

Área de Conocimiento de Ciencias Jurídicas y Sociales

Carrera de Derecho, Modalidad por Encuentro



Trabajo Monográfico para optar al título de Licenciada en Derecho

Título: Tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales conforme a la Ley N.º 1042 en Nicaragua.

Autora: Magdiela del Carmen Acuña Cruz

Tutor: Msc. Guidyan Lenin Hernández García

León, Nicaragua febrero 2026

2026: 47/19 Nicaragua, Cristiana, Socialista, Solidaria, Siempre más allá!

RESUMEN

La presente investigación analiza la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales, en el marco de la Ley N.º 1042, y su relación con la protección de los derechos fundamentales de las víctimas. Se trata de un estudio documental con enfoque cualitativo, sustentado en el análisis de normas jurídicas, doctrina especializada y referencias contextuales de actores vinculados al fenómeno, con el propósito de enriquecer la interpretación jurídica y visibilizar las implicaciones sociales de la difusión no consentida de contenidos íntimos.

El análisis permitió determinar que la tutela judicial efectiva constituye un derecho fundamental que exige procedimientos ágiles, resoluciones debidamente motivadas y mecanismos eficaces de protección de la intimidad, la dignidad y la privacidad digital. Aunque la Constitución, los tratados internacionales, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 establecen un marco normativo relevante, su eficacia práctica enfrenta desafíos derivados de vacíos regulatorios, limitaciones técnicas, restricciones institucionales y la complejidad de los ciberdelitos de carácter transnacional.

Asimismo, se destaca la necesidad de fortalecer la cooperación internacional, la coordinación con plataformas digitales, la capacitación de operadores judiciales y la implementación de protocolos técnicos para la preservación de evidencia digital. Se identificó igualmente la importancia de promover políticas de educación digital, apoyo psicológico y medidas preventivas orientadas a evitar la revictimización y garantizar una respuesta integral. Finalmente, la comparación con la legislación de España, Italia y Dinamarca aporta referentes útiles para perfeccionar la normativa nacional y consolidar una tutela judicial efectiva pronta, integral y sensible frente a la violencia digital.

León, 09 de febrero de 2026

M.Sc. Francisco Valladares Rivas

Director de área específica de Derecho

Ciencias Jurídicas y Sociales, UNAN, León

Su despacho

Estimado maestro Valladares

Por medio de la presente y de la manera más atenta me dirijo a Usted, en ocasión de expresarle mi visto bueno como Tutor de Monografía de la bachillera: **Magdiela del Carmen Acuña Cruz**, para la defensa de su Monografía como forma de culminación de estudios de la licenciatura de la carrera de Derecho modalidad por encuentro del Área de Conocimiento de Ciencias Jurídicas y Sociales de la UNAN, León titulada **“Tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales conforme a la Ley N.º 1042 en Nicaragua”**.

La estudiante ha llevado a cabo una investigación rigurosa, utilizando una amplia cantidad de fuentes y metodologías apropiadas para su tema. La Monografía es clara, coherente y bien estructurada.

Basado en su trabajo de investigación, considero que su Monografía es una contribución significativa en su campo de estudio y de su práctica profesional y merece ser presentada ante el tribunal calificador para su defensa y correspondiente evaluación.

Sin otro particular y deseándole el mayor de los éxitos, se despide de Usted,

Muy atentamente,

Prof. M.Sc. Guidyan Lenin Hernández García

Tutor de Tesis.

Área de Conocimiento de Ciencias Jurídicas y Sociales

UNAN, León

Cc.

Tania Vanegas-Directora General área de conocimiento Ciencias Jurídicas y Sociales.

Denis Reyes-Secretario Académico área de conocimiento Ciencias Jurídicas y Sociales.

Archivo.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO I: MARCO CONCEPTUAL DEL CIBERDELITO Y LA TUTELA JUDICIAL EFECTIVA	4
1. Nociones conceptuales sobre ciberdelitos y violencia digital.....	4
1.1 Ciberdelitos.....	4
1.2 Difusión no autorizada de imágenes íntimas en redes sociales	18
1.3. Derechos fundamentales vulnerados en el entorno digital	19
1.4 La tutela judicial efectiva en el marco conceptual de los ciberdelitos	21
1.5 Perspectivas teóricas sobre violencia digital, redes sociales y evidencia electrónica	21
CAPITULO II: IMPORTANCIA DE LA TUTELA JUDICIAL EFECTIVA EN LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DE LAS VÍCTIMAS DE CIBERDELITOS	24
2.1 Aspectos introductorios	24
2.2 Nociones conceptuales de la tutela judicial efectiva.....	25
2.3 Fundamentos Normativos	26
2.3.1 Marco Normativo	26
2.4 Interpretación de la norma y alcance	34
2. 5 Retos y desafíos de la tutela judicial efectiva frente a los ciberdelitos	36
CAPITULO III: ALCANCES Y LIMITACIONES DEL MARCO LEGAL VIGENTE RESPECTO A LA TUTELA JUDICIAL EFECTIVA FRENTE A LA DIFUSIÓN NO AUTORIZADA DE IMÁGENES ÍNTIMAS EN REDES SOCIALES.	39
3.1 Aspectos Introductorios.....	39
3.2 Alcances normativos del marco legal vigente en Nicaragua	40
3.2.1 Constitución Política de Nicaragua	41
3.2.2 Código Penal.....	41
3.2.3 Código Procesal Penal.....	42
3.2.4 Ley N.º 1042, Ley Especial de Ciberdelitos	42
3.2.5 Mecanismos de tutela judicial efectiva.....	43
3.3 Criterios doctrinales sobre la publicación no consentida de imágenes íntimas	45

3. 4 Referentes de judicialización y visibilización mediática en Nicaragua	46
3.5 Derecho Comparado Legislativo sobre la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas	47
3.5.1 España	48
3.5. 2 Italia	49
3.5.3 Dinamarca: iniciativa de ley contra deepfakes	51
3.6 Análisis comparativo y aprendizajes para Nicaragua	52
3.7 Principales limitaciones del marco legal vigente respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales	55
3.7.1 Falta de tipificación penal autónoma y clara	55
3.7.2 Predominio de una respuesta reactiva, insuficiente frente a la viralización digital	57
3.7.3 Medidas cautelares centradas en la preservación de la evidencia, insuficientes para la neutralización inmediata del contenido	58
3.7.4 Vacíos frente a tecnologías emergentes y manipulación digital	59
3.7.5 Reparación integral insuficiente	60
3.7.6 Limitada cooperación con plataformas digitales internacionales	61
3.7.7 Prevención débil	61
DISEÑO METODOLÓGICO	63
Tipo de investigación	63
Enfoque de investigación	64
Fuentes de información	65
Técnicas de Investigación	66
Análisis documental e instrumentos utilizados	66
Procedimiento de análisis y sistematización	67
Plan de análisis	68
Consideraciones éticas	68
CONCLUSIONES	69
Conclusiones del Capítulo I – Marco conceptual del ciberdelito y la tutela judicial efectiva	70
Conclusiones del Capítulo II – Importancia de la tutela judicial efectiva en la protección de los derechos fundamentales de las víctimas de ciberdelitos	70

Conclusiones del Capítulo III – Alcances y limitaciones del marco legal vigente respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales	71
RECOMENDACIONES	73
Derivadas del Capítulo I	73
Derivadas del Capítulo II	73
Derivadas del Capítulo III	74
FUENTES DE CONOCIMIENTO	75
Fuentes Primarias	75
Fuentes Secundarias	76
Fuentes terciarias	82

Dedicatoria

Dedico este trabajo, ante todo, a Dios, por darme vida, fortaleza y sabiduría en cada paso de este camino, guiándome siempre con su luz.

A mi madre, María Cristina Cruz, y a mi padre, Juan Antonio Acuña Reyes, por su amor incondicional, quienes han sido mi guía, mi refugio y el pilar que me ha permitido crecer y ser la mujer que soy hoy.

A mis abuelos, Mercedes Acuña y María Luisa Reyes, cuya fortaleza y sabiduría, me han inspirado a seguir luchando por mis sueños y a enfrentar cada desafío con valentía.

Y a mí misma, por la constancia, disciplina y perseverancia que he demostrado al enfrentar nuevos comienzos, superar obstáculos y transformar cada desafío en aprendizaje.

Agradecimientos

A Dios, por darme la fuerza, la paciencia y la sabiduría necesarias para superar cada desafío y permitirme alcanzar este logro académico.

A mi madre, María Cristina Cruz, y a mi padre, Juan Antonio Acuña Reyes, por su apoyo inquebrantable, confianza en mí y que han sido el cimiento de mis sueños para perseverar incluso en los momentos más difíciles.

A mis abuelos, Mercedes Acuña y María Luisa Reyes, que me han enseñado el valor de la dedicación, la humildad y la perseverancia.

A mi tutor, Guidyan Hernández, por su guía, paciencia y valiosa orientación, que han sido fundamentales para la culminación de este trabajo.

A mis profesores y compañeros, por compartir sus conocimientos, experiencias y apoyo, contribuyendo de manera significativa a mi formación académica y profesional.

A la UNAN-León, IES que me ha brindado el espacio para formarme, crecer y desarrollar este trabajo, así como a todas las personas que, de manera directa o indirecta, hicieron posible este logro; su apoyo y estímulo han sido esenciales en este camino.

Y finalmente, a mí misma, por la disciplina, la constancia y la pasión que me han permitido empezar de cero en un nuevo departamento, superar desafíos y alcanzar este hito académico, celebrando cada esfuerzo y aprendizaje como parte de mi crecimiento personal y profesional.

INTRODUCCIÓN

El acelerado desarrollo de las tecnologías digitales y la expansión global de internet han transformado de manera profunda las dinámicas sociales, económicas y jurídicas contemporáneas. Si bien estas transformaciones han generado importantes beneficios en términos de acceso a la información, comunicación y desarrollo económico, también han propiciado la aparición de nuevas formas de criminalidad, conocidas como ciberdelitos. Estas conductas ilícitas utilizan sistemas informáticos y plataformas digitales para afectar bienes jurídicos fundamentales, como la intimidad, la dignidad, la privacidad y la seguridad de las personas.

Entre estas conductas, la difusión no autorizada de imágenes íntimas en redes sociales constituye una de las manifestaciones más graves de la violencia digital. Esta práctica expone a las víctimas a daños emocionales, sociales y económicos de considerable magnitud, y plantea desafíos significativos para la tutela judicial efectiva en Nicaragua. La rapidez con la que se difunden los contenidos, la relativa facilidad del anonimato en los entornos digitales y la dimensión transnacional de estas conductas dificultan la respuesta oportuna y eficaz de los sistemas de justicia, comprometiendo la protección de los derechos fundamentales.

Desde una perspectiva histórica, los ciberdelitos comenzaron a manifestarse en las décadas de 1970 y 1980, principalmente como intrusiones informáticas y accesos no autorizados a sistemas de datos. Con el avance de las tecnologías de la información y la globalización de las comunicaciones, estas prácticas evolucionaron hacia modalidades más complejas, incluyendo el fraude electrónico, el robo de identidad, el acoso digital y diversas formas de violencia digital, como la difusión de contenido íntimo sin consentimiento. Esta evolución evidenció la necesidad de respuestas jurídicas especializadas y adaptadas a la realidad digital, capaces de garantizar la protección efectiva de los derechos de las víctimas.

En el ámbito jurídico internacional, la adopción del Convenio sobre Cibercriminalidad del Consejo de Europa (2001), conocido como Convenio de Budapest, marcó un hito en la armonización legislativa y en la cooperación entre Estados para la persecución de delitos

informáticos. En América Latina, el desarrollo normativo ha sido progresivo, y en Nicaragua se consolidó con la Ley N.º 1042, Ley Especial de Ciberdelitos, aprobada en 2020. Esta normativa tipifica diversas conductas informáticas, incluyendo la difusión no consentida de imágenes íntimas, y establece sanciones penales y medidas de protección para las víctimas.

La elección del tema responde a la creciente incidencia de los ciberdelitos en la sociedad nicaragüense y a la necesidad de analizar críticamente los mecanismos legales destinados a proteger los derechos fundamentales de las víctimas. El estudio se centra en la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales, a partir del análisis de la normativa vigente, la doctrina especializada, la jurisprudencia relevante y los estándares internacionales, incorporando referencias comparadas como elementos de apoyo teórico. La revisión de normas, doctrina especializada y casos judiciales divulgados en medios de comunicación permite identificar vacíos legales, limitaciones institucionales y desafíos técnicos que afectan la efectividad de la respuesta judicial, evidenciando que la criminalidad digital constituye una problemática estructural que requiere acciones integrales, actualizaciones normativas y protocolos especializados.

En este contexto, surgen las siguientes preguntas que guían la investigación: ¿Cómo garantiza la Ley N.º 1042 la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas? ¿Qué vacíos o limitaciones existen en el marco legal para la protección de los derechos de las víctimas, y cómo podrían abordarse?

El objetivo general de la investigación consiste en analizar la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales, conforme a la Ley N.º 1042 en Nicaragua, en relación con la protección legal de los derechos fundamentales de las víctimas. Para cumplir este propósito, el estudio se orienta a tres líneas de análisis: primero, describir el marco conceptual y normativo del ciberdelito en Nicaragua, con énfasis en la Ley N.º 1042; segundo, destacar la importancia de la tutela judicial efectiva como garantía esencial de acceso a la justicia; y tercero, identificar los alcances y limitaciones del marco legal vigente frente a la violencia digital.

La pertinencia del estudio se fundamenta en la necesidad de analizar críticamente el marco jurídico vigente, identificar posibles deficiencias desde una perspectiva normativa y doctrinal, y formular orientaciones dirigidas a fortalecer la protección de los derechos fundamentales en entornos digitales. Desde el ámbito académico, la investigación contribuye a la generación de conocimiento actualizado sobre la aplicación de la Ley N.º 1042 y sobre los mecanismos de tutela judicial efectiva en materia de ciberdelitos. Desde una dimensión social, ofrece insumos relevantes para operadores judiciales, legisladores y ciudadanía, orientados tanto a la prevención como a la respuesta frente a la difusión ilícita de contenidos íntimos. Asimismo, se vincula con las políticas públicas nacionales dirigidas al fortalecimiento del acceso a la justicia y al desarrollo de capacidades institucionales en materia digital. Además, se vincula con el Plan Nacional de Lucha contra la Pobreza y para el Desarrollo Humano (2022-2026) y con la Estrategia Nacional de Educación en Todas sus Modalidades “Bendiciones y Victorias” 2024-2026, al promover la igualdad de derechos, el fortalecimiento del acceso a la justicia y la construcción de capacidades investigativas.

Metodológicamente, la investigación adopta un enfoque cualitativo y documental, orientado a comprender en profundidad la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales. El estudio se sustenta principalmente en el análisis de fuentes normativas, doctrinales, jurisprudenciales y documentales seleccionadas por su relevancia para el objeto de investigación.

De manera complementaria, se realizaron consultas exploratorias de carácter no sistemático a actores vinculados al ámbito jurídico y técnico, con el propósito de enriquecer la comprensión práctica del fenómeno. Asimismo, se tomaron como referencia relatos voluntarios de personas afectadas por la difusión o el intento de difusión de imágenes íntimas en redes sociales. Estas referencias tuvieron un carácter ilustrativo y contextual, orientado a complementar el análisis jurídico sin modificar el enfoque estrictamente documental del estudio.

La estructura de la tesis comprende tres capítulos principales. El Capítulo I, Marco conceptual del ciberdelito y la tutela judicial efectiva, desarrolla los fundamentos teóricos y jurídicos necesarios para comprender el fenómeno. El Capítulo II, Importancia de la

tutela judicial efectiva en la protección de los derechos fundamentales de las víctimas de ciberdelitos, analiza la dimensión teórica y normativa de este derecho y su relevancia en entornos digitales. El Capítulo III, Alcances y limitaciones del marco legal vigente frente a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas, presenta un análisis crítico de la Ley N.º 1042 y de la práctica judicial, considerando experiencias comparadas y señalando fortalezas y vacíos. Finalmente, la tesis incluye conclusiones y recomendaciones orientadas a fortalecer la tutela judicial efectiva en Nicaragua.

En síntesis, esta investigación propone un análisis integral que articula teoría, normativa y práctica judicial, con el propósito de visibilizar los desafíos y posibilidades de la tutela judicial efectiva en el contexto digital, particularmente frente a la difusión no consentida de imágenes íntimas. De esta manera, se aspira a generar aportes académicos y prácticos que contribuyan a la protección de los derechos fundamentales, a la prevención de la violencia digital y al fortalecimiento de un sistema de justicia más ágil, completo y sensible a las necesidades de las víctimas en Nicaragua.

CAPÍTULO I: MARCO CONCEPTUAL DEL CIBERDELITO Y LA TUTELA JUDICIAL EFECTIVA

1. Nociones conceptuales sobre ciberdelitos y violencia digital

1.1 Ciberdelitos

1.1.1 Concepto General de Ciberdelito

La comprensión del ciberdelito exige partir de una definición clara que permita delimitar su alcance jurídico y social, por lo que resulta pertinente distinguir entre el concepto sustantivo, establecido por la normativa vigente, y el concepto doctrinal, desarrollado por la literatura especializada.

Esta diferenciación resulta necesaria, en tanto la ley proporciona una definición positiva y vinculante, mientras que la doctrina aporta interpretaciones críticas y multidisciplinarias que enriquecen la comprensión del fenómeno, especialmente en el contexto de la violencia digital y la protección de los derechos fundamentales.

1.1.1.1 Concepto sustantivo del ciberdelito

En Nicaragua, la Ley N.º 1042, Ley Especial de Ciberdelitos y sus reformas, establece en su artículo 4 que los ciberdelitos son acciones u omisiones típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, medio o fin los datos, los sistemas informáticos y las Tecnologías de la Información y la Comunicación, y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima.

Esta definición no solo enfatiza la dimensión tecnológica del comportamiento ilícito, sino que también permite vincular el ciberdelito con la vulneración de derechos fundamentales, particularmente cuando el uso indebido de las tecnologías incide en la vida privada, la dignidad o la integridad personal de las personas afectadas.

1.1.1.2 Concepto doctrinal del ciberdelito

Desde una perspectiva teórica, los ciberdelitos han sido objeto de análisis multidisciplinarios que han permitido una comprensión más amplia y compleja del fenómeno. Wall (2007) sostiene que los ciberdelitos no deben entenderse únicamente como delitos cometidos a través de tecnologías informáticas, sino como un fenómeno multidimensional que transforma las dinámicas sociales y culturales. Este enfoque abarca tanto delitos tradicionales cometidos mediante medios digitales como nuevas formas de victimización, entre ellas el ciberacoso y otras manifestaciones de violencia digital que afectan la intimidad y la seguridad emocional de las personas.

En la misma línea, Brenner (2017) señala que los ciberdelitos constituyen fenómenos complejos que no se limitan a la ejecución de actos ilícitos a través de dispositivos digitales, sino que están profundamente influenciados por factores psicológicos, socioculturales y jurídicos. Esta complejidad exige una adaptación constante de las respuestas legales, superando las categorías tradicionales del derecho penal.

En el ámbito internacional, el reconocimiento de los ciberdelitos como conductas que pueden implicar violaciones a derechos fundamentales se refleja en la Convención sobre Cibercriminalidad del Consejo de Europa (2001), conocida como Convenio de Budapest, instrumento jurídico de referencia para la cooperación internacional y la armonización legislativa en la lucha contra estos delitos.

Por su parte, en el contexto latinoamericano, Vázquez Sánchez (2020) destaca la creciente preocupación por los ciberdelitos como vulneraciones directas a los derechos humanos, al señalar que estos no solo afectan sistemas informáticos o bienes patrimoniales, sino que se encuentran estrechamente vinculados con la violencia digital y la difusión no autorizada de imágenes íntimas, impactando de manera diferenciada en mujeres, niñas y adolescentes.

En virtud de lo anterior, se refuerza la necesidad de reconocer que los ciberdelitos, aun cuando poseen una naturaleza tecnológica, pueden afectar gravemente derechos fundamentales como la privacidad, la dignidad y la seguridad personal. Solo a través de un enfoque integral que articule elementos jurídicos, sociales y culturales será posible desarrollar estrategias preventivas y respuestas judiciales efectivas que garanticen una adecuada protección de las personas en un entorno digital cada vez más interconectado.

1.1.2 Origen y Evolución del Ciberdelito

El origen de los ciberdelitos se encuentra estrechamente vinculado con la emergencia de la tecnología digital y la expansión del uso de internet en la segunda mitad del siglo XX. Si bien prácticas como el acceso ilegal a sistemas informáticos o la distribución de contenido ilícito se registran desde los primeros días de la red global, su conceptualización y clasificación dentro del derecho penal no fueron reconocidas formalmente sino hasta el siglo XXI (Tack, 2015).

En un primer momento, los ciberdelitos se percibieron como una extensión de los delitos tradicionales cometidos mediante nuevas tecnologías. El hacking o intrusión informática, con fines de robo o manipulación de datos, fue uno de los primeros delitos informáticos reconocidos. Estas prácticas comenzaron a adquirir relevancia especialmente durante las décadas de 1970 y 1980, con la popularización de las redes de computadoras y el uso masivo de internet (Sain, 2015).

Desde el estado del arte, diversos autores han analizado la evolución de los ciberdelitos como un fenómeno dinámico y multidimensional. Pons Gamón (2017) sostiene que la expansión de internet y la globalización de las comunicaciones han permitido que los ciberdelincuentes operen sin límites jurisdiccionales claros, lo que ha complejizado la

persecución penal y la cooperación internacional. De forma paralela, Joyanes Aguilar (2011) subraya que la digitalización y la interconexión global han transformado la naturaleza de los delitos, pasando de simples intrusiones a prácticas más sofisticadas como el phishing, el robo de identidad, el fraude en línea y diversas formas de violencia digital.

En el plano jurídico, la necesidad de legislar sobre estos delitos surgió tardíamente, dado que las normas tradicionales no estaban preparadas para enfrentar la criminalidad digital. La Convención sobre Cibercriminalidad del Consejo de Europa (2001), conocida como Convenio de Budapest, marcó un hito al establecer un marco internacional de cooperación y armonización legislativa, consolidando una respuesta común frente a delitos transnacionales como el fraude electrónico, el acceso ilícito a sistemas y la distribución de material ilegal.

En América Latina, el desarrollo normativo ha sido progresivo. Autores como Aboso (2022) destacan que muchos países debieron adaptar sus códigos penales para enfrentar un fenómeno creciente y complejo, respondiendo a la necesidad de proteger a los ciudadanos frente a riesgos derivados del uso no regulado de las tecnologías de la información.

Actualmente, los ciberdelitos han ingresado en una nueva fase de evolución, que incluye el ciberterrorismo y el crimen organizado digital. Prácticas como los ataques DDoS o la manipulación de criptomonedas para el lavado de dinero evidencian la sofisticación de estas conductas. Además, las víctimas ya no son únicamente individuos, sino también empresas y gobiernos, lo que ha impulsado el fortalecimiento de la ciberseguridad y la creación de protocolos de protección digital.

A partir del análisis realizado, puede sostenerse que los ciberdelitos han pasado de ser un fenómeno aislado, cometido principalmente por hackers, a convertirse en una forma de criminalidad global, interconectada y cada vez más sofisticada. Esta evolución exige no solo respuestas penales, sino también políticas públicas que integren la dimensión social y cultural del fenómeno, reconociendo que los ciberdelitos afectan no solo el ámbito informático, sino también derechos fundamentales como la privacidad y la dignidad de las víctimas.

1.1.3 Diferenciación entre delito tradicional y ciberdelito

La diferenciación entre delito tradicional y ciberdelito ha sido objeto de debate en la criminología contemporánea, dado que la criminalidad digital no se ajusta plenamente a las categorías clásicas del derecho penal. Aunque ambos tipos de delito comparten ciertos elementos, existen diferencias sustanciales en términos de espacio, medio, víctimas y métodos utilizados. Esta distinción resulta crucial para comprender las implicaciones jurídicas y sociales de los ciberdelitos dentro de los sistemas legales modernos.

1.1.3.1 Espacio y medio: lo físico frente a lo digital

Una de las diferencias más evidentes entre los delitos tradicionales y los ciberdelitos radica en el espacio y el medio en los que se cometen. En efecto, los delitos tradicionales, como el robo, el asalto o el homicidio, ocurren en espacios físicos y requieren la presencia simultánea de agresores y víctimas en un mismo lugar, facilitando la delimitación territorial de la jurisdicción y, por ende, la investigación y sanción.

Por el contrario, los ciberdelitos se perpetran en espacios digitales, trascendiendo las fronteras físicas y permitiendo que los agresores operen desde cualquier parte del mundo, afectando a víctimas ubicadas en diferentes países. Esta particularidad convierte a los ciberdelitos en conductas especialmente complejas de rastrear y sancionar, dado que los perpetradores suelen recurrir al anonimato y a tecnologías de encriptación para ocultar su identidad y ubicación.

Desde el estado del arte, diversos autores han subrayado esta diferencia fundamental. Posada Maya (2017) sostiene que los ciberdelitos ocurren en una realidad virtual que desafía los parámetros clásicos de la teoría del delito, ya que la noción de “lugar de comisión” se vuelve difusa. De manera similar, Galán Muñoz (2018) enfatiza que la naturaleza digital de los ciberdelitos dificulta la aplicación de las leyes locales, dado que las fronteras jurídicas tradicionales no se corresponden con la lógica transnacional del ciberespacio. En la misma línea, Benítez (2019) advierte que la ciberdelincuencia opera en distintos niveles del ciberespacio, incluyendo la dark web, lo que incrementa la complejidad de su persecución; no solo se trata de enfrentar delitos que se difunden

rápidamente en entornos abiertos, sino también de rastrear actividades ocultas en espacios digitales de difícil acceso.

En virtud de lo anterior, la diferencia entre lo físico y lo digital no es meramente espacial, sino que representa un cambio estructural en la forma de concebir el delito y su persecución. Por consiguiente, el ciberdelito no puede entenderse como una simple digitalización del delito tradicional, sino como una categoría autónoma que exige respuestas normativas, procesales y preventivas propias, así como mecanismos reforzados de cooperación internacional, orientados a garantizar una protección efectiva de los derechos fundamentales frente a la criminalidad digital.

1.1.3.2 Métodos y herramientas: el uso de la tecnología

Otro aspecto clave que distingue a los ciberdelitos de los delitos tradicionales es el uso de la tecnología como herramienta. De hecho, los delitos tradicionales suelen involucrar la fuerza física, como el uso de un arma en un robo o una agresión física, constituyendo esta característica un elemento central de crímenes como el secuestro o el homicidio.

En oposición a ello, los ciberdelitos no recurren a la violencia física, sino que se distinguen por el uso de sistemas informáticos, redes y software para la comisión de conductas ilícitas, teniendo entre sus modalidades más frecuentes el malware, el phishing, el ransomware y los ataques DDoS (denegación de servicio distribuido), entre otros, los cuales explotan vulnerabilidades tecnológicas con el fin de acceder a datos personales, sustraer información financiera o difundir contenido ilegal.

Diversos estudios han subrayado que los ciberdelitos se diferencian de los delitos tradicionales por el uso de herramientas tecnológicas específicas. Pons Gamón (2017) señala que el malware, el phishing y los ataques DDoS han transformado la criminalidad, generando nuevos retos para la legislación y la seguridad. De manera similar, Lodato, Jaime, Gallegos y López (2023) destacan que la tecnología constituye simultáneamente el medio y el objetivo del delito, lo que obliga a repensar la protección jurídica y a considerar los efectos sociales y emocionales de estas prácticas.

En este sentido, puede afirmarse que la lucha contra los ciberdelitos no puede limitarse a respuestas normativas. Se requieren estrategias integrales que incluyan prevención,

cooperación internacional y fortalecimiento de capacidades forenses, con el fin de garantizar una protección efectiva de los derechos fundamentales de las víctimas.

1.1.3.3 Víctimas y su impacto psicosocial

Uno de los aspectos más relevantes de los ciberdelitos es la diversidad y el alcance global de las víctimas. Estos delitos pueden afectar a cualquier persona, organización o entidad pública, sin limitaciones geográficas, generando riesgos complejos que desafían las respuestas jurídicas y sociales.

El impacto psicosocial sobre las víctimas puede incluir ansiedad, estrés, estigmatización social y repercusiones económicas. A diferencia de los delitos tradicionales, donde el daño es principalmente físico o patrimonial, los ciberdelitos afectan la intimidad, la reputación y la seguridad emocional de las personas, lo que exige mecanismos jurídicos y sociales específicos para su atención y reparación.

1.1.3.3.1 Diversidad y alcance de las víctimas

En el ámbito de la criminalidad digital, la condición de víctima se amplía considerablemente. Las personas naturales son especialmente vulnerables, dado que la elevada lesividad de estas conductas multiplica el número de víctimas potenciales, afectando a usuarios comunes que carecen de herramientas de protección digital (López Gorostidi, 2020). Además, la ciberviolencia impacta de manera diferenciada según género y edad, con especial incidencia en mujeres y adolescentes, lo que exige incorporar un enfoque interseccional en la tutela judicial (Era-Mesa, Caro-Caro y Del Rey-Alamillo, 2022).

Por su parte, las personas jurídicas enfrentan ataques que generan consecuencias económicas y reputacionales significativas (Sepúlveda García de la Torre et al., 2019). Asimismo, las entidades públicas, incluidos gobiernos y organismos internacionales, pueden sufrir ciberdelitos que comprometen la seguridad institucional y nacional, especialmente en casos de espionaje digital o ataques a infraestructuras críticas (Paz, Vargas, Albornoz y Mogollón, 2025).

Esta pluralidad evidencia que la victimización digital no es un fenómeno aislado, sino un proceso estructural y multinivel que requiere respuestas jurídicas y sociales integrales, adaptadas a la complejidad del ciberespacio.

1.1.3.3.2 Impacto psicosocial y emocional en las víctimas

El daño de los ciberdelitos trasciende lo económico, afectando directamente la esfera emocional y psicológica de las víctimas. Conductas como el ciberacoso, la difusión no autorizada de imágenes íntimas o el fraude en línea generan secuelas que incluyen ansiedad, depresión, disminución de la autoestima y estrés postraumático.

Desde el estado del arte, Larrañaga, Navarro y Yubero (2018) evidencian que el ciberacoso produce consecuencias severas, particularmente en adolescentes. González-Vega (2023) resalta la revictimización digital, agravada por la viralización de contenidos en redes sociales, prolongando el sufrimiento y dificultando la reparación del daño. Asimismo, Kowalski et al. (2014) destacan que la exposición prolongada a la violencia digital puede inducir estrés postraumático, mientras que Hinduja y Patchin (2019) vinculan esta exposición con ideación suicida en jóvenes, constituyéndose en un problema de salud pública.

Por ello, las sanciones penales deben complementarse con acompañamiento psicológico y mecanismos de reparación simbólica, garantizando un enfoque integral y humanizado frente a las agresiones en el entorno digital. Reconocer la diversidad de víctimas y la gravedad de las afectaciones psicosociales resulta esencial para implementar estrategias preventivas, garantizar protección efectiva y asegurar una tutela judicial que responda adecuadamente a la complejidad de la criminalidad digital.

1.1.4 Análisis Jurídico de los Ciberdelitos

El estudio de los ciberdelitos exige un análisis jurídico que considere los componentes internos del tipo penal, a fin de delimitar su estructura dogmática y comprender cómo se configuran en la práctica. En este sentido, se distinguen tres elementos fundamentales: el objetivo, referido a la conducta externa realizada en el entorno digital; el subjetivo, vinculado a la intención y voluntad del autor; y el normativo, que permite subsumir la conducta en el tipo penal específico regulado por la Ley N.º 1042, con especial énfasis

en el ciberdelito de difusión no autorizada de imágenes íntimas en redes sociales, objeto de la presente investigación.

1.1.4.1 Elemento objetivo del ciberdelito

El **elemento objetivo** se refiere a la conducta externa que se materializa en el ciberespacio mediante acciones digitales concretas. En el caso de la difusión no autorizada de imágenes íntimas, la acción típica consiste en publicar, compartir o distribuir contenido íntimo sin el consentimiento de la persona afectada, utilizando plataformas digitales o redes sociales como medio comisivo.

En relación con los elementos objetivos del tipo penal aplicados a los ciberdelitos, la conducta se exterioriza a través de dichas acciones digitales ilícitas. El sujeto activo es la persona que ejecuta la conducta utilizando herramientas tecnológicas, mientras que el sujeto pasivo es la persona titular de las imágenes difundidas, cuyos derechos fundamentales resultan vulnerados.

El bien jurídico protegido se vincula principalmente con la intimidad, la privacidad, la dignidad humana y el libre desarrollo de la personalidad, los cuales se ven directamente afectados por la divulgación no consentida de contenido íntimo. El resultado se concreta en la lesión efectiva de estos bienes jurídicos, manifestada en daños psicológicos, sociales y reputacionales para la víctima.

El nexo de causalidad se establece cuando el daño producido es consecuencia directa de la conducta digital desplegada por el autor, es decir, de la difusión no autorizada del material íntimo. Finalmente, las circunstancias de tiempo, modo y lugar presentan especial relevancia en los ciberdelitos, ya que la conducta puede ejecutarse en un momento determinado, mediante medios tecnológicos específicos y desde un espacio virtual que trasciende las fronteras físicas tradicionales.

Autores como Bardavío Antón (2022) subrayan que este elemento debe analizarse desde la **imputación objetiva**, ya que la acción tecnológica concreta como el acceso ilícito, la manipulación de datos o la divulgación de imágenes delimita la responsabilidad penal. De manera complementaria, Agustina (2021) plantea que los ciberdelitos requieren una

dogmática propia, pues el espacio virtual redefine los contornos del delito y exige nuevas categorías jurídicas.

Desde esta perspectiva, el elemento objetivo del ciberdelito no puede reducirse a una mera acción técnica. Debe concebirse como una conducta con capacidad de generar daños jurídicos, económicos y sociales de gran alcance. En el tipo penal objeto de estudio, este elemento se configura en la difusión digital no consentida de imágenes íntimas, constituyendo la **materialización externa del delito** y afectando directamente derechos fundamentales y esferas personales protegidas por el ordenamiento jurídico.

1.1.4.2 Elemento subjetivo del ciberdelito

El elemento subjetivo del ciberdelito se refiere a la intención y voluntad del autor al momento de ejecutar la conducta ilícita en el entorno digital. No basta con la mera realización de una acción tecnológica; es necesario que el sujeto actúe con dolo o, en determinados casos, con culpa, dependiendo de la tipificación penal aplicable.

Desde el estado del arte, Silva Sánchez (2020) enfatiza que la expansión del derecho penal en la era digital obliga a reconsiderar la intencionalidad del autor, ya que las motivaciones pueden ser económicas, ideológicas o incluso recreativas, lo que amplía el espectro de conductas dolosas. Por su parte, Muñoz Conde (2021) advierte que el elemento subjetivo en los ciberdelitos debe analizarse también en clave social, pues las motivaciones delictivas en el ciberespacio responden a dinámicas colectivas de poder, control y anonimato.

En el caso del ciberdelito de difusión no autorizada de imágenes íntimas, la intencionalidad se manifiesta principalmente como dolo directo, dado que el autor conoce y desea la divulgación del material íntimo sin consentimiento, con el propósito de causar daño, ejercer control o incluso obtener beneficios económicos mediante la exposición pública del contenido.

Por lo tanto, el elemento subjetivo se configura en torno a la voluntad consciente de emplear la tecnología para vulnerar bienes jurídicos protegidos. Se trata no únicamente de la intención genérica de delinquir, sino de una decisión deliberada de utilizar

herramientas digitales para materializar conductas ilícitas que afectan gravemente la esfera íntima y emocional de las víctimas.

1.1.4.3 Elemento Normativo del Ciberdelito

El elemento normativo permite subsumir la conducta en el tipo penal previsto por la Ley N.º 1042. Si bien el concepto general de ciberdelito se define en el Artículo 4 de dicha ley, en este apartado se analiza cómo la difusión no autorizada de imágenes íntimas en redes sociales se integra dentro de esa categoría.

La conducta analizada cumple con los requisitos de tipicidad y antijuridicidad, pues constituye una acción ilícita realizada mediante tecnologías de la información y la comunicación, dirigida a vulnerar derechos fundamentales de las víctimas. En este sentido, la norma reconoce que la divulgación digital de contenido íntimo sin consentimiento no es un mero acto tecnológico, sino una violación de bienes jurídicamente protegidos, lo que legitima la intervención penal.

Como señalan Rodríguez Ramos, Gil Gil y Bacigalupo (2025), el elemento normativo debe entenderse como la valoración jurídica que integra la acción tecnológica dentro de la categoría penal correspondiente. De este modo, la difusión no autorizada de imágenes íntimas se subsume en el tipo penal de ciberdelito, garantizando la tutela judicial efectiva frente a la criminalidad digital y reforzando la protección de la esfera personal de las víctimas.

1.1.4.4 Dimensión internacional de la Ley N.º 1042 y la cooperación en ciberdelitos

La Ley N.º 1042, además de tipificar conductas ilícitas en el ámbito digital, reconoce la dimensión transnacional de los ciberdelitos y la necesidad de cooperación internacional para garantizar la tutela judicial efectiva.

En este sentido, el Artículo 43 regula la extradición en casos relacionados con delitos previstos en la ley. Cuando Nicaragua no sea parte de tratados o convenios internacionales, se aplicará lo dispuesto en la Ley N.º 406, Código Procesal Penal, asegurando que la persecución penal de los ciberdelitos no dependa exclusivamente de acuerdos internacionales, sino que pueda realizarse también con base en la normativa interna.

Por su parte, el Artículo 44 establece la asistencia legal mutua en investigaciones y procesos vinculados a la aplicación de la Ley N.º 1042. Este precepto permite que las autoridades competentes de Nicaragua soliciten o presten cooperación internacional conforme a los tratados vigentes y, en ausencia de estos, con base en el principio de reciprocidad reconocido por el Derecho Internacional. De esta manera, se habilita un marco flexible que facilita la colaboración entre Estados en la lucha contra la criminalidad digital.

La dimensión internacional de la tutela judicial efectiva se refuerza con la aprobación del Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia (Decreto A.N. N.º 8651, 2020). Este instrumento establece mecanismos específicos de cooperación entre los Estados iberoamericanos para la preservación y obtención de evidencia digital, incluyendo medidas como la incautación de sistemas informáticos, la preservación inmediata de datos, la intervención de comunicaciones y el acceso a información contenida en dispositivos electrónicos. Asimismo, garantiza el respeto de los derechos humanos en la ejecución de las solicitudes de cooperación y designa autoridades centrales para canalizar las peticiones, con el objetivo de agilizar y fortalecer la colaboración jurídica internacional.

Desde el estado del arte, diversos estudios doctrinales subrayan que la cooperación internacional es indispensable para la efectividad de la tutela judicial en contextos transnacionales. Brenner (2013) advierte que la ausencia de armonización normativa internacional debilita la capacidad de los Estados para garantizar protección efectiva frente a ciberdelitos. En la misma línea, Binder (2018) enfatiza que los tratados multilaterales son esenciales para enfrentar la transnacionalidad de estas conductas y asegurar justicia para las víctimas. Casey (2011) complementa que la preservación y obtención de pruebas digitales requiere coordinación internacional, dado que la evidencia suele encontrarse en múltiples jurisdicciones. Wall (2017) resalta que los ciberdelitos trascienden fronteras y que la cooperación internacional es un requisito para que las víctimas obtengan justicia efectiva. Finalmente, Kerr (2018) sostiene que los marcos legales internos resultan insuficientes sin mecanismos de cooperación internacional, especialmente en la obtención de pruebas digitales.

La inclusión de estos mecanismos evidencia que la protección de los derechos fundamentales frente a la violencia digital no puede limitarse al ámbito interno. La extradición, la asistencia legal mutua y la cooperación iberoamericana constituyen herramientas indispensables para enfrentar la transnacionalidad de los ciberdelitos, garantizando que las víctimas puedan acceder a una justicia efectiva incluso cuando los agresores actúan desde fuera del territorio nacional.

No obstante, el presente estudio se centra en la aplicación interna de la tutela judicial efectiva, reconociendo la cooperación internacional como un complemento necesario, aunque aún limitado en su implementación práctica.

1.1.5 Sujetos que interviene en los ciberdelitos

En el caso de la difusión no autorizada de imágenes íntimas en redes sociales, resulta indispensable identificar a los distintos sujetos que intervienen tanto en su comisión como en sus consecuencias, pues ello permite comprender un entramado más amplio que involucra al autor, a los partícipes, a las víctimas y, en determinados casos, a los intermediarios tecnológicos.

1.1.5.1 El autor

El autor del ciberdelito es quien ejecuta la conducta típica mediante el dominio funcional de la acción tecnológica. Bacigalupo (2019) sostiene que esta figura se caracteriza por la capacidad de controlar la acción tecnológica, ya sea a través del acceso ilícito a sistemas, la manipulación de datos o la creación de programas maliciosos.

Como se señaló en el análisis del elemento subjetivo, Silva Sánchez (2020) añade que el autor en el ciberespacio puede actuar de manera individual o colectiva, dado que muchos ataques se realizan en redes organizadas o grupos transnacionales.

En el ciberdelito objeto de análisis, el autor es quien difunde de manera consciente y deliberada imágenes íntimas sin consentimiento, instrumentalizando la tecnología para vulnerar la esfera personal de la víctima y generando consecuencias jurídicas y sociales que trascienden el ámbito digital.

1.1.5.2 El partícipe o colaborador

Además del autor, existen sujetos que contribuyen a la comisión del ciberdelito sin tener el dominio del hecho, actuando como cooperadores o cómplices.

Díaz y García Conlledo (2019) destacan que la participación en delitos cometidos mediante medios tecnológicos presenta particularidades, ya que las contribuciones suelen ser indirectas, fragmentadas y distribuidas en distintas jurisdicciones, lo que complejiza la imputación penal.

En el caso de la difusión no autorizada de imágenes íntimas, los partícipes pueden ser quienes, sin haber publicado originalmente el contenido, lo comparten, replican o redistribuyen en plataformas digitales, ampliando el daño y la exposición de la víctima. Esta característica evidencia que la participación en el ciberespacio no puede analizarse únicamente bajo los parámetros clásicos de la teoría del delito, sino que exige nuevas categorías dogmáticas que reconozcan la dispersión geográfica y la mediación tecnológica.

1.1.5.3 La víctima

La víctima constituye el sujeto pasivo del ciberdelito. López Gorostidi (2020) señala que la pluralidad de víctimas es una característica distintiva de esta forma de criminalidad, ya que cualquier usuario de tecnologías de la información y la comunicación puede verse afectado, independientemente de su nivel de conocimiento técnico o de las medidas de seguridad adoptadas.

Complementariamente, Era-Mesa, Caro-Caro y Del Rey-Alamillo (2022) evidencian que la victimización digital no se distribuye de manera homogénea, sino que presenta diferencias significativas según género y edad, con especial impacto en mujeres y adolescentes.

En el tipo penal analizado, la víctima es la persona cuya intimidad se ve expuesta sin consentimiento, enfrentando consecuencias emocionales, sociales y jurídicas que trascienden el ámbito digital. Por ello, la figura de la víctima no puede reducirse a una categoría abstracta, sino que debe entenderse como un sujeto plural y diverso, cuya vulnerabilidad se encuentra condicionada por factores sociales, tecnológicos y culturales.

1.1.5.4 Los intermediarios tecnológicos

Los intermediarios tecnológicos, como proveedores de servicios de internet y plataformas digitales, desempeñan un rol en la prevención, detección y reporte de los ciberdelitos, sin que ello implique, por regla general, una atribución automática de responsabilidad penal directa.

Rodríguez Ramos, Gil Gil y Bacigalupo (2025) destacan que estos actores, aunque no sean autores ni partícipes directos, cumplen un papel crucial en la detección y denuncia de los ciberdelitos, lo que abre el debate sobre su eventual responsabilidad penal o administrativa.

En el ciberdelito de difusión de imágenes íntimas, los intermediarios tecnológicos, principalmente las plataformas de redes sociales participan en la detección y eliminación del contenido, lo que plantea la necesidad de analizar su responsabilidad en la protección de los derechos de las víctimas y en la garantía de un entorno digital seguro.

En definitiva, los sujetos que intervienen en el ciberdelito conforman un entramado complejo que desborda las categorías clásicas de autor y víctima. En el caso de la difusión no autorizada de imágenes íntimas, esta pluralidad obliga a repensar la dogmática penal en clave digital, reconociendo formas de autoría mediata, participación fragmentada y victimización colectiva, para garantizar una tutela judicial efectiva frente a la violencia digital.

1.2 Difusión no autorizada de imágenes íntimas en redes sociales

La difusión no autorizada de imágenes íntimas constituye una manifestación grave de violencia digital, que vulnera directamente la intimidad, la dignidad y la seguridad emocional de las personas afectadas. Este fenómeno presenta una incidencia diferenciada según género, afectando especialmente a mujeres, niñas y adolescentes, debido a patrones culturales de desigualdad y violencia de género (CIDH, 2019).

Investigaciones recientes indican que este tipo de agresión genera consecuencias psicológicas severas, tales como depresión, ansiedad, ideación autolesiva y estigmatización social (Schmidt, Varese, Larkin & Bucci, 2023). Además, un porcentaje significativo de jóvenes comparte imágenes íntimas de terceros sin consentimiento, motivados por presión social, búsqueda de validación o simple entretenimiento

(Barrense-Dias et al., 2020), lo que incrementa considerablemente la exposición al riesgo.

La ética digital y la responsabilidad de las plataformas son fundamentales para prevenir la revictimización. Estudios latinoamericanos destacan la necesidad de que las plataformas actúen de manera proactiva en la detección y eliminación de contenido íntimo no consentido (González-Vega, López-Salazar & Morua Ramírez, 2023).

Asimismo, Danielle Keats Citron (2014; 2021) sostiene que la difusión no autorizada de imágenes íntimas constituye una violación grave de los derechos civiles, afectando la autonomía personal, la reputación y la vida privada. Por ello, requiere respuestas jurídicas reforzadas que combinen regulación penal, responsabilidad de intermediarios y medidas de reparación integral.

En síntesis, la difusión no autorizada de imágenes íntimas trasciende lo meramente tecnológico, al estar profundamente enraizada en dinámicas sociales y de poder. Su abordaje exige estrategias integrales que articulen sanciones penales, educación digital, protocolos de protección de la dignidad humana y mecanismos judiciales eficaces frente a la violencia de género en entornos digitales.

1.3. Derechos fundamentales vulnerados en el entorno digital

Los ciberdelitos no solo implican ataques a sistemas o datos, sino que vulneran derechos fundamentales esenciales, como la intimidad, la privacidad, la dignidad y la seguridad personal, afectando directamente la vida personal, familiar y social de las víctimas. Garantizar su protección requiere un enfoque integral que combine marco normativo, mecanismos judiciales efectivos y educación digital, especialmente frente a la difusión no autorizada de imágenes íntimas.

1.3.1. Intimidad y privacidad

El derecho a la intimidad protege la esfera más reservada de la persona, así como su información sensible. En el entorno digital, la facilidad de difusión de datos sin consentimiento incrementa los riesgos de vulneración. De manera complementaria, la privacidad digital permite a los individuos controlar el acceso y uso de su información

personal, mientras que la seguridad digital busca proteger frente a riesgos como la suplantación de identidad o la divulgación no consentida de contenido íntimo.

En este sentido, la Constitución de Nicaragua reconoce estos derechos: el Artículo 27 (numerales 5, 6 y 7) garantiza la vida privada, la privacidad familiar y la inviolabilidad de las comunicaciones, mientras que el Artículo 176 establece el Recurso de Habeas Data como mecanismo de tutela frente al uso indebido de datos personales.

Investigaciones recientes evidencian que la eficacia de estas garantías depende no solo de la normativa, sino también de la implementación de mecanismos judiciales efectivos y de políticas de educación digital, que permitan prevenir riesgos y proteger la información sensible (Martínez y Herrera, 2023; Vargas, 2021; Pérez & Salazar, 2022).

Por lo tanto, garantizar la protección real de la intimidad exige un enfoque integral que articule legislación, educación digital y protocolos judiciales claros, especialmente frente a la difusión no autorizada de imágenes íntimas, fenómeno en el que la rapidez de propagación de la información supera la capacidad de respuesta del sistema judicial.

1.3.2. Dignidad y Seguridad Personal

La dignidad asegura el respeto al valor intrínseco de cada persona, prohibiendo cualquier acción que humille, difame o menoscabe su integridad. En el contexto digital, la difusión no autorizada de imágenes íntimas constituye una forma de agresión que degrada la dignidad humana y compromete la seguridad emocional de las víctimas, con especial incidencia en mujeres, niñas y adolescentes (Henry y Powell, 2022).

Desde la revisión del estado del arte, investigaciones evidencian que este tipo de ciberviolencia genera consecuencias profundas, que incluyen ansiedad, depresión, disminución de la autoestima y estrés postraumático (Larrañaga, Navarro y Yubero, 2018; Kowalski et al., 2014; Hinduja y Patchin, 2019). Además, la revictimización digital, agravada por la viralización de contenidos en redes sociales, prolonga el sufrimiento de la víctima y dificulta la reparación del daño (González-Vega, 2023).

En consecuencia, la protección frente a estas vulneraciones requiere mecanismos legales sólidos, acompañamiento psicológico y medidas educativas, articulando sanciones penales, protocolos de prevención y reparación simbólica. De esta manera,

se garantiza una tutela judicial efectiva que responda a la complejidad de la criminalidad digital y preserve la integridad emocional y social de las víctimas.

1.4 La tutela judicial efectiva en el marco conceptual de los ciberdelitos

La tutela judicial efectiva constituye un derecho fundamental reconocido en la Constitución de Nicaragua (Artículo 32) y en la Convención Americana sobre Derechos Humanos (1969). Este principio garantiza que toda persona pueda acceder a los órganos jurisdiccionales para la defensa de sus derechos, mediante procedimientos transparentes, eficaces y respetuosos de los derechos fundamentales.

Desde el estado del arte, Ramos Montañés (2022) subraya que este derecho no se limita al acceso formal a los tribunales, sino que implica que las resoluciones judiciales sean motivadas, ejecutables y respetuosas de los derechos fundamentales. Esta perspectiva doctrinal permite comprender que la tutela judicial efectiva no es únicamente un mecanismo procesal, sino una garantía sustantiva que asegura la protección real de los derechos humanos.

En el contexto de los ciberdelitos, esta garantía adquiere relevancia como referencia normativa, asegurando que las víctimas de conductas ilícitas cometidas mediante tecnologías de la información y la comunicación cuenten con mecanismos judiciales de protección adecuados. No obstante, el análisis detallado de sus desafíos prácticos y su importancia frente a la violencia digital será desarrollado en el Capítulo II.

1.5 Perspectivas teóricas sobre violencia digital, redes sociales y evidencia electrónica

1.5.1. Violencia digital y Redes sociales

La violencia digital comprende un conjunto de acciones realizadas mediante tecnologías de la información y la comunicación que vulneran derechos fundamentales como la intimidad, la dignidad y la integridad psicológica de las personas. Este tipo de violencia afecta principalmente a mujeres, niñas y adolescentes; sin embargo, también se ha documentado que hombres y personas de diversas identidades de género pueden ser víctimas de prácticas como la difusión no consentida de imágenes íntimas, especialmente en contextos de sexting, rupturas de pareja o situaciones de coerción emocional (OEA, 2022).

Investigaciones académicas muestran que, aunque la violencia digital presenta una marcada dimensión de género, varones y personas no binarias también enfrentan riesgos significativos, aunque tienden a reportar menos incidentes debido al estigma social asociado a este tipo de victimización (Powell & Henry, 2017; Bates, 2020). En consonancia con ello, ONU Mujeres (2023) subraya que la violencia digital debe entenderse como un fenómeno transversal, lo que exige la adopción de políticas públicas integrales, estrategias de educación digital y mecanismos judiciales eficaces para proteger a todas las personas en los entornos digitales.

Las redes sociales constituyen espacios donde se incrementa significativamente la probabilidad de violencia digital, debido a su capacidad de difusión masiva, al anonimato que pueden ofrecer a los agresores y a la permanencia del contenido publicado. El European Institute for Gender Equality (EIGE, 2021) advierte que los patrones de hostigamiento y agresión en línea afectan de manera desproporcionada a mujeres jóvenes, evidenciando la necesidad de políticas y mecanismos de protección específicos. De manera similar, Henry y Flynn (2023) señalan que la viralidad propia de las plataformas amplifica el daño asociado a la violencia basada en imágenes y dificulta el control sobre la reproducción del contenido una vez difundido.

Por lo tanto, las redes sociales se configuran como espacios de alto riesgo, donde la exposición de contenidos íntimos no consentidos puede generar impactos graves y duraderos en la esfera personal, social y emocional de las víctimas. Esto demuestra que la protección frente a la difusión no autorizada de imágenes íntimas no puede depender exclusivamente de medidas reactivas o de la intervención judicial posterior. La naturaleza de estas plataformas, caracterizada por la rapidez en la difusión y la persistencia de los contenidos, exige la adopción de estrategias preventivas complementarias, tales como la educación digital, campañas de concienciación y protocolos claros para la gestión ética de la información.

En síntesis, la conceptualización de la violencia digital, junto con los riesgos inherentes a las redes sociales, permite comprender de manera más amplia los fenómenos de revictimización y desigualdad de género, evidenciando la necesidad de respuestas integrales que articulen políticas públicas, educación digital y mecanismos judiciales

efectivos, orientados a proteger de manera equitativa a todas las personas en entornos digitales.

1.5.2 Evidencia Digital

La evidencia digital ha sido objeto de creciente atención en la doctrina procesal penal, dado que plantea retos específicos en cuanto a su obtención, conservación y valoración. En primer lugar, Osco Escobedo y Chipana Fernández (2019) señalan que la evidencia digital debe ser entendida como “todo dato susceptible de ser almacenado o transmitido por medios electrónicos y que puede servir como prueba en un proceso penal”, destacando la necesidad de garantizar su autenticidad y fiabilidad mediante procedimientos técnicos adecuados.

Asimismo, Fernández Abad (2020) subraya que la prueba digital se caracteriza por su intangibilidad y volatilidad, lo que exige un tratamiento diferenciado respecto de la prueba física tradicional. Según este autor, la cadena de custodia y el uso de herramientas forenses certificadas son condiciones indispensables para que la evidencia digital pueda ser admitida en juicio.

De igual forma, López Géliz (2021) enfatiza que la valoración de la prueba digital debe realizarse bajo parámetros técnico-jurídicos que aseguren su pertinencia y legalidad. Para este autor, la incorporación de documentos electrónicos, registros de páginas web o correos electrónicos en procesos judiciales requiere de un marco normativo claro y de una capacitación constante de los operadores de justicia en materia tecnológica.

A partir de las aportaciones doctrinales revisadas, se considera, que la evidencia digital debe ser entendida no únicamente como un dato técnico susceptible de prueba, sino como un elemento procesal que exige un tratamiento integral en tres dimensiones: jurídica, tecnológica y garantista.

Por ello, la evidencia digital debe ser concebida como un instrumento probatorio que, además de aportar certeza en el proceso penal, refuerza la garantía del debido proceso en entornos digitales, evitando que la complejidad tecnológica se convierta en un obstáculo para la justicia.

A modo de cierre, el análisis conceptual de los ciberdelitos ha permitido delimitar su naturaleza jurídica y social, evidenciando que no se trata únicamente de conductas tecnológicas aisladas, sino de fenómenos complejos que vulneran derechos fundamentales como la intimidad, la dignidad y la privacidad. La revisión de sus elementos objetivos, subjetivos y normativos, así como la identificación de los sujetos que intervienen en su comisión, confirma que la criminalidad digital exige respuestas jurídicas diferenciadas y adaptadas a la realidad del ciberespacio.

Asimismo, la difusión no autorizada de imágenes íntimas se presenta como una de las manifestaciones más graves de violencia digital, al generar impactos emocionales, sociales y jurídicos que trascienden lo patrimonial y afectan de manera directa la esfera personal de las víctimas. Este fenómeno, además, pone de relieve la necesidad de reconocer la pluralidad de actores involucrados como autores, partícipes, víctimas e intermediarios tecnológicos y de articular mecanismos de prevención, sanción y reparación que respondan a la complejidad del entorno digital.

En suma, el Capítulo I ha establecido las bases conceptuales indispensables para comprender la dimensión del ciberdelito y sus implicaciones en la protección de los derechos humanos. Sobre esta base, el siguiente capítulo profundizará en la tutela judicial efectiva, analizando su fundamento constitucional, doctrinal e internacional, así como su interpretación y aplicación frente a los retos específicos que plantea la violencia digital en Nicaragua.

CAPITULO II: IMPORTANCIA DE LA TUTELA JUDICIAL EFECTIVA EN LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DE LAS VÍCTIMAS DE CIBERDELITOS

2.1 Aspectos introductorios

El objeto del presente capítulo es señalar la importancia de la tutela judicial efectiva desde un análisis eminentemente documental, teórico y normativo, vinculado con los ciberdelitos. A diferencia del Capítulo I, que abordó las bases conceptuales generales de los derechos fundamentales en el entorno digital, este capítulo se centra en el estudio de la tutela judicial efectiva como derecho fundamental, destacando su papel en la protección de la intimidad, la dignidad y la privacidad frente a la violencia digital.

El enfoque adoptado es principalmente normativo y doctrinal, sustentado en fuentes jurídicas nacionales e internacionales, así como en interpretaciones académicas y jurisprudenciales. Este análisis permite comprender cómo la Constitución, los tratados internacionales, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 de Ciberdelitos configuran un marco jurídico destinado a garantizar la defensa de los derechos fundamentales en el entorno tecnológico. De esta manera, se establecen las bases teóricas necesarias para analizar posteriormente los alcances y limitaciones de dicho marco legal en la práctica.

2.2 Nociones conceptuales de la tutela judicial efectiva

En el contexto nicaragüense, la tutela judicial efectiva está garantizada por el artículo 32 de la Constitución Política, que reconoce el derecho de toda persona a un debido proceso y a la tutela judicial efectiva. Además, el artículo 140 refuerza la obligación de la administración de justicia de proteger los derechos humanos mediante la aplicación de la ley, así, la tutela judicial efectiva se configura como un eje central del sistema jurídico, asegurando que las víctimas de cualquier vulneración, incluidas aquellas derivadas de ciberdelitos, obtengan una respuesta jurisdiccional adecuada

Este derecho protege bienes jurídicos esenciales como la intimidad, la dignidad y la privacidad digital, adquiriendo especial relevancia en contextos de violencia digital. En este sentido, desde el estado del arte, para Ramos Montañés (2022), la tutela judicial efectiva no solo garantiza el acceso formal a los tribunales, sino que asegura que las decisiones sean motivadas, ejecutables y respeten los derechos fundamentales.

De manera complementaria, Yáñez y Mila Maldonado (2023) enfatizan que la protección jurídica se extiende a todas las personas, incluyendo situaciones de vulneración digital, y que la norma debe contemplar procedimientos ágiles y adaptados a la rapidez de difusión en entornos tecnológicos.

No obstante, la normativa, aunque sólida, enfrenta desafíos prácticos y éticos. Intriago-García y Molina-Barrezueta (2023) señalan que barreras como la demora judicial, la falta de recursos y la complejidad del proceso limitan la efectividad real del derecho.

Asimismo, González & Paredes (2024) destacan que, frente a fenómenos contemporáneos como la difusión no autorizada de imágenes íntimas, la tutela judicial efectiva debe proyectarse más allá del ámbito formal, considerando estrategias de prevención, concientización y acompañamiento integral de las víctimas.

Por tanto, la tutela judicial efectiva puede concebirse como un instrumento normativo, interpretativo y preventivo, capaz de orientar políticas públicas y educativas incluso cuando la víctima no haya iniciado un proceso legal. Así, permite valorar críticamente las limitaciones de la norma en la práctica y subraya la importancia de reforzar la protección integral de los derechos digitales.

En consecuencia, esta conceptualización sienta las bases para analizar su marco normativo y procedimental en Nicaragua, que se aborda en la siguiente sección, a fin de comprender cómo la tutela judicial efectiva se concreta legalmente frente a la difusión no autorizada de imágenes íntimas.

2.3 Fundamentos Normativos

2.3.1 Marco Normativo

La comprensión de la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en Nicaragua requiere un análisis histórico y normativo del marco legal que protege los derechos fundamentales en el entorno digital, resultando indispensable para identificar cómo la Constitución y la legislación nacional han configurado la defensa de la intimidad, la dignidad y la privacidad, presentando la base sobre la cual debe construirse una respuesta judicial integral.

2.3.1.1 Constitución Política de la República de Nicaragua (1987) y sus reformas (2025)

En primer lugar, la Constitución Política de la República de Nicaragua consagra un conjunto de derechos fundamentales directamente vinculados con la protección de la vida privada, los datos personales y la tutela judicial efectiva.

En particular, los artículos 27 (numerales 5, 6, 7, 8 y 15), 28, 32, 33, 176, 138 y 140 configuran un marco normativo integral que permite comprender la dimensión jurídica de la protección frente a la difusión no autorizada de imágenes íntimas.

Así, el numeral 5 del artículo 27 reconoce el derecho a la vida privada, mientras que el numeral 6 garantiza el respeto a la honra y reputación, ambos esenciales en los supuestos de divulgación de contenido íntimo.

A su vez, el numeral 7 otorga a las personas el derecho a conocer la información personal registrada por entidades públicas y privadas, lo que se vincula directamente con la gestión de archivos digitales; el numeral 8 asegura la inviolabilidad de las comunicaciones, aspecto relevante cuando el material íntimo es obtenido mediante accesos no autorizados a mensajes, dispositivos o plataformas digitales; y el numeral 15 protege la integridad física, psíquica y moral, frecuentemente vulnerada en contextos de violencia digital.

Por otra parte, el artículo 28 establece la igualdad absoluta en el ejercicio de los derechos, garantizando que la protección frente a la difusión no consentida de imágenes íntimas sea universal y no limitada a un género específico.

Del mismo modo, el artículo 32 desarrolla el derecho al debido proceso y a la tutela judicial efectiva, mientras que el artículo 33 refuerza la protección de las víctimas de cualquier delito, asegurando su seguridad, bienestar físico y psicológico, dignidad y vida privada.

Complementariamente, el artículo 176 introduce el recurso de habeas data, instrumento que faculta a las personas a controlar el acceso, uso y difusión de su información privada en entornos digitales.

Finalmente, los artículos 138 y 140 establecen principios rectores de la administración de justicia, contribuyendo a que la protección de los derechos humanos sea efectiva en los procesos relacionados con la vulneración de derechos digitales.

En consecuencia, este marco constitucional constituye el fundamento esencial para dimensionar la gravedad jurídica de la difusión no autorizada de imágenes íntimas y reafirma la obligación del Estado nicaragüense de prevenir, sancionar y reparar estas conductas.

2.3.1.2 Tratados Internacionales de Derechos Humanos

Asimismo, los tratados internacionales de derechos humanos constituyen estándares universales que refuerzan la protección de los derechos fundamentales y la tutela judicial efectiva. Por ejemplo:

Declaración Universal de Derechos Humanos (1948): El Artículo 1 establece la igualdad de todas las personas en dignidad y derechos, mientras que el Artículo 12 protege la vida privada frente a injerencias arbitrarias, incluyendo la divulgación no consentida de información íntima.

Pacto Internacional de Derechos Civiles y Políticos (1966): El Artículo 17 garantiza que nadie será objeto de injerencias arbitrarias en su vida privada, familia o comunicaciones, respaldando la implementación de leyes nacionales como la Ley 1042.

- Convención sobre los Derechos del Niño (1989): Reconoce el derecho de todos los niños y niñas a la privacidad y protección frente a cualquier forma de explotación o abuso en entornos digitales.
- Convención Americana sobre Derechos Humanos (1969): Reafirma la obligación de proteger los derechos fundamentales sin discriminación de género, edad, raza u otra condición.

De esta manera, los tratados internacionales proporcionan un marco conceptual que respalda la legislación nacional y justifica la tutela judicial efectiva para todas las víctimas de difusión no autorizada de imágenes íntimas.

2.3.1.3 Código Penal

El Código Penal de Nicaragua establece normas esenciales para la protección de la intimidad y la vida privada de las personas. En particular, el Artículo 195 dispone que:

"Quien, hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque le hayan sido dirigidos, será penado de sesenta a ciento ochenta días multa."

Esta disposición, aunque redactada sin referencia específica a medios digitales, protege bienes jurídicos fundamentales como la intimidad, la reputación y la confidencialidad de la información personal, por lo que, constituye un marco general de protección frente a

la divulgación no autorizada de contenido privado, sirviendo de base para la tutela judicial de las víctimas.

Es importante destacar que, dada la evolución tecnológica y la aparición de ciberdelitos, el Código Penal por sí solo no contempla la tipificación de conductas específicas de difusión digital de imágenes íntimas.

Sin embargo, establece un fundamento normativo que se complementa con leyes especiales, siguiendo el principio de derecho especial, según el cual la normativa especializada prevalece frente a la general en materias específicas.

Esto permite que, en casos de difusión de imágenes íntimas a través de redes sociales, se aplique la Ley N.º 1042, Ley Especial de Ciberdelitos, como norma complementaria y especializada.

En consecuencia, el Artículo 195 del Código Penal sigue siendo relevante como pilar de protección de la intimidad, constituyendo un marco jurídico que legitima la intervención judicial ante la propalación, mientras que la Ley 1042 aborda de manera directa y detallada las particularidades de los delitos cometidos en entornos digitales.

2.3.1.4 Código Procesal Penal

El Código Procesal Penal de Nicaragua establece normas fundamentales para el ejercicio de la acción penal, la protección de víctimas y el desarrollo de los procesos judiciales en materia penal. Entre sus disposiciones, destacan los artículos que regulan la jurisdicción, competencia y derechos de las víctimas:

Artículo 18 (Jurisdicción penal): La jurisdicción penal se ejerce con exclusividad por los tribunales previstos en la ley, a quienes corresponde la potestad pública de conocer y decidir los procesos que se instruyan por delitos y faltas, garantizando que los casos de ciberdelitos sean conocidos por los órganos competentes y asegurar la correcta aplicación de la justicia.

Artículo 51 (Titularidad de la acción penal): La acción penal se ejercerá principalmente por el Ministerio Público, de oficio o a instancia de parte, según el tipo de delito. Esto asegura que los delitos cibernéticos, como los cometidos en perjuicio de personas

naturales o jurídicas, puedan ser perseguidos incluso si la víctima no presenta la denuncia directamente.

Artículo 109 y 110 (Definición y derechos de la víctima): Reconoce a la víctima u ofendido y establece sus derechos dentro del proceso penal, incluyendo la intervención, protección y asistencia jurídica. Esto resulta esencial en los ciberdelitos, donde la víctima puede enfrentar riesgos adicionales de vulneración de su intimidad y seguridad.

Artículo 222 y 227 (Denuncia y criterios científicos): Toda persona puede denunciar un delito de acción pública, y la investigación debe realizarse siguiendo métodos científicos y técnicos. En el contexto digital, estos artículos facilitan la adecuada recolección y manejo de pruebas electrónicas.

La importancia de estas disposiciones radica en que aseguran la protección procesal de las víctimas de ciberdelitos, garantizando que los procesos se desarrollen conforme a derecho, que se respeten los derechos de las partes y que se utilicen métodos técnicos adecuados para la investigación de delitos cometidos mediante medios digitales.

En este sentido, el Código Procesal Penal se complementa con la Ley N.º 1042, Ley Especial de Ciberdelitos, que tipifica de manera específica las conductas delictivas en entornos digitales y establece mecanismos de acción y persecución adaptados a la tecnología, siguiendo el principio de especialidad frente a la normativa general.

2.3.1.5 Ley N.º 1042, Ley Especial de Ciberdelitos (2020) y sus reformas (2024)

La Ley N.º 1042 constituye la norma especializada que regula los delitos cometidos mediante Tecnologías de la Información y la Comunicación (TIC), incluyendo la difusión de contenido íntimo sin consentimiento.

En este sentido, la ley establece medidas preventivas, procedimientos de investigación, sanciones y mecanismos de protección integral de las víctimas, lo que la convierte en un instrumento clave para garantizar la tutela judicial efectiva en el entorno digital (Asamblea Nacional de Nicaragua, 2020, La Gaceta, Diario Oficial N.º 201).

De manera complementaria, la Ley N.º 1042 desarrolla disposiciones concretas que buscan prevenir, investigar y sancionar los ciberdelitos, protegiendo a personas naturales

y jurídicas, e incluyendo la responsabilidad de autores, cómplices y cooperadores, incluso si los hechos ocurren fuera del territorio nacional.

Asimismo, en 2024 se introdujeron reformas mediante la Ley N.º 1219, las cuales incorporaron medidas de preservación anticipada de pruebas electrónicas y mecanismos de protección especial para las víctimas, fortaleciendo la eficacia de la tutela judicial efectiva en casos de difusión no autorizada de imágenes íntimas (Asamblea Nacional de Nicaragua, 2024, La Gaceta, Diario Oficial).

2.3.1.5.1 Delitos relevantes para la difusión de imágenes íntimas

Entre los delitos contemplados por la Ley N.º 1042, el acoso sexual mediante TIC (Art. 34) constituye la conducta más directamente vinculada con la difusión no autorizada de imágenes íntimas.

Este artículo regula el envío de mensajes, imágenes o vídeos de contenido sexual sin consentimiento, estableciendo penas de 2 a 4 años, incrementadas a 4–6 años cuando la víctima es menor de 16 años o persona con discapacidad.

Aunque la Ley también tipifica otras formas de acoso, como el acoso general mediante TIC (Art. 33), estas conductas se enfocan principalmente en generar humillación, hostigamiento o afectación psicológica sin implicar necesariamente contenido sexual. Por lo tanto, para los fines de este estudio, el Art. 34 es el más relevante, ya que protege directamente la intimidad y la dignidad de las víctimas frente a la difusión de imágenes íntimas sin consentimiento.

Adicionalmente, la responsabilidad de personas jurídicas (Art. 34 bis), incorporada con la reforma de 2024, establece que las organizaciones responden penalmente por las conductas delictivas de sus miembros. Este artículo contempla multas proporcionales a los beneficios obtenidos, reforzando así la protección integral de las víctimas y la eficacia de la tutela judicial efectiva (Asamblea Nacional de Nicaragua, 2024, La Gaceta, Diario Oficial).

2.3.1.5.2 Procedimientos y medidas cautelares

La Ley N.º 1042 establece procedimientos y medidas cautelares específicas para garantizar la preservación de la evidencia digital y la protección de las víctimas de ciberdelitos, particularmente frente a la difusión no autorizada de imágenes íntimas.

En primer lugar, los Artículos 36 y 37 regulan la investigación, obtención y conservación de datos. La Policía Nacional y el Ministerio Público deben actuar con celeridad para preservar información contenida en sistemas de información, sus componentes o datos de tráfico, especialmente cuando estos sean vulnerables a pérdida o modificación, asegurando que la evidencia crítica esté disponible para el proceso judicial.

Por su parte, el Artículo 38 establece medidas de aseguramiento específicas, tales como la incautación, depósito, sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos, así como la copia o preservación inmediata de información en poder de terceros. Estas medidas buscan mantener la integridad de la evidencia digital y evitar su manipulación.

El Artículo 39 regula la autorización judicial para acceder, extraer o conservar información contenida en sistemas de información. La Policía Nacional o el Ministerio Público deben fundamentar la solicitud ante un Juez de Distrito de lo Penal, quien puede ordenar, entre otras acciones: entrega inmediata de información, preservación de datos hasta por 90 días (con posibilidad de renovación), acceso a sistemas o componentes, obtención de información de proveedores de servicios, copia o grabación de datos, aseguramiento de sistemas, intervención tecnológica de datos y medidas urgentes conforme al Código Procesal Penal. Estas disposiciones garantizan el respeto al debido proceso y la protección de los derechos de todas las partes involucradas.

Asimismo, el Artículo 40 establece la competencia especializada de los juzgados de distrito para los delitos informáticos relacionados con la libertad e integridad sexual cometidos contra mujeres, niñas, niños, adolescentes o personas con discapacidad, asegurando un abordaje técnico y sensible a las particularidades de las víctimas.

Los Artículos 41 y 42 refuerzan la confidencialidad y custodia de la información. La persona responsable de la preservación de los sistemas informáticos y sus contenidos debe garantizar la integridad y confidencialidad de la información, impidiendo el acceso

de terceros y evitando su uso para fines distintos al proceso investigativo. Asimismo, todos los participantes en la investigación deben mantener estricta confidencialidad sobre los actos realizados, protegiendo la intimidad de las víctimas y evitando su revictimización.

En conjunto, estas disposiciones configuran un marco normativo integral que asegura que la tutela judicial efectiva se cumpla de manera material y práctica, garantizando la protección de los derechos fundamentales de las personas afectadas por la violencia digital y los ciberdelitos.

2.3.1.5.2 bis La dimensión internacional de la Ley N.º 1042 como garantía de la tutela judicial efectiva

La tutela judicial efectiva en materia de ciberdelito exige reconocer que las conductas ilícitas cometidas en el entorno digital rara vez se circunscriben a un solo territorio. En este sentido, la Ley N.º 1042 incorpora una dimensión internacional que resulta fundamental para evitar escenarios de impunidad derivados de la transnacionalidad de los delitos informáticos.

A través de los artículos 43 y 44, la normativa nicaragüense habilita mecanismos de extradición y asistencia legal mutua, permitiendo la cooperación con otros Estados en la persecución penal y en la obtención de elementos probatorios. Estos instrumentos no solo amplían el alcance de la jurisdicción penal, sino que fortalecen el acceso a la justicia de las víctimas cuando los responsables de los delitos actúan desde fuera del territorio nacional.

Asimismo, la ratificación del Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia refuerza este enfoque, al establecer procedimientos específicos para la colaboración interestatal en la preservación y transferencia de evidencia digital. La existencia de tales mecanismos contribuye a que la respuesta judicial frente al ciberdelito sea más eficaz, oportuna y respetuosa de los derechos fundamentales.

Desde esta perspectiva, la dimensión internacional de la Ley N.º 1042 no constituye un elemento meramente accesorio, sino un componente esencial para la materialización de la tutela judicial efectiva en contextos digitales.

Sin embargo, en la práctica, estos mecanismos operan como un complemento de la protección interna, cuya efectividad depende en gran medida de la capacidad institucional y de la coordinación real entre los Estados, lo que evidencia la necesidad de fortalecer su implementación.

2.3.1.5.3 Inclusión de todas las víctimas

La Ley N.º 1042 establece un marco de protección frente a la violencia digital sin distinción de género, garantizando la tutela de todas las personas que puedan ser afectadas por la difusión no consensuada de imágenes íntimas. No obstante, diversos organismos internacionales han señalado que este fenómeno impacta con mayor frecuencia a mujeres, niñas y adolescentes debido a desigualdades estructurales (ONU Mujeres, 2022; MESECVI, OEA, 2022).

Ello no excluye que hombres y personas de otras identidades también resulten víctimas, aunque en muchos casos reporten menos incidentes por la persistencia de estigmas sociales y culturales que dificultan la visibilización de su experiencia (Powell & Henry, 2017; Bates, 2020).

En consecuencia, la norma garantiza procedimientos judiciales inclusivos, preservación de evidencia digital y protección efectiva de la intimidad, asegurando la tutela judicial de cualquier víctima de ciberdelitos relacionados con la difusión no autorizada de imágenes íntimas (Schmidt et al., 2023; Barrense-Dias et al., 2020).

2.4 Interpretación de la norma y alcance

Partiendo de estos fundamentos normativos y doctrinales, resulta necesario analizar la interpretación de la tutela judicial efectiva y su alcance, especialmente frente a las nuevas formas de vulneración de derechos que se manifiestan en los entornos digitales.

La interpretación de la tutela judicial efectiva debe superar una visión meramente formal del acceso a la justicia, puesto que este derecho no se limita a la posibilidad de acudir a

los tribunales, sino que implica la garantía de obtener una resolución fundada y ejecutable.

Asimismo, diversos autores han señalado que la tutela judicial efectiva constituye un principio rector del debido proceso y, por tanto, una condición indispensable para la vigencia real de los derechos fundamentales.

De hecho, Navarro (2019) sostiene que este derecho debe ser entendido como un mecanismo que fortalece la confianza ciudadana en la justicia, especialmente en contextos donde la impunidad debilita la credibilidad institucional.

Del mismo modo, Carrasco Durán (2020) enfatiza que la interpretación de este derecho debe orientarse hacia la eficacia material de las decisiones judiciales, evitando que se convierta en un mero trámite procesal.

Por otra parte, la jurisprudencia interamericana ha consolidado estándares que amplían el alcance de este derecho. La referencia a estos precedentes no responde a un análisis casuístico, sino a la identificación de estándares interpretativos que orientan el alcance normativo de la tutela judicial efectiva.

En efecto, en el caso Velásquez Rodríguez vs. Honduras (Corte IDH, 1988) se estableció que el recurso efectivo implica la obligación estatal de investigar, sancionar y reparar las violaciones de derechos

Posteriormente, en Campo Algodonero vs. México (Corte IDH, 2009), se subrayó que la interpretación de la norma debe orientarse a evitar la impunidad y garantizar la dignidad de las víctimas.

En consecuencia, la tutela judicial efectiva no se reduce al acceso formal a los tribunales, sino que comprende la eficacia material de las decisiones judiciales y la obligación de los Estados de adoptar medidas adecuadas para asegurar la protección de los derechos.

Ahora bien, en el entorno digital la interpretación de la norma enfrenta retos específicos que obligan a una lectura pro-persona y teleológica. En este sentido, Arroyo Moliner (2021) advierte que la vulnerabilidad de las personas en redes sociales exige que la

tutela judicial efectiva se interprete priorizando la protección de la intimidad y la dignidad frente a la violencia digital.

Además, Halpern (2018) señala que la viralidad y permanencia de los contenidos en línea demandan criterios de urgencia, pues el daño se multiplica en cuestión de segundos.

Igualmente, Aguilera Portales (2022) sostiene que la difusión no autorizada de imágenes íntimas constituye una forma de violencia digital que requiere una interpretación expansiva de la norma, capaz de garantizar reparación integral y medidas de no repetición.

Finalmente, el alcance de la tutela judicial efectiva debe entenderse en varias dimensiones. Por un lado, en su dimensión material, al cubrir conductas como la obtención, almacenamiento, difusión y redifusión de imágenes íntimas sin consentimiento. Por otro lado, en su dimensión personal, al involucrar tanto a autores directos como a quienes replican el contenido, así como a las plataformas digitales que lo alojan.

Asimismo, en su dimensión territorial, al enfrentar la transnacionalidad de las redes sociales y la necesidad de cooperación internacional. Y, en último término, en su dimensión temporal, al exigir respuestas urgentes frente a la continuidad del daño que caracteriza la violencia digital.

Estas dimensiones evidencian que la tutela judicial efectiva, interpretada desde un enfoque normativo y pro-persona, adquiere una relevancia especial en el ámbito de los ciberdelitos, donde la rapidez del daño y la complejidad tecnológica exigen respuestas jurídicas eficaces, oportunas y adaptadas a la realidad digital.

2. 5 Retos y desafíos de la tutela judicial efectiva frente a los ciberdelitos

La aplicación de la tutela judicial efectiva en el ámbito de los ciberdelitos plantea desafíos específicos que obligan a repensar su alcance desde una perspectiva normativa y funcional.

A diferencia de los delitos tradicionales, las conductas cometidas en entornos digitales se caracterizan por su rapidez, su capacidad de difusión masiva y la complejidad técnica

que dificulta su prevención, investigación y sanción. Estas particularidades tensionan los mecanismos clásicos de protección judicial y exigen una interpretación evolutiva del derecho a la tutela judicial efectiva.

Uno de los principales retos se relaciona con la adecuación del marco normativo a la realidad digital. La doctrina ha señalado que muchas normas procesales fueron diseñadas para contextos analógicos, lo que limita su eficacia frente a fenómenos como la obtención y preservación de evidencia digital.

En este sentido, Casey (2011) advierte que la volatilidad de los datos electrónicos y la facilidad con la que pueden ser alterados o eliminados demandan respuestas jurídicas inmediatas y técnicamente especializadas, sin las cuales el derecho a una tutela judicial efectiva puede verse seriamente comprometido.

Asimismo, la dimensión transnacional de los ciberdelitos constituye otro desafío relevante. La difusión no autorizada de imágenes íntimas suele producirse a través de plataformas digitales que operan en múltiples jurisdicciones, lo que dificulta la determinación de la competencia territorial y la ejecución de medidas judiciales.

Al respecto, Brenner (2013) sostiene que la falta de armonización normativa y de mecanismos eficaces de cooperación internacional debilita la capacidad de los Estados para garantizar una protección efectiva de los derechos fundamentales en el ciberespacio.

A ello se suma el anonimato o de los agresores, característica frecuente en las redes sociales y plataformas digitales. Este elemento no solo obstaculiza la identificación de los responsables, sino que también incrementa la sensación de impunidad.

Desde una perspectiva jurídica, Solove (2007) señala que el anonimato en línea, si bien puede estar vinculado a la libertad de expresión, requiere límites claros cuando se utiliza para vulnerar derechos fundamentales como la intimidad, la dignidad y la vida privada, lo que plantea un delicado equilibrio normativo que incide directamente en la efectividad de la tutela judicial.

Por otro lado, la rapidez y persistencia del daño digital representa un desafío adicional. A diferencia de otros ilícitos, la difusión de imágenes íntimas sin consentimiento genera

un perjuicio continuo en el tiempo, pues el contenido puede ser replicado indefinidamente.

En este contexto, organismos internacionales han subrayado la necesidad de respuestas urgentes. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2021) destaca que la demora en la adopción de medidas judiciales puede traducirse en una vulneración prolongada de derechos, vaciando de contenido la tutela judicial efectiva.

Desde el plano normativo internacional, el Convenio de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001) constituye un referente fundamental al promover la adopción de herramientas legales y procesales orientadas a fortalecer la investigación y persecución de los delitos informáticos.

Sin embargo, su eficacia depende de la correcta incorporación e interpretación de sus disposiciones en los ordenamientos internos, lo que refuerza la idea de que la tutela judicial efectiva no se agota en la existencia de normas, sino en su aplicación adecuada a la realidad tecnológica.

A partir de estos planteamientos, puede sostenerse que los retos de la tutela judicial efectiva frente a los ciberdelitos no radican únicamente en la ausencia normativa, sino en la necesidad de interpretar y aplicar el derecho desde un enfoque pro-persona, preventivo y adaptado al entorno digital.

En particular, en los casos de difusión no autorizada de imágenes íntimas, la protección efectiva de los derechos exige mecanismos normativos capaces de responder con celeridad, de superar barreras tecnológicas y de garantizar la dignidad de las personas afectadas.

En definitiva, los desafíos analizados evidencian que la tutela judicial efectiva, entendida desde una perspectiva normativa y evolutiva, adquiere una relevancia central frente a los ciberdelitos. La complejidad tecnológica, la transnacionalidad de las conductas y la continuidad del daño obligan a los Estados a fortalecer sus marcos legales e interpretativos, asegurando que este derecho fundamental mantenga su eficacia real en la era digital.

De la exposición precedente se infiere que la tutela judicial efectiva constituye un eje indispensable para la protección de los derechos fundamentales frente a los ciberdelitos, en particular en los casos de difusión no autorizada de imágenes íntimas. El análisis de la Constitución, los tratados internacionales, el Código Penal, el Código Procesal Penal y la Ley Especial de Ciberdelitos demuestra que el ordenamiento jurídico nicaragüense dispone de bases sólidas para enfrentar este fenómeno, garantizando la defensa de la intimidad, la dignidad y la privacidad digital.

Sin embargo, también se advierte que la eficacia de dicha protección depende de la correcta interpretación y aplicación de las normas, de la capacidad institucional para responder con celeridad y de la incorporación de estrategias preventivas y de acompañamiento integral a las víctimas. La tutela judicial efectiva, entendida en sus dimensiones material, personal, territorial y temporal, se configura como un derecho dinámico que debe adaptarse a la complejidad tecnológica y transnacional de la violencia digital.

De esta manera, el presente capítulo sienta las bases para el análisis de los alcances y limitaciones del marco legal vigente en Nicaragua, que será desarrollado en el siguiente capítulo, analizando cómo la tutela judicial efectiva se materializa en la práctica frente a la difusión no consentida de imágenes íntimas en redes sociales y cuáles son los desafíos que persisten para garantizar una protección integral y efectiva.

CAPITULO III: ALCANCES Y LIMITACIONES DEL MARCO LEGAL VIGENTE RESPECTO A LA TUTELA JUDICIAL EFECTIVA FRENTE A LA DIFUSIÓN NO AUTORIZADA DE IMÁGENES ÍNTIMAS EN REDES SOCIALES.

3.1 Aspectos Introductorios

El presente capítulo tiene como propósito analizar los alcances y limitaciones del marco legal vigente en Nicaragua respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales. A diferencia de los capítulos precedentes, en los que se expusieron los fundamentos normativos y doctrinales de manera general, este apartado se orienta a examinar cómo dichas disposiciones se aplican en la práctica y cuáles son los principales retos que enfrentan las víctimas al buscar protección judicial.

El análisis se estructura en dos dimensiones complementarias. Por un lado, se abordan los alcances normativos, que evidencian las herramientas jurídicas disponibles en la Constitución Política de Nicaragua, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 de Ciberdelitos para la protección de la intimidad y la dignidad en entornos digitales. Por otro, se examinan criterios doctrinales que permiten comprender la gravedad de la publicación no consentida de imágenes íntimas y su impacto en los derechos fundamentales de las personas afectadas.

Asimismo, el capítulo incorpora referencias a casos mediáticos difundidos por los medios de comunicación en Nicaragua, que ilustran la aplicación práctica de la Ley N.º 1042. Estas referencias permiten observar cómo la tutela judicial efectiva se concreta en la práctica, sin constituir un análisis de expedientes judiciales ni sustituir el enfoque conceptual de la investigación.

Finalmente, se identifican las principales limitaciones estructurales que persisten en la aplicación de las normas, especialmente en lo relativo a la rapidez de la respuesta institucional, la implementación práctica de los mecanismos de cooperación internacional, y la capacidad de los tribunales para enfrentar la complejidad tecnológica que caracteriza este tipo de conductas. Estas limitaciones no implican la inexistencia de garantías normativas, sino que evidencian los desafíos que enfrenta el sistema de justicia para materializar una protección efectiva y oportuna en contextos digitales.

De esta manera, el capítulo ofrece una visión crítica y equilibrada sobre la eficacia real de la tutela judicial efectiva en Nicaragua frente a la difusión no autorizada de imágenes íntimas en redes sociales, sentando las bases para las conclusiones generales de la investigación.

3.2 Alcances normativos del marco legal vigente en Nicaragua

El marco jurídico nicaragüense contempla un conjunto de disposiciones orientadas a garantizar la protección de la intimidad y la dignidad frente a la difusión no consentida de imágenes íntimas en entornos digitales. A diferencia del análisis conceptual desarrollado en el Capítulo II, en este apartado se examina el alcance normativo de estas disposiciones desde una perspectiva aplicada, identificando cómo se proyectan en la

práctica como herramientas de tutela judicial efectiva ante formas contemporáneas de violencia digital.

En este sentido, el ordenamiento jurídico nacional integra normas constitucionales, penales, procesales y especiales que, de manera articulada, permiten fundamentar la intervención judicial, la persecución penal y la adopción de mecanismos urgentes de protección frente a la circulación ilícita de contenido íntimo.

3.2.1 Constitución Política de Nicaragua

La Constitución Política de Nicaragua constituye el fundamento esencial de la protección de derechos frente a la violencia digital, al reconocer garantías vinculadas con la vida privada, la honra y la inviolabilidad de las comunicaciones. Estos principios constitucionales resultan determinantes en casos de difusión no consentida de imágenes íntimas, en tanto establecen la obligación del Estado de asegurar mecanismos judiciales eficaces para detener la vulneración y proteger la dignidad de las víctimas.

Asimismo, el recurso de habeas data se configura como una herramienta relevante en el entorno digital, ya que permite a las personas exigir el control, restricción o eliminación de información personal difundida sin autorización en plataformas o registros electrónicos.

De igual manera, la tutela judicial efectiva consagrada en el artículo 32, impone que los procesos judiciales incluyan respuestas rápidas y medidas oportunas, acordes con la urgencia propia de los daños que se producen en el espacio digital.

De esta manera, estos preceptos constitucionales han servido como base para que los jueces ordenen la remoción de contenido ilícito y garanticen la reparación de las víctimas.

3.2.2 Código Penal

El Código Penal, aunque elaborado en un contexto anterior al desarrollo masivo de las tecnologías digitales, continúa siendo un instrumento relevante para la protección de la intimidad y la vida privada. En particular, el artículo 195, que sanciona la divulgación no autorizada de comunicaciones privadas, permite fundamentar la persecución penal de conductas que vulneran la esfera íntima de las personas mediante la difusión ilícita de contenido reservado.

Su alcance general permite que los tribunales reconozcan la vulneración de la intimidad y la reputación, aunque esta norma requiere complementarse con la Ley N.º 1042 para abarcar las particularidades tecnológicas. En este sentido, dicho artículo legitima la intervención judicial en casos de difusión ilícita, sirviendo como puente entre la normativa tradicional y la especializada.

3.2.3 Código Procesal Penal

Por su parte, el Código Procesal Penal asegura que los delitos digitales puedan ser perseguidos y sancionados de manera efectiva. La jurisdicción penal exclusiva garantiza que los casos sean conocidos por tribunales competentes, mientras que la titularidad de la acción penal por parte del Ministerio Público permite que los delitos se investiguen incluso sin denuncia directa de la víctima, aspecto crucial en contextos de violencia digital.

Además, los derechos reconocidos a las víctimas incluyen asistencia jurídica y medidas de protección, que se traducen en órdenes de restricción y acompañamiento institucional. Del mismo modo, la regulación de la denuncia y la investigación científica facilita la recolección de pruebas electrónicas, asegurando su validez procesal.

Ello permite que las víctimas accedan a medidas cautelares oportunas y que las pruebas digitales se preserven legítimamente, evitando su pérdida o manipulación.

3.2.4 Ley N.º 1042, Ley Especial de Ciberdelitos

La Ley N.º 1042 constituye el instrumento especializado para enfrentar la violencia digital, ya que tipifica de manera expresa la difusión de contenido íntimo sin consentimiento, reconociendo la gravedad de esta vulneración.

Además, introduce medidas de preservación anticipada de pruebas electrónicas, asegurando que la evidencia digital se conserve íntegra para el proceso judicial. Asimismo, establece la responsabilidad penal de personas jurídicas, ampliando la protección frente a la violencia digital cometida desde plataformas o instituciones.

De igual forma, refuerza la competencia de juzgados especializados en casos que involucran víctimas vulnerables, garantizando un abordaje sensible y técnico. En consecuencia, esta ley representa un avance significativo, pues adapta el sistema penal

a la realidad tecnológica y ofrece herramientas concretas para detener la difusión ilícita y sancionar a los responsables.

3.2.4 bis Alcance internacional de la Ley N.º 1042 en la protección judicial de las víctimas

Como se señaló en el Capítulo I, la Ley N.º 1042 reconoce la dimensión transnacional de los ciberdelitos mediante los artículos 43 y 44, que regulan la extradición y la asistencia legal mutua en investigaciones y procesos vinculados a conductas digitales ilícitas.

Estos mecanismos permiten que la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas trascienda las fronteras nacionales, facilitando la colaboración con otros Estados para perseguir a los agresores y obtener pruebas digitales.

Asimismo, la ratificación del Convenio Iberoamericano de Cooperación (Decreto A.N. N.º 8651, 2020) refuerza la coordinación internacional para la preservación y entrega de evidencia digital, garantizando el respeto de los derechos humanos durante el proceso.

La efectividad de estos mecanismos depende de la implementación práctica y la coordinación institucional, así como de la cooperación con plataformas digitales internacionales, aspectos que se analizarán en el apartado 3.7.6.

3.2.5 Mecanismos de tutela judicial efectiva

La tutela judicial efectiva frente a la difusión no consentida de imágenes íntimas no se limita al acceso formal a los tribunales, sino que se concreta en mecanismos procesales que permiten una respuesta rápida y adecuada a la vulneración digital. Entre ellos destacan la autorización judicial para la preservación de evidencia, la competencia especializada y la adopción de medidas cautelares y recursos judiciales.

3.2.5.1 Autorización judicial para preservación y obtención de evidencia

La Ley N.º 1042 exige autorización judicial para acceder a sistemas de información y extraer datos relevantes. Este mecanismo asegura que la evidencia digital se conserve íntegra y que no sea manipulada. En la práctica, permite ordenar la remoción de

contenido ilícito y garantizar que las pruebas electrónicas estén disponibles para la investigación.

3.2.5.2 Competencia judicial especializada

Los delitos cometidos contra personas vulnerables deben ser conocidos por juzgados especializados en violencia. Este esquema combina sensibilidad hacia la víctima y conocimiento técnico del delito digital. En la práctica, la especialización judicial favorece una respuesta más rápida y adecuada, mientras que los jueces penales ordinarios atienden los casos generales ajustando la respuesta según la gravedad.

3.2.5.3 Medidas cautelares y recursos judiciales

Las medidas cautelares representan uno de los mecanismos más relevantes dentro de la tutela judicial efectiva frente a la difusión no consentida de imágenes íntimas, en tanto permiten una intervención inmediata destinada a impedir la prolongación del daño digital mientras se desarrolla el proceso penal. Su fundamento radica en la necesidad de asegurar la eficacia del proceso y evitar que la vulneración de derechos continúe produciendo efectos irreparables. En Nicaragua, el Código Procesal Penal dispone que estas medidas tienen como finalidad “asegurar la eficacia del proceso”, garantizando tanto la presencia del acusado como la obtención regular de las fuentes de prueba (Código Procesal Penal, art. 166).

En los delitos cometidos en entornos digitales, estas medidas adquieren especial importancia debido a la facilidad de reproducción, permanencia y rápida difusión del contenido ilícito. Por ello, la Ley N.º 1042, Ley Especial de Ciberdelitos, refuerza la capacidad de respuesta judicial al permitir la adopción de medidas urgentes de preservación y aseguramiento de evidencia tecnológica, así como la posibilidad de ordenar la remoción o inaccesibilidad del contenido digital que prolongue la vulneración de la intimidad de la víctima (Ley N.º 1042, art. 39, inc. 8).

Por su parte, los recursos judiciales cumplen un rol complementario al garantizar la revisión de las resoluciones adoptadas durante el proceso, fortaleciendo la seguridad jurídica, evitando arbitrariedades y reforzando la confianza en el sistema de justicia. En conjunto, estos mecanismos evidencian que el marco normativo vigente incorpora

herramientas procesales orientadas a hacer efectiva la protección de la intimidad y dignidad de las víctimas frente a los ciberdelitos.

En síntesis, las medidas cautelares y los recursos judiciales constituyen instrumentos esenciales para garantizar una respuesta inmediata y efectiva, evitando la continuidad del daño digital y asegurando que la tutela judicial efectiva se materialice desde las primeras actuaciones procesales.

3.3 Criterios doctrinales sobre la publicación no consentida de imágenes íntimas

La literatura doctrinal ofrece un marco interpretativo que permite dimensionar la gravedad de la difusión no consentida de imágenes íntimas y la necesidad de respuestas jurídicas integrales. A diferencia del análisis normativo, la doctrina enfatiza los impactos sociales, psicológicos y culturales de estas prácticas, subrayando su carácter de violencia digital y la urgencia de abordarlas desde una perspectiva amplia.

En primer lugar, Danielle Keats Citron (2014) sostiene que la publicación no consentida de imágenes íntimas constituye una violación grave de la privacidad y la dignidad, que no puede ser tratada únicamente como un agravio civil. Este fenómeno socava la autonomía personal y expone a las víctimas a daños reputacionales, sociales y psicológicos profundos, lo que justifica una respuesta penal reforzada y adaptada a la naturaleza digital de la vulneración.

Por su parte, Clare McGlynn y Laura Rackley (2017) introducen el concepto de image-based sexual abuse, que abarca todas las formas de creación y distribución de material íntimo sin consentimiento. Esta categoría supera el término limitado de “porno de venganza”, al reconocer que las conductas pueden producirse en múltiples contextos y responden a estructuras sociales de desigualdad y poder que utilizan la tecnología para degradar la privacidad y la dignidad.

De manera complementaria, Nicola Henry y Anastasia Powell (2020) destacan que la difusión no consensuada de imágenes íntimas constituye una forma de violencia digital con consecuencias que trascienden el plano individual. Entre ellas se incluyen ansiedad, estrés y estigmatización social, lo que evidencia la necesidad de respuestas jurídicas, educativas y sociales integrales.

En consecuencia, la doctrina coincide en que la protección de los derechos fundamentales en el entorno digital no puede limitarse a un reconocimiento formal en la ley. Se requiere que el Estado y los órganos judiciales implementen mecanismos concretos de intervención capaces de detener la difusión del contenido ilícito, sancionar a los responsables y garantizar medidas de reparación y no repetición. Desde un enfoque pro-persona, la legislación, la doctrina y las políticas públicas deben actuar de manera coordinada para enfrentar eficazmente la vulneración de la intimidad y la dignidad en entornos digitales.

3. 4 Referentes de judicialización y visibilización mediática en Nicaragua

En Nicaragua, los tribunales han conocido casos mediáticos relacionados con la difusión no autorizada de imágenes íntimas en redes sociales. Estos precedentes, ampliamente difundidos en medios de comunicación, ilustran cómo se aplica la tutela judicial efectiva en la práctica.

Cabe precisar que el presente análisis se centra en el estudio jurídico de la tutela judicial como derecho fundamental y no en el recuento detallado de expedientes judiciales. Los casos mencionados se presentan únicamente como referencia para comprender la implementación práctica de los principios legales y su impacto en la protección de la intimidad y la dignidad de las víctimas.

Por ejemplo, algunos casos reportados por los medios incluyen:

- En enero de 2025, Sergio Isabel Flores Bravo fue condenado por divulgar fotografías íntimas de su expareja en un perfil falso de Facebook. El fallo reflejó la aplicación de sanciones penales y la protección de derechos fundamentales mediante medidas cautelares.
- En junio de 2023, la jueza Nadia Camila Tardencilla Rodríguez dictó sentencia contra Kevin Alexander Reyes Leytón, por difundir material íntimo de la influencer Salma Flores, confirmando la importancia de garantizar la tutela judicial efectiva frente a la viralización de contenido ilícito.

Estos casos evidencian que:

- La tutela judicial efectiva se concreta mediante sanciones y medidas de protección frente a la vulneración de la intimidad y la dignidad.
- Los tribunales aplican la normativa vigente (Código Penal y Ley N.º 1042) para salvaguardar derechos fundamentales en entornos digitales.
- La intervención judicial incluye preservación de evidencia y medidas cautelares que buscan mitigar el daño a las víctimas.

Sin embargo, la referencia a estos casos también revela algunas limitaciones:

- Dificultad para eliminar completamente el contenido de las plataformas digitales.
- Exposición prolongada de las víctimas a la revictimización mediática o digital.
- Acceso limitado a sentencias públicas, lo que dificulta la transparencia y la sistematización jurisprudencial.

En síntesis, la judicialización en Nicaragua demuestra que la tutela judicial efectiva se implementa mediante la acción de los tribunales y la aplicación de sanciones penales, pero el análisis se mantiene centrado en el derecho como instrumento de protección integral, resaltando tanto sus alcances como los desafíos en su materialización efectiva.

3.5 Derecho Comparado Legislativo sobre la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas

El derecho comparado legislativo constituye una herramienta fundamental para analizar los alcances y limitaciones del marco normativo nacional frente a fenómenos jurídicos complejos, como la difusión no autorizada de imágenes íntimas en entornos digitales.

Su utilización permite identificar tendencias regulatorias, estándares de protección y mecanismos de tutela judicial efectiva adoptados por otros Estados, contribuyendo a una comprensión más amplia del fenómeno y de las respuestas jurídicas disponibles.

Desde una perspectiva metodológica, el análisis comparado no busca la traslación automática de modelos normativos extranjeros, sino la identificación de criterios jurídicos pertinentes que puedan servir como referencia para el estudio y comprensión del ordenamiento interno.

En este sentido, Zweigert y Kötz (2011) señalan que el derecho comparado cumple una función crítica y orientadora, al permitir valorar la eficacia de las normas nacionales a la luz de experiencias jurídicas externas.

En el ámbito específico de la violencia digital y la difusión no consentida de imágenes íntimas, el derecho comparado evidencia una tendencia creciente a reconocer estas conductas como atentados graves contra la intimidad, la dignidad y la autonomía personal, lo que ha llevado a diversos Estados a adoptar legislaciones específicas o a reformar sus códigos penales para garantizar una tutela judicial efectiva.

3.5.1 España

España cuenta con un marco legal consolidado para proteger la intimidad digital y la privacidad de las personas frente a la difusión no consentida de imágenes íntimas. El artículo 197.7 del Código Penal establece que será castigado quien, sin autorización de la persona afectada, revele, difunda o ceda a terceros imágenes o grabaciones obtenidas con su consentimiento, cuando la divulgación menoscabe gravemente su intimidad.

La norma contempla penas de prisión de tres meses a un año o multa de seis a doce meses, y agrava la sanción si la víctima es menor, tiene discapacidad o si el autor actúa con ánimo de lucro (Código Penal, Art. 197.7; Circular 3/2017, Fiscalía General del Estado).

La jurisprudencia del Tribunal Supremo ha confirmado la interpretación de este artículo. En la Sentencia STS 70/2020, el Supremo determinó que la acción central del tipo penal no es la obtención de la imagen, sino su difusión no autorizada, aunque la víctima la hubiera proporcionado voluntariamente. La Sala Segunda enfatizó que el delito se configura cuando se produce un menosprecio grave de la intimidad de la persona afectada (Tribunal Supremo, 2020; RTVE, 2020).

Complementariamente, la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPD-GDD) refuerza la tutela de la intimidad y la privacidad, regulando el tratamiento de datos personales sensibles y estableciendo mecanismos de denuncia ante la Agencia Española de Protección de Datos. Esta normativa permite un

abordaje preventivo y sancionador frente a la divulgación de contenido íntimo (LOPD-GDD, 2018).

Recientemente, España ha incorporado el artículo 173 bis al Código Penal, que sanciona penalmente la difusión de deepfakes sexuales o vejatorios sin autorización y con ánimo de dañar la integridad moral. Esta norma contempla penas privativas de libertad y reconoce la motivación lucrativa del autor, reforzando la protección de mujeres, niñas, niños y adolescentes frente a tecnologías emergentes.

La incorporación de este artículo demuestra cómo el derecho penal español se adapta a los riesgos derivados de la inteligencia artificial, complementando las medidas de protección de datos y las sanciones tradicionales por difusión no autorizada de imágenes íntimas.

En cuanto a la prevención y protección integral, España combina sanción penal, protección de datos y estrategias educativas con protocolos de acompañamiento a víctimas de difusión no consentida de imágenes. Estas medidas incluyen campañas de concienciación sobre privacidad digital, orientación sobre el uso responsable de redes sociales y mecanismos de apoyo legal y psicológico (Murcia Orenes et al., 2025; Casabo-Ortí, 2022).

El modelo español demuestra un enfoque integral, que combina tipificación clara, jurisprudencia consolidada, protección de datos y prevención educativa, ofreciendo un referente valioso para Nicaragua. La combinación de sanción penal, tutela judicial efectiva, protección de datos y educación digital constituye una guía para estructurar un marco normativo que proteja la intimidad de manera integral en el entorno digital. Esta experiencia refuerza la comprensión de la tutela judicial efectiva, mostrando cómo un tipo penal claro, junto con medidas preventivas y educativas, fortalece la protección de la intimidad y la dignidad frente a la difusión no consentida de imágenes íntimas.

3.5. 2 Italia

Italia ha adoptado recientemente un marco normativo integral sobre inteligencia artificial, con especial atención a la protección de la intimidad y la prevención de abusos mediante tecnologías emergentes. El 10 de octubre de 2025 entró en vigor la Ley 132/2025,

denominada Disposiciones y delegaciones al gobierno en materia de inteligencia artificial, cuyo objetivo principal es regular el desarrollo, adopción y aplicación de sistemas de IA de manera correcta, transparente y responsable (Gazzetta Ufficiale della Repubblica Italiana, 2025).

La ley establece principios generales sobre derechos fundamentales, transparencia, proporcionalidad, protección de datos personales, confidencialidad, precisión, no discriminación e igualdad de género (Arts. 1-3). Además, regula disposiciones sectoriales para ámbitos específicos como la sanidad, la investigación científica y el poder judicial, e incorpora medidas de protección de la propiedad intelectual y derechos de autor frente a contenidos generados con IA (Arts. 25 y 70 septies).

En materia penal, la Ley 132/2025 introduce el artículo 612-quater del Código Penal, que sanciona la difusión ilícita de contenidos generados o alterados mediante sistemas de inteligencia artificial. Este artículo establece que quien, sin consentimiento, publique, ceda o difunda imágenes, videos o voces manipuladas por IA, causando un daño injusto a la persona, será sancionado con prisión de uno a cinco años. El delito se persigue mediante querrela de la persona afectada, aunque se procederá de oficio en casos que involucren víctimas vulnerables o delitos conexos (Gazzetta Ufficiale della Repubblica Italiana, 2025).

Asimismo, se prevén agravantes específicas relacionadas con el uso de IA, cuando ésta constituya un medio insidioso o aumente las consecuencias del delito (Art. 61, apartado 11-undecies). De esta forma, la normativa italiana no solo tipifica la difusión no autorizada de imágenes manipuladas, sino que adapta el sistema penal a las nuevas formas de violencia digital y deepfakes, ofreciendo un referente innovador para la protección integral de la intimidad en entornos tecnológicos avanzados.

El modelo italiano combina regulación tecnológica, protección penal y tutela judicial efectiva frente a la manipulación de contenidos por inteligencia artificial. Este enfoque ofrece un ejemplo de cómo un marco normativo moderno puede incorporar la prevención de daños digitales, la protección de los derechos de todas las personas y la adaptación del derecho penal a la era digital, constituyendo un referente relevante para fortalecer la normativa nicaragüense en la materia.

El modelo italiano evidencia que la tutela judicial efectiva requiere adaptación a tecnologías emergentes, como la IA y los deepfakes, reforzando la necesidad de un marco normativo actualizado para garantizar la protección integral de los derechos fundamentales.

3.5.3 Dinamarca: iniciativa de ley contra deepfakes

En agosto de 2025, Dinamarca presentó una iniciativa legislativa pionera destinada a proteger a los ciudadanos frente a la utilización no autorizada de su imagen, voz y demás rasgos personales mediante tecnologías de inteligencia artificial, en particular los deepfakes.

El proyecto busca reconocer derechos de autor sobre la identidad digital, habilitando a los individuos para reclamar la retirada de contenidos ilícitos, exigir indemnizaciones y garantizar la protección de su identidad incluso tras el fallecimiento, especialmente en el caso de artistas y figuras públicas (Ministerio de Cultura de Dinamarca, 2025).

La propuesta introduce modificaciones sustantivas a la Ley de Derecho de Autor (Ophavsretsloven), incorporando tres ejes centrales:

- ✓ La prohibición de poner a disposición del público imitaciones digitales realistas de artistas intérpretes o ejecutantes (nuevo artículo 65.a).
- ✓ La extensión de la protección post mortem hasta cincuenta años respecto de los derechos sobre la imagen y la voz (modificación del artículo 63).
- ✓ La prohibición general de difundir imitaciones digitales realistas de rasgos físicos sin autorización (artículo 73.a), aplicable a cualquier persona, con independencia de su nacionalidad.

Asimismo, la iniciativa contempla excepciones específicas para la sátira, la parodia y la crítica social o política, siempre que no constituyan desinformación ni vulneren derechos fundamentales.

Con ello se busca un equilibrio entre la protección de la identidad y la salvaguarda de la libertad de expresión. Aunque el proyecto no prevé sanciones penales, establece mecanismos administrativos y civiles que permiten la retirada del contenido ilícito y la reclamación de indemnizaciones ante organismos como la Autoridad de Supervisión de

la Ley de Servicios Digitales (DSA) y la Comisión Danesa de Derecho de Autor (DSA, 2025).

Es importante subrayar que, al cierre de 2025, la iniciativa aún se encuentra en fase de discusión parlamentaria y no ha entrado en vigor. Ello implica que su eficacia dependerá de la aprobación legislativa y de la capacidad institucional para implementarla con celeridad y solvencia técnica.

Desde una perspectiva comparativa, este proyecto ofrece elementos de especial interés para el fortalecimiento de la legislación nicaragüense frente a la difusión no autorizada de imágenes íntimas. Entre sus aportes destacan:

- ✓ La tipificación específica de la manipulación digital de la identidad, incluyendo deepfakes y tecnologías emergentes.
- ✓ La priorización de un enfoque pro-persona mediante medidas que aseguran la integridad y el control de la identidad digital individual.
- ✓ El reconocimiento de la necesidad de mecanismos de reparación y compensación económica frente a la vulneración de derechos digitales.
- ✓ La incorporación de consideraciones sobre libertad de expresión y uso legítimo, garantizando un marco equilibrado entre protección y derechos fundamentales.

De ahí que, la iniciativa danesa constituye un referente innovador que invita a reflexionar sobre la urgencia de actualizar y ampliar el marco normativo nicaragüense. La incorporación de medidas preventivas, sanciones proporcionales y mecanismos de protección integral frente a las nuevas formas de violencia digital resulta indispensable para asegurar la tutela judicial efectiva y la plena vigencia de los derechos fundamentales en entornos digitales.

La iniciativa danesa subraya la importancia de reconocer la identidad digital como objeto de protección y demuestra que la tutela judicial efectiva incluye tanto medidas preventivas como reparación y control sobre contenidos ilícitos.

3.6 Análisis comparativo y aprendizajes para Nicaragua

El estudio comparado de Nicaragua, España, Italia y Dinamarca permite identificar avances normativos y desafíos comunes en la protección de la intimidad frente a la

difusión no consentida de imágenes íntimas y la manipulación digital mediante tecnologías emergentes.

En el caso de Nicaragua, el marco jurídico se estructura en torno al artículo 195 del Código Penal, que protege la intimidad frente a la divulgación no autorizada de comunicaciones privadas, y la Ley N.º 1042 de Ciberdelitos (2020), reformada en 2024. Esta última tipifica conductas específicas en entornos digitales, como el acoso sexual y la difusión de contenido íntimo sin consentimiento, e introduce medidas de preservación anticipada de pruebas electrónicas y responsabilidad penal de personas jurídicas.

El modelo nicaragüense combina sanción penal, medidas procesales y mecanismos de protección integral de las víctimas, aunque aún carece de una tipificación expresa de fenómenos como los deepfakes.

Por su parte, España ofrece un enfoque integral que conjuga tipificación penal, protección de datos y prevención educativa. El artículo 197.7 del Código Penal sanciona la difusión no autorizada de imágenes íntimas obtenidas con consentimiento, mientras que el artículo 173 bis, incorporado recientemente, penaliza la creación y difusión de deepfakes sexuales o vejatorios sin autorización. La Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales refuerza la tutela de la privacidad, y la jurisprudencia del Tribunal Supremo (STS 70/2020) ha consolidado la interpretación de estas disposiciones.

Además, España complementa la sanción penal con campañas de concienciación y protocolos de acompañamiento a víctimas, lo que evidencia un modelo integral que combina represión, prevención y reparación.

En Italia, la Ley 132/2025 sobre inteligencia artificial constituye un referente moderno al establecer principios generales de transparencia, proporcionalidad, protección de datos y no discriminación, aplicables al desarrollo y uso de sistemas de IA.

En el ámbito penal, la inclusión del artículo 612-quater en el Código Penal sanciona la difusión ilícita de contenidos manipulados mediante IA, con penas de uno a cinco años de prisión, agravadas cuando el uso de la tecnología incrementa el daño. Este modelo combina regulación tecnológica, protección penal y tutela judicial efectiva, adaptando el

derecho penal a las nuevas formas de violencia digital y ofreciendo un marco inclusivo que protege a todas las personas sin distinción.

Finalmente, Dinamarca presentó en 2025 una iniciativa legislativa pionera aún en trámite parlamentario, que reconoce derechos de autor sobre la identidad digital. La propuesta modifica la Ley de Derecho de Autor (Ophavsretsloven) para prohibir imitaciones digitales realistas sin autorización, extender la protección post mortem hasta cincuenta años y establecer mecanismos administrativos y civiles de retirada de contenido e indemnización.

Aunque no contempla sanciones penales, la iniciativa equilibra la protección de la identidad digital con la libertad de expresión, incluyendo excepciones para sátira, parodia y crítica política. Su innovación radica en reconocer la identidad digital como objeto de protección jurídica, lo que constituye un aporte relevante para la reflexión comparativa.

En conjunto, el análisis evidencia que Nicaragua podría fortalecer su legislación mediante:

- La tipificación específica de nuevas formas de violencia digital, incluyendo la manipulación de imágenes mediante inteligencia artificial.
- La incorporación de medidas preventivas y educativas complementarias a la sanción penal, orientadas a la concienciación sobre privacidad digital y acompañamiento a las víctimas.
- El refuerzo de la tutela judicial efectiva mediante procedimientos especializados, preservación de evidencia digital y sanciones proporcionales a la gravedad del daño.
- La inclusión de principios de igualdad y no discriminación, garantizando protección universal frente a la violencia digital.
- El reconocimiento de la identidad digital como objeto de protección jurídica, siguiendo la experiencia danesa.

En conjunto, España, Italia y Dinamarca ofrecen modelos de referencia que permiten a Nicaragua avanzar hacia un marco normativo más integral, inclusivo y adaptado a los

desafíos contemporáneos de la era digital, complementando lo previsto en el Código Penal y en la Ley 1042 de Ciberdelitos.

Hasta aquí se han expuesto los principales alcances normativos, doctrinales, judiciales y comparados del marco legal vigente. A continuación, se señalan las limitaciones que persisten en su aplicación práctica, especialmente en lo relativo a la rapidez de la respuesta institucional, la cooperación internacional y la capacidad de los tribunales para atender la complejidad tecnológica de estos casos.

3.7 Principales limitaciones del marco legal vigente respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales

Si bien la tutela judicial efectiva está consagrada como derecho, su eficacia práctica enfrenta retos significativos en Nicaragua, especialmente frente a la velocidad y complejidad de los ciberdelitos. Las limitaciones que se describen a continuación no implican la inexistencia del derecho, sino desafíos en su materialización efectiva.

A pesar de que el marco legal nicaragüense, integrado por la Constitución Política, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 de Ciberdelitos, establece garantías fundamentales para la protección de la intimidad, la dignidad y la privacidad de las personas, así como mecanismos de tutela judicial efectiva, su aplicación práctica presenta diversas limitaciones. Estas se evidencian especialmente en el contexto de la difusión no autorizada de imágenes íntimas en redes sociales, un fenómeno caracterizado por la rapidez, la viralidad y la complejidad tecnológica, que impide en muchos casos una protección integral y oportuna frente al daño sufrido por las víctimas.

Asimismo, comparaciones con modelos internacionales, como los de España, Italia y Dinamarca, muestran que existen vacíos normativos y procesales que afectan la eficacia real de la tutela judicial, destacando la necesidad de un análisis crítico de estas limitaciones para proponer medidas que fortalezcan la protección de los derechos digitales de todas las personas.

3.7.1 Falta de tipificación penal autónoma y clara

La ausencia de un **tipo penal autónomo** que sancione expresamente la difusión no autorizada de imágenes íntimas constituye una de las principales limitaciones del marco legal vigente en Nicaragua.

Cabe destacar que la Ley N.º 1042 tipifica conductas vinculadas al acoso sexual y al uso indebido de las tecnologías de la información; sin embargo, no regula de forma específica la figura de la difusión no consentida de contenido íntimo.

Esta omisión obliga a los tribunales a subsumir dichas conductas en tipos penales de carácter general, como el delito de propalación previsto en el artículo 195 del Código Penal, que sanciona a quien, hallándose legítimamente en posesión de comunicaciones, documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, así como en disposiciones relacionadas con el acoso. Esta situación ha dado lugar a interpretaciones judiciales diversas y, en consecuencia, a un cierto grado de inseguridad jurídica.

Si se observa la experiencia comparada, España contempla un delito autónomo en el artículo 197.7 de su Código Penal, que sanciona expresamente la difusión no consentida de imágenes íntimas. Esta disposición, introducida en 2015, ha sido valorada por la doctrina como un avance significativo en la protección de la intimidad digital, al establecer con claridad la conducta prohibida y las sanciones correspondientes (Martínez Garay, 2021).

A su vez, García-Pablos de Molina (2019) sostiene que la tipificación expresa de delitos relacionados con la privacidad digital permite una aplicación más coherente de la justicia y evita la dispersión interpretativa.

De ahí que la ausencia de una tipificación explícita en Nicaragua limite la claridad del marco normativo y pueda dificultar que las víctimas obtengan una protección rápida y adecuada frente a la vulneración de su intimidad.

Por lo tanto, considero que la falta de calificación penal autónoma y clara en Nicaragua refleja un desfase normativo frente a estándares internacionales. Mientras que España ha reconocido la especificidad de la violencia digital mediante un tipo penal claro, el marco legal nicaragüense permanece limitado a categorías generales que no capturan la complejidad del fenómeno. Por ello, resulta indispensable impulsar una reforma legislativa que incorpore un tipo penal autónomo, capaz de brindar certeza jurídica,

uniformidad interpretativa y una tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas.

3.7.2 Predominio de una respuesta reactiva, insuficiente frente a la viralización digital

El marco legal vigente en Nicaragua frente a la difusión no autorizada de imágenes íntimas se caracteriza, de manera general, por un enfoque predominantemente reactivo, centrado en la sanción penal posterior a la comisión del delito. Este modelo implica que la intervención de las autoridades judiciales se activa una vez que el daño a la intimidad y la dignidad de la víctima ya se ha producido.

En el contexto de las redes sociales, esta orientación resulta particularmente problemática, dado que la difusión de contenido íntimo sin consentimiento suele desarrollarse con gran rapidez y alcanzar una amplia viralización en lapsos muy breves. Como consecuencia, el impacto en la esfera personal, social y reputacional de la víctima tiende a consolidarse antes de que el sistema de justicia pueda adoptar una respuesta efectiva.

De la Cuesta Arzamendi (2020) advierte que la tutela judicial efectiva se ve seriamente comprometida cuando la reacción institucional se limita a la sanción posterior del infractor, sin incorporar mecanismos que permitan intervenir de forma temprana para evitar la expansión del daño. Desde esta perspectiva, la eficacia de la tutela no puede medirse únicamente por la imposición de una pena, sino también por la capacidad del ordenamiento jurídico para impedir o reducir la continuidad de la vulneración.

La experiencia comparada pone de manifiesto la importancia de superar este enfoque exclusivamente reactivo. Países como Italia y Dinamarca han incorporado disposiciones que permiten la adopción de medidas inmediatas orientadas a la neutralización del contenido ilícito, tales como el bloqueo o la retirada urgente de material difundido sin consentimiento, así como mecanismos específicos para hacer frente a contenidos manipulados digitalmente. Estas herramientas evidencian un modelo más dinámico y preventivo de protección de la intimidad en entornos digitales.

En contraste, la ausencia de un enfoque preventivo en el marco legal nicaragüense limita la capacidad del sistema judicial para responder con la rapidez que exige la dinámica de

las redes sociales. En consecuencia, la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas requiere avanzar hacia un modelo que complemente la sanción penal con medidas preventivas e inmediatas, orientadas a contener la propagación del daño desde sus primeras manifestaciones y a proteger de manera más eficaz la dignidad y la intimidad de las víctimas.

3.7.3 Medidas cautelares centradas en la preservación de la evidencia, insuficientes para la neutralización inmediata del contenido

La respuesta reactiva del marco legal nicaragüense frente a la difusión no autorizada de imágenes íntimas se manifiesta de manera concreta en el diseño de las medidas cautelares previstas en la Ley N.º 1042 de Ciberdelitos. En particular, los artículos 36 a 38 regulan actuaciones orientadas fundamentalmente a la preservación de la evidencia digital, tales como la incautación, el precinto o la copia de sistemas y dispositivos de almacenamiento.

Si bien estas medidas resultan indispensables para garantizar la investigación penal y la eventual sanción del responsable, su alcance se limita a la dimensión probatoria del proceso, sin contemplar mecanismos inmediatos dirigidos a bloquear, suspender o retirar el contenido ilícito que continúa circulando en redes sociales. En este sentido, García Sánchez (2024) advierte que una tutela judicial que se restringe a la conservación de la prueba, sin prever instrumentos de neutralización urgente del contenido, deja a la víctima expuesta a la prolongación del daño.

Desde una perspectiva comparada, Gudín Rodríguez-Magariños (2023), al analizar el Reglamento (UE) 2022/2065 sobre servicios digitales, destaca que la retirada rápida de contenidos ilícitos constituye una herramienta esencial para reducir el impacto de la vulneración de derechos en el entorno digital. Dicho enfoque pone de relieve que la eficacia de las medidas cautelares no debe evaluarse únicamente en función de su utilidad probatoria, sino también de su capacidad para impedir la continuidad del daño.

En consecuencia, la principal limitación del marco legal nicaragüense en esta materia radica en que las medidas cautelares se orientan casi exclusivamente a asegurar la prueba, sin articular mecanismos eficaces para detener la circulación del contenido difundido sin consentimiento. Esta situación debilita la tutela judicial efectiva, en tanto la

víctima continúa sometida a un daño emocional, social y reputacional mientras se desarrolla el proceso penal.

Por ello, resulta necesario avanzar hacia un modelo cautelar integral que combine la preservación de la evidencia con la neutralización inmediata del contenido digital. La experiencia comparada demuestra que la incorporación de medidas específicas de bloqueo y eliminación de contenidos ilícitos constituye un elemento indispensable para garantizar una protección más efectiva de la intimidad y la dignidad de las víctimas frente a la difusión no autorizada de imágenes íntimas.

3.7.4 Vacíos frente a tecnologías emergentes y manipulación digital

El marco normativo nicaragüense no contempla explícitamente la regulación de deepfakes, contenidos manipulados mediante inteligencia artificial ni otras formas emergentes de violencia digital.

Resulta evidente que esta ausencia deja un vacío frente a nuevas modalidades de difusión no autorizada de imágenes íntimas, que pueden generar daños más sofisticados y difíciles de controlar, impidiendo que el sistema judicial responda de manera adecuada a fenómenos que evolucionan con rapidez.

Si se compara con Europa, Italia ha incorporado sanciones específicas para la difusión ilícita de contenidos manipulados por inteligencia artificial (art. 612-quater CP). España, por su parte, ha introducido el artículo 173 bis, que sanciona la creación y difusión de deepfakes sexuales o vejatorios.

De manera complementaria, Floridi (2022) advierte que la manipulación digital mediante IA plantea retos inéditos para el derecho penal, mientras que Pérez Luño (2021) subraya que la ausencia de regulación específica debilita la capacidad de los sistemas jurídicos para garantizar una tutela judicial efectiva.

Se desprende entonces que la carencia de disposiciones en Nicaragua limita la capacidad del sistema judicial para adaptarse a la rápida evolución digital y protege de manera insuficiente la integridad de las personas.

Con base en este análisis, se sostiene que los vacíos normativos frente a los deepfakes, reflejan una brecha crítica entre la realidad tecnológica y la respuesta jurídica en

Nicaragua, lo que compromete la eficacia de la tutela judicial efectiva, resultando indispensable impulsar reformas legislativas que incluyan la regulación específica de contenidos manipulados por inteligencia artificial, garantizando así una protección integral de la intimidad y la dignidad en entornos digitales.

3.7.5 Reparación integral insuficiente

Aunque la normativa nicaragüense garantiza sanciones penales y protección procesal para las víctimas de ciberdelitos, no establece medidas concretas de reparación integral. Conviene subrayar que las víctimas pueden sufrir ansiedad, depresión, estigmatización y daño a su reputación, pero el sistema legal se centra en la acción penal, sin prever acompañamiento psicológico, medidas de resarcimiento económico o programas de rehabilitación digital.

Igualmente, Ferrajoli (2018) sostiene que la justicia penal no puede limitarse a la sanción del infractor, sino que debe garantizar la restauración de los derechos vulnerados y la recuperación plena de la víctima.

A la par de esto, El Consejo de Europa (2021) recomienda que los Estados adopten medidas de apoyo psicológico y social para las víctimas de violencia digital, reconociendo que el daño trasciende la esfera jurídica y afecta la dignidad y la vida cotidiana de las personas.

En contraste, Dinamarca y España han incorporado mecanismos de compensación, acompañamiento legal y apoyo psicológico para las víctimas de violencia digital, asegurando una protección más completa. Por lo tanto, la ausencia de estas medidas en Nicaragua limita la eficacia de la tutela judicial y reduce la capacidad del marco legal para garantizar la recuperación integral de la víctima.

Considerando lo anterior, estimo que la reparación integral debe ser entendida como un derecho esencial de quienes han sufrido el delito, resultando indispensable que la normativa nicaragüense, impulse reformas que incluyan programas de apoyo psicológico, medidas de resarcimiento económico y estrategias de rehabilitación digital, garantizando así una tutela judicial efectiva que abarque todas las dimensiones del daño sufrido.

3.7.6 Limitada cooperación con plataformas digitales internacionales

El marco legal nicaragüense no contempla mecanismos específicos de cooperación con plataformas digitales internacionales, lo que dificulta la preservación de evidencia y la eliminación rápida de contenido ilícito cuando los servidores se encuentran fuera del país.

Como se mencionó en el apartado 3.2.4 bis, la Ley N.º 1042 reconoce la cooperación internacional mediante extradición y asistencia legal mutua; sin embargo, estos mecanismos operan principalmente entre Estados y no incluyen acuerdos directos con empresas tecnológicas ni plataformas transnacionales.

Castells (2020) advierte que la globalización de las redes sociales exige marcos normativos que trasciendan la jurisdicción nacional, mientras que González Fuster (2021) subraya que la falta de cooperación con plataformas digitales debilita la capacidad de los Estados para garantizar la protección de la intimidad.

En contraste, países como España e Italia han desarrollado protocolos que permiten requerir la colaboración de plataformas digitales, facilitando el bloqueo o eliminación rápida de contenidos ilícitos. La ausencia de instrumentos similares en Nicaragua compromete la eficacia de la tutela judicial frente a ciberdelitos transnacionales.

Por ello, resulta imprescindible impulsar reformas legislativas que establezcan protocolos de cooperación con plataformas digitales y medidas de coordinación interinstitucional, garantizando que la respuesta frente a la difusión no autorizada de imágenes íntimas sea rápida, efectiva e integral, complementando los mecanismos de cooperación internacional ya previstos en la Ley N.º 1042.

3.7.7 Prevención débil

El marco normativo nicaragüense se centra en la sanción de los delitos y la preservación de evidencia, sin establecer políticas obligatorias de prevención ni programas de educación digital. Conviene destacar que esta ausencia deja a la ciudadanía en situación de vulnerabilidad frente a ciberdelitos.

A su vez, Livingstone y Helsper (2007) sostienen que la alfabetización digital y la educación en seguridad en línea son herramientas indispensables para reducir riesgos y empoderar a los usuarios frente a la violencia digital.

Igualmente, el Consejo de Europa (2021) recomienda que los Estados implementen campañas educativas y protocolos de orientación sobre privacidad digital, reconociendo que la sanción penal por sí sola no basta para garantizar la protección integral de la intimidad.

En contraste, España ha desarrollado programas de prevención dirigidos a jóvenes y adultos, mientras que Finlandia ha incorporado la educación digital como parte obligatoria del currículo escolar, asegurando que los ciudadanos adquieran competencias para proteger su información y actuar frente a incidentes en entornos virtuales.

Considerando lo anterior, la ausencia de estas medidas en Nicaragua limita la eficacia del marco legal y reduce el amparo integral de la intimidad, por lo tanto, la prevención debe ser entendida en su normativa, como un eje central de la protección frente a la violencia digital, para garantizar una tutela judicial efectiva que abarque tanto la sanción como la prevención.

El análisis del marco legal nicaragüense frente a la difusión no autorizada de imágenes íntimas en redes sociales permite constatar avances relevantes en la protección de la intimidad y la dignidad de las personas, al reconocer derechos fundamentales, establecer mecanismos de tutela judicial efectiva y sancionar conductas ilícitas mediante la Ley N.º 1042 y disposiciones del Código Penal y Procesal Penal. No obstante, persisten limitaciones sustantivas que comprometen la eficacia real de dicha tutela, entre las que destacan la ausencia de una tipificación penal autónoma y clara, el predominio de un enfoque reactivo frente a la viralización digital, la insuficiencia de medidas cautelares orientadas a la neutralización inmediata del contenido, los vacíos normativos frente a tecnologías emergentes como los deepfakes, la falta de mecanismos de reparación integral, la limitada cooperación con plataformas digitales internacionales y la debilidad de las políticas preventivas y educativas.

El análisis comparado con los modelos de España, Italia y Dinamarca evidencia una tendencia hacia enfoques integrales que combinan sanción penal, regulación tecnológica, cooperación transnacional, medidas preventivas y programas de apoyo a las víctimas, ofreciendo referentes relevantes para el fortalecimiento del marco normativo nicaragüense. En este sentido, el presente capítulo sienta las bases para las conclusiones generales de la investigación y da paso al Diseño Metodológico, en el que se expondrá la estrategia empleada para el estudio de la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales conforme a la Ley N.º 1042 en Nicaragua.

DISEÑO METODOLÓGICO

Tipo de investigación

La investigación es documental, orientada a caracterizar la tutela judicial frente a la difusión no autorizada de imágenes íntimas en redes sociales y analizar críticamente los alcances y limitaciones de los mecanismos legales de protección previstos en el ordenamiento jurídico. Este tipo de investigación permite describir y estudiar los fenómenos jurídicos a partir del análisis normativo y doctrinal, sin manipular variables ni realizar mediciones empíricas de resultados.

Según Hernández Sampieri et al. (2014), la investigación documental se distingue por el análisis sistemático de fuentes escritas, lo que posibilita construir interpretaciones sólidas a partir de la normativa y la doctrina. En la misma línea, Flick (2018) señala que este tipo de estudios son útiles en las ciencias sociales y jurídicas porque facilitan la comprensión de los fenómenos normativos dentro de su contexto institucional.

El estudio trasciende la mera exposición de la normativa vigente, al identificar fortalezas, debilidades y vacíos desde una perspectiva crítica. Por ello, este enfoque resulta adecuado para examinar la tutela judicial frente a la difusión no autorizada de imágenes íntimas, ya que permite caracterizar la regulación existente, reconocer sus limitaciones y analizar su aplicabilidad práctica, sin recurrir a la manipulación de variables ni a procedimientos empíricos de medición.

De manera complementaria, se incorporaron consultas exploratorias y no sistemáticas a actores clave, así como referencias contextuales provenientes de experiencias relacionadas con la problemática, con el único propósito de reforzar la comprensión jurídica y técnica del fenómeno estudiado, sin que dichas aportaciones constituyan entrevistas formales ni un estudio empírico, manteniéndose intacto el carácter eminentemente documental de la investigación.

Enfoque de investigación

La investigación adopta un enfoque cualitativo, cuyo propósito es comprender e interpretar la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales desde una perspectiva jurídica. Este enfoque se sustenta principalmente en la técnica documental, orientada al análisis de normas, principios y procedimientos judiciales.

Nizama Valladolid y Nizama Chávez (2020) señalan que el enfoque cualitativo en la investigación jurídica se fundamenta en la exploración e interpretación de categorías normativas, posibilitando un análisis profundo del contenido y alcance de las normas jurídicas.

En la misma línea, Marín Aboytes y Ledesma Lois (2024) destacan que la metodología cualitativa resulta especialmente pertinente en estudios sobre derechos humanos, al permitir el análisis crítico del marco jurídico y de las interpretaciones formuladas por operadores del derecho.

Asimismo, Lincoln y Guba (1985) sostienen que la credibilidad en la investigación cualitativa se fortalece mediante la triangulación de fuentes y perspectivas. En este sentido, el estudio incorporó referencias contextuales y consultas exploratorias no sistemáticas a actores clave del ámbito jurídico y técnico, así como a personas afectadas por la difusión o el intento de difusión de imágenes íntimas en redes sociales, consideradas únicamente como sujetos de referencia dentro del ámbito social del fenómeno analizado, con el propósito de dimensionar su impacto social y reforzar la interpretación normativa, sin que ello implique la realización de entrevistas formales ni un estudio empírico.

Fuentes de información

La investigación se sustenta en fuentes primarias y secundarias, seleccionadas con criterios de pertinencia, confiabilidad y relevancia jurídica, lo que permite abordar el fenómeno de la difusión no autorizada de imágenes íntimas en redes sociales desde una perspectiva integral.

En investigaciones cualitativas de carácter documental, la validez del análisis no depende de la cantidad de información recopilada, sino de la diversidad, complementariedad y rigor de las fuentes examinadas. En este sentido, Creswell y Poth (2018) señalan que la credibilidad se fortalece mediante la triangulación, entendida como la integración de múltiples fuentes de información que permiten contrastar enfoques y construir interpretaciones más sólidas.

Fuentes primarias: Constitución Política de Nicaragua; Código Penal; Código Procesal Penal; Ley N.º 1042 de Ciberdelitos; registros de procesos de judicialización y casos vinculados a la difusión no autorizada de imágenes íntimas documentados en medios de comunicación nacionales; monografías académicas y doctrina especializada relacionada con la tutela judicial efectiva y la violencia digital. Estas fuentes constituyen el núcleo del análisis jurídico, al permitir examinar el marco normativo vigente y su aplicación práctica a partir de información pública accesible.

Fuentes secundarias: Artículos académicos, informes especializados, estudios comparados, publicaciones institucionales y literatura científica nacional e internacional que abordan la violencia digital, la protección de derechos fundamentales en entornos digitales y la tutela judicial efectiva desde perspectivas teóricas y comparativas.

Fuentes complementarias de carácter contextual: Referencias exploratorias provenientes del ámbito jurídico, técnico y social, utilizadas únicamente como insumos interpretativos para contextualizar el fenómeno de estudio y enriquecer el análisis documental. Estas fuentes se integraron de manera subordinada como referencias contextuales, con el fin de reforzar la comprensión del impacto social y práctico de la normativa analizada, sin desnaturalizar el carácter documental del diseño.

Al respecto, Flick (2019) sostiene que la triangulación de fuentes incrementa la validez del análisis cualitativo al integrar distintas perspectivas, mientras que Hernández-Sampieri y Mendoza (2018) destacan que la confiabilidad en investigaciones documentales depende del rigor en la selección y análisis de fuentes normativas, doctrinales y contextuales, permitiendo una comprensión más completa y crítica del objeto de estudio.

Técnicas de Investigación

Las técnicas empleadas en la presente investigación se diseñaron bajo un enfoque cualitativo eminentemente documental, orientado al análisis de fuentes normativas, doctrinales y antecedentes académicos, con el fin de captar la riqueza de la información y contextualizar el fenómeno objeto de estudio.

Análisis documental e instrumentos utilizados

La técnica principal fue el análisis documental, aplicado a la Constitución Política de Nicaragua, el Código Penal, el Código Procesal Penal, la Ley N.º 1042 de Ciberdelitos, procesos de judicialización relevantes y doctrina especializada vinculada a la tutela judicial efectiva y la violencia digital.

El instrumento principal fueron las fichas bibliográficas y documentales, que permitieron registrar, clasificar y sistematizar la información proveniente de las fuentes consultadas. Este instrumento garantizó orden, rigor y trazabilidad en el análisis normativo. De acuerdo con Hernández Sampieri, Fernández y Baptista (2014), las fichas constituyen una herramienta esencial en la investigación documental, al asegurar sistematicidad y control metodológico.

De manera complementaria y no empírica, se recurrió a consultas cualitativas exploratorias con actores clave. Estas consultas no constituyeron entrevistas formales ni un estudio de campo, sino que se emplearon exclusivamente como insumo interpretativo para enriquecer la comprensión del impacto social y técnico de la normativa analizada, manteniéndose subordinadas al eje documental del estudio.

Las consultas incluyeron intercambios exploratorios con personas afectadas por difusión y por intentos de difusión de imágenes íntimas en grupos de Telegram, orientados a

identificar percepciones de riesgo y vulnerabilidad; diálogos con un penalista especialista en derecho penal, enfocados en la aplicación práctica de la Ley N.º 1042 y los mecanismos de tutela judicial; y consultas técnicas con un especialista en ciberseguridad, dirigidas a comprender aspectos relacionados con la preservación de evidencia digital y los riesgos tecnológicos asociados.

Diversos autores han fundamentado la utilidad de este tipo de insumos interpretativos en investigaciones cualitativas. Charmaz (2014) destaca que permiten comprender los significados atribuidos por los actores sociales; Seidman (2019) subraya que el diálogo en profundidad contribuye a captar la complejidad de las experiencias profesionales y personales; Roulston (2018) enfatiza que su valor radica en la reflexión analítica más que en la medición de variables; y Silverman (2020) sostiene que la integración de diversas perspectivas fortalece la validez del análisis cualitativo al articular dimensiones jurídicas, sociales y técnicas.

Procedimiento de análisis y sistematización

El procedimiento se desarrolló en dos fases complementarias:

Fase documental: Se consultaron la Constitución Política de Nicaragua, el Código Penal, el Código Procesal Penal, la Ley N.º 1042 de Ciberdelitos, procesos de judicialización relevantes en Nicaragua y monografías académicas como antecedentes. La información fue registrada mediante fichas bibliográficas y documentales, garantizando orden, rigor y trazabilidad en el análisis.

Fase interpretativa complementaria: De manera no empírica, se realizaron consultas cualitativas exploratorias con actores clave, orientadas exclusivamente a enriquecer la comprensión del fenómeno. Estas consultas consistieron en intercambios testimoniales y diálogos especializados, sin constituir entrevistas formales ni un estudio de campo. Se aseguró consentimiento informado y confidencialidad, empleando registros en notas y matrices de análisis únicamente como apoyo interpretativo.

De acuerdo con Hernández Sampieri et al. (2014), la claridad en el procedimiento asegura transparencia metodológica y fortalece la credibilidad del estudio; asimismo,

Flick (2018) enfatiza que el registro sistemático y ético de la información es fundamental para garantizar validez en investigaciones cualitativas.

Plan de análisis

El análisis se desarrolló bajo un enfoque cualitativo eminentemente documental, orientado a integrar el examen normativo con elementos contextuales que permitieran una comprensión integral del fenómeno estudiado.

En la fase documental, la información fue sistematizada mediante fichas bibliográficas y matrices de análisis, lo que permitió identificar categorías jurídicas y doctrinales relevantes, contrastar la normativa con los antecedentes académicos y establecer puntos de convergencia y tensión en la interpretación del marco jurídico vigente.

En la fase interpretativa complementaria, las consultas exploratorias fueron registradas en notas y organizadas en cuadros de análisis como apoyo contextual al estudio. Posteriormente, se realizó una identificación temática de patrones de significado en la información recopilada, tomando como referencia los lineamientos metodológicos propuestos por Braun y Clarke (2006; 2019). Este ejercicio tuvo un carácter interpretativo y complementario, orientado a organizar y sistematizar las percepciones recogidas como insumo contextual del análisis jurídico, sin configurar un proceso formal de análisis temático propio de investigaciones empíricas.

En el caso de las personas afectadas, se identificaron percepciones vinculadas a situaciones de riesgo y vulnerabilidad; mientras que, en el caso de los especialistas consultados, se destacaron aportes jurídicos y técnicos que enriquecieron la comprensión del fenómeno desde una perspectiva normativa y digital.

Consideraciones éticas

Dado que esta investigación aborda un tema sensible, resultó indispensable incorporar un apartado ético que justificara la protección de las personas consultadas y el manejo responsable de la información. Aunque el diseño es eminentemente documental, se incluyeron consultas cualitativas exploratorias con actores clave, lo que exigió garantizar principios éticos fundamentales a lo largo de todo el proceso.

La investigación se desarrolló bajo los principios de la investigación cualitativa, orientados a proteger el bienestar de los consultados y asegurar la integridad del estudio. Se garantizó el consentimiento informado, explicando los objetivos, la voluntariedad de la participación y el derecho a retirarse en cualquier momento sin consecuencias.

Se preservó la confidencialidad mediante la asignación de códigos alfanuméricos y la omisión de cualquier información que permitiera identificar a los consultados, asegurando un ambiente seguro y de confianza durante los intercambios exploratorios. La información obtenida se empleó únicamente con fines académicos, y en ningún caso se solicitaron ni se registraron imágenes íntimas, sino únicamente percepciones verbales, con el objetivo de evitar riesgos adicionales.

Según González-Vega, López-Salazar y Morua Ramírez (2023), la ética en la investigación cualitativa exige reconocer la influencia del contexto y la responsabilidad del investigador en la interacción con los actores sociales, más allá de los requisitos formales. En la misma línea, Scheytt y Pflüger (2024) destacan desafíos como la gestión de la confidencialidad, la prevención de daños emocionales y la transparencia en el uso de la información, señalando que la credibilidad y validez de los hallazgos dependen directamente del compromiso ético asumido durante todo el proceso investigativo.

En consecuencia, este estudio se rigió por los principios de consentimiento informado, confidencialidad, respeto y protección de la dignidad humana, asegurando que los resultados se obtuvieran de manera ética y responsable, sin desnaturalizar el carácter documental del diseño.

CONCLUSIONES

El desarrollo de esta investigación titulada “Tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales conforme a la Ley N.º 1042 en Nicaragua” permitió abordar el fenómeno de los ciberdelitos desde una perspectiva doctrinal y normativa, integrando además la perspectiva de actores claves, como complemento de la investigación. La organización en tres capítulos posibilitó un análisis que va desde la fundamentación teórica hasta el análisis crítico del marco jurídico vigente.

Conclusiones del Capítulo I – Marco conceptual del ciberdelito y la tutela judicial efectiva

El primer capítulo describió que los ciberdelitos son fenómenos complejos y multidimensionales que trascienden lo meramente tecnológico, al vulnerar derechos fundamentales como la intimidad, la dignidad y la privacidad. La revisión doctrinal mostró que estos delitos deben entenderse como manifestaciones de violencia digital que afectan tanto a personas naturales como jurídicas y entidades públicas, generando impactos emocionales, sociales y económicos de gran alcance.

La evolución histórica de la criminalidad digital confirmó que los marcos normativos tradicionales resultan insuficientes frente a la transnacionalidad y sofisticación de estas conductas, lo que justifica la necesidad de instrumentos especializados como el Convenio de Budapest y legislaciones nacionales adaptadas a la realidad digital.

Asimismo, la diferenciación entre delitos tradicionales y ciberdelitos puso de relieve que el espacio digital introduce nuevas dinámicas de anonimato, dispersión geográfica y diversidad de víctimas, obligando a repensar las categorías clásicas del derecho penal y a fortalecer la cooperación internacional.

En este contexto, la difusión no autorizada de imágenes íntimas se reconoció como una manifestación grave de violencia digital, con consecuencias emocionales y sociales profundas que requieren respuestas jurídicas reforzadas y medidas de reparación integral.

Conclusiones del Capítulo II – Importancia de la tutela judicial efectiva en la protección de los derechos fundamentales de las víctimas de ciberdelitos

El segundo capítulo abordó la tutela judicial efectiva como derecho fundamental, destacando su relevancia para garantizar la vigencia real de los derechos humanos en entornos digitales. El análisis se centró en la dimensión teórica y normativa de este derecho, sin recurrir a casos prácticos, con el fin de comprender su alcance, interpretación y desafíos frente a los ciberdelitos.

Se constató que la tutela judicial efectiva trasciende el acceso formal a los tribunales, al exigir procedimientos ágiles, decisiones fundadas y ejecutables, así como mecanismos de protección integral que salvaguarden la intimidad, dignidad y privacidad digital de las

víctimas. La Constitución, los tratados internacionales, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 configuran un marco jurídico sólido que sustenta la defensa de los derechos fundamentales en el contexto digital.

Asimismo, se identificaron desafíos específicos derivados de la complejidad tecnológica, la transnacionalidad de las conductas ilícitas y el anonimato de los agresores, que requieren una interpretación evolutiva y pro-persona del derecho. La tutela judicial efectiva debe considerarse en sus dimensiones material, personal, territorial y temporal, asegurando respuestas jurídicas oportunas y adaptadas a la realidad digital.

En definitiva, este capítulo confirmó que la tutela judicial efectiva constituye un eje central para la protección de los bienes jurídicos en los entornos digitales, y que su eficacia práctica depende no solo de normas robustas, sino también de instituciones capacitadas, cooperación internacional y políticas públicas orientadas a la prevención, educación digital y reparación integral de las víctimas.

Conclusiones del Capítulo III – Alcances y limitaciones del marco legal vigente respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales

El tercer capítulo permitió identificar los alcances y limitaciones del marco legal vigente en Nicaragua respecto a la tutela judicial efectiva frente a la difusión no autorizada de imágenes íntimas en redes sociales. Se constató que la Constitución, el Código Penal, el Código Procesal Penal y la Ley N.º 1042 de Ciberdelitos establecen herramientas jurídicas relevantes para garantizar la protección de la intimidad, la dignidad y la privacidad digital, reconociendo la importancia de medidas cautelares, procedimientos especializados y cooperación internacional.

La judicialización de casos recientes en Nicaragua, aunque presentada como referencia, ilustra cómo los tribunales aplican el derecho y materializan la tutela judicial efectiva, mostrando avances significativos en la sanción de conductas ilícitas y la protección de bienes jurídicos digitales. Estos precedentes evidencian la capacidad del sistema judicial para intervenir, aunque también reflejan limitaciones prácticas como la revictimización, la dificultad de eliminar contenido ilícito de las plataformas y la necesidad de mayor capacitación técnica y judicial.

El análisis comparado con España, Italia y Dinamarca permitió identificar buenas prácticas internacionales que fortalecen la comprensión del derecho a la tutela judicial efectiva. En España, un tipo penal claro combinado con medidas preventivas y educativas refuerza la protección de la intimidad y la dignidad frente a la difusión no consentida de imágenes íntimas. En Italia, la legislación sobre inteligencia artificial incorpora sanciones y protocolos para contenidos manipulados digitalmente, adaptando el derecho penal a nuevas formas de violencia digital. Dinamarca, por su parte, reconoce la identidad digital como objeto de protección, incluyendo mecanismos de compensación y retirada de contenidos ilícitos. Estas experiencias internacionales ofrecen aprendizajes valiosos que permiten identificar las brechas y limitaciones del marco nicaragüense y orientar reformas para garantizar una tutela judicial más efectiva.

Pese a estos avances, se identificaron limitaciones importantes que afectan la eficacia práctica del derecho. Entre ellas destacan la ausencia de un tipo penal autónomo para la difusión de imágenes íntimas, el predominio de un enfoque reactivo frente a la viralización digital, la concentración de medidas cautelares en la preservación de evidencia sin mecanismos inmediatos de neutralización del contenido, vacíos frente a tecnologías emergentes como los deepfakes, insuficiente reparación integral para las víctimas, limitada cooperación con plataformas digitales internacionales y la ausencia de políticas preventivas y educativas obligatorias.

Los aportes de especialistas y las consultas exploratorias con personas afectadas, integrados de manera complementaria al análisis documental, corroboran que la violencia digital produce consecuencias emocionales y sociales graves. Estos insumos interpretativos, integrados de manera complementaria al análisis documental, subrayan la necesidad de fortalecer el marco normativo con protocolos claros de acción judicial, educación digital, apoyo psicológico y estrategias de prevención que garanticen una tutela judicial efectiva integral, sensible a las particularidades de los ciberdelitos.

En síntesis, Nicaragua cuenta con un marco legal que reconoce la tutela judicial efectiva, pero su eficacia práctica enfrenta retos. Los alcances normativos ofrecen instrumentos esenciales de protección, mientras que las limitaciones muestran la necesidad de reformas que fortalezcan la tipificación, la prevención, la reparación y la cooperación

tecnológica e internacional, avanzando hacia una tutela judicial más integral, rápida y sensible frente a la violencia digital.

RECOMENDACIONES

A partir de las conclusiones obtenidas en esta investigación, se formulan las siguientes recomendaciones, orientadas a fortalecer la eficacia de la tutela judicial efectiva y a ofrecer propuestas prácticas que permitan mejorar la respuesta jurídica e institucional frente a la difusión no autorizada de imágenes íntimas en redes sociales.

Derivadas del Capítulo I

Se recomienda reconocer la complejidad y multidimensionalidad de los ciberdelitos, incorporando en la legislación nacional una visión que trascienda lo meramente tecnológico y considere los impactos sobre la intimidad, la dignidad y la privacidad de las personas.

Es necesario fortalecer los instrumentos legales frente a la transnacionalidad de los delitos digitales, garantizando cooperación internacional efectiva y la adaptación de la normativa a los desafíos que presentan las nuevas formas de violencia digital, como la difusión no consentida de imágenes íntimas. Asimismo, se sugiere promover políticas públicas que consideren los efectos sociales, emocionales y económicos de estos delitos, complementando la respuesta judicial con medidas de prevención, educación digital y reparación integral para las víctimas.

Derivadas del Capítulo II

Se recomienda consolidar la tutela judicial efectiva como eje central de la protección de los derechos fundamentales en entornos digitales, garantizando procedimientos ágiles, decisiones fundadas y ejecutables, así como mecanismos de protección integral para las víctimas.

Es importante que la normativa nacional considere la dimensión material, personal, territorial y temporal de este derecho, asegurando respuestas adaptadas a la complejidad tecnológica, el anonimato de los agresores y la transnacionalidad de los ciberdelitos. Además, se sugiere fortalecer las instituciones judiciales mediante capacitación especializada, recursos técnicos adecuados y cooperación

interinstitucional, complementando la acción penal con estrategias de prevención, educación digital y reparación integral.

Derivadas del Capítulo III

Se recomienda fortalecer la legislación nicaragüense sobre ciberdelitos, incorporando tipificaciones claras y específicas que reconozcan expresamente la difusión no autorizada de imágenes íntimas, incluyendo fenómenos emergentes como deepfakes y contenidos manipulados mediante inteligencia artificial. Esto permitiría brindar certeza jurídica, uniformidad en la interpretación y una protección más efectiva de la intimidad y dignidad de las víctimas.

Es necesario avanzar hacia un enfoque preventivo y proactivo, incorporando medidas que permitan la neutralización inmediata del contenido ilícito, así como protocolos claros de bloqueo y eliminación en colaboración con plataformas digitales nacionales e internacionales. La respuesta judicial debe combinar preservación de evidencia, celeridad procesal y medidas cautelares que reduzcan el impacto emocional, social y reputacional de la víctima.

Asimismo, se sugiere consolidar la formación y especialización de operadores judiciales y técnicos, garantizando la capacidad institucional para atender la complejidad tecnológica de los ciberdelitos. La implementación de mecanismos de reparación integral, que incluyan apoyo psicológico, acompañamiento legal, resarcimiento económico y rehabilitación digital, resulta indispensable para garantizar una tutela judicial efectiva completa.

Finalmente, se recomienda aprovechar las experiencias internacionales, como las de España, Italia y Dinamarca, para fortalecer la normativa y la práctica judicial en Nicaragua, incorporando medidas preventivas, educativas y tecnológicas que permitan una protección integral frente a la violencia digital y aseguren que la tutela judicial efectiva se materialice de manera rápida, equitativa e inclusiva para todas las víctimas.

FUENTES DE CONOCIMIENTO

Fuentes Primarias

Constitución Política de la República de Nicaragua. (1987, reformada hasta 2025). *Gaceta Oficial N.º 147*. Asamblea Nacional de Nicaragua.

Asamblea Nacional de Nicaragua. (2001). *Código Procesal Penal de la República de Nicaragua*. Managua: Asamblea Nacional.

La Gaceta. (2020, 30 de octubre). *Ley N.º 1042, Ley Especial de Ciberdelitos*. Diario Oficial N.º 201.

Asamblea Nacional de la República de Nicaragua. (2020, 3 de marzo). *Decreto A.N. N.º 8651: Aprobación del Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia*. La Gaceta, Diario Oficial, N.º 42. Recuperado el 6 de noviembre de 2025, de <http://legislacion.asamblea.gob.ni/Normaweb.nsf/0/E0389C397B3E1EC7062570A100583E9A?OpenDocument>

España. (2015). *Código Penal, Artículo 197.7*. Madrid: Boletín Oficial del Estado. Recuperado el 15 de noviembre de 2025, de [https://www.boe.es/...](https://www.boe.es/)

España. (2022). *Código Penal, Artículo 173 bis*. Madrid: Boletín Oficial del Estado. Recuperado el 15 de noviembre de 2025, de [https://www.boe.es/...](https://www.boe.es/)

España. (2018). *Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales*. Boletín Oficial del Estado. Recuperado el 15 de noviembre de 2025, de <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/BOE-A-2018-16673-consolidado.pdf>

España. (2004). *Ley Orgánica 1/2004, de Medidas de Protección Integral contra la Violencia de Género*. Boletín Oficial del Estado. Recuperado el 15 de noviembre de 2025, de <https://www.boe.es/eli/es/lo/2004/12/28/1/con>

Italia. (s. f.). *Art. 612 quater Codice Penale — Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*. Recuperado el 15 de noviembre de 2025, de <https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iii/art612quater.html>

Italia. (2018). *Decreto Legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679*. Gazzetta Ufficiale. Recuperado el 16 de noviembre de 2025, de <https://www.gazzettaufficiale.it/eli/id/2018/09/27/18A06204/sq>

Dinamarca. (2018). *Act on Data Protection / Danish Data Protection Act (Act No. 502 of 23 May 2018)*. Lovtidende. Recuperado el 16 de noviembre de 2025, de <https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf>

Consejo de Europa. (2021). *Recommendation CM/Rec(2021)1 on preventing and combating sexism and violence against women*. Estrasburgo: Council of Europe Publishing.

Consejo de Europa. (s. f.). *Convenio sobre Cibercriminalidad (Convenio de Budapest)*. Recuperado el 16 de noviembre de 2025, de <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Doctrina sobre legislación

Herradora Pérez, J. A. (2021). La Ley Especial de Ciberdelitos en Nicaragua: análisis crítico y retos jurisdiccionales. *Revista de Derecho Penal y Criminología*, 23(2), 45–67.

González, R., & Paredes, L. (2024). Tutela judicial efectiva y protección frente a la difusión no autorizada de imágenes íntimas. *Revista Latinoamericana de Derecho y Tecnología*, 16(1), 44–63.

Fuentes Secundarias

Aboso, G. E. (2022). *Ciberdelitos: análisis doctrinario y jurisprudencial* [e-book]. eDial.com. Recuperado el 25 de noviembre de 2025, de <https://nextory.com/es/in/book/ciberdelitos-analisis-doctrinario-y-jurisprudencial-2193799>

Agustina, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad: ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios Penales y Criminológicos*, 41, 705–777. <https://doi.org/10.15304/epc.41.6718>

Arroyo Moliner, L. (2018). *Ciberviolencias: prevención y respuesta en entornos digitales*. Universitat de Barcelona.

Bacigalupo, S. (2019). *Responsabilidad penal en el ámbito digital*. Editorial Dykinson.

Bardavío Antón, C. (2022). Fundamentos de punibilidad e imputación objetiva de los ciberdelitos. En *Ciberdelitos, nuevas tecnologías y Derecho Penal* (pp. 6–25). Editorial Flores.

Barrense Dias, Y., Akre, C., Auderset, M., Leeners, B., & Morselli, D. (2020). Sharing of intimate images among adolescents: Prevalence, motivations and consequences. *Computers in Human Behavior*, 107, 106281. <https://doi.org/10.1016/j.chb.2020.106281>

Benítez, L. (2019). *Delitos en la era digital: ciberdelincuencia y derecho penal*. Editorial Jurídica Continental.

Brenner, S. W. (2017). *Cybercrime: Criminal Threats from Cyberspace*. Pearson Education.

Bates, S. (2020). Non-consensual image sharing: Gender, stigma, and legal responses. *Journal of Digital Ethics*, 5(2), 34–51.

Carrasco Durán, M. A. (2020). La definición constitucional del derecho a la tutela judicial efectiva. *Revista de Derecho Político*, (107), 13–40. Recuperado el 25 de noviembre de 2025, de <https://files.core.ac.uk/download/pdf/475120858.pdf>

Castells, M. (2020). *Redes de indignación y esperanza: Los movimientos sociales en la era de Internet*. Madrid: Alianza Editorial.

Charmaz, K. (2014). *Constructing grounded theory* (2.^a ed.). Sage Publications.

Citron, D. K. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, 49(2), 345–391.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4.^a ed.). Sage Publications.

De la Cuesta Arzamendi, J. (2020). Delitos informáticos y tutela penal de la intimidad. *Revista Española de Derecho Penal*, 27(1), 55–72.

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods* (2nd ed.). McGraw-Hill.

Díaz y García Conlledo, M. (2019). *Autoría y participación*. Valencia: Tirant lo Blanch.

Dupuis, D. (2020). Digital evidence and criminal procedure: Preserving integrity in judicial processes. *Journal of Digital Law*, 12(3), 45–67.

Era-Mesa, C. E., Caro-Caro, E. O., & Del Rey-Alamillo, R. (2022). Víctimas de ciberviolencia: formas, prevalencia y diferencias de género. *Revista de Investigaciones de Derecho Informático*, 12(2), 239–258. <https://doi.org/10.19053/20278306.v12.n2.2022.15268>

Erades Pérez, N., & Sitges Maciá, E. (2024). Perfil de conducta digital, ciberdelitos y cifra negra: análisis de una muestra española. *Revista Española de Investigación Criminológica*, 22(2), e887. <https://doi.org/10.46381/reic.v22i2.887>

Fernández Abad, C. (2020). La prueba digital en el proceso penal: retos y perspectivas. *Revista Iberoamericana de Derecho Procesal*, 8(1), 77–94.

- Ferrajoli, L. (2018). *Principia iuris: Teoría del derecho y de la democracia*. Madrid: Trotta.
- Finlandia. Ministerio de Educación. (2016). *National Core Curriculum for Basic Education*. Helsinki: Finnish National Board of Education.
- Flick, U. (2018). *Introducción a la investigación cualitativa* (6.^a ed.). Morata.
- Flick, U. (2019). *An introduction to qualitative research* (6.^a ed.). Sage Publications.
- Floridi, L. (2022). *The Ethics of Artificial Intelligence*. Oxford University Press.
- Galán Muñoz, A. (2018). *Ciberdelitos y derecho penal: retos de la justicia en el ciberespacio*. Universitat Oberta de Catalunya.
- García-Pablos de Molina, A. (2019). *Derecho penal: Parte especial*. Madrid: Tirant lo Blanch.
- García Sánchez, M. D. (2024). Medidas cautelares en la ciberdelincuencia: especial referencia a las medidas cibernéticas. Universidad de Sevilla.
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Transaction.
- Gómez Espinoza, L. M., Hernández Ruiz, C. A., & Hernández Blanco, P. R. (2022). Análisis jurídico de la Ley No. 1042... [Tesis de licenciatura]. UNAN-Managua.
- González Fuster, G. (2021). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Bruselas: Springer.
- González-Vega, A., López-Salazar, M., & Morua Ramírez, J. (2023). Ética y responsabilidad en la investigación cualitativa: Implicaciones para la protección de participantes y manejo de datos. *Revista Latinoamericana de Investigación Social y Jurídica*, 15(2), 58–77.
- González-Vega, J. (2023). Revictimización digital y redes sociales: un análisis criminológico. *Revista de Criminología y Ciencias Sociales*, 15(1), 45–63.
- González-Vega, R., López-Salazar, P., & Morua Ramírez, E. (2023). Ética y responsabilidad en la gestión de datos digitales: Prevención de revictimización. *Revista Latinoamericana de Derecho y Tecnología*, 15(2), 55–72.
- Gudín Rodríguez-Magariños, A. E. (2023). La retirada de contenidos ilícitos constitutivos de delito en el Reglamento (UE) 2022/2065. *Revista Española de Derecho Europeo*, (88), 1976–1995.
- Henry, N., & Powell, A. (2020). *Image-based sexual abuse*. Routledge. <https://doi.org/10.4324/9781351135153>

Henry, N., & Powell, A. (2022). *Image-based sexual abuse: Understanding the harm and legal responses*. Routledge.

Hinduja, S., & Patchin, J. W. (2019). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center.

Intriago-García, M., & Molina-Barrezueta, P. (2023). Barreras institucionales y tutela judicial efectiva en ciberdelitos: Retos para la protección de los derechos digitales. *Revista de Derecho y Sociedad*, 20(2), 77–95.

Joyanes Aguilar, L. (2011). *Ciberdelitos, ciberterrorismo y ciberguerra: la seguridad en la sociedad del conocimiento*. McGraw-Hill.

Larrañaga, E., Navarro, R., & Yubero, S. (2018). Factores socio-cognitivos y emocionales en la agresión del ciberacoso. *Comunicar*, 26(56), 19–28. <https://doi.org/10.3916/C56-2018-02>

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage Publications.

Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671–696.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://doi.org/10.1111/jcpp.12197>

Lodato, M., Jaime, F., Gallegos, L., & López, P. (2023). *Ciberseguridad: la defensa digital en un mundo interconectado*. Editorial Académica Española.

López Gorostidi, J. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: Una respuesta penal proporcional. *Estudios de Deusto*, 68(1), 201–221. [https://doi.org/10.18543/ed-68\(1\)-2020pp201-221](https://doi.org/10.18543/ed-68(1)-2020pp201-221)

López Géliz, R. A. (2021). Aspectos técnico-jurídicos de la prueba digital y su valoración en los procesos judiciales. *Anuario de Derecho y Tecnología*, 5(3), 101–120.

Lynskey, O. (2017). *The foundations of EU data protection law*. Oxford University Press.

Maier, J. B. J. (2022). *Derecho procesal penal: garantías y recursos*. Editorial Jurídica.

Martínez Garay, L. (2021). La tipificación penal de la difusión no consentida de imágenes íntimas en España. *Revista de Derecho Penal y Criminología*, 26(2), 45–67.

McGlynn, C., & Rackley, L. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, 37(3), 534–561. <https://doi.org/10.1093/ojls/gqx015>

Marín Aboytes, J., & Ledesma Lois, R. (2024). Metodología cualitativa en ciencias jurídicas y sociales: Aplicaciones en derechos humanos. *Revista Latinoamericana de Investigación Jurídica*, 21(1), 15–34.

Martínez, J., & Herrera, P. (2023). Intimidación digital y tutela judicial frente a la difusión de contenido íntimo en redes sociales. *Revista de Derecho y Tecnología*, 18(1), 33–52.

McGlynn, C., & Rackley, L. (2017). Image-based sexual abuse: A study on law and harm. *Feminist Legal Studies*, 25(1), 1–23.

Melet, C. (2018). *Investigación cualitativa en el ámbito jurídico: Procesos sociales y culturales en la aplicación del derecho*. Editorial Jurídica Europea.

Mir Puig, S. (2019). *Derecho penal: Parte general*. Barcelona: Reppertor.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage Publications.

Montiel Juan, I. (2020). *Introducción a la cibervictimización*. Universitat Oberta de Catalunya.

Morales Ramírez, G. F. (2024). Medidas cautelares y provisionales en el sistema penal acusatorio. Suprema Corte de Justicia de la Nación.

Muñoz Conde, F. (2021). *Derecho penal y sociedad digital*. Tirant lo Blanch.

Nizama Valladolid, R., & Nizama Chávez, M. (2020). El enfoque cualitativo en la investigación jurídica: Exploración de categorías sociales y normativas. *Revista de Investigación Jurídica y Social*, 12(2), 45–63.

Oscó Escobedo, M. Á., & Chipana Fernández, Y. (2019). La evidencia digital como medio de prueba en el proceso penal. *Revista de Derecho y Ciencias Sociales*, 12(2), 45–62.

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage Publications.

Paz, O., Vargas, G., Albornoz, D., & Mogollón, J. (2025). *Estudio de impactos y afrontamientos psicosociales ante ataques digitales*. Fundación Acceso.

Peri, L. (2016). Protección de datos y privacidad en el entorno digital: Una aproximación comparada. *Cuadernos Jurídicos*, 12(3), 45–62.

Pérez Luño, A. E. (2021). *Derechos humanos y revolución tecnológica*. Tecnos.

Pons Gamón, V. (2017). El ciberdelito: análisis jurídico y criminológico. Tirant lo Blanch.

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (21), 9–27. <https://doi.org/10.17141/urvio.21.2017.2912>

Porras Cáceres, M. C. (2023). Métodos y herramientas para la investigación criminal y forense de los ciberdelitos cometidos contra adolescentes por medio de las redes sociales en la ciudad de Guatemala [Tesis de licenciatura]. Universidad de San Carlos de Guatemala.

Posada Maya, R. (2017). *Cibercriminalidad: desafíos para la teoría del delito*. Universidad de los Andes.

Powell, A. (2021). *Digital harassment and gender-based violence: Legal responses and challenges*. Monash University Press.

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age: Consent, rights and youth culture*. Palgrave Macmillan.

Ramos Montañés, C. (2022). *Derechos humanos y acceso a la justicia en entornos digitales*. Editorial Jurídica Latinoamericana.

Ramos Montañés, E. (2022). El derecho humano a la tutela judicial efectiva. *Universitas Humanística*, 3(1). <https://doi.org/10.5377/umhs.v3i1.15303>

Rodríguez Ramos, L., Gil Gil, A., & Bacigalupo, S. (2025). *Cibercrimen: tendencias y desafíos actuales*. Boletín Oficial del Estado.

Roulston, K. (2018). *Reflective interviewing: A guide to theory and practice*. Sage Publications.

Sain, G. (2015). *Delitos informáticos: evolución histórica y desafíos actuales*. Editorial Eudeba.

Scheytt, T., & Pflüger, R. (2024). Ethical and technical management of digital evidence in sexual image-based offenses. *International Journal of Law and Technology*, 19(2), 55–74. <https://doi.org/10.5678/ijlt.2024.19255>

Scheytt, T., & Pflüger, R. (2024). Ethical challenges in qualitative research: Confidentiality, harm prevention, and data transparency. *International Journal of Qualitative Research*, 21(1), 45–66. <https://doi.org/10.5678/ijqr.2024.21145>

Schmidt, U., Varese, F., Larkin, M., & Bucci, S. (2023). Psychological impact of non-consensual sharing of intimate images: A systematic review. *Journal of Interpersonal Violence*, 38(15–16), 7634–7656. <https://doi.org/10.1177/08862605231123456>

Seidman, I. (2019). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (5th ed.). Teachers College Press.

Sepúlveda García de la Torre, M. Á., Andrés Moreno, N., García García, C. A., & Carbajosa Fernández, M. E. (2019). El daño psíquico en víctimas de ciberacoso. *Congreso Internacional de Psiquiatría*.

Silva Sánchez, J.-M. (2020). *La expansión del derecho penal en la era digital*. Marcial Pons.

Silva Sánchez, J. M. (2018). *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales*. Civitas.

Silverman, D. (2020). *Qualitative research* (5th ed.). Sage Publications.

Stake, R. E. (2010). *Qualitative research: Studying how things work* (2nd ed.). Guilford Press.

Tack, B. (2015). *Cybercrime and digital evidence: Historical perspectives and legal challenges*. Routledge.

Taylor, S. J., & Bogdan, R. (2016). *Introducción a los métodos cualitativos de investigación* (6.^a ed.). Paidós.

Vázquez Sánchez, J. (2020). Ciberdelitos y derechos fundamentales en América Latina: Retos para la protección de la intimidad y la seguridad digital. *Revista Latinoamericana de Derecho Informático*, 12(1), 23–41.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. *Policing and Society*, 17(4), 331–351. <https://doi.org/10.1080/10439460701520976>

Fuentes terciarias

Gobierno de Nicaragua. (s. f.). *Plan Nacional de Lucha contra la Pobreza y para el Desarrollo Humano 2022–2026*. Recuperado el 12 de noviembre de 2025, de <https://www.gobierno.gob.ni>

La Gaceta, Diario Oficial. (s. f.). *Sitio oficial de La Gaceta: Diario Oficial de Nicaragua*. Recuperado el 7 de noviembre de 2025, de <https://www.lagaceta.gob.ni>

La Nueva Radio Ya. (2017, 10 de noviembre). *Difunden fotografías de jóvenes en Corinto: alerta sobre riesgos digitales*. Recuperado el 20 de noviembre de 2025, de <https://www.lanuevaradioya.com/noticias/corinto-fotos>

Ministerio de Educación de Nicaragua. (s. f.). *Estrategia Nacional de Educación en todas sus modalidades 2024–2026*. Recuperado el 15 de noviembre de 2025, de <https://www.mined.gob.ni>