



Revista Hambatu Science

Ambato – Ecuador / ISSN 3151-815X (en línea) / julio - septiembre 2026

Volumen 1, Número 3

<https://doi.org/10.63862/rhs-v1n3-254-274-2026>

Victimología del Siglo XXI: Transformaciones, Desafíos y Nuevas Formas de Victimización en Sociedades Digitales

*Victimology in the 21st Century: Transformations, Challenges,
and New Forms of Victimization in Digital Societies*

Gerardo Martin Valencia Guerrero
Universidad Autónoma de Sinaloa

Juan Eustorgio Sánchez Conde
Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas

Acela del Carmen Cruz Díaz
Universidad Autónoma de Querétaro

Manuela Mitchel Elizalde
Universidad Autónoma de Sinaloa



DOI: <https://doi.org/10.63862/rhs-v1n3-254-274-2026>

Victimología del Siglo XXI: Transformaciones, Desafíos y Nuevas Formas de Victimización en Sociedades Digitales

Gerardo Martin Valencia Guerrero

Universidad Autónoma de Sinaloa

gerardo1martin@gmail.com

<https://orcid.org/0009-0000-9661-3319>

México

Acela del Carmen Cruz Díaz

Universidad Autónoma de Querétaro

aceladelcarmencruzdiaz@gmail.com

<https://orcid.org/0009-0003-4579-5046>

México

Juan Eustorgio Sánchez Conde

Centro de Estudios Superiores en Ciencias
Jurídicas y Criminológicas

segabox1982@hotmail.com

<https://orcid.org/0009-0004-4259-0499>

México

Manuela Mitchel Elizalde

Universidad Autónoma de Sinaloa

eventosuas@uas.edu.mx

<https://orcid.org/0009-0000-7102-4243>

México

Recibido: 2026-07-15

Aceptado: 2026-07-17

Publicado: 2026-07-24

Resumen

La transformación digital ha modificado profundamente las dinámicas sociales, económicas y culturales de las sociedades contemporáneas, generando nuevos escenarios de interacción que, además de múltiples beneficios, han propiciado la aparición de formas emergentes de victimización. La victimología, como disciplina científica dedicada al estudio de las víctimas, enfrenta actualmente el desafío de comprender fenómenos como la ciberdelincuencia, la violencia digital, el acoso en línea, la sextorsión, la difusión no consentida de contenido íntimo, la suplantación de identidad y los riesgos asociados al uso de sistemas basados en inteligencia artificial. El presente artículo analiza la evolución de la victimología en el contexto de las sociedades digitales, identificando las principales transformaciones en los procesos de victimización, los factores de vulnerabilidad y los retos para la protección de los derechos humanos. Asimismo, se examina la necesidad de fortalecer mecanismos de prevención, atención integral y reparación del daño mediante enfoques interdisciplinarios que incorporen la perspectiva tecnológica, psicológica, criminológica y jurídica. Se concluye que la victimología del siglo XXI debe adaptarse a las nuevas realidades digitales para garantizar una protección efectiva de las víctimas y promover entornos virtuales más seguros.

Palabras clave: victimología, victimización digital, ciberdelincuencia, inteligencia artificial, derechos humanos, violencia digital.

Victimology in the 21st Century: Transformations, Challenges, and New Forms of Victimization in Digital Societies

Abstract

Digital transformation has profoundly reshaped the social, economic, and cultural dynamics of contemporary societies, creating new forms of interaction that, while offering numerous benefits, have also contributed to the emergence of new forms of victimization. Victimology, as the scientific discipline devoted to the study of victims, currently faces the challenge of understanding phenomena such as cybercrime, digital violence, online harassment, sextortion, the non-consensual dissemination of intimate content, identity theft, and the risks associated with the use of artificial intelligence-based systems. This article examines the evolution of victimology within the context of digital societies, identifying the main transformations in victimization processes, vulnerability factors, and challenges related to the protection of human rights. Furthermore, it explores the need to strengthen prevention mechanisms, comprehensive victim support, and damage reparation through interdisciplinary approaches that integrate technological, psychological, criminological, and legal perspectives. It is concluded that twenty-first-century victimology must adapt to emerging digital realities in order to ensure effective victim protection and promote safer virtual environments.

Keywords: victimology, digital victimization, cybercrime, artificial intelligence, human rights, digital violence.

Introducción

La victimología ha experimentado una notable evolución desde sus primeras aproximaciones centradas exclusivamente en la víctima del delito tradicional hasta convertirse en una disciplina multidimensional que analiza los procesos de victimización en diversos contextos sociales. Durante gran parte del siglo XX, el estudio victimológico se enfocó principalmente en delitos convencionales como homicidios, robos, agresiones sexuales y violencia familiar. Sin embargo, el desarrollo acelerado de las tecnologías de la información y la comunicación ha generado escenarios inéditos de interacción humana, transformando significativamente las formas en que las personas pueden ser victimizadas.

Actualmente, millones de individuos participan diariamente en espacios digitales mediante redes sociales, plataformas de comunicación, sistemas financieros electrónicos y entornos virtuales interconectados. Esta realidad ha favorecido la aparición de nuevas modalidades delictivas y de violencia que trascienden las fronteras geográficas y dificultan la identificación de los agresores. En consecuencia, la victimología contemporánea enfrenta el reto de comprender las características, impactos y mecanismos de prevención de estas nuevas formas de victimización.

La creciente digitalización de la vida cotidiana exige una actualización conceptual y metodológica de la victimología para responder adecuadamente a los desafíos que plantea la ciberdelincuencia, la inteligencia artificial, la violencia digital y la protección integral de los derechos humanos en el entorno virtual.

Estado del arte

- **Victimología**

La Sociedad Mundial de Victimología define la victimología como: "the scientific study of victims, including the relationships between victims and offenders, victims and the criminal justice system, and victims and other social groups and institutions" (World Society of Victimology, 2023). Esta definición destaca que la victimología no se limita al análisis de las consecuencias que experimenta una persona tras sufrir un delito, sino que estudia de manera

integral las interacciones que se producen entre la víctima, el agresor, las instituciones de justicia y la sociedad.

En el contexto actual, la victimología ha ampliado considerablemente su campo de estudio para incluir fenómenos asociados a las tecnologías digitales, la ciberdelincuencia y las nuevas formas de violencia que surgen en Internet. Esta disciplina resulta fundamental para comprender los factores de vulnerabilidad, los procesos de victimización y las estrategias de prevención y atención integral que permitan garantizar la protección de los derechos de las víctimas.

- **Victimización Digital**

Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE): "Digital victimisation refers to harmful experiences suffered through the use of digital technologies, including online harassment, cyberbullying, identity theft, fraud and other forms of technology-facilitated abuse" (OECD, 2023). La victimización digital comprende todas aquellas experiencias dañinas que ocurren mediante el uso de tecnologías de la información y comunicación. A diferencia de la victimización tradicional, este tipo de violencia puede producirse sin contacto físico entre víctima y agresor, lo que amplía significativamente el alcance del daño.

La difusión masiva de contenidos, el anonimato de los agresores y la permanencia de la información en Internet incrementan los efectos psicológicos, sociales y económicos sobre las víctimas. Desde la victimología contemporánea, la victimización digital representa uno de los principales desafíos debido a la rapidez con la que evolucionan las tecnologías y las modalidades delictivas asociadas.

- **Ciberdelincuencia**

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) define la ciberdelincuencia como: "criminal activities carried out using computers or the Internet, either as the target of the offence or as the tool used to commit the offence" (UNODC, 2024). Esta definición permite comprender que la ciberdelincuencia incluye tanto delitos dirigidos contra sistemas informáticos como aquellos que utilizan la tecnología para cometer actos ilícitos.

Entre los ejemplos más frecuentes se encuentran el phishing, el fraude electrónico, el robo de identidad, el ransomware y la sextorsión. La expansión global de Internet ha favorecido el crecimiento de estas actividades criminales, convirtiéndolas en una amenaza transnacional. Desde la victimología, resulta esencial analizar las consecuencias que estos delitos generan en las víctimas, las cuales pueden experimentar pérdidas económicas, afectaciones emocionales y vulneraciones a su privacidad y seguridad personal.

- **Inteligencia Artificial**

La UNESCO (2024) define la inteligencia artificial como: "systems that have the ability to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control" (UNESCO, 2024). La inteligencia artificial constituye una de las innovaciones tecnológicas más relevantes del siglo XXI. Su capacidad para analizar grandes volúmenes de información y generar respuestas automatizadas ha transformado múltiples sectores, incluyendo la educación, la salud, la seguridad y la justicia. Sin embargo, también ha generado nuevos riesgos victimológicos relacionados con los deepfakes, la automatización del fraude, la vigilancia masiva y la manipulación digital. Por ello, el estudio de la inteligencia artificial desde una perspectiva victimológica resulta indispensable para comprender cómo estas tecnologías pueden ser utilizadas tanto para la protección como para la victimización de las personas.

- **Derechos Humanos**

La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos establece que: "Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status" (OHCHR, 2024). Los derechos humanos constituyen el fundamento ético y jurídico de la protección de las víctimas. Su carácter universal implica que todas las personas poseen derechos inherentes que deben ser respetados y garantizados por los Estados y la sociedad.

En los entornos digitales, la protección de derechos como la privacidad, la dignidad, la libertad de expresión y el acceso a la justicia adquiere una relevancia especial debido a los riesgos asociados con la ciberdelincuencia y la violencia tecnológica. La victimología contemporánea

incorpora una perspectiva de derechos humanos para asegurar que las víctimas reciban protección integral y reparación efectiva frente a las vulneraciones sufridas.

- **Violencia Digital**

ONU Mujeres define la violencia digital como: "any act of gender-based violence that is committed, assisted or aggravated in part or fully by the use of information and communication technologies" (UN Women, 2024). La violencia digital comprende una amplia variedad de conductas dañinas realizadas mediante tecnologías digitales, incluyendo el ciberacoso, la sextorsión, el hostigamiento en línea, la difusión no consentida de imágenes íntimas y las campañas de odio en redes sociales. Aunque puede afectar a cualquier persona, las mujeres y las adolescentes suelen experimentar mayores niveles de victimización debido a factores estructurales relacionados con la desigualdad de género. Desde la victimología, la violencia digital representa una manifestación contemporánea de violencia que requiere estrategias específicas de prevención, atención y protección. Su impacto trasciende el espacio virtual, generando consecuencias reales sobre la salud mental, la seguridad y la calidad de vida de las víctimas.

Evolución de la Victimología hacia los Entornos Digitales

La victimología surgió formalmente durante la década de 1940 con las contribuciones de Benjamin Mendelsohn y Hans von Hentig, quienes propusieron el estudio científico de las víctimas y su papel dentro del fenómeno criminal. Posteriormente, la disciplina amplió su objeto de estudio incorporando factores psicológicos, sociales, jurídicos y culturales relacionados con la victimización.

En el siglo XXI, la expansión de Internet y las tecnologías digitales ha impulsado una nueva etapa de desarrollo victimológico caracterizada por la necesidad de comprender fenómenos que ocurren en espacios virtuales. La victimización ya no se limita a la interacción física entre agresor y víctima, sino que puede producirse mediante plataformas digitales capaces de amplificar el daño psicológico, emocional, económico y reputacional.

La denominada victimología digital estudia precisamente las dinámicas de victimización que surgen en entornos tecnológicos, considerando tanto los riesgos asociados al uso de Internet como las consecuencias derivadas de la exposición permanente en espacios virtuales.

Nuevas Formas de Victimización en las Sociedades Digitales

- **Ciberacoso (Cyberbullying)**

El ciberacoso constituye una de las formas más extendidas de victimización digital. Consiste en conductas reiteradas de hostigamiento, intimidación, amenazas o humillaciones realizadas mediante medios electrónicos.

Las víctimas experimentan frecuentemente:

- Ansiedad.
- Depresión.
- Baja autoestima.
- Aislamiento social.
- Ideación suicida.

Los adolescentes y jóvenes representan uno de los grupos más vulnerables debido a su elevada interacción en redes sociales.

El ciberacoso constituye una de las expresiones más frecuentes de victimización digital en las sociedades contemporáneas. A diferencia del acoso tradicional, este fenómeno se caracteriza por el uso de tecnologías de la información para intimidar, hostigar, amenazar, ridiculizar o excluir a una persona mediante mensajes, imágenes, videos o publicaciones difundidas a través de redes sociales, aplicaciones de mensajería y plataformas digitales. Su alcance es particularmente preocupante debido a la posibilidad de que las agresiones permanezcan disponibles en línea de forma permanente y sean observadas por una audiencia masiva.

La UNESCO (2023) señala que "la creciente utilización de dispositivos digitales ha exacerbado el ciberacoso", destacando que los niveles de victimización aumentan significativamente durante la adolescencia.

Los adolescentes constituyen una población especialmente vulnerable porque gran parte de su identidad social se construye en espacios digitales. La victimología contemporánea debe analizar no solo las conductas de los agresores, sino también los factores tecnológicos que facilitan la amplificación del daño. En consecuencia, resulta indispensable fortalecer la

educación digital, los protocolos escolares de intervención y los mecanismos de denuncia para reducir la incidencia de este fenómeno.

Asimismo, Eric Falt y Senapaty (2023) afirman que "la violencia y el acoso, incluido el ciberacoso, dejan una huella en la vida de los estudiantes y suelen producir ansiedad, depresión, vergüenza y baja autoestima". La exposición constante a mensajes ofensivos, rumores o amenazas genera consecuencias psicológicas profundas que afectan el rendimiento académico, la autoestima y las relaciones interpersonales.

Por su parte, Garthe et al. (2023) encontraron que "experimentar mayores niveles de cibervictimización se asoció con incrementos significativos de ansiedad, depresión y estrés social". Desde una perspectiva victimológica, el ciberacoso representa un desafío sin precedentes debido a la eliminación de las barreras espacio-temporales que tradicionalmente limitaban la conducta agresiva. Actualmente, la víctima puede ser acosada las veinticuatro horas del día, independientemente de su ubicación física.

- **Sextorsión y Violencia Sexual Digital**

La sextorsión implica la utilización de imágenes, videos o información íntima para extorsionar, manipular o controlar a una persona.

Esta modalidad presenta características particulares:

- Alto impacto emocional.
- Vergüenza y estigmatización social.
- Riesgo de difusión masiva del contenido.
- Revictimización constante.

La violencia sexual digital se ha convertido en una problemática global que afecta principalmente a mujeres y adolescentes.

Robo de Identidad y Fraudes Electrónicos

La digitalización financiera ha incrementado significativamente los delitos relacionados con el robo de identidad.

Los delincuentes utilizan diversas estrategias:

- Phishing.
- Ingeniería social.
- Malware.
- Suplantación de identidad.
- Clonación de cuentas.

Las víctimas pueden sufrir pérdidas económicas importantes y daños prolongados a su reputación personal y profesional.

El robo de identidad constituye una de las modalidades delictivas con mayor crecimiento en la era digital. Los delincuentes obtienen información personal mediante técnicas de phishing, malware, ingeniería social o acceso ilícito a bases de datos para realizar fraudes financieros o actividades ilícitas en nombre de la víctima.

La Oficina de las Naciones Unidas contra la Droga y el Delito señala que "el robo de identidad genera alrededor de mil millones de dólares cada año para las organizaciones criminales". Las Naciones Unidas indican que los delitos cibernéticos incluyen prácticas como "phishing, robo de identidad y despliegue de malware y ransomware", las cuales afectan a millones de personas alrededor del mundo.

Asimismo, durante la Operación First Light 2026, INTERPOL identificó más de 142,000 víctimas relacionadas con fraudes y delitos cibernéticos en 97 países.

Metodología

La presente investigación se desarrolló bajo un enfoque cualitativo, mediante un diseño no experimental y de tipo documental, sustentado en una revisión bibliográfica de carácter descriptivo y analítico. Este enfoque permitió examinar de manera sistemática la evolución de la victimología en el contexto de las sociedades digitales, así como identificar las principales transformaciones en los procesos de victimización, los factores de vulnerabilidad emergentes y los desafíos asociados con la protección de los derechos humanos frente al avance de las tecnologías digitales.

La estrategia metodológica consistió en la recopilación, selección y análisis crítico de literatura científica y documentación técnica publicada por organismos internacionales, instituciones especializadas y revistas académicas de reconocido prestigio. Se consultaron principalmente documentos provenientes de la Organización de las Naciones Unidas (ONU), la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), UNICEF, ONU Mujeres, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), INTERPOL, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR), así como artículos científicos indexados y literatura especializada relacionada con la victimología, la ciberdelincuencia, la inteligencia artificial y la violencia digital.

Para la localización de la información se emplearon palabras clave en español e inglés, entre ellas: victimología, victimización digital, digital victimization, cybercrime, cybervictimization, digital violence, artificial intelligence, deepfakes, identity theft, human rights y cybersecurity. La búsqueda priorizó publicaciones recientes, principalmente del período 2023–2026, con el propósito de incorporar evidencia científica actualizada sobre las nuevas formas de victimización derivadas del acelerado desarrollo tecnológico.

Como criterios de inclusión se consideraron documentos científicos, informes institucionales, artículos arbitrados, informes técnicos y publicaciones oficiales que abordaran directamente la victimización en entornos digitales, las implicaciones victimológicas de la inteligencia artificial, la violencia digital, la ciberdelincuencia y la protección de los derechos humanos. Se excluyeron publicaciones sin respaldo institucional o científico, documentos duplicados y trabajos cuya temática no guardara relación directa con el objeto de estudio.

El análisis de la información se realizó mediante un proceso de análisis documental de contenido, organizando la evidencia recopilada en categorías temáticas previamente definidas: evolución de la victimología, victimización digital, ciberacoso, sextorsión, robo de identidad, discurso de odio, inteligencia artificial, revictimización, derechos humanos, atención integral a las víctimas y perspectivas futuras de la disciplina. Posteriormente, se efectuó un análisis interpretativo que permitió identificar tendencias comunes, riesgos emergentes, desafíos jurídicos y tecnológicos, así como propuestas orientadas al fortalecimiento de la prevención, la protección y la reparación integral de las víctimas en las sociedades digitales.

Finalmente, la información fue sintetizada mediante un enfoque integrador que articuló aportes provenientes de la victimología, la criminología, el derecho, la psicología, la ciberseguridad y los estudios sobre inteligencia artificial, con el propósito de ofrecer una visión interdisciplinaria del fenómeno de la victimización digital y de las transformaciones que enfrenta la victimología en el siglo XXI. Este procedimiento permitió construir un análisis actualizado y fundamentado sobre los principales retos que plantean las nuevas formas de victimización en los entornos tecnológicos contemporáneos.

Resultados

La revisión documental permitió identificar una transformación significativa de la victimología como consecuencia del acelerado desarrollo de las tecnologías digitales y de la creciente interconexión de la sociedad. El análisis de la literatura científica y de los informes emitidos por organismos internacionales evidenció que las formas tradicionales de victimización han evolucionado hacia escenarios digitales caracterizados por una mayor complejidad, alcance global e impacto multidimensional sobre las víctimas. Los estudios revisados coinciden en señalar que la victimización digital constituye actualmente uno de los principales desafíos para la criminología, el derecho y las políticas públicas de protección.

Tabla 1.

Resultados relevantes identificados en la revisión documental

Hallazgo	Evidencia encontrada
Expansión de la victimización digital	Incremento de delitos cometidos mediante tecnologías digitales y redes sociales.
Modalidades predominantes	Ciberacoso, sextorsión, robo de identidad, fraude electrónico, difusión no consentida de contenido íntimo y suplantación de identidad.
Grupos con mayor vulnerabilidad	Adolescentes, mujeres, personas adultas mayores y usuarios con limitada alfabetización digital.
Impactos identificados	Consecuencias psicológicas, sociales, económicas y reputacionales derivadas de la victimización digital.
Riesgos asociados a la inteligencia artificial	Deepfakes, automatización del fraude, generación de contenido falso y sofisticación de ataques cibernéticos.
Necesidades identificadas	Fortalecimiento de la prevención, alfabetización digital, cooperación internacional y actualización de los marcos jurídicos para la protección de las víctimas.

Fuente: Elaboración propia a partir de la revisión documental (2026).

El examen comparativo de las investigaciones también permitió establecer que la expansión de Internet, las redes sociales, la inteligencia artificial y las plataformas digitales ha favorecido la aparición de nuevas modalidades delictivas que incrementan los niveles de exposición de la

población. Estas transformaciones han ampliado el objeto de estudio de la victimología contemporánea, que actualmente incorpora fenómenos relacionados con la violencia digital, la ciberdelincuencia, el fraude tecnológico y los riesgos derivados del uso indebido de sistemas automatizados.

Principales modalidades de victimización digital identificadas

Uno de los hallazgos más consistentes de la revisión documental fue la identificación de un conjunto de modalidades de victimización que aparecen de forma recurrente en la literatura especializada. Entre ellas destacan el ciberacoso, la sextorsión, el robo de identidad, el fraude electrónico, la difusión no consentida de contenido íntimo, la suplantación de identidad y la manipulación de información mediante inteligencia artificial.

Los documentos analizados coinciden en que estas modalidades presentan características diferentes a las observadas en la delincuencia convencional. La facilidad para reproducir contenidos digitales, el anonimato de los agresores, la velocidad de difusión de la información y la dificultad para eliminar permanentemente el material publicado incrementan la duración e intensidad del proceso de victimización. En consecuencia, el daño experimentado por las víctimas trasciende las pérdidas económicas o materiales, extendiéndose hacia dimensiones psicológicas, sociales, familiares y laborales.

Asimismo, la revisión permitió identificar que muchas de estas conductas delictivas se desarrollan de forma combinada. Por ejemplo, el robo de identidad suele constituir el punto de partida para fraudes financieros, mientras que la obtención ilícita de contenido íntimo puede evolucionar hacia procesos de sextorsión o violencia sexual digital. Esta convergencia evidencia que la victimización digital debe analizarse desde una perspectiva integral que considere la interacción entre diferentes factores tecnológicos, sociales y jurídicos.

Poblaciones con mayor vulnerabilidad

Otro resultado importante de la revisión documental fue la identificación de los grupos poblacionales que presentan mayor exposición a las nuevas formas de victimización digital. La evidencia científica revisada señala que adolescentes, mujeres, personas adultas mayores, usuarios con limitada alfabetización digital y colectivos históricamente vulnerables concentran una proporción significativa de los casos reportados.

Los adolescentes aparecen de forma reiterada como uno de los grupos de mayor riesgo debido a la elevada utilización de redes sociales y plataformas de comunicación digital durante los procesos de socialización. Por otra parte, la literatura consultada evidencia que las mujeres experimentan mayores niveles de violencia digital, especialmente en conductas relacionadas con la difusión no consentida de imágenes íntimas, el acoso en línea y la sextorsión. De igual manera, las personas mayores suelen presentar una mayor vulnerabilidad frente a fraudes electrónicos y estrategias de ingeniería social debido a las dificultades para identificar mecanismos de engaño cada vez más sofisticados.

Estos hallazgos permiten comprender que la vulnerabilidad digital no depende exclusivamente del acceso a la tecnología, sino también de factores educativos, sociales, económicos y culturales que condicionan la capacidad de las personas para reconocer riesgos y adoptar medidas preventivas.

Inteligencia artificial como factor emergente de victimización

La revisión bibliográfica permitió identificar un crecimiento sostenido de investigaciones relacionadas con la utilización de inteligencia artificial en actividades delictivas. Diversos organismos internacionales advierten que estas tecnologías están siendo utilizadas para automatizar fraudes, desarrollar campañas de desinformación, crear identidades falsas y generar contenidos audiovisuales manipulados mediante técnicas de *deepfake*.

La evidencia analizada muestra que estas herramientas incrementan considerablemente la capacidad de los delincuentes para personalizar ataques y dificultar la detección de actividades ilícitas. Como consecuencia, la victimización adquiere nuevas características asociadas a la manipulación automatizada de información, la afectación de la reputación digital y la vulneración de derechos fundamentales relacionados con la identidad y la privacidad.

La revisión también evidenció que la rapidez con la cual evolucionan estas tecnologías supera, en numerosos casos, la capacidad de adaptación de los marcos normativos y de las instituciones encargadas de la prevención del delito, lo que representa uno de los principales desafíos identificados en la literatura especializada.

Tendencias identificadas en la evidencia internacional

El análisis comparativo de los documentos revisados permitió identificar una tendencia común: el crecimiento sostenido de los delitos tecnológicos durante los últimos años. Como ejemplo representativo, los resultados de la Operación First Light 2026 desarrollada por INTERPOL reflejan la dimensión internacional que ha alcanzado la ciberdelincuencia.

Tabla 2.

Resultados globales de la Operación First Light 2026 de INTERPOL

Indicador	Resultado
Países y territorios participantes	97
Período de ejecución	15 de enero – 30 de abril de 2026
Víctimas identificadas	Más de 142 000
Personas arrestadas	5 811
Casos analizados	152 808
Casos resueltos	23 715
Sospechosos identificados	15 606
Cuentas bancarias bloqueadas	31 014
Notificaciones y difusiones emitidas	99
Activos ilícitos interceptados	USD 293 millones
Modalidades delictivas predominantes	Sextorsión, fraude de inversión, phishing, fraude romántico, suplantación de identidad, compromiso de correo empresarial (BEC) y lavado de dinero

Fuente: Elaboración propia con base en INTERPOL (2026).

Estos datos evidencian que la victimización digital constituye un fenómeno transnacional cuya atención requiere mecanismos permanentes de cooperación internacional. La revisión documental demuestra además que la mayor parte de las investigaciones recientes coincide en señalar la necesidad de fortalecer la educación digital, mejorar los sistemas de protección de datos personales y desarrollar estrategias preventivas orientadas tanto a la ciudadanía como a las instituciones públicas y privadas.

En conjunto, los hallazgos obtenidos permiten afirmar que la victimología contemporánea enfrenta un escenario de transformación permanente impulsado por la innovación tecnológica. La revisión evidencia que las nuevas formas de victimización ya no pueden abordarse únicamente desde perspectivas tradicionales centradas en el delito convencional, sino mediante enfoques interdisciplinarios capaces de integrar conocimientos provenientes de la criminología, el derecho, la psicología, la ciberseguridad y la inteligencia artificial. Estos resultados constituyen la base para la discusión presentada en el apartado siguiente, donde se analizan las

implicaciones de estos hallazgos para la evolución de la victimología en las sociedades digitales.

Discusión

Los resultados del presente análisis evidencian que la victimología atraviesa un proceso de transformación impulsado por la acelerada digitalización de las relaciones humanas, la expansión de la ciberdelincuencia y el desarrollo de tecnologías basadas en inteligencia artificial. Mientras que la victimología clásica concentró históricamente su atención en las víctimas de delitos convencionales, la evidencia científica revisada demuestra que las sociedades digitales han generado escenarios inéditos de victimización caracterizados por la ausencia de límites geográficos, la permanencia del daño en los entornos virtuales y la creciente sofisticación de las estrategias utilizadas por los agresores.

Las investigaciones consultadas coinciden en señalar que fenómenos como el ciberacoso, la sextorsión, el robo de identidad, los discursos de odio y la difusión de contenido sintético generado mediante inteligencia artificial representan nuevas expresiones de violencia con importantes repercusiones psicológicas, sociales, económicas y jurídicas. Organismos internacionales como la UNESCO, la UNODC, UNICEF e INTERPOL han advertido que estos delitos presentan un crecimiento sostenido a nivel mundial, impulsado por la masificación del acceso a Internet, la conectividad permanente y la disponibilidad de herramientas tecnológicas cada vez más sofisticadas.

Uno de los aspectos más relevantes identificados durante la revisión corresponde a la aparición de nuevas modalidades de victimización asociadas con la inteligencia artificial generativa. Los deepfakes, la clonación de voz, la automatización del fraude y la creación de identidades digitales falsas modifican profundamente la naturaleza de los delitos tecnológicos, incrementando las posibilidades de manipulación y dificultando la identificación de los responsables. Esta realidad confirma que los conceptos tradicionales de víctima, agresor y daño requieren ser actualizados para responder a los desafíos que plantea la transformación digital.

Asimismo, la literatura analizada pone de manifiesto que la victimización digital posee características particulares que la diferencian de la delincuencia convencional. La permanencia de la información en Internet, la posibilidad de difusión masiva de contenidos, el anonimato de

los agresores y la continua exposición pública favorecen procesos de revictimización que prolongan el sufrimiento de las personas afectadas. Estas condiciones generan consecuencias que trascienden las pérdidas económicas, afectando la salud mental, la reputación, las relaciones sociales y el ejercicio efectivo de derechos fundamentales como la privacidad, la dignidad y la libertad de expresión.

Otro hallazgo significativo es el consenso existente entre los organismos internacionales respecto a la necesidad de fortalecer la cooperación internacional frente a los delitos digitales. La naturaleza transnacional de la ciberdelincuencia dificulta la actuación aislada de los Estados, haciendo indispensable el intercambio de información, la armonización normativa y el fortalecimiento de mecanismos de asistencia judicial y tecnológica. La reciente Convención de las Naciones Unidas contra la Ciberdelincuencia constituye un avance importante en este sentido; sin embargo, diversos autores advierten que su implementación deberá garantizar un adecuado equilibrio entre la persecución del delito y la protección de los derechos humanos, evitando prácticas de vigilancia excesiva o restricciones injustificadas a las libertades fundamentales.

Desde una perspectiva victimológica, los hallazgos también evidencian que la respuesta institucional debe evolucionar hacia modelos integrales de atención que combinen asistencia psicológica, asesoría jurídica, acompañamiento tecnológico y mecanismos efectivos de reparación del daño. La intervención no puede limitarse únicamente a la investigación penal, sino que debe orientarse a reducir la revictimización, fortalecer la resiliencia de las personas afectadas y promover una cultura de prevención basada en la alfabetización digital y el uso responsable de las tecnologías.

Finalmente, el estudio confirma que la victimología del siglo XXI se consolida como una disciplina profundamente interdisciplinaria, en la que convergen conocimientos provenientes de la criminología, el derecho, la psicología, la informática, la ciberseguridad, la inteligencia artificial y los derechos humanos. Esta integración resulta indispensable para comprender la complejidad de las nuevas formas de victimización y para diseñar estrategias preventivas y de protección acordes con la rápida evolución tecnológica. En consecuencia, futuras investigaciones deberán profundizar en fenómenos emergentes como la victimización algorítmica, los delitos en entornos inmersivos, el metaverso y las implicaciones éticas y jurídicas de la inteligencia artificial, con el propósito de fortalecer la capacidad de respuesta de

la victimología frente a los desafíos que caracterizan a las sociedades digitales contemporáneas.

Conclusiones

La evolución tecnológica ha transformado profundamente las dinámicas de victimización contemporáneas, generando escenarios que desafían los modelos tradicionales de análisis e intervención victimológica. La expansión de la ciberdelincuencia, la violencia digital y las amenazas derivadas de la inteligencia artificial han ampliado significativamente el campo de estudio de la victimología, obligando a desarrollar nuevas herramientas conceptuales y metodológicas.

La victimización digital presenta características particulares, entre ellas la permanencia del daño, la rápida difusión de contenidos, la anonimidad de los agresores y la posibilidad de revictimización constante. Estas condiciones incrementan la vulnerabilidad de las víctimas y requieren respuestas institucionales más eficaces.

La protección de los derechos humanos en los entornos digitales constituye uno de los principales desafíos de las sociedades contemporáneas. Por ello, resulta indispensable fortalecer políticas públicas orientadas a la prevención, educación digital, atención integral y reparación del daño.

La victimología del siglo XXI debe consolidarse como una disciplina interdisciplinaria capaz de comprender las complejas interacciones entre tecnología, criminalidad, vulnerabilidad humana y derechos fundamentales. Solo mediante enfoques integrales será posible construir entornos digitales más seguros y garantizar una protección efectiva para las víctimas de las nuevas formas de violencia y criminalidad emergentes.

Referencias bibliográficas

- Amerini, I., Caldelli, R., Del Bimbo, A., & Becarelli, R. (2024). Deepfake media forensics: State of the art and challenges ahead. arXiv. <https://arxiv.org>
- Garthe, R. C., Sullivan, T. N., & Larsen, R. A. A. (2023). Cyber-victimization and mental health concerns among middle school students before and during the COVID-19 pandemic.

Journal of Youth and Adolescence, 52(4), 840–851. <https://doi.org/10.1007/s10964-023-01737-2>

Guterres, A. (2024). Welcoming adoption of historic cybercrime convention, Secretary-General urges all States to join to promote safe cyberspace. United Nations. <https://press.un.org>

International Criminal Police Organization (INTERPOL). (2026). Over 5,800 arrests, USD 293 million intercepted in global fraud bust. INTERPOL. <https://www.interpol.int>

Kale, N., Portnoff, R., Thaker, P., Simpson, M., Wang, R., Kuo, K., Yadav, C., & Smith, V. (2026). Preventing AI-generated child sexual abuse material necessitates new approaches to AI safety. arXiv. <https://arxiv.org/abs/2607.05407>

Kamachee, M., Casper, S., Ding, M. L., Yew, R. J., Reuel, A., Biderman, S., & Hadfield-Menell, D. (2025). Video deepfake abuse: How company choices predictably shape misuse patterns. arXiv. <https://arxiv.org/abs/2512.11815>

Le Monde. (2024). In South Korea, young people are victims and perpetrators of pornographic deepfakes. Le Monde. <https://www.lemonde.fr>

Miotti, A., & Wasil, A. (2024). Combatting deepfakes: Policies to address national security threats and rights violations. arXiv. <https://arxiv.org>

Office of the United Nations High Commissioner for Human Rights (OHCHR). (2024). What are human rights? United Nations Human Rights. <https://www.ohchr.org>

Organisation for Economic Co-operation and Development (OECD). (2023). Digital environment and well-being of children and young people. OECD Publishing. <https://www.oecd.org>

Organización de las Naciones Unidas (ONU). (2024). Basic facts about the global cybercrime treaty. United Nations. <https://www.un.org>

Organización de las Naciones Unidas (ONU). (2024). Making the digital and physical world safer: Why the Convention against Cybercrime matters. United Nations Office at Geneva. <https://www.ungeneva.org>

-
- Organización de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). Cybercrime and cyber-enabled crime framework. United Nations Office on Drugs and Crime. <https://www.unodc.org>
- Organización de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). Transnational organized crime: The globalized illegal economy. United Nations. <https://www.unodc.org>
- Reuters. (2025). UN cybercrime pact to be signed in Hanoi raises hopes and concerns. Reuters. <https://www.reuters.com>
- TechRadar. (2026). USD 293 million seized and 5,811 arrests made in huge anti-scam and fraud action by INTERPOL and law enforcement agencies across 97 countries. TechRadar. <https://www.techradar.com>
- Twomey, J., Foley, S., Robinson, S., Quayle, M., Aylett, M. P., Linehan, C., & Murphy, G. (2025). “What do you expect? You're part of the internet”: Analyzing celebrities' experiences as users of deepfake technology. arXiv. <https://arxiv.org/abs/2507.13065>
- UN Women. (2024). Online and technology-facilitated violence against women and girls. United Nations Women. <https://www.unwomen.org>
- UNESCO. (2023). Defining school bullying and its implications on education, teachers and learners. United Nations Educational, Scientific and Cultural Organization. <https://www.unesco.org>
- UNESCO. (2024). AI and the Holocaust: Rewriting history? The risks of generative artificial intelligence. United Nations Educational, Scientific and Cultural Organization. <https://www.unesco.org>
- UNESCO. (2024). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization. <https://www.unesco.org>
- UNESCO. (2024). Technology on her terms: Social media, girls' well-being and education. United Nations Educational, Scientific and Cultural Organization. <https://www.unesco.org>

UNICEF. (2025). Deepfake abuse is abuse. United Nations Children's Fund. <https://www.unicef.org>

UNICEF. (2026). Artificial intelligence and child sexual abuse and exploitation. United Nations Children's Fund. <https://www.unicef.org>

UNICEF. (2026). Deepfake abuse is abuse: Statement by UNICEF on AI-generated sexualised images of children. United Nations Children's Fund. <https://www.unicef.org>

UNICEF México. (2026). IA y deepfakes: Nuevos riesgos de violencia sexual contra la niñez. Fondo de las Naciones Unidas para la Infancia. <https://www.unicef.org/mexico>

Umbach, R., Henry, N., Beard, G., & Berryessa, C. (2024). Non-consensual synthetic intimate imagery: Prevalence, attitudes, and knowledge in 10 countries. arXiv. <https://arxiv.org>

World Society of Victimology. (2023). Victimology: Definition and scope. World Society of Victimology. <https://www.worldsocietyofvictimology.org>

Declaraciones finales

Conflicto de intereses: Los autores declaran que no existe conflicto de interés posible.

Financiamiento: No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento: N/A

Nota editorial: El artículo no es producto de una publicación anterior.