. En estos casos, la investigación requiere conocimientos especializados para identificar, preservar y analizar evidencias que no siempre tienen una manifestación física inmediata.

Este panorama también ha generado nuevas preguntas para el derecho, la criminalística y las ciencias forenses. La obtención de evidencia digital, la cooperación entre instituciones de distintos países, la regulación de tecnologías emergentes o la incorporación de herramientas informáticas en las investigaciones son algunos de los temas que actualmente forman parte de la discusión académica y profesional.

En este contexto, resulta importante comprender cómo cambian las formas de delincuencia, cuáles son las herramientas disponibles para investigarlas y qué desafíos enfrentan las instituciones encargadas de procurar e impartir justicia. Por estos motivos, en marzo de 2026, el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas (CESCIJUC), en colaboración con el Departamento de Derecho Penal de la Universidad de Granada, realizó la Jornada Internacional sobre Inteligencia Artificial y Ciberdelincuencia



El encuentro reunió a investigadores de ambas instituciones para dialogar sobre algunos de los cambios que experimentan la investigación criminal, el derecho penal y las ciencias forenses frente al desarrollo de las tecnologías digitales.

La entrevista que se presenta a continuación fue realizada al Dr. Francisco Rodríguez Almirón, profesor contratado doctor de la Universidad de Granada, cuya investigación se ha centrado en el estudio de la política criminal, el derecho penal y la ciberdelincuencia. A lo largo de la conversación, nuestro invitado reflexiona sobre la evolución de las formas de criminalidad, la necesidad de revisar los marcos jurídicos conforme aparece nuevos fenómenos delictivos, el valor de la cooperación internacional y la importancia de la formación especializada para quienes estudian o trabajan en este campo.

Las ideas del Dr. Rodríguez que se exponen a continuación, permiten observar que la ciberdelincuencia no constituye únicamente un conjunto de delitos cometidos mediante tecnologías digitales. También representa un ámbito de investigación donde convergen distintas disciplinas y donde las respuestas institucionales se construyen a partir de la colaboración entre especialistas, el intercambio de conocimientos y la actualización permanente de las capacidades técnicas y jurídicas.



# Entrevista

## ¿Cómo comenzó su interés por el estudio de la ciberdelincuencia?

**Dr. Francisco Rodríguez Almirón (DFRA):** Actualmente soy profesor contratado doctor en la Universidad de Granada. Soy doctor en Derecho y mi formación se orientó inicialmente hacia la política criminal y el derecho penal. Con el paso de los años, mi trayectoria de investigación se ha ido centrando en la ciberdelincuencia, principalmente porque se trata de un fenómeno que evoluciona con mucha rapidez y que está modificando la forma en que entendemos la criminalidad.

La sociedad cambia constantemente y las tecnologías forman parte de esa transformación. En consecuencia, el derecho penal también debe adaptarse para responder a nuevas formas de delincuencia. Si los sistemas jurídicos no evolucionan al mismo ritmo que estos fenómenos, inevitablemente aparecerán vacíos que dificultarán su prevención y persecución.

## ¿Qué papel deberían desempeñar actualmente los sistemas jurídicos para comprender este nuevo escenario?

**DFRA:** Lo primero es reconocer que el problema existe y comprender cómo está evolucionando. La ciberdelincuencia ya ocupa un lugar muy importante dentro de las estadísticas criminales porque, para muchos delincuentes, representa una actividad altamente rentable. Actúan desde el anonimato, pueden operar desde distintos países y obtener beneficios económicos con relativa facilidad.

Una vez identificado el problema, corresponde analizar cuáles son las conductas que todavía no están suficientemente reguladas por el derecho penal. En esos espacios es donde suelen aprovecharse los delincuentes. Posteriormente deben proponerse reformas que permitan incorporar esas conductas a la legislación, pero el trabajo no termina ahí. También resulta necesario anticiparse a los escenarios que probablemente surgirán en los próximos años.

Por ello, considero que la cooperación entre instituciones, el intercambio de información y, sobre todo, la formación especializada serán aspectos cada vez más relevantes para enfrentar este tipo de delincuencia.

## Desde su experiencia, ¿qué cambios han ocurrido en España en la investigación de los ciberdelitos?

**DFRA:** Los cambios han sido muy rápidos. En un ámbito como este, aquello que hoy representa una innovación jurídica puede quedar superado en muy poco tiempo. Un ejemplo es el ransomware o secuestro de datos. En algunos países se ha discutido si debe prohibirse el pago de rescates o, al menos, obligar a las empresas que deciden pagar a informar públicamente esa decisión. La intención es reducir el incentivo económico que mantiene este tipo de delitos.





## SECURED NETWORK ANALYTICS

## GLOBAL CONNECTIONS







También se han creado nuevas estructuras especializadas. En España, por ejemplo, la Guardia Civil estableció la denominada Cibercomandancia, ubicada en las instalaciones del Instituto Nacional de Ciberseguridad (INCIBE), desde donde se fortalecen las tareas de coordinación con entidades bancarias para responder con rapidez ante intentos de fraude o estafas digitales. En este tipo de investigaciones, el tiempo suele ser un factor determinante.

Otro ámbito de desarrollo es el ciberpatrullaje. Actualmente se trabaja en sistemas automatizados que permitan identificar actividades sospechosas dentro de las redes mediante herramientas basadas en inteligencia artificial. Estos sistemas no sustituyen el análisis humano, pero pueden facilitar la detección temprana de posibles conductas delictivas. A ello se suman programas dirigidos a combatir el lavado de activos, el abuso sexual de menores en entornos digitales y otras formas de criminalidad que requieren herramientas tecnológicas cada vez más especializadas.

## **Durante su conferencia habló de varios temas. ¿Cuáles considera que son las ideas principales que deberían permanecer en la discusión?**

**DFRA:** La primera tiene que ver con lo que algunos denominamos crime as a service. Cada vez existen más organizaciones criminales que prestan servicios a otras organizaciones delictivas, por ejemplo, mediante sistemas de cifrado, infraestructura tecnológica o mecanismos seguros de comunicación.

Una segunda idea es que continuamente aparecen nuevas modalidades delictivas y nuevos procedimientos para cometerlas. El uso de criptomonedas, criptoactivos y otras tecnologías obliga a comprender fenómenos que hace algunos años prácticamente no existían. Finalmente, considero necesario abrir una discusión sobre la edad de quienes participan en este tipo de delitos. Observamos que muchos ciberdelincuentes son cada vez más jóvenes y poseen un nivel importante de especialización tecnológica. En España, incluso, recientemente se han desarticulado organizaciones integradas principalmente por menores de edad.

## **¿Cuáles considera que serán los principales desafíos que enfrentarán los sistemas jurídicos en los próximos años?**

**DFRA:** Recientemente se aprobó un convenio internacional sobre ciberdelincuencia cuya implementación puede contribuir a fortalecer la cooperación entre distintos países. Ese tipo de instrumentos resulta especialmente importante porque muchos de estos delitos tienen un carácter transnacional.

Será necesario incorporar progresivamente nuevas conductas a los códigos penales, fortalecer los mecanismos de cooperación internacional y desarrollar estrategias conjuntas para asegurar la obtención y preservación de la prueba digital. También será cada vez más relevante la responsabilidad corporativa de las organizaciones y el fortalecimiento de los programas de compliance, especialmente en aquellos sectores expuestos a riesgos tecnológicos.

## **Finalmente, ¿qué recomendaría a quienes desean especializarse en este campo desde el derecho o las ciencias forenses?**

**DFRA:** Les recomendaría invertir en su formación. La ciberdelincuencia exige una perspectiva multidisciplinaria y una actualización permanente. Comprender estos fenómenos requiere conocimientos jurídicos, tecnológicos y científicos.

Siempre insisto en una idea: la mejor inversión que puede hacer cualquier profesional es invertir en su propia formación. Solo mediante el aprendizaje continuo será posible comprender estos nuevos escenarios, prevenir los riesgos que plantean y contribuir al desarrollo de respuestas más eficaces desde el derecho y las ciencias forenses.

*\*Entrevista realizada durante la Jornada Internacional sobre Inteligencia Artificial y Ciberdelincuencia, organizada por el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas, en colaboración con el Departamento de Derecho Penal de la Universidad de Granada.*



## Sobre el Dr. Francisco Rodríguez Almirón

Francisco Rodríguez Almirón es profesor contratado doctor del Departamento de Derecho Penal de la Universidad de Granada (España). Es doctor en Derecho y desarrolla actividades de docencia e investigación en derecho penal, política criminal y criminología. Sus líneas de trabajo se centran en la ciberdelincuencia, la responsabilidad penal, la recuperación de activos y los desafíos que las tecnologías digitales plantean para los sistemas de justicia. Ha participado en proyectos de investigación sobre ciberataques, protección de infraestructuras críticas e inteligencia artificial aplicada al ámbito jurídico, además de publicar artículos y capítulos de libro relacionados con el phishing, la criminalidad organizada, la responsabilidad civil derivada del delito y la protección de las víctimas.

### Cuando el delito transita de escenarios análogos al espacio digital

Una conversación con el Dr. Francisco Rodríguez Almirón

### When Crime Moves from the Physical World to the Digital Space

A Conversation with Dr. Francisco Rodríguez Almirón

Cynthia Cruz Herrera

**Resumen:** La transformación digital ha modificado la manera en que se cometen, investigan y previenen diversas conductas delictivas. En este contexto, la ciberdelincuencia representa uno de los principales retos para los sistemas de justicia, al incorporar nuevas modalidades de fraude, extorsión, robo de información y ataques contra infraestructuras críticas. En esta entrevista, el Dr. Francisco Rodríguez Almirón, profesor de la Universidad de Granada, reflexiona sobre la evolución de la criminalidad en entornos digitales y los desafíos que este fenómeno plantea para el derecho penal, la política criminal y las ciencias forenses. A lo largo de la conversación aborda temas como la adaptación de los marcos jurídicos, la cooperación internacional, el papel de la inteligencia artificial en la investigación criminal, el crime as a service y la necesidad de fortalecer la formación especializada de los profesionales encargados de prevenir e investigar estos delitos.

**Palabras clave:** Ciberdelincuencia; derecho penal; ciencias forenses; inteligencia artificial; investigación criminal; política criminal.

**Abstract:** Digital transformation has changed the ways in which criminal activities are committed, investigated, and prevented. In this context, cybercrime has become a major challenge for justice systems by introducing new forms of fraud, extortion, data theft, and attacks against critical infrastructure. In this interview, Dr. Francisco Rodríguez Almirón, Associate Professor at the University of Granada, reflects on the evolution of crime in digital environments and the challenges it poses for criminal law, criminal policy, and forensic sciences. The conversation explores issues such as the adaptation of legal frameworks, international cooperation, the role of artificial intelligence in criminal investigations, crime as a service, and the importance of specialized training for professionals involved in preventing and investigating cybercrime.

**Keywords:** Cybercrime; Criminal law; Forensic sciences; Artificial intelligence; Criminal investigation; Criminal policy.

## Cómo citar:

Rodríguez Almirón, F. (2026). Cuando el delito transita de escenarios análogos al espacio digital. *El Mundo de la Criminalística*, 1, 84-90.



# CESCIJUC®

Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas  
Escuela Libre Universitaria por Decreto Presidencial del 11 de enero de 1937. Registro No. 4 del Libro 1 de  
Escuelas Profesionales de la Dirección General de Profesiones



**PROFESORADO CON GRADO DE MAESTRÍA Y DOCTORADO QUE OCUPA LOS  
MÁS ALTOS CARGOS EN LA ADMINISTRACIÓN Y PROCURACIÓN DE JUSTICIA**

# Licenciaturas®

**LÍDERES  
EN TODO  
MÉXICO,  
ORGULLO  
CESCIJUC**

**NUESTROS PLANES ESTÁN A LA VANGUARDIA**

- DERECHO
- CRIMINALÍSTICA
- ADMÓN. DE INST. PENITENCIARIAS
- ADMINISTRACIÓN DE EMPRESAS
- CONTADURÍA PÚBLICA
- INGENIERÍA EN MECATRÓNICA
- PSICOPEDAGOGÍA
- PEDAGOGÍA
- CIENCIAS DE LA COMUNICACIÓN

[www.cescijuc.edu.mx](http://www.cescijuc.edu.mx)





# ¿Qué ocurre cuando un ciberataque afecta la vida cotidiana?



## Entrevista con el Dr. Miguel Olmedo Cardenete

Las infraestructuras suelen pasar inadvertidas mientras funcionan. Encender la luz, retirar dinero de un cajero automático, consultar un expediente clínico, utilizar una aplicación bancaria o acceder a internet forman parte de actividades cotidianas que dependen de sistemas tecnológicos distribuidos en distintos niveles. Cuando alguno de estos sistemas presenta una interrupción, ya sea por una falla técnica o por un ataque informático, sus efectos pueden extenderse a diferentes ámbitos de la vida social.

Durante las últimas décadas, la incorporación de tecnologías digitales ha modificado la forma en que operan numerosos servicios públicos y privados. Redes eléctricas, hospitales, sistemas financieros, telecomunicaciones, transporte y otras infraestructuras integran plataformas digitales que permiten coordinar procesos, intercambiar información y ofrecer servicios de manera continua. Al mismo tiempo, esta interconexión ha generado nuevas formas de riesgo que hoy forman parte de las preocupaciones de la investigación criminal, las ciencias forenses y el derecho.

La ciberdelincuencia constituye uno de los fenómenos que acompañan esta transformación tecnológica. Además de afectar a personas o empresas, algunos ataques pueden dirigirse a infraestructuras cuya operación resulta necesaria para el funcionamiento de ciudades, instituciones o servicios esenciales. En estos casos, la investigación no se limita al análisis de dispositivos electrónicos o bases de datos; también requiere comprender cómo se organizan los sistemas tecnológicos, cuáles son sus puntos de vulnerabilidad y qué mecanismos existen para documentar y preservar la evidencia digital.

Los análisis de estos procesos permiten observar que las tecnologías forman parte de la organización de la vida colectiva. Su diseño, regulación, mantenimiento y uso involucran decisiones técnicas, jurídicas, institucionales y políticas que influyen en la manera en que se gestionan los riesgos y se construyen las respuestas frente a nuevas formas de criminalidad. En consecuencia, el estudio de la ciberdelincuencia también requiere aproximaciones interdisciplinarias donde convergen el derecho, la criminalística, la informática, la ingeniería y otras áreas del conocimiento.



En este escenario, la inteligencia artificial ocupa un lugar cada vez más visible. Sus aplicaciones comienzan a incorporarse en actividades relacionadas con el análisis de información, la detección de patrones, el apoyo a determinadas tareas de investigación y el desarrollo de herramientas para fortalecer la seguridad digital. De forma paralela, estas mismas tecnologías también pueden ser utilizadas para automatizar fraudes, generar contenidos falsificados o desarrollar nuevas modalidades de engaño. Estos procesos forman parte de un campo de investigación que continúa evolucionando conforme aparecen nuevas aplicaciones tecnológicas.

Por estos motivos, en esta entrevista, se presentan las reflexiones del Dr. Miguel Olmedo Cardenete, catedrático de Derecho Penal de la Universidad de Granada y responsable de un grupo de investigación dedicado al estudio de la ciberdelincuencia, la inteligencia artificial y la protección de infraestructuras críticas. Esta charla fue realizada durante la Jornada Internacional sobre Inteligencia Artificial y Ciberdelincuencia, organizada por el Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas, en colaboración con el Departamento de Derecho Penal de la Universidad de Granada.

A lo largo de esta conversación, el Dr. Olmedo Cardenete explica cómo surgieron estas líneas de investigación dentro de su grupo académico y reflexiona sobre algunos temas que actualmente orientan el estudio de la ciberdelincuencia: la protección de infraestructuras críticas, la cooperación internacional, la justicia digital, la obtención de evidencia electrónica y la formación de especialistas capaces de trabajar en escenarios donde convergen el derecho, las ciencias forenses y las tecnologías digitales.



## Entrevista

Su trayectoria académica se ha desarrollado en el derecho penal, pero en los últimos años ha impulsado una agenda de investigación sobre ciberdelincuencia, inteligencia artificial e infraestructuras críticas.

### ¿Qué motivó esa transición y cómo se consolidó esta línea de trabajo en la Universidad de Granada?

**Dr. Miguel Olmedo Cardenete (DMOC):** Actualmente soy catedrático de Derecho Penal en la Universidad de Granada y también ejerzo como abogado litigante en España. Mi formación ha tenido un carácter internacional, con estancias de investigación en Alemania, Italia y el Reino Unido. En los últimos años conformamos un grupo de investigación en la Universidad de Granada dedicado al estudio de la ciberdelincuencia, lo que nos ha permitido obtener diversos proyectos de investigación competitivos.

Uno de ellos se centra en el análisis de la ciberdelincuencia dirigida contra infraestructuras críticas. Tradicionalmente, la atención se ha concentrado en los ataques que afectan el patrimonio o los datos personales de los ciudadanos. Sin embargo, existe otra dimensión de la ciberdelincuencia que puede comprometer servicios esenciales e incluso relacionarse con escenarios de conflicto internacional. Hoy los ataques ya no se limitan al uso de armamento convencional; también incluyen acciones dirigidas contra sistemas tecnológicos cuya interrupción puede afectar el funcionamiento de un país.

Posteriormente obtuvimos un segundo proyecto orientado al estudio de los ciberataques dirigidos contra las personas, especialmente hacia sectores vulnerables como menores de edad y personas mayores. Analizamos estrategias de prevención y herramientas que contribuyan a reducir su exposición frente a fraudes, ciberacoso y otras formas de delincuencia digital.

Actualmente trabajamos en nuevas propuestas relacionadas con el ciberpatrullaje y la justicia digital. Nos interesa estudiar el uso de herramientas basadas en inteligencia artificial para apoyar la investigación criminal y desarrollar sistemas que faciliten el trabajo judicial sin sustituir la función de jueces y tribunales.

### Una parte importante de sus investigaciones se centra en la protección de las infraestructuras críticas. ¿Por qué este tema se ha convertido en una prioridad para el estudio de la ciberdelincuencia?

**DMOC:** Porque el funcionamiento cotidiano de nuestras sociedades depende de sistemas tecnológicos que normalmente pasan inadvertidos. Hospitales, redes eléctricas, telecomunicaciones, servicios financieros o sistemas de transporte operan mediante plataformas digitales cuya interrupción puede producir consecuencias que trascienden el ámbito informático.

Cuando hablamos de infraestructuras críticas hablamos precisamente de esos servicios cuya continuidad resulta necesaria para el funcionamiento de la sociedad. La protección de estos sistemas constituye una prioridad porque un ataque puede afectar simultáneamente a miles de personas y comprometer actividades esenciales.

### **La inteligencia artificial comienza a incorporarse tanto en la comisión como en la investigación de los ciberdelitos. ¿Cómo está modificando este panorama?**

**DMOC:** La inteligencia artificial ya forma parte de este escenario desde distintas perspectivas. Por un lado, facilita tareas relacionadas con el análisis de información, la identificación de patrones y el desarrollo de herramientas de apoyo para la investigación criminal. También abre posibilidades para fortalecer el denominado ciberpatrullaje mediante programas capaces de detectar actividades sospechosas en entornos digitales.

Al mismo tiempo, estas tecnologías también pueden ser utilizadas para cometer delitos. Hoy es posible crear identidades falsas, imitar voces, desarrollar asistentes virtuales o automatizar mecanismos de fraude con un nivel de sofisticación que hace algunos años resultaba difícil de imaginar. Por ello, cualquier análisis sobre inteligencia artificial debe considerar tanto sus posibilidades de aplicación como los riesgos derivados de su uso indebido.

### **Desde su experiencia, ¿cómo han respondido las instituciones encargadas de procurar e impartir justicia frente al crecimiento de la ciberdelincuencia?**

**DMOC:** Observo diferencias entre las distintas instituciones. En España, tanto las fuerzas policiales como la fiscalía han mostrado una disposición creciente para actualizar sus capacidades y comprender que una parte importante de la delincuencia se desarrolla actualmente en el ciberespacio.

En cambio, dentro del poder judicial el proceso de especialización ha sido más gradual. Existen iniciativas impulsadas por jueces y magistrados interesados en estos temas, pero todavía queda camino por recorrer para fortalecer la formación especializada y consolidar estructuras que permitan responder con mayor eficacia a este tipo de investigaciones.

### **Si observamos la evolución de estos delitos durante la última década, ¿cuáles considera que han sido las transformaciones más significativas?**

**DMOC:** Hace algunos años uno de los ejemplos más conocidos eran las llamadas “cartas nigerianas”: correos electrónicos muy simples que anunciaban falsas herencias o premios inexistentes. Aquellas estrategias constituyeron algunas de las primeras manifestaciones de la ciberdelincuencia organizada.

Hoy el panorama es distinto. La inteligencia artificial permite crear voces sintéticas, desarrollar asistentes virtuales, producir imágenes falsas y construir escenarios de interacción capaces de generar confianza en las víctimas. Desde el punto de vista jurídico, muchas de estas conductas siguen respondiendo al mismo objetivo: obtener un beneficio económico mediante el engaño. Lo que ha cambiado son las herramientas utilizadas para lograrlo.







**Durante su conferencia abordó distintos ejemplos relacionados con ciberataques e infraestructuras críticas. ¿Qué ideas considera fundamentales para comprender este fenómeno?**

**DMOC:** En primer lugar, es importante reconocer la diversidad de los ciberataques. Existen modalidades dirigidas contra personas, empresas, instituciones públicas e infraestructuras esenciales. En segundo lugar, considero necesario fortalecer la cultura de la prevención. La autoprotección continúa siendo una herramienta importante para reducir riesgos. Finalmente, la inteligencia artificial introduce nuevas posibilidades tanto para proteger sistemas como para vulnerarlos. Comprender estas transformaciones requiere analizar simultáneamente los desarrollos tecnológicos, los marcos jurídicos y las capacidades institucionales disponibles para responder a ellos.

**La cooperación internacional aparece de manera constante en las discusiones sobre ciberdelincuencia. ¿Qué formas de colaboración considera prioritarias para los próximos años?**

**DMOC:** La cooperación internacional será determinante en distintos niveles. En primer lugar, mediante el intercambio de información entre Estados. En segundo lugar, a través de la colaboración entre policías, fiscalías y organismos especializados durante las investigaciones. Finalmente, mediante mecanismos de cooperación judicial que permitan compartir pruebas, localizar activos, coordinar procedimientos y facilitar la persecución de delitos cuyo carácter es claramente transnacional.

La ciberdelincuencia supera con frecuencia las fronteras nacionales. Por ello, las respuestas también requieren mecanismos de coordinación internacional.

**Para quienes hoy estudian derecho, criminalística o ciencias forenses, ¿qué oportunidades profesionales observa en este campo?**

**DMOC:** Existen oportunidades tanto para los profesionales del derecho como para quienes trabajan en criminalística y ciencias forenses. Cada vez será más frecuente la necesidad de abogados especializados en litigios relacionados con ciberdelitos, así como de especialistas capaces de analizar evidencia digital y apoyar técnicamente los procesos judiciales. La investigación de estos delitos requiere conocimientos jurídicos y tecnológicos. Por ello considero que la formación interdisciplinaria representa una de las principales herramientas para quienes desean desarrollarse profesionalmente en este ámbito.



## Sobre el Dr. Miguel Olmedo Cardenete

Miguel Olmedo Cardenete es catedrático de Derecho Penal de la Universidad de Granada (España), donde desarrolla actividades de docencia e investigación desde hace más de dos décadas. Es doctor en Derecho por la misma institución, con Premio Extraordinario de Doctorado, y su trayectoria académica se ha centrado en el estudio del derecho penal, la política criminal y los desafíos que las transformaciones tecnológicas plantean para los sistemas de justicia.

Ha dirigido y participado en numerosos proyectos de investigación competitivos sobre ciberdelincuencia, inteligencia artificial, protección de infraestructuras críticas, blanqueo de capitales y cooperación internacional en materia penal. Su producción científica comprende libros, capítulos de obra colectiva y artículos publicados en revistas especializadas, además de una amplia participación en congresos y redes académicas nacionales e internacionales.

A lo largo de su carrera también ha desempeñado responsabilidades de gestión universitaria, entre ellas el cargo de decano de la Facultad de Derecho de la Universidad de Granada. Su trabajo académico combina la investigación, la docencia y la colaboración con instituciones nacionales e internacionales interesadas en el estudio de la criminalidad contemporánea y la evolución de los sistemas de justicia frente a los retos que plantea la transformación digital.

### ¿Qué ocurre cuando un ciberataque afecta la vida cotidiana?

Entrevista con el Dr. Miguel Olmedo Cardenete

### What Happens When a Cyberattack Affects Everyday Life?

Interview with Dr. Miguel Olmedo Cardenete

Néstor Daniel Martínez Domínguez

**Resumen:** La creciente digitalización de los servicios públicos y privados ha modificado la manera en que las sociedades organizan actividades esenciales como las telecomunicaciones, la atención médica, los sistemas financieros o el suministro de energía. En este contexto, la ciberdelincuencia ha ampliado su alcance al dirigirse no solo contra personas y organizaciones, sino también contra infraestructuras cuya operación resulta necesaria para la vida cotidiana. En esta entrevista, el Dr. Miguel Olmedo Cardenete, reflexiona sobre la evolución de la investigación en ciberdelincuencia y los desafíos que plantea la protección de infraestructuras críticas en un entorno cada vez más digitalizado. Asimismo, aborda el papel de la inteligencia artificial en la investigación criminal, las posibilidades de la justicia digital, la cooperación internacional y la necesidad de fortalecer la formación interdisciplinaria de quienes participan en la prevención, investigación y persecución de los ciberdelitos.

**Palabras clave:** Ciberdelincuencia; Infraestructuras críticas; Inteligencia artificial; ciencias forenses; justicia digital; derecho penal.

**Abstract:** The increasing digitalization of public and private services has transformed the way societies organize essential activities such as telecommunications, healthcare, financial systems, and energy supply. In this context, cybercrime has expanded beyond individuals and organizations to target infrastructures that support everyday life. In this interview, Dr. Miguel Olmedo Cardenete, reflects on the evolution of cybercrime research and the challenges involved in protecting critical infrastructure in an increasingly digital environment. He also discusses the role of artificial intelligence in criminal investigations, the development of digital justice, international cooperation, and the importance of interdisciplinary training for professionals involved in preventing, investigating, and prosecuting cybercrime.

**Keywords:** Cybercrime; Critical infrastructure; Artificial intelligence; Forensic sciences; Digital justice; Criminal law.

## Cómo citar:

Olmedo Cardenete, M. (2026). ¿Qué ocurre cuando un ciberataque afecta la vida cotidiana? *El Mundo de la Criminalística*, 1, 92-99.



CESCIJUC®