UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA PROFESIONAL DE DERECHO

TRABAJO DE SUFICIENCIA PROFESIONAL

"La evolución del derecho en la era digital: retos y oportunidades frente a los delitos cibernéticos"

AUTOR:

Bach. Perez Castro, Ricardo Robert

PARA OPTAR EL TITULO PROFESIONAL DE:

ABOGADO

ASESOR:

Abg. Castillo Figueroa, Carlos Francisco

ORCID: 0009-0009-6953-651X

DNI: 09530087

LIMA-PERÚ

2026

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

INFORME DE SIMILITUD

Nº050-2026-UPCI-FDCP-REHO-T

A : **MG. HERMOZA OCHANTE RUBÉN EDGAR**
Decano (e) de la Facultad de Derecho y Ciencias Políticas

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional:
BACHILLER PEREZ CASTRO, RICARDO ROBERT

FECHA : Lima, 16 de julio de 2026.

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: **"LA EVOLUCIÓN DEL DERECHO EN LA ERA DIGITAL: RETOS Y OPORTUNIDADES FRENTE A LOS DELITOS CIBERNÉTICOS"**, presentado por el Bachiller **PEREZ CASTRO, RICARDO ROBERT.**
2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 13%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).
3. Al término análisis, el Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

.....
MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

Adjunto:
**Resultado de similitud*

Dedicatoria

Quiero dedicarle este trabajo de investigación a mis padres, por su eterna dedicación a mi persona y por haberme formado ética y moralmente solvente para afrontar todos los avatares de la vida.

……..

Agradecimiento

Quiero agradecer por medio de estas líneas a todas las personas que me apoyaron en este largo camino académico, a mis amigos y familiares, a mis maestros y la autoridades de mi alma mater.

.....

Declaración de Autoría

Nombres : RICARDO ROBERT

Apellidos : PEREZ CASTRO

Código : 1304000510

DNI : 08419544

Declaro que, soy el autor del trabajo realizado y que es la versión final que he entregado a la oficina del Decanato de la Facultad de Derecho y Ciencias Políticas de la Universidad Peruana de Ciencias e Informática.

Asimismo, declaro que he citado debidamente las palabras o ideas de otros autores, refiriendo expresamente el nombre de la obra y página o páginas que me sirvieron de fuente.

Jesús María, julio del 2026.

ÍNDICE

INTRODUCCION

La irrupción de la era digital ha supuesto una de las transformaciones más profundas en la historia reciente de la humanidad, alterando no solo la forma en que las personas se comunican, trabajan y acceden a la información, sino también los cimientos mismos de la organización social y jurídica (Castells, 2001). La digitalización ha propiciado la emergencia de una nueva "galaxia" informativa, en la que las fronteras físicas se diluyen y los flujos de datos adquieren una centralidad inédita en la vida cotidiana y en la economía global.

En este contexto, el derecho se enfrenta al reto de adaptarse a una realidad en constante mutación, donde los paradigmas normativos tradicionales resultan, en muchos casos, insuficientes para dar respuesta a los desafíos emergentes (Barrio Andrés, 2018; Quadra Salcedo & Piñar Mañas, 2018).

Uno de los fenómenos más significativos de esta revolución digital es la proliferación de los delitos cibernéticos, cuya magnitud y sofisticación han alcanzado niveles sin precedentes, según la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2024), con dos tercios de la población mundial conectada a Internet, el cibercrimen se ha convertido en una amenaza global, con pérdidas económicas anuales equiparables al producto interno bruto de las principales economías del mundo.

Solo en el sudeste asiático, las pérdidas financieras derivadas del fraude cibernético se estimaron entre 18.000 y 37.000 millones de dólares en 2023, lo que evidencia la dimensión transnacional y el impacto sistémico de estas conductas ilícitas (UNODC, 2024).

La naturaleza dinámica y transfronteriza del cibercrimen plantea desafíos singulares para los sistemas jurídicos, las amenazas más prevalentes en la Unión Europea, según el informe ENISA Threat Landscape 2024, incluyen los ataques de denegación de servicio (DDoS), que encabezan la lista de riesgos, seguidos por el ransomware y las brechas de datos; el phishing, por su parte, constituye el vector inicial en el 60% de los incidentes, y más del 80% de las campañas de phishing ya emplean inteligencia artificial para aumentar su eficacia (ENISA, 2024). Esta evolución tecnológica de la criminalidad digital exige una respuesta jurídica ágil y coordinada, capaz de anticipar y contrarrestar las nuevas formas de ataque (Miró Llinares, 2021).

Frente a este panorama, los marcos normativos tradicionales muestran claras limitaciones; el derecho penal clásico, concebido para delitos cometidos en el espacio físico, se ve desbordado por la volatilidad, anonimato y ubicuidad de las conductas delictivas en el ciberespacio (Miró Llinares, 2012; Davara Rodríguez, 2020); la dificultad para atribuir responsabilidades, la complejidad probatoria y la fragmentación jurisdiccional obstaculizan la persecución efectiva de los ciberdelitos. Además, la rápida obsolescencia tecnológica desafía la capacidad de los legisladores para mantener actualizadas las normas y garantizar la protección de los derechos fundamentales en el entorno digital (Barrio Andrés, 2021).

Ante la insuficiencia de las respuestas nacionales aisladas, la comunidad internacional ha impulsado instrumentos jurídicos de cooperación y armonización normativa, el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001) constituye el principal tratado internacional en la

materia, orientado a la armonización legislativa, la facilitación de investigaciones transfronterizas y el fortalecimiento de la cooperación judicial. Más recientemente, la Convención de las Naciones Unidas contra la Ciberdelincuencia (UNODC, 2024) ha reforzado el compromiso global para enfrentar estos desafíos, promoviendo la adopción de mejores prácticas y el desarrollo de capacidades en los Estados miembros; paralelamente, la Unión Europea ha establecido marcos estratégicos como la Década Digital para 2030, que priorizan la ciberseguridad y la resiliencia digital como ejes fundamentales de la agenda comunitaria (Unión Europea, 2022).

A nivel nacional, España ha adaptado su legislación penal para tipificar y sancionar las nuevas formas de criminalidad digital, incorporando reformas recientes al Código Penal que abordan el acceso no autorizado, las brechas de datos y la difusión no consentida de imágenes íntimas, en consonancia con los estándares internacionales y las exigencias del Convenio de Budapest (BOE, 2026); sin embargo, persisten importantes desafíos en materia de recursos, formación y cooperación interinstitucional, como lo refleja el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT, 2024), donde solo 46 países han alcanzado el nivel más alto de madurez, y la media global se sitúa en 65,7 sobre 100 puntos.

En este contexto, la presente tesis se propone analizar la evolución del derecho en la era digital, con especial atención a los retos y oportunidades que plantean los delitos cibernéticos, el objetivo es examinar críticamente la adecuación de los marcos normativos actuales, identificar las principales lagunas y proponer líneas de acción para una modernización jurídica efectiva.

Para ello, se abordarán, en primer lugar, los fundamentos teóricos y sociológicos de la transformación digital y su impacto en el derecho; en segundo término, se analizarán las tipologías y tendencias del cibercrimen, así como las respuestas legales a nivel internacional y nacional; finalmente, se evaluarán las oportunidades que ofrece la digitalización para la innovación normativa, la protección de los derechos digitales y el fortalecimiento de la cooperación global. De este modo, se aspira a contribuir al debate académico y jurídico sobre la construcción de un derecho adaptado a los desafíos de la sociedad digital, capaz de garantizar la seguridad, la justicia y la protección de los derechos fundamentales en el ciberespacio.

CAPITULO I.- Planificación del Trabajo de Suficiencia Profesional

1.1. Título y descripción del trabajo

Título del Trabajo

La presente investigación la he denominado: La evolución del derecho en la era digital: Retos y oportunidades frente a los delitos cibernéticos.

1.2. Objetivo del presente trabajo

La presente investigación tiene como propósito principal analizar la transformación del derecho en el contexto de la era digital, con un enfoque particular en los retos y oportunidades que surgen frente a los delitos cibernéticos, este objetivo general se desglosa en una serie de metas específicas que buscan abordar las múltiples dimensiones de este fenómeno desde una perspectiva jurídica, tecnológica y social.

Objetivo general

Explorar y evaluar la evolución del derecho en la era digital, identificando los desafíos que plantea la ciberdelincuencia y proponiendo soluciones normativas y estratégicas que permitan una respuesta jurídica eficaz, respetuosa de los derechos fundamentales y adaptada a las dinámicas del ciberespacio.

Objetivos específicos

1. **Analizar el impacto de la digitalización en el derecho tradicional**

   Examinar cómo las tecnologías de la información y la comunicación (TIC) han transformado los principios y fundamentos del derecho, especialmente en el ámbito penal, y cómo estas transformaciones han dado lugar a nuevas categorías jurídicas, como los derechos digitales y los bienes jurídicos protegidos en el ciberespacio.

2. **Identificar las principales tipologías de delitos cibernéticos y sus características distintivas**

   Estudiar las conductas delictivas más prevalentes en el entorno digital, como el acceso ilícito, el fraude cibernético, el ransomware, el phishing y la difusión no consentida de datos personales, analizando su impacto social, económico y jurídico.

3. **Evaluar la adecuación de los marcos normativos actuales frente a los delitos cibernéticos**

   Realizar un análisis crítico de las legislaciones nacionales e internacionales vigentes, como el Convenio de Budapest, para determinar su eficacia en la prevención, persecución y sanción de los

ciberdelitos, así como su capacidad para adaptarse a las nuevas amenazas tecnológicas.

4. **Explorar las oportunidades que ofrece la digitalización para la innovación jurídica**

   Investigar cómo las herramientas digitales, como la inteligencia artificial y el big data, pueden ser utilizadas para mejorar la administración de justicia, optimizar los procesos de investigación y fortalecer la cooperación internacional en la lucha contra el cibercrimen.

5. **Proponer estrategias para la modernización del derecho frente a los desafíos del ciberespacio**

   Diseñar recomendaciones normativas y políticas públicas que permitan una respuesta jurídica más ágil y efectiva frente a los delitos cibernéticos, garantizando al mismo tiempo la protección de los derechos humanos en el entorno digital.

6. **Fomentar la cooperación internacional en la lucha contra el cibercrimen**

   Analizar los mecanismos de colaboración entre Estados, organizaciones internacionales y actores privados para enfrentar la naturaleza transnacional de los delitos cibernéticos, destacando la importancia de la armonización legislativa y la creación de redes globales de ciberseguridad.

7. **Contribuir al debate académico sobre el derecho en la era digital**
   Generar un marco teórico y práctico que sirva como referencia para futuras investigaciones en el ámbito del derecho digital, promoviendo una comprensión más profunda de los retos y oportunidades que plantea la ciberdelincuencia en el siglo XXI.

Justificación de los objetivos

La elección de estos objetivos responde a la necesidad de abordar un fenómeno complejo y en constante evolución, como es la ciberdelincuencia, desde una perspectiva integral. La investigación no solo busca identificar las limitaciones de los marcos normativos actuales, sino también explorar las oportunidades que ofrece la digitalización para transformar el derecho en una herramienta más eficaz, inclusiva y adaptada a las necesidades de la sociedad contemporánea. Al hacerlo, se pretende contribuir al desarrollo de un derecho que no solo reacciona ante los desafíos del ciberespacio, sino que también anticipa y previene las amenazas futuras, garantizando la seguridad, la justicia y la protección de los derechos fundamentales en el entorno digital.

1.3. Justificación

La transformación digital ha revolucionado el campo jurídico, exigiendo nuevas perspectivas teóricas, prácticas, legales, metodológicas y epistemológicas para comprender y enfrentar los delitos cibernéticos; esta tesis se justifica ampliamente por la magnitud del fenómeno, la complejidad de los desafíos regulatorios y la necesidad de enfoques

interdisciplinarios y comparados, sustentados en autores y marcos reconocidos internacionalmente.

1. Justificación teórica

La evolución del derecho en la era digital requiere una profunda revisión de los marcos teóricos tradicionales. Lawrence Lessig (1999, 2006) sostiene que, en el ciberespacio, el código informático actúa como una forma de regulación tan poderosa como la ley misma, lo que implica que las normas jurídicas deben dialogar con las arquitecturas tecnológicas para ser efectivas.

Manuel Castells (2001) introduce la teoría de la sociedad roja, explicando cómo las infraestructuras digitales transforman las relaciones sociales, económicas y legales, y generan nuevas formas de criminalidad y control; David Wall (2007) argumenta que el cibercrimen representa una transformación radical del delito, que exige marcos criminológicos y jurídicos innovadores; Susan Brenner (2010) profundiza en los desafíos legales que plantea la ciberdelincuencia, como la jurisdicción, la obtención de pruebas y la adaptación de los sistemas penales; Yochai Benkler (2000) destaca la importancia de los bienes comunes digitales y la necesidad de modelos regulatorios que reconozcan la participación activa de los usuarios.

Estas perspectivas teóricas fundamentan la necesidad de repensar el derecho en la era digital, considerando la interacción entre tecnología, sociedad y normatividad.

2. Justificación práctica

El impacto práctico de los delitos cibernéticos es innegable y creciente, según la UNODC (2025), el cibercrimen genera pérdidas económicas comparables al PIB de las grandes economías, con costos que se duplican cada pocos años; en 2023, el FBI registró solo en Estados Unidos 2.825 denuncias de ransomware (un aumento del 18% respecto a 2022) y pérdidas por 59,6 millones de dólares (un 74% más que el año anterior)

INTERPOL advierte que en África, los informes de estafa aumentarán hasta un 3.000% en algunos países en 2024; los delitos más frecuentes incluyen ransomware, phishing, fraude en línea, explotación infantil y violaciones de datos. La sofisticación de los ataques, impulsada por inteligencia artificial y automatización, y la naturaleza transnacional de los delitos, dificultan la persecución y la cooperación internacional; estos datos evidencian la urgencia de adaptar el derecho para proteger a individuos, empresas y Estados, y aprovechar las oportunidades que ofrece la digitalización para la prevención y persecución eficaz del delito.

3. Justificación legal

El marco jurídico internacional y nacional enfrenta el reto de mantenerse actualizado frente a la rápida evolución tecnológica, el Convenio de Budapest sobre Ciberdelincuencia (2001) es el principal tratado internacional que armoniza las legislaciones y promueve la cooperación en la investigación y persecución de delitos informáticos.

Su Segundo Protocolo Adicional (2022) refuerza la cooperación transfronteriza y el acceso a pruebas electrónicas; la Convención de las Naciones Unidas contra la Ciberdelincuencia (2024) representa el primer tratado global que busca fortalecer la respuesta internacional, en la Unión Europea, la Directiva 2013/40/UE armoniza los delitos y sanciones relacionadas con ataques a sistemas de información, mientras que el Reglamento General de Protección de Datos (RGPD) establece obligaciones estrictas en materia de seguridad y notificación de brechas

A nivel nacional, leyes como la Computer Fraud and Abuse Act (EE. UU.) y normativas latinoamericanas reflejan la tendencia a tipificar nuevos delitos y fortalecer la ciberseguridad; sin embargo, autores como Marco Gercke (2014) y Stein Schjolberg (2021) advierten sobre la fragmentación y los vacíos legales, subrayando la necesidad de reformas y armonización.

Así, la justificación legal radica en la urgencia de actualizar y coordinar los marcos normativos para responder eficazmente a los desafíos del cibercrimen.

4. Justificación metodológica

El estudio del derecho digital y la ciberdelincuencia exige enfoques metodológicos flexibles e interdisciplinarios. John W. Creswell (2013) defiende la integración de métodos cualitativos, cuantitativos y mixtos para captar la complejidad del fenómeno; Reza Banakar y Max Travers (2005) proponen la combinación de métodos doctrinales (análisis de normas y jurisprudencia) con enfoques sociojurídicos (entrevistas,

estudios de caso, análisis de discurso) para comprender el impacto social y normativo de la tecnología; Mark Van Hoecke (2024) destaca la importancia de la metodología comparada para identificar buenas prácticas y oportunidades de armonización entre jurisdicciones.

En América Latina, Alfonso Ortega Giménez (2014) y estudios empíricos regionales subrayan la necesidad de adaptar los métodos a los contextos locales y la diversidad normativa; así, la investigación metodológica en derecho digital debe ser plural, integrando análisis doctrinal, comparado y empírico, para ofrecer respuestas pertinentes y contextualizadas.

5. Justificación epistemológica

Desde el punto de vista epistemológico, la investigación sobre la evolución del derecho en la era digital se apoya en marcos críticos y constructivistas, la teoría crítica del derecho, representada por autores como Roberto Mangabeira Unger (1983) y Duncan Kennedy (1997), cuestiona la neutralidad de la ley y analiza cómo las normas pueden perpetuar o desafiar estructuras de poder, lo que resulta esencial para examinar los sesgos y desigualdades que pueden reproducirse en la regulación digital.

Los estudios sociojurídicos, impulsados por Banakar y Travers (2005), abogan por una visión contextualizada del derecho, considerando la interacción entre normas, tecnología y sociedad; los enfoques de Science and Technology Studies (CTS) y el constructivismo, con autores

como Langdon Winner y Andrew Feenberg, sostienen que la tecnología y el derecho se co-construyen, y que las respuestas jurídicas deben adaptarse a los cambios sociales y técnicos.

El pluralismo jurídico y la comparación internacional, inspirados en Benda-Beckmann y Van Hoecke, permiten analizar la coexistencia de múltiples órdenes normativos en el ciberespacio; estos marcos epistemológicos legitiman una aproximación crítica, interdisciplinaria y dinámica al estudio del derecho digital y la ciberdelincuencia.

CAPITULO II.- Marco Teórico

2.1. Evolución histórica del derecho frente a la tecnología. -

El punto de partida de la reflexión jurídica sobre la tecnología se sitúa en la obra de Norbert Wiener, quien en “Cibernética o el control y comunicación en animales y máquinas” (1949) anticipó la influencia de los sistemas automáticos y la comunicación digital en la sociedad y el derecho (Wiener, 1949); Wiener planteó la necesidad de repensar los marcos normativos ante la irrupción de máquinas capaces de procesar información y tomar decisiones, sentando así las bases de la cibernética jurídica.

En la década de 1960, surgió la informática jurídica, entendida como la aplicación de la informática al derecho para optimizar el acceso, gestión y análisis de la información legal (CarlosAudaz.com, 2026); Mario Losano, desde la Universidad de Bolonia, acuñó el término “iuscibernética” para referirse al estudio de la interacción entre derecho y sistemas automáticos, y fundó uno de los primeros centros de investigación en la

materia (La Escuela y los Juicios, 2026), en esta etapa, la preocupación principal era el almacenamiento y recuperación de datos jurídicos, pero pronto surgieron inquietudes sobre la protección de datos personales y el uso indebido de la información.

El avance de la tecnología informática y la creciente digitalización de la información impulsaron la promulgación de las primeras leyes específicas sobre protección de datos personales; Francia fue pionera con la Ley Nº 78-17 de 1978, que estableció principios fundamentales para la protección de la privacidad frente al tratamiento automatizado de datos (ADR Formación, 2025), en Estados Unidos, la Privacy Act de 1974 y la Data Protection Act de 1978 sentaron las bases para legislaciones posteriores en todo el mundo (CarlosAudaz.com, 2026).

Durante este periodo, varios países europeos, como Suecia, Alemania, Noruega, Austria y Dinamarca, desarrollaron instrumentos legislativos para proteger a los individuos frente al mal uso de su información mediante tecnologías informáticas (ADR Formación, 2025), estas normativas sentaron las bases para la futura armonización internacional en materia de protección de datos.

La masificación de las computadoras personales y la interconexión de sistemas trajo consigo nuevas formas de criminalidad, en 1986, Estados Unidos promulgó la Computer Fraud and Abuse Act (CFAA), la primera ley específica sobre delitos informáticos, que tipificó el acceso no autorizado a sistemas protegidos y otras conductas ilícitas en el entorno digital (ADR Formación, 2025), en el Reino Unido, la Computer Misuse

Act de 1990 abordó delitos como el hacking y el sabotaje informático (CarlosAudaz.com, 2026).

En Alemania, se reconoció por primera vez el delito de sabotaje informático con la condena de un hacker que provocó daños significativos a una empresa mediante un programa malicioso (La Escuela y los Juicios, 2026), estos hitos legislativos marcaron el inicio de la criminalización específica de conductas informáticas y sentaron precedentes para la regulación penal en otros países.

La expansión de Internet en los años noventa revolucionó la investigación jurídica y la práctica jurídica, dando lugar a la necesidad de nuevos marcos regulatorios y teóricos; Lawrence Lessig, en su influyente obra “Code and Other Laws of Cyberspace” (1999), argumentó que el “código es ley”, es decir, que la arquitectura técnica de Internet regula el comportamiento tanto como las leyes tradicionales (Lessig, 1999), Lessig propuso que el ciberespacio requería nuevas formas de regulación y planteó debates sobre la jurisdicción y el control estatal en entornos digitales.

Por su parte, Manuel Castells, en “La galaxia Internet” (2001), analizó cómo la tecnología digital estaba configurando una nueva civilización y subrayó la necesidad de establecer marcos de protección para los derechos fundamentales en entornos digitales (Castells, 2001); en el ámbito normativo, la Unión Europea aprobó la Directiva 95/46/CE sobre protección de datos personales, estableciendo principios comunes para el tratamiento de datos en los Estados miembros y consolidando la

protección de la privacidad como un derecho fundamental en la era digital (ADR Formación, 2025).

El siglo XXI ha estado marcado por la internacionalización y armonización de los marcos legales frente a los delitos cibernéticos, el Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001, fue el primer tratado internacional vinculante en la materia, estableciendo estándares para la tipificación de delitos informáticos, la cooperación internacional y la protección de derechos humanos (Consejo de Europa, 2001). El Protocolo Adicional de 2006 amplió el alcance del Convenio para incluir la criminalización de la difusión de material racista y xenófobo (Consejo de Europa, 2006).

En el ámbito europeo, la Directiva 2013/40/EU armonizó las disposiciones penales sobre ataques a sistemas de información, mientras que la Directiva NIS2 (2022) y el Reglamento General de Protección de Datos (GDPR, 2016/2018) fortalecieron la ciberseguridad y la protección de datos en la región (Unión Europea, 2013; Unión Europea, 2022; Unión Europea, 2016).

A nivel global, la adopción de la Convención de las Naciones Unidas sobre Ciberdelincuencia en 2024 representa un hito reciente, orientada a fortalecer la cooperación internacional, armonizar la criminalización de conductas y facilitar la obtención de pruebas electrónicas (UNODC, 2024); sin embargo, autores como Brenner (2006) y Wall (2007) han advertido sobre los riesgos de una regulación excesivamente amplia y la necesidad de salvaguardas para los derechos fundamentales.

En América Latina, la evolución normativa ha sido heterogénea pero progresiva. Chile fue pionero con la Ley N° 19.223 de 1993, que tipificó los delitos informáticos, y posteriormente con la Ley 21.459 de 2022, que actualizó la normativa conforme al Convenio de Budapest (Ley N° 19.223, 1993; Ley 21.459, 2022); México inició reformas en 1996 y 1999, incorporando delitos informáticos en su Código Penal Federal, aunque aún enfrenta desafíos para alcanzar los estándares internacionales (Salt, 2012).

Colombia promulgó la Ley 1273 de 2009, creando el bien jurídico de la protección de la información y los datos, y posicionándose como referente regional (Ley 1273, 2009); Argentina sancionó la Ley 26.388 en 2008, reformando el Código Penal para tipificar delitos informáticos y avanzar hacia la armonización legislativa (Ley 26.388, 2008); Perú, con la Ley 30096 de 2013, y otros países como Ecuador y Venezuela, han desarrollado marcos penales específicos, aunque con distintos grados de actualización y sistematicidad.

La Organización de los Estados Americanos (OEA) ha promovido la cooperación regional, la adopción de estándares comunes y la capacitación de operadores jurídicos, aunque la implementación efectiva varía según el país (OEA, sf).

La evolución del derecho frente a la tecnología continúa enfrentando retos significativos; la actualización constante ante nuevas modalidades delictivas (como el ransomware, la inteligencia artificial y la suplantación de identidad), la armonización regional e internacional, y el equilibrio entre

seguridad y derechos fundamentales; autores como Gercke (2012) y Brenner (2006) subrayan la importancia de los marcos flexibles, la cooperación internacional y salvaguardas efectivas para los derechos humanos en la lucha contra la ciberdelincuencia.

La historia del derecho frente a la tecnología es la historia de la adaptación, la innovación y la cooperación; desde la cibernética de Wiener hasta los tratados internacionales del siglo XXI, el derecho ha debido reinventarse para proteger a la sociedad en la era digital, enfrentando retos inéditos y aprovechando oportunidades para fortalecer la justicia y la seguridad global.

2.2 Teorías y enfoques jurídicos sobre los delitos cibernéticos. –

1. Teorías Jurídicas Fundamentales sobre los Delitos Cibernéticos

1.1. El "Código como Ley" (Lawrence Lessig, 1999, 2006)

Lawrence Lessig revolucionó la comprensión del derecho en el entorno digital al proponer que el código informático el software y la arquitectura de Internet actúa como un regulador tan poderoso como la misma ley, en su obra *Code and Other Laws of Cyberspace* (1999) y su versión ampliada *Code 2.0* (2006), Lessig sostiene que la conducta en el ciberespacio está determinada por cuatro reguladores: la ley, las normas sociales, el mercado y la arquitectura (el código), en el entorno digital, el código puede limitar o habilitar conductas, incluso por encima de la ley tradicional, desplazando el equilibrio de derechos y libertades, su célebre frase "el código es ley" sintetiza la idea de que el diseño de sistemas y

plataformas puede condicionar la libertad, la privacidad y la seguridad de los usuarios, planteando retos regulatorios inéditos para el derecho.

1.2. El Cibercrimen como Nueva Forma de Criminalidad (Susan Brenner, 2006, 2010)

Susan Brenner conceptualiza el cibercrimen como una categoría emergente que desafía los marcos jurídicos convencionales; en *Cybercrime: Criminal Threats from Cyberspace* (2006), Brenner argumenta que los delitos cibernéticos presentan características únicas deslocalización, anonimato, velocidad que dificultan su persecución y sanción bajo los esquemas legales tradicionales, proponer la necesidad de adaptar las definiciones y respuestas jurídicas, enfatizando la urgencia de enfoques transnacionales y adaptativos para enfrentar la criminalidad digital.

1.3. Transformación del Crimen en la Era Digital (David Wall, 2007)

David Wall, en *Cybercrime: The Transformation of Crime in the Information Age* (2007), analiza cómo la digitalización ha modificado la naturaleza del crimen, Wall distingue entre delitos informáticos puros (como el hacking), delitos tradicionales facilitados por la tecnología (fraude en línea) y delitos híbridos, su enfoque destaca la importancia de respuestas jurídicas flexibles y multidisciplinarias, capaces de adaptarse a la evolución constante de las amenazas digitales.

1.4. Jurisdicción y Soberanía en el Ciberespacio (Jack Goldsmith y Tim Wu, 2006)

¿Quién controla Internet? (2006), Goldsmith y Wu abordan el problema de la jurisdicción en el ciberespacio, cuestionando la idea de un Internet sin regulación estatal, argumentan que los Estados nación mantienen y ejercen su soberanía sobre el ciberespacio mediante la aplicación de sus leyes nacionales y la cooperación internacional, proponen un modelo híbrido donde coexisten la autorregulación y la regulación estatal, reconociendo la pluralidad de fuentes normativas en el entorno digital.

1.5. Autorregulación versus Regulación Estatal

El debate entre autorregulación y regulación estatal es central en la gobernanza del ciberespacio, mientras la autorregulación implica que los propios actores tecnológicos establecen normas de conducta, la regulación estatal supone la intervención de los poderes públicos mediante leyes y políticas específicas, la tendencia doctrinal actual apunta hacia modelos híbridos, donde la autorregulación se complementa con la supervisión estatal para garantizar la protección de derechos y la eficacia en la lucha contra el cibercrimen.

2. Teorías Criminológicas y Enfoques Jurídico-Penales

2.1. Teoría de las Actividades Rutinarias (Teoría de las actividades rutinarias, Cohen y Felson, 1979; Grabosky, 2001; Choi, 2008)

La Teoría de las Actividades Rutinarias (RAT), desarrollada por Cohen y Felson (1979) y aplicada al cibercrimen por Grabosky (2001) y Choi (2008), sostiene que la ocurrencia de un delito depende de la convergencia de un delincuente motivado, un objetivo adecuado y la ausencia de un guardián eficaz, en el ciberespacio, se adaptan estos elementos: el ciberdelincuente,

la víctima vulnerable y los mecanismos de protección digital (antivirus, firewalls), esta teoría ha sido fundamental para explicar la victimización en línea y orientar estrategias preventivas centradas en la conducta de la víctima y la protección tecnológica.

2.2. Teoría de la transición espacial (K. Jaishankar, 2007, 2008)

K. Jaishankar propuso la Teoría de la Transición Espacial, que sostiene que el comportamiento delictivo puede variar al transitar entre el espacio físico y el ciberespacio, el anonimato, la desinhibición y la ausencia de controles sociales tradicionales en el entorno digital facilitan la comisión de delitos que no se cometen en el mundo físico, esta teoría explica por qué personas sin antecedentes delictivos pueden involucrarse en ciberdelitos y subraya la necesidad de enfoques legales adaptados a la naturaleza única del ciberespacio.

2.3. Teorías del Bien Jurídico Protegido (Morón Lerma, 2002; Romeo Casabona, 2006)

Morón Lerma (2002) y Romeo Casabona (2006) abordan la identificación y protección de los bienes jurídicos afectados por los delitos informáticos; sostienen que los bienes jurídicos tradicionales patrimonio, privacidad, integridad de datos adquieren nuevas dimensiones en el ciberespacio y requieren una protección penal específica, la correcta identificación del bien jurídico protegido es esencial para la elaboración de tipos penales claros y eficaces frente a los delitos informáticos.

2.4. Derecho Penal del Enemigo en el Ciberespacio (Günther Jakobs, 2003)

La teoría del Derecho Penal del Enemigo, desarrollada por Jakobs (2003), justifica respuestas penales más severas y preventivas frente a sujetos que representan una amenaza grave y permanente, como los cibercriminales organizados, en el ciberespacio, esta teoría ha influido en la formulación de políticas criminales y en la cooperación internacional contra el cibercrimen organizado, aunque plantea dilemas sobre la proporcionalidad y los límites del derecho penal en la era digital.

2.5. Enfoques de Ulrich Sieber sobre Derecho Penal Internacional y Cibercrimen (1992 y posteriores)

Ulrich Sieber ha sido pionero en el análisis del cibercrimen desde una perspectiva internacional, subrayando la necesidad de cooperación transfronteriza y armonización legislativa para enfrentar delitos que trascienden fronteras nacionales, sus aportes han sido fundamentales para el desarrollo de políticas globales y la promoción de instrumentos internacionales como el Convenio de Budapest.

2.6. Perspectivas Latinoamericanas (Salt, 2012; Téllez Valdés, 2009)

Salt (2012) y Téllez Valdés (2009) analizan el cibercrimen desde la perspectiva latinoamericana, destacando desafíos como la falta de armonización legislativa, la escasa capacitación de operadores jurídicos y la necesidad de políticas públicas integrales, estos enfoques han impulsado reformas legislativas y estrategias nacionales de ciberseguridad en la región.

3. Enfoques Jurídicos Internacionales y de Derechos Humanos

3.1. El Convenio de Budapest (Consejo de Europa, 2001)

El Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, es el principal instrumento internacional en la materia, adoptado en 2001, su objetivo es armonizar las legislaciones nacionales, fortalecer la cooperación internacional y establecer mecanismos procesales eficaces para la investigación y persecución de delitos informáticos, ha sido ratificado por más de 78 países y ha servido de modelo para reformas legislativas en diversas regiones.

3.2. Convención Internacional de la ONU/UNODC sobre Ciberdelincuencia (2024)

La nueva convención global de la ONU, aprobada en 2024, establece obligaciones para la tipificación de delitos informáticos en los ordenamientos internos, siguiendo criterios similares a los del Convenio de Budapest, incorpora salvaguardias de derechos humanos y prevé mecanismos de cooperación y asistencia técnica, especialmente para países en desarrollo.

3.3. Cooperación Internacional y Jurisdicción Universal (Marco Gercke, 2012; Klimburg, 2017)

Marco Gercke (2012) sostiene que la cooperación internacional debe materializarse en tratados multilaterales y mecanismos ágiles de asistencia legal mutua, superando la lentitud de los sistemas tradicionales; Klimburg (2017) argumenta que la jurisdicción universal en materia de cibercrimen enfrenta límites prácticos y políticos, por lo que la alternativa viable es la armonización penal y la cooperación judicial internacional.

3.4. Enfoque de Derechos Humanos: Privacidad y Libertad de Expresión

El combate al cibercrimen plantea desafíos para los derechos humanos, especialmente la privacidad y la libertad de expresión, diversos informes de la ONU y organizaciones como Human Rights Watch advierten sobre el riesgo de que leyes de ciberseguridad se utilicen para restringir indebidamente derechos fundamentales, el enfoque basado en derechos humanos exige que las medidas contra el cibercrimen sean proporcionales, necesarias y sujetas a control judicial.

3.5. Ciberseguridad como Bien Público Global (Domínguez Bascoy, 2014)

La teoría de la ciberseguridad como bien público global sostiene que la protección del ciberespacio beneficia a toda la comunidad internacional y requiere la cooperación de Estados, sector privado y sociedad civil, la cooperación internacional, el intercambio de información y la adopción de estándares comunes son elementos clave para garantizar la seguridad y la confianza en el ciberespacio.

3.6. Perspectivas doctrinales: Giovanni Ziccardi (2013) y Marco Gercke

Giovanni Ziccardi (2013) destaca la necesidad de un marco regulatorio internacional específico para los delitos informáticos, señalando que el derecho penal tradicional resulta insuficiente ante la complejidad y transnacionalidad del cibercrimen; Marco Gercke subraya la importancia de

la cooperación internacional, la adaptación constante de los marcos legales y el equilibrio entre seguridad y derechos humanos.

Las teorías y enfoques jurídicos sobre los delitos cibernéticos reflejan la complejidad y dinamismo del entorno digital, desde la regulación a través del código, la adaptación de teorías criminológicas, la protección de bienes jurídicos emergentes, hasta la cooperación internacional y la integración de los derechos humanos, el derecho enfrenta el reto de evolucionar para responder a los desafíos y oportunidades de la era digital, la tendencia actual apunta hacia modelos híbridos, adaptativos y colaborativos, que reconozcan la pluralidad de actores y la necesidad de cooperación global.

CAPITULO III.- Desarrollo de actividades programadas

3.1. Tipología de los delitos cibernéticos. –

La clasificación de los delitos cibernéticos constituye uno de los mayores retos para el derecho penal contemporáneo, la naturaleza transnacional, la velocidad de evolución tecnológica y la multiplicidad de conductas ilícitas dificultan la construcción de una tipología única y estable (Wall, 2007); además, la convergencia entre delitos tradicionales y nuevas formas de criminalidad digital exige marcos flexibles y tecnológicamente neutros (Gercke, 2012), por ello, la doctrina y los instrumentos internacionales han desarrollado diversos grados, que se analizan a continuación.

David S. Wall (2007): Cuatro grandes categorías

Wall (2007) propone una de las tipologías más influyentes, distinguiendo entre:

- **Cyber-trespass:** Acceso no autorizado a sistemas y redes (hacking, malware).

- **Cyber-deception/theft:** Fraudes, robo de identidad y phishing.
- **Cyber-pornography/obscenity:** Distribución de contenidos ilegales u obscenos.
- **Cyber-violence:** Ciberacoso, amenazas y violencia digital.

Esta clasificación destaca por su claridad y por vincularse a categorías jurídicas tradicionales, facilitando su aplicación práctica (Wall, 2007).

Susan W. Brenner (2006, 2010): Rol del ordenador en el delito

Brenner (2010) clasifica los delitos cibernéticos según el papel del ordenador:

- **Como objetivo:** Ataques directos a sistemas (hacking, DDoS).
- **Como herramienta:** Fraudes, acoso, distribución de contenido ilegal.
- **Como incidental:** El ordenador es accesorio en la comisión del delito.

Este enfoque es útil para determinar estrategias de investigación y aplicación normativa (Brenner, 2010).

Marco Gercke (2012): Clasificación internacional armonizada

Gercke (2012) propone una tipología alineada con los tratados internacionales:

- **Delitos contra la confidencialidad, integridad y disponibilidad de datos/sistemas.**
- **Delitos informáticos patrimoniales.**
- **Delitos de contenido.**
- **Delitos contra la propiedad intelectual.**

Su objetivo es facilitar la armonización legislativa y la cooperación internacional (Gercke, 2012).

Ulrich Sieber (2008+): Dimensión tecnológica y jurídica

Sieber distingue entre:

- **Delitos de integridad informática.**
- **Delitos asistidos por ordenador.**
- **Delitos de contenido.**

Su enfoque resalta la interacción entre tecnología y derecho penal.

La tipología del Convenio de Budapest (Consejo de Europa, 2001) y su influencia normativa global

El Convenio de Budapest (2001) es el primer tratado internacional que sistematiza los delitos cibernéticos en cuatro grandes grupos:

1. **Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas** (arts. 2-6): acceso ilícito, interceptación, interferencia en datos y sistemas, abuso de dispositivos.
2. **Delitos informáticos patrimoniales** (arts. 7-8): falsificación y fraude informático.
3. **Delitos de contenido** (art. 9): pornografía infantil.
4. **Delitos contra la propiedad intelectual** (art. 10).

   Esta estructura ha sido adoptada por numerosas legislaciones nacionales y tratados posteriores (Consejo de Europa, 2001).

Categorías específicas desarrolladas en profundidad

a) Delitos contra la confidencialidad, integridad y disponibilidad de sistemas e información

Incluyen hacking, malware, ataques DDoS y ransomware; según ENISA (2024), el ransomware representó el 70% de los ciberataques globales en 2023, con pérdidas superiores a 1.100 millones de dólares, los ataques DDoS han escalado en frecuencia y sofisticación, afectando especialmente al sector público y transporte (ENISA, 2024). Kaspersky (2024) reporta un incremento del 20% en ataques de ransomware a sistemas industriales y un crecimiento exponencial de troyanos bancarios en móviles, estos delitos suelen estar tipificados como atentados contra la seguridad de la información y la infraestructura crítica, con agravantes cuando afectan servicios esenciales o datos sensibles (Gercke, 2012).

b) Delitos económicos cibernéticos

Engloban phishing, carding, fraude informático, fraude con criptomonedas y robo de identidad, el phishing es el vector dominante, representando el 60% de los accesos iniciales en incidentes reportados en la UE en 2024 (ENISA, 2024), el fraude con criptomonedas generó pérdidas globales de hasta 37 mil millones de dólares en Asia Oriental y Sudeste Asiático en 2023 (UNODC, 2024), el robo de identidad y el carding se han visto facilitados por brechas masivas de datos y plataformas en la dark web (Anderson et al., 2019).

c) Delitos cibernéticos contra las personas

Incluyen cyberbullying, cyberstalking, Grooming, sexting no consentido y difusión de imágenes íntimas sin consentimiento (revenge porn/NCII); Hinduja y Patchin (2009, 2021) destacan la prevalencia del ciberbullying entre jóvenes y su impacto psicológico; Bocij (2004) define el ciberacoso

como la persecución reiterada mediante medios electrónicos, con graves consecuencias psicológicas; el Grooming y la difusión no consentida de imágenes íntimas han aumentado con el uso de redes sociales y mensajería instantánea (Consejo de Europa, 2024).

d) Ciberterrorismo y ciberespionaje

El ciberterrorismo implica el uso de tecnologías digitales para causar terror o desestabilización social, política o económica (Denning, 2001; Rid, 2013); el ciberespionaje se refiere a la obtención ilícita de información confidencial, generalmente por actores estatales o grupos organizados. ENISA (2024) identifica a los actores estatales y “hacker-for-hire” como principales responsables de campañas de espionaje digital.

Marcos normativos internacionales y regionales

a) Convención de la ONU contra la Ciberdelincuencia (UNODC, 2024)

La Convención de la ONU (2024) amplía la tipología del Convenio de Budapest, incorporando delitos como la difusión no consentida de imágenes íntimas y el grooming (arts. 6-17), introduce la responsabilidad penal de personas jurídicas y adapta la normativa a los desafíos contemporáneos (UNODC, 2024).

b) Directiva 2013/40/UE

Armoniza la tipificación penal en la UE respecto a ataques contra sistemas de información: acceso ilícito, interferencia en sistemas y datos, interceptación ilícita y producción de herramientas para cometer estos delitos (arts. 3-8) (Parlamento Europeo, 2013).

c) Estrategia Interamericana OEA/CICTE

La OEA promueve una estrategia que reconoce delitos contra la confidencialidad, integridad y disponibilidad de datos, delitos patrimoniales, delitos de contenido y delitos contra la privacidad e identidad, destaca la necesidad de cooperación regional y actualización legislativa (OEA, 2004).

d) Informes EUROPOL IOCTA 2024 e INTERPOL 2024-2026

Europol (2024) identifica tres grandes categorías: ciberataques (ransomware, DDoS, malware), explotación sexual infantil en línea y fraudes económicos (phishing, fraude de pagos, BEC). INTERPOL (2026) resalta el crecimiento del ransomware, delitos financieros y crímenes facilitados por IA (INTERPOL, 2026).

Doctrina hispanoparlante

Romeo Casabona (2006)

Distinguir entre delitos informáticos en sentido estricto (acceso ilícito, sabotaje, manipulación de datos) y en sentido amplio (fraude, amenazas, delitos contra la intimidad) (Romeo Casabona, 2006).

Morón Lerma (2002)

Clasificación en delitos contra la confidencialidad, integridad y disponibilidad de datos, delitos patrimoniales, delitos contra la privacidad y delitos de contenido (Morón Lerma, 2002).

Miró Llinares (2012)

Propone una tipología funcional: delitos contra sistemas y datos, delitos patrimoniales, delitos de contenido y delitos contra la intimidad e identidad (Miró Llinares, 2012).

Perspectiva latinoamericana

Téllez Valdés (2009) y Salt (2012) subrayan la necesidad de adaptar los marcos legales a la realidad tecnológica y social de América Latina, donde el ransomware y el fraude electrónico son especialmente prevalentes, la OEA/CICTE (2024) destaca la urgencia de armonizar legislaciones y fortalecer las capacidades técnicas y judiciales.

La tipología de los delitos cibernéticos es dinámica y multifacética, a abarcar desde ataques a infraestructuras críticas hasta conductas que lesionan derechos individuales, la convergencia doctrinal e internacional apunta a cuatro grandes categorías: delitos contra sistemas y datos, delitos patrimoniales, delitos de contenido y delitos contra la intimidad e identidad. La respuesta jurídica y técnica debe ser versátil, adaptándose a la evolución constante de las amenazas y considerando las particularidades regionales y globales.

3.2 Impacto de los delitos cibernéticos en los derechos fundamentales. –

La digitalización global ha propiciado una revolución en la forma en que las personas interactúan, acceden a la información y ejercen sus derechos. Sin embargo, este avance ha traído consigo la proliferación de delitos cibernéticos que afectan de manera directa y transversal a los derechos fundamentales, el cibercrimen, entendido como toda conducta ilícita cometida a través de medios digitales, plantea retos complejos para los sistemas jurídicos, que deben equilibrar la protección de la seguridad y el orden público con la salvaguarda de libertades esenciales (Miró

Llinares, 2012; Romeo Casabona, 2006); la magnitud y sofisticación de estas amenazas exigen una reflexión profunda sobre la evolución del derecho en la era digital y la necesidad de adaptar los marcos normativos a los nuevos riesgos y oportunidades.

El derecho a la privacidad y la protección de datos personales se ha visto gravemente amenazado por delitos como el hacking, las brechas de datos, el robo de identidad, el phishing, el stalking y la vigilancia digital; estas conductas vulneran la confidencialidad, la autonomía y la autodeterminación informativa de los individuos (Solove, 2007; Nissenbaum, 2004).

Solove (2023) advierte que los marcos legales tradicionales resultan insuficientes ante la complejidad de los riesgos digitales, mientras que Nissenbaum (2009) introduce el concepto de "integridad contextual" para subrayar la importancia de los flujos apropiados de información en cada contexto social.

La explotación masiva de datos personales por parte de plataformas digitales, fenómeno que Zuboff (2019) denomina "capitalismo de la vigilancia", ha erosionado la capacidad de los individuos para controlar el destino de su información. Bygrave (2014) destaca los desafíos de la protección transfronteriza de datos, y Lessig (2006) señala que el propio diseño del código digital puede limitar o expandir la privacidad.

A nivel normativo, instrumentos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Privacidad del Consumidor de California (CCPA) han establecido estándares

globales para la protección de datos, reconociendo derechos como el acceso, la rectificación, la portabilidad y el "derecho al olvido" (Parlamento Europeo y Consejo de la UE, 2016; Usercentrics, 2025), las resoluciones del Consejo de Derechos Humanos de la ONU han reafirmado la privacidad como derecho humano fundamental en la era digital (United Nations Human Rights Council, 2024).

Las estadísticas recientes evidencian la magnitud del problema: en 2024, el FBI reportó más de 859.000 denuncias de cibercrimen solo en Estados Unidos, con pérdidas superiores a 16 mil millones de dólares, y brechas como la de Ticketmaster afectarán a 560 millones de usuarios a nivel global (Mohsin, 2024). Estos hechos demuestran la urgente necesidad de fortalecer la protección de la autodeterminación informativa (Lissens, 2024).

Los delitos cibernéticos también afectan gravemente la libertad de expresión, la dignidad humana y la integridad personal, fenómenos como el ciberacoso, el discurso de odio, la difusión no consentida de imágenes íntimas (NCII), el hostigamiento en línea, los deepfakes y las campañas de desinformación generan efectos devastadores sobre las víctimas y el debate público (Citron, 2009; Waldron, 2010).

Waldron (2010) sostiene que el discurso de odio en línea erosiona la cohesión social y causa angustia y ansiedad en los grupos vulnerables, mientras que Citron (2014) y MacKinnon (2014) subrayan el impacto desproporcionado de estos delitos sobre mujeres y minorías, la proliferación de deepfakes y desinformación, además de dañar la

reputación y la autoestima de las víctimas, socava la confianza en la comunicación digital y en los procesos democráticos (Romero-Moreno, 2024).

El marco jurídico internacional, como la Convención Europea de Derechos Humanos (artículos 8 y 10), exige un equilibrio entre la protección de la privacidad y la dignidad y la salvaguarda de la libertad de expresión (Parlamento Europeo, 2021), el Digital Services Act de la UE impone obligaciones a las plataformas para mitigar riesgos como la desinformación y la violencia digital, aunque persisten debates sobre la proporcionalidad de las restricciones (Kuźnicka-Błaszkowska & Kostyuk, 2025).

El "derecho al olvido", reconocido por el Tribunal de Justicia de la Unión Europea, se ha convertido en un mecanismo esencial para que las víctimas de cibercrimen puedan recuperar el control sobre su identidad digital (Capital Markets Law Journal, 2024), los daños psicológicos y sociales derivados de estos delitos incluyen ansiedad, depresión, aislamiento y humillación pública, con efectos duraderos sobre la salud mental y la participación social (Journal of International Criminal Justice, 2024).

El cibercrimen representa una amenaza directa a la seguridad personal y pública, especialmente a través de ataques a infraestructuras críticas y el ciberterrorismo. Miró Llinares (2012) y Romeo Casabona (2006) advierten que la digitalización de servicios esenciales ha incrementado la vulnerabilidad de la sociedad ante ataques que pueden

paralizar sistemas de energía, agua o telecomunicaciones, poniendo en riesgo la vida y el bienestar de la población.

El ciberterrorismo utiliza el ciberespacio para causar daños masivos, infundir miedo y desestabilizar sociedades enteras (Pons Gamón, 2019). La OEA (2024) subraya la importancia de fortalecer los sistemas de prevención y respuesta ante amenazas cibernéticas, considerando la protección de infraestructuras críticas como un pilar de la seguridad pública contemporánea.

La investigación y persecución de los delitos cibernéticos plantea retos significativos al debido proceso y al derecho a un juicio justo, la obtención y preservación de pruebas digitales requiere marcos legales y técnicos específicos, ya que la evidencia puede estar distribuida globalmente y ser fácilmente alterada (Brenner & Koops, 2004), la cooperación internacional es indispensable, pero la diversidad normativa y la falta de armonización dificultan la persecución efectiva y pueden generar vacíos de protección (UNODC, 2018).

El uso de la vigilancia masiva y la interceptación de comunicaciones electrónicas, aunque útil para combatir el cibercrimen, plantea riesgos para la privacidad y la protección de datos personales, y puede derivar en prácticas incompatibles con los estándares internacionales de derechos humanos (Miró Llinares, 2012; Romeo Casabona, 2006; Téllez Valdés, 2009), el debate sobre el cifrado y el acceso de las autoridades a la información cifrada enfrenta el interés público de la seguridad con el derecho a la privacidad (Koops, 2010; Kerr, 2018).

El derecho a la igualdad y la no discriminación se ve amenazado en el entorno digital por la discriminación algorítmica y los ciberdelitos de odio; los sistemas de inteligencia artificial pueden reproducir o amplificar sesgos existentes, afectando de manera desproporcionada a grupos vulnerables (Miró Llinares, 2012; Romeo Casabona, 2006); además, delitos como el acoso y la difusión no consentida de imágenes afectan especialmente a mujeres, niñas y minorías, lo que ha llevado a la OEA y la CIDH a recomendar la tipificación específica de estas conductas y la adopción de medidas de protección reforzadas (OEA, 2024); la jurisprudencia europea, como el caso KU v. Finlandia de la Corte Europea de Derechos Humanos (2008), ha establecido la obligación positiva de los Estados de proteger a las víctimas de ciberdelitos discriminatorios y garantizar investigaciones efectivas.

El acceso a la justicia para las víctimas de cibercrimen en América Latina enfrenta obstáculos estructurales, como la falta de recursos, la escasa capacitación de operadores judiciales y la limitada cooperación internacional (Miró Llinares, 2012; Romeo Casabona, 2006; OEA, 2024): la recolección de pruebas digitales y la identificación de los responsables suelen ser complejas debido a la naturaleza transnacional y anónima de muchos delitos (Brenner & Koops, 2004), la victimización diferenciada por género y la criminalización de discursos en línea han generado preocupación por el uso excesivo del derecho penal y la posible afectación de derechos como la libertad de expresión y la privacidad (OEA, 2024); Téllez Valdés (2009) destaca la necesidad de adaptar los

sistemas judiciales a los desafíos tecnológicos y garantizar mecanismos efectivos de denuncia, protección y reparación.

La Corte Interamericana de Derechos Humanos ha reconocido la importancia de garantizar el acceso a la justicia y la protección de los derechos fundamentales en el entorno digital, especialmente para grupos en situación de vulnerabilidad (CIDH, 2013), la Corte Europea de Derechos Humanos, en casos como KU v. Finlandia, ha establecido la obligación positiva de los Estados de proteger a las víctimas de ciberdelitos y de garantizar la investigación efectiva. Instrumentos regionales como la Declaración sobre Seguridad de las Américas (OEA, 2003) y la Convención de las Naciones Unidas contra la Ciberdelincuencia (UNODC, 2024) insisten en la armonización de la lucha contra el cibercrimen con el respeto a los derechos humanos.

La evolución del derecho en la era digital exige una respuesta integral y multidisciplinaria frente a los delitos cibernéticos, la protección de los derechos fundamentales requiere no solo la actualización de los marcos normativos, sino también la cooperación internacional, la capacitación de los operadores jurídicos y la promoción de una cultura digital basada en el respeto a la dignidad, la privacidad y la igualdad, solo así será posible enfrentar los retos y aprovechar las oportunidades que plantea la revolución digital para la protección de los derechos humanos.

CAPITULO IV.- Resultados Obtenidos

1. Panorama empírico: Magnitud y tendencias de la ciberdelincuencia (2020–2025)

Durante el último quinquenio, los delitos cibernéticos han alcanzado niveles históricos tanto en frecuencia como en impacto económico y social, según el FBI Internet Crime Complaint Center (IC3), en 2025 se superó el millón de denuncias globales, con pérdidas económicas que ascendieron a $20.9 mil millones de dólares, lo que representa un incremento del 400% respecto a 2020, los delitos más prevalentes incluyen el phishing, el fraude de inversiones (especialmente con criptomonedas), la suplantación de identidad y el ransomware, siendo el fraude de inversiones el más costoso, con pérdidas de $8.65 mil en 2025.

Un fenómeno emergente es el uso de inteligencia artificial (IA) en la comisión de delitos, con más de 22.000 denuncias y pérdidas cercanas a $893 millones en 2025, la IA ha facilitado la creación de deepfakes, la clonación de voces y la automatización de ataques, elevando la sofisticación y el alcance de las

amenazas (FBI IC3, 2025), en América Latina y el Caribe, los informes de la OEA y el BID evidencian avances en la madurez de las capacidades de ciberseguridad, aunque persisten brechas en recursos, talento y coordinación intersectorial. La región ha fortalecido sus marcos legales, pero enfrenta desafíos en la persecución penal y la cooperación internacional, especialmente en la recolección y uso de evidencia electrónica transfronteriza.

2. Avances legislativos y normativos: Respuestas del derecho ante la ciberdelincuencia (2018–2025)

La respuesta jurídica a la expansión de los delitos cibernéticos ha sido dinámica y multifacética, marcada por la adopción de instrumentos internacionales, la actualización de marcos normativos y la consolidación de mecanismos de cooperación.

a) Instrumentos internacionales y regionales

- **Convención de las Naciones Unidas contra la Ciberdelincuencia (2024):**

  Este tratado global, conocido como la Convención de Hanói, establece un marco legal universal para la prevención, investigación y enjuiciamiento de delitos cibernéticos, así como para la cooperación internacional y la protección de derechos humanos, si bien representa un avance histórico, académicos como Koops (2025) advierten que su eficacia dependerá de la implementación nacional y de la existencia de salvaguardas efectivas para los derechos fundamentales.

- **Convenio de Budapest y su Segundo Protocolo Adicional (2022):** El Convenio de Budapest sigue siendo el estándar internacional para la armonización legislativa y la cooperación transfronteriza, el Segundo Protocolo Adicional facilita el acceso directo a pruebas electrónicas y refuerza la protección de la privacidad, aunque persisten desafíos en la armonización de estándares entre jurisdicciones (Brenner, 2023).
- **Regulaciones europeas (GDPR, NIS2, Digital Services Act):** El Reglamento General de Protección de Datos (GDPR) ha fortalecido la protección de datos personales y la imposición de sanciones por incumplimiento, mientras que la Directiva NIS2 y la Digital Services Act amplían la ciberseguridad y la responsabilidad de las plataformas digitales en la gestión de contenidos ilícitos (Miró Llinares, 2021; Romeo Casabona, 2024).
- **Reformas en América Latina y marcos OEA:** Países como Colombia, México, Argentina, Chile y Perú han reformado sus legislaciones para tipificar delitos informáticos y mejorar la cooperación internacional, siguiendo las recomendaciones de la OEA y los estándares del Convenio de Budapest (Brenner, 2022).

b) Evaluación académica

La doctrina coincide en que la eficacia de estos instrumentos depende de la adaptación nacional, la capacitación de operadores jurídicos y el equilibrio entre la persecución penal y la protección de derechos fundamentales (Miró Llinares, 2022; Romeo Casabona, 2024).

3. Jurisprudencia clave: Protección de derechos fundamentales en el entorno digital

La evolución del derecho en la era digital se ha visto reflejada en una jurisprudencia cada vez más sofisticada, que busca equilibrar la lucha contra la ciberdelincuencia con la salvaguarda de los derechos fundamentales.

a) Tribunal de Justicia de la Unión Europea (TJUE)

- **Schrems I y II:**

  El TJUE invalidó los acuerdos Safe Harbour y Privacy Shield, redefiniendo los estándares internacionales de transferencia de datos y reforzando la protección de la privacidad frente a la vigilancia estatal (TJUE, 2015, 2020).

- **Google Spain v. AEPD (derecho al olvido):**

  Reconoció el derecho de los ciudadanos a solicitar la eliminación de enlaces a información personal obsoleta, sentando las bases para el control de la huella digital.

b) Tribunal Europeo de Derechos Humanos (TEDH)

- **Podchasov v. Rusia (2024):**

  El TEDH determinó que debilitar la encriptación para permitir el acceso estatal a las comunicaciones viola el derecho a la vida privada, subrayando la importancia de la proporcionalidad y el control judicial.

- **Big Brother Watch v. Reino Unido:**

  Exigió salvaguardias estrictas y supervisión judicial efectiva en los regímenes de interceptación masiva de comunicaciones.

c) Corte Interamericana de Derechos Humanos (CIDH)

- **CAJAR vs. Colombia (2023):**

  Por primera vez, la CIDH reconoció el derecho autónomo a la autodeterminación informativa, imponiendo obligaciones estatales de reforma legislativa y creación de mecanismos ágiles para el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición).

d) Tendencias doctrinales

La doctrina destaca que la protección de la privacidad y la autodeterminación informativa son pilares para la democracia digital y la confianza ciudadana, aunque persisten riesgos de vigilancia masiva y falta de transparencia en el uso de tecnologías de vigilancia (González Fuster, 2019; De Hert & Papakonstantinou, 2021; Pérez Luño, 2022).

4. Retos y oportunidades: Hacia un derecho penal digital robusto y garantista

Los resultados obtenidos evidencian que, si bien se han logrado avances significativos en la consolidación de un derecho penal digital más robusto, persisten desafíos estructurales:

- **Retos:**
  - Fragmentación normativa y dificultades en la armonización internacional.
  - Limitaciones en la persecución penal y en la recolección/admisibilidad de evidencia electrónica.
  - Riesgos de sobrerregulación y vigilancia excesiva, con potenciales afectaciones a los derechos fundamentales.

- Brechas en recursos, talento y coordinación institucional, especialmente en América Latina.

- **Oportunidades:**
  - Fortalecimiento de la cooperación internacional y la asistencia técnica.
  - Desarrollo de tecnologías seguras (encriptación, IA responsable).
  - Creación de autoridades independientes de protección de datos y mecanismos ágiles de tutela judicial.
  - Promoción de una cultura de ciberseguridad y educación digital.

5. Síntesis visual de los resultados

Indicador	2020	2024	2025
Pérdidas globales por ciberdelito	4.200 millones de dólares	16.600 millones de dólares	20.900 millones de dólares
Denuncias globales (IC3)	DAKOTA DEL NORTE	859.532	1.008.597
Pérdidas por fraude de inversión	DAKOTA DEL NORTE	6.500 millones de dólares	8.650 millones de dólares
Pérdidas por BEC	DAKOTA DEL NORTE	2.770 millones de dólares	3.050 millones de dólares
Pérdidas por ransomware	DAKOTA DEL NORTE	12,47 millones de dólares	32,3 millones de dólares
Denuncias por IA-facilitada	DAKOTA DEL NORTE	DAKOTA DEL NORTE	22.000
Pérdidas por IA-facilitada	DAKOTA DEL NORTE	DAKOTA DEL NORTE	893 millones de dólares

La evolución del derecho en la era digital frente a los delitos cibernéticos ha sido vertiginosa y multifacética. Los avances legislativos, la consolidación de una jurisprudencia protectora de los derechos fundamentales y la creciente cooperación internacional constituyen logros notables. Sin embargo, la magnitud y complejidad de la ciberdelincuencia, sumadas a los desafíos tecnológicos y normativos, exigen respuestas jurídicas ágiles, coordinadas y garantistas. El futuro del derecho penal digital dependerá de la capacidad de los Estados y la comunidad internacional para armonizar la persecución eficaz de los delitos con la protección efectiva de los derechos humanos en el entorno digital.

CONCLUSIONES

1. Transformación del fenómeno delictivo y adaptación jurídica

La era digital ha redefinido el concepto y alcance de la criminalidad, dando lugar a nuevas formas de ciberdelincuencia que trascienden fronteras, desafían la territorialidad y exigen respuestas jurídicas ágiles y coordinadas, entre 2020 y 2025, se observa una sofisticación creciente de los delitos cibernéticos, impulsada por la proliferación de tecnologías como la inteligencia artificial, el internet de las cosas y la automatización de ataques, este contexto ha obligado al derecho penal y procesal a repensar sus categorías tradicionales, adaptando conceptos como la autoridad, la prueba y la jurisdicción a un entorno digital caracterizado por la volatilidad y la ubicuidad de la evidencia electrónica.

2. Avances y tensiones en el marco normativo internacional

El desarrollo normativo internacional ha sido dinámico, pero también conflictivo, el Convenio de Budapest (2001) se consolidó como el principal referente global, estableciendo estándares mínimos en materia de tipificación, cooperación y salvaguardas procesales, con un énfasis notable en la protección de derechos fundamentales; sin embargo, su alcance geográfico limitado y la exclusión de actores clave motivaron la negociación de la Convención de Hanói (2024), adoptada bajo el auspicio de Naciones Unidas.

A pesar de su ambición universalista con 76 signatarios a mayo de 2026, pero solo tres ratificaciones, la Convención de Hanói enfrenta críticas sustantivas; organizaciones de la sociedad civil y la academia advierten sobre la insuficiencia de salvaguardas en materia de derechos humanos, la ampliación de poderes estatales de vigilancia sin controles efectivos y el riesgo de facilitar

los abusos transfronterizos, especialmente en contextos autoritarios, además, el proceso de negociación, eminentemente estado céntrico y con escasa participación de actores no estatales, ha sido señalado como deficitario en transparencia y legitimidad, la lenta ratificación y los desafíos de implementación reflejan la complejidad de armonizar intereses soberanos, estándares de derechos y necesidades operativas en un entorno globalizado.

3. Jurisprudencia reciente: equilibrio entre seguridad y derechos fundamentales

La jurisprudencia de los tribunales regionales europeos y americanos entre 2023 y 2026 ha sido decisiva para delimitar los contornos de la protección de derechos en la era digital, el Tribunal Europeo de Derechos Humanos (TEDH) y el Tribunal de Justicia de la Unión Europea (TJUE) han reafirmado que la privacidad, la protección de datos y la libertad de expresión deben ser respetadas incluso frente a la amenaza de la ciberdelincuencia, destacan fallos que exigen que toda medida de vigilancia o acceso a datos esté sujeta a legalidad, necesidad, proporcionalidad y control judicial de efectivo.

En particular, el TEDH ha reconocido el cifrado como un derecho fundamental, rechazando la imposición de puertas traseras que debilitan la seguridad de las comunicaciones para todos los usuarios, el caso EncroChat y otros similares han puesto de relieve la importancia de la integridad de la prueba digital y el derecho de defensa, exigiendo transparencia en la obtención y manejo de evidencia electrónica, el TJUE, por su parte, ha profundizado en la responsabilidad de los controladores de datos y la necesidad de que las

restricciones a los derechos digitales sean justificadas y proporcionadas, especialmente en el contexto de investigaciones penales.

4. Recomendaciones doctrinales e institucionales: hacia una gobernanza adaptativa y garantista

La doctrina y los organismos internacionales coinciden en que el futuro del derecho penal digital exige una armonización normativa progresiva, capaz de superar la fragmentación actual y de establecer estándares comunes en tipificación, jurisdicción y salvaguardas procesales, se recomienda avanzar hacia marcos multilaterales que equilibren la cooperación internacional con la protección efectiva de los derechos humanos, evitando la instrumentalización de la lucha contra la ciberdelincuencia para multas represivas o de control social.

En América Latina, la prioridad es fortalecer capacidades institucionales, mediante asistencia técnica, formación especializada y el desarrollo de estándares regionales compatibles con los principios internacionales, la colaboración público-privada y la participación de la sociedad civil son esenciales para construir resiliencia y legitimidad en la respuesta a los delitos cibernéticos.

La irrupción de la inteligencia artificial plantea retos adicionales, tanto como vector de nuevas amenazas como herramienta para la investigación y prevención del delito. Se impone la necesidad de marcos regulatorios flexibles, basados en la gestión de riesgos, la transparencia algorítmica y la supervisión humana, que permitan aprovechar el potencial innovador de la IA sin sacrificar derechos fundamentales.

5. Síntesis final: oportunidades y desafíos para el derecho en la era digital

La evolución del derecho frente a los delitos cibernéticos es un proceso inacabado, marcado por la tensión entre la urgencia de respuestas eficaces y la obligación de preservar el Estado de derecho y las libertades fundamentales, las oportunidades radican en la posibilidad de construir una gobernanza digital más inclusiva, cooperativa y respetuosa de los derechos humanos, capaz de adaptarse a la velocidad del cambio tecnológico, los desafíos, en cambio, se concentran en la superación de la fragmentación normativa, la prevención de abusos estatales, la protección de la privacidad y la consolidación de capacidades institucionales, especialmente en contextos de desigualdad y vulnerabilidad.

El derecho en la era digital debe ser, ante todo, un derecho de garantías: flexible ante la innovación, firme en la protección de derechos y eficaz en la persecución de la ciberdelincuencia, solo así podrás responder a los retos del presente y aprovechar las oportunidades del futuro digital.

RECOMENDACIONES

1. Fortalecimiento de los marcos normativos internacionales y nacionales

La lucha contra los delitos cibernéticos requiere un marco normativo robusto, coherente y adaptado a las particularidades del entorno digital, es fundamental que los Estados trabajen en la armonización de sus legislaciones nacionales con estándares internacionales, como los establecidos en el Convenio de Budapest y otros instrumentos emergentes, como la Convención de Hanói; sin embargo, esta armonización debe ir acompañada de un enfoque garantista que respete los derechos fundamentales, como la privacidad, la libertad de expresión y el debido proceso.

- **Recomendación específica:** Los Estados deben priorizar la adopción de normativas que regulen el acceso a datos personales y la vigilancia digital, asegurando que estas prácticas estén sujetas a principios de legalidad, necesidad y proporcionalidad, tal como lo han señalado tribunales internacionales como el Tribunal Europeo de Derechos Humanos.

2. Desarrollo de capacidades institucionales y formación especializada

El combate a los delitos cibernéticos exige instituciones sólidas y personal capacitado en el manejo de tecnologías avanzadas, las agencias de seguridad, los fiscales y los jueces deben contar con formación especializada en ciberseguridad, inteligencia artificial y manejo de evidencia digital; además, es crucial que los Estados inviertan en infraestructura tecnológica que permita una respuesta eficaz y coordinada frente a las amenazas cibernéticas.

- **Recomendación específica:** Se deben establecer programas de formación continua para operadores jurídicos y fuerzas de seguridad, con énfasis en el manejo de evidencia digital y el respeto a los derechos humanos en el contexto de investigaciones cibernéticas.

3. Promoción de la cooperación internacional

Dado que los delitos cibernéticos trascienden fronteras, la cooperación internacional es esencial para su prevención, investigación y sanción, los Estados deben fortalecer los mecanismos de colaboración, como el intercambio de información, la asistencia judicial mutua y la creación de equipos conjuntos de investigación; sin embargo, esta cooperación debe estar regulada por acuerdos claros que respetan la soberanía de los Estados y los derechos fundamentales de las personas involucradas.

- **Recomendación específica:** Se recomienda la creación de plataformas digitales seguras para el intercambio de información entre Estados, con protocolos claros que garanticen la protección de datos personales y la transparencia en el uso de la información compartida.

4. Regulación de la inteligencia artificial y tecnologías emergentes

La inteligencia artificial (IA) y otras tecnologías emergentes, como el blockchain y el internet de las cosas, presentan tanto oportunidades como riesgos en el ámbito jurídico, por un lado, estas tecnologías pueden ser herramientas valiosas para la prevención y detección de delitos cibernéticos; por otro, su uso indebido puede generar nuevas formas de criminalidad y vulnerar derechos fundamentales.

- **Recomendación específica:** Los Estados deben adoptar marcos regulatorios específicos para la IA, como el Reglamento de Inteligencia Artificial de la Unión Europea, que establece principios de transparencia, supervisión humana y gestión de riesgos, además, es necesario fomentar la investigación sobre el impacto ético y jurídico de estas tecnologías.

5. Protección de los derechos fundamentales en el entorno digital

El derecho en la era digital debe garantizar que las medidas adoptadas para combatir los delitos cibernéticos no vulneren los derechos fundamentales de las personas, esto incluye la protección de la privacidad, el derecho al olvido, la libertad de expresión y el acceso a la justicia; en este sentido, es crucial que los Estados adopten políticas públicas y normativas que equilibren la seguridad con el respeto a los derechos humanos.

- **Recomendación específica:** Se debe garantizar que toda medida de vigilancia digital esté sujeta a control judicial efectivo y que las personas afectadas tengan acceso a mecanismos de reparación en caso de abusos.

6. Fomento de la colaboración público-privada

El sector privado desempeña un papel clave en la lucha contra los delitos cibernéticos, especialmente en lo que respeta a la protección de infraestructuras críticas, la detección de amenazas y el desarrollo de tecnologías de ciberseguridad, por ello, es fundamental que los Estados promuevan la colaboración entre el sector público y privado, estableciendo marcos claros de cooperación y responsabilidad compartida.

- **Recomendación específica:** Se recomienda la creación de alianzas estratégicas entre gobiernos, empresas tecnológicas y organizaciones de la sociedad civil para desarrollar soluciones innovadoras y fortalecer la resiliencia frente a los delitos cibernéticos.

7. Sensibilización y educación ciudadana

La prevención de los delitos cibernéticos no solo depende de las instituciones, sino también de la ciudadanía, es fundamental que las personas estén informadas sobre los riesgos del entorno digital y las medidas que pueden tomar para protegerse, esto incluye la promoción de buenas prácticas en el uso de tecnologías, la protección de datos personales y la denuncia de actividades sospechosas.

- **Recomendación específica:** Los Estados deben implementar campañas de sensibilización y programas educativos sobre ciberseguridad, dirigidos a diferentes grupos de la población, con especial atención a los niños, adolescentes y personas mayores.

8. Fomento de la investigación y la innovación jurídica

El derecho debe evolucionar al ritmo de los avances tecnológicos, lo que requiere una constante investigación y reflexión sobre los desafíos y oportunidades que plantea la era digital, las universidades, centros de investigación y organismos internacionales deben desempeñar un papel activo en este proceso, generando conocimiento y propuestas innovadoras para la regulación del entorno digital.

- **Recomendación específica:** Se recomienda la creación de observatorios interdisciplinarios sobre derecho y tecnología, que analicen las tendencias emergentes y propongan soluciones adaptadas a las necesidades del contexto global y local.

REFERENCIAS BIBLIOGRAFICAS

ADR Formación. (2025). Fundamentos del Derecho informático en la era digital. https://www.adrformacion.com/knowledge/administracion-publica/fundamentos_del_derecho_informatico_en_la_era_digital.html

AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Banakar, R., & Travers, M. (2005). Theory and Method in Socio-Legal Research. Hart Publishing. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1511112

Barrio Andrés, M. (2018). Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet. Madrid: Reus. https://ocw.uc3m.es/mod/page/view.php?id=6418

Barrio Andrés, M. (2021). Los derechos digitales: de la LOPDGDD a la Carta de Derechos Digitales de España

Benda-Beckmann, F. von. (2002). Legal Pluralism and Social Justice in Economic and Political Development. IDS Bulletin, 32(1), 46–56. https://bulletin.ids.ac.uk/index.php/idsbo/article/view/2367

Benkler, Y. (2000). From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access. Federal Communications Law Journal, 52(3), 561–579. https://www.repository.law.indiana.edu/fclj/vol52/iss3/2/

Bocij, P. (2004). Cyberstalking: Harassment in the Internet Age and How to Protect Your Family. Praeger.

Brenner, S. W. (2006). Cybercrime: Criminal Threats from Cyberspace. Praeger.

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger. https://www.researchgate.net/publication/266090469_Cybercrime_Criminal_Threats_from_Cyberspace

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger. https://www.abc-clio.com/products/a3122c/

Brenner, S., & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. UNODC Cybercrime Module 7. https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press. https://global.oup.com/academic/product/data-privacy-law-9780199675555

Capital Markets Law Journal. (2024). Deepfakes, financial stability, and EU regulation: navigating the risks of synthetic media. https://academic.oup.com/cmlj/article/21/2/kmag008/8644171

CarlosAudaz.com. (2026). Antecedentes Históricos del Derecho Informático: Evolución y Contexto Legal. https://carlosaudaz.com/antecedentes-historicos-del-derecho-informatico/

Castells, M. (2001). La galaxia Internet. https://revista.cortesgenerales.es/rcg/article/download/1572/1541/

Castells, M. (2001). La galaxia Internet: Reflexiones sobre Internet, empresa y sociedad. Madrid: Plaza & Janés. https://www.academia.edu/3709642/La_galaxia_Internet_Manuel_Castells

Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press. https://global.oup.com/academic/product/the-internet-galaxy-9780199255771

Choi, K. S. (2008). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis.

Citron, D. K. (2009). Cyber Civil Rights. Boston University Law Review, 89(1), 61–125. https://www.bu.edu/law/journals-archive/bulr/volume89n1/documents/CITRON.pdf

Comisión Interamericana de Derechos Humanos (CIDH). (2013). Verdad, justicia y reparación: Cuarto informe sobre la situación de los derechos humanos. https://www.oas.org/es/cidh/

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia (Convenio de Budapest). https://www.coe.int/es/web/cybercrime/the-budapest-convention

Consejo de Europa. (2001). Convention on Cybercrime (ETS No. 185). https://www.coe.int/en/web/cybercrime/the-budapest-convention-old

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest). https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Consejo de Europa. (s.f.). Resumen del Convenio de Budapest sobre delitos cibernéticos. [https://eur-lex.europa.eu/ES/legal-content/summarary/convention-on-cybercrime.html)

Corte Europea de Derechos Humanos (ECtHR). (2008). K.U. v. Finland. https://hudoc.echr.coe.int/eng?i=001-90029

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2006). Additional Protocol to the Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/second-additional-protocol

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications. https://scholar.google.com/scholar_lookup?title=Research+Design:+Qualitative,+Quantitative,+and+Mixed+Methods+Approaches&author=Creswell,+J.W.&publication_year=2013

Davara Rodríguez, M. A. (Coord.) (2020). Manual de Derecho Informático. Madrid: Reus. https://ocw.uc3m.es/mod/page/view.php?id=6418

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla & D. Ronfeldt (Eds.), Networks and Netwars. RAND.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors, 23(3), 1151. https://www.mdpi.com/1424-8220/23/3/1151

Domínguez Bascoy, J. (2014). La ciberseguridad: aspectos jurídicos internacionales. https://derinter-vitoria-gasteiz.eus/wp-content/uploads/2024/12/2014-Jeronimo-Dominguez-Bascoy.pdf

ENISA. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

España. (2026). Código Penal y legislación complementaria. https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=038_Codigo_Penal_y_legislacion_complementaria

European Parliament & Council of the EU. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament. (2021). The fight against disinformation and the right to freedom of expression. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf

European Union. (2013). Directive 2013/40/EU on attacks against information systems. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040

European Union. (2013). Directive 2013/40/EU on attacks against information systems. https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

European Union. (2016). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

European Union. (2016). General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en

Federal Bureau of Investigation (FBI). (2024). Internet Crime Report 2023. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

Gercke, M. (2009). International Harmonization of Cybercrime Legislation. https://www.coe.int/en/web/cybercrime/international-harmonisation

Gercke, M. (2012). 10 Years Convention on Cybercrime. In S. W. Brenner et al. (Eds.), Cybercrime and the Law. https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. https://www.coe.int/en/web/cybercrime/understanding-cybercrime

Gercke, M. (2014). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf

Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Oxford University Press. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-F-2007-10044100464

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies, 10(2), 243-249.

Hinduja, S., & Patchin, J. W. (2009). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Corwin Press.

Hinduja, S., & Patchin, J. W. (2021). Cyberbullying: Identification, Prevention, and Response. Cyberbullying Research Center.

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

https://biblioteca.mpf.gov.ar/meran/getDocument.pl?id=8217

https://laescuelaylosjuicios.com/antecedentes-del-derecho-informatico/

https://produccioncientificaluz.org/index.php/rcs/article/view/39981

https://produccioncientificaluz.org/index.php/rcs/article/view/39981

https://revistaius.com/index.php/ius/article/view/27

https://www.pensamientopenal.com.ar/system/files/2016/01/doctrina42792.pdf

https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002

https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Human Rights Watch. (2024). El Salvador: Nuevas leyes amenazan la libertad de expresión y la privacidad. https://www.hrw.org/es/news/2024/12/12/el-salvador-nuevas-leyes-amenazan-la-libertad-de-expresion-y-la-privacidad

Interpol. (2023). Cybercrime Analysis Reports. https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports

INTERPOL. (2025). New INTERPOL report warns of sharp rise in cybercrime in Africa. https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

INTERPOL. (2026). Asia and South Pacific Cyberthreat Assessment Report. https://www.interpol.int/en/News-and-Events/News/2026/New-INTERPOL-report-highlights-escalating-cyber-threats-across-Asia-and-South-Pacific

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5082409

Journal of International Criminal Justice. (2024). Is International Criminal Law Ready to Accommodate Online Harm? 22(1), 169–197. https://academic.oup.com/jicj/article/22/1/169/7667859

Kaspersky. (2024). Security Bulletin 2024.

Kennedy, D. (1997). A Critique of Adjudication. Harvard University Press. https://www.hup.harvard.edu/books/9780674177642

Kerr, O. (2018). The Law of Electronic Surveillance. https://scholarship.law.gwu.edu/faculty_publications/1432/

Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.

Koops, B.-J. (2010). The Crypto Controversy. https://pure.uvt.nl/ws/portalfiles/portal/1292952/Koops_Crypto_Controversy_2010.pdf

Kuźnicka-Błaszkowska, D., & Kostyuk, N. (2025). Emerging need to regulate deepfakes in international law: the Russo–Ukrainian war as an example. Journal of Cybersecurity, 11(1). https://doi.org/10.1093/cybsec/tyaf008

La Escuela y los Juicios. (2026). Antecedentes del derecho informático: evolución y conceptos clave.

Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books. https://en.wikipedia.org/wiki/Code_and_Other_Laws_of_Cyberspace

Lessig, L. (2006). Code: And Other Laws of Cyberspace, Version 2.0. Basic Books. https://en.wikipedia.org/wiki/Code_and_Other_Laws_of_Cyberspace

Lessig, L. (2006). Code: Version 2.0. Basic Books. https://codev2.cc/

Ley 1273 de 2009 (Colombia). (2009).

Ley 19.223 (Chile). (1993).

Ley 21.459 (Chile). (2022).

Ley 26.388 (Argentina). (2008).

Ley 30096 (Perú). (2013).

Lissens, S. (2024). The foundations of EU personal data protection law: Privacy and human dignity. Cyberpolitik Journal. http://cyberpolitikjournal.org/index.php/main/article/view/263

Media Defence. (2025). Cibercrímenes - Latinoamérica. https://www.mediadefence.org/resource-hub/cibercrimenes-latinoamerica/

Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Editorial Marcial Pons. https://www.infoem.org.mx/doc/biblioteca/accesoytrans/ciberdelitos/crimencibercrimen.pdf

Miró Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial

Pons. https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DP-2025-361

Miró Llinares, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. https://ddd.uab.cat/pub/tfg/2022/tfg_1911603/El_ciberderecho_como_disciplina_juridica.pdf

Miró Llinares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. IDP. Revista de Internet, Derecho y Política, (32), 1–17. https://idp.uoc.edu/articles/10.7238/idp.v0i32.397116/galley/397116/download/

Mohsin, K. (2024). Cybercrime and Privacy in the Digital Age: Legal Frameworks, Emerging Challenges, and Future Trends. SSRN. https://papers.ssrn.com/sol3/Delivery.cfm/5169894.pdf?abstractid=5169894&mirid=1

Morón Lerma, E. (2002). Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red. Editorial Aranzadi.

Morón Lerma, E. (2002). Nuevas tecnologías e instrumentos internacionales: Consecuencias penales.

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/2

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press. https://www.sup.org/books/title/?id=8862

ocw.uc3m.es/mod/page/view.php?id=6418] (https://ocw.uc3m.es/mod/page/view.php?id=6418)

OEA. (2004). Comprehensive Inter-American Cybersecurity Strategy. http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_i.asp

OEA. (s.f.). Ciberseguridad y cooperación regional.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). Convención internacional contra la ciberdelincuencia. https://www.unodc.org/unodc/es/cybercrime/convention/text/convention-full-text.html

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). Cibercrimen Programme. https://www.unodc.org/unodc/en/cybercrime/index.html

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). United Nations Convention against Cybercrime. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR). (2021). El derecho a la privacidad en la era digital: informe. https://www.ohchr.org/es/calls-for-input/2021/right-privacy-digital-age-report-2021

Organización de los Estados Americanos (OEA). (2024). Cibercrímenes en Latinoamérica. https://www.mediadefence.org/resource-hub/cibercrimenes-latinoamerica/

Ortega Giménez, A. (2014). Protección de datos y derecho digital en América Latina.
Dialnet. https://dialnet.unirioja.es/metricas/investigadores/3486091

Parlamento Europeo. (2013). Directive 2013/40/EU on attacks against information systems. https://www.europarl.europa.eu/doceo/document/B-7-2013-0386_EN.html?redirect

Pons Gamón, V. (2019). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad.

Quadra Salcedo, T., & Piñar Mañas, J. L. (Dirs.) (2018). Sociedad digital y Derecho. Madrid: Reus./ocw.uc3m.es/mod/page/view.php?id=6418](https://ocw.uc3m.es/mod/page/view.php?id=6418)

Rid, T. (2013). Cyber War Will Not Take Place. Oxford University Press.

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen. En C. M. Romeo Casabona (Coord.), El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Editorial Comares. https://dialnet.unirioja.es/servlet/articulo?codigo=5105395

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal. Editorial Comares.

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen. Comares. https://www.comares.com/media/comares/files/toc-149832.pdf

Romero-Moreno, F. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law, Computers & Technology, 38(2). https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540

Salt, J. (2012). Cibercrimen en América Latina: Retos y perspectivas.

Salt, J. (2012). Ciberdelitos en América Latina. OEA/CICTE.

Salt, M. (2012). Delitos informáticos: aspectos de Derecho Penal Internacional.

Schjolberg, S. (2021). Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them. University of York. https://www.york.ac.uk/media/law/documents/eventsandnewsdocs/2.%20Investigating%20Cybercrime_The%20Key%20Jurisdictional%20and%20Technical%20Challenges%20Faced%20by%20Law%20Enforcement%20and%20Ways%20to%20Address%20Them.pdf

Sieber, U. (1992). The International Emergence of Cybercrime.

Solove, D. J. (2007). The digital person: Technology and privacy in the information age. NYU Press. https://nyupress.org/9780814740377/the-digital-person/

Solove, D. J. (2023). The Limitations of Privacy Rights. Notre Dame Law Review, 98, 975–1002. https://scholarship.law.nd.edu/ndlr/vol98/iss3/2

Subijana Zunzunegui, J. I. (2019). El ciberterrorismo: una perspectiva legal y judicial.

Téllez Valdés, J. (2009). Delitos informáticos en América Latina. Editorial Porrúa.

Téllez Valdés, J. (2009). Derecho informático latinoamericano: Retos y perspectivas.

Téllez Valdés, J. (2009). Derecho informático. México: McGraw Hill. https://revistas-colaboracion.juridicas.unam.mx/index.php/judicatura/article/download/32202/29199

Unger, R. M. (1983). The Critical Legal Studies Movement. Harvard Law Review, 96(3), 561–675. https://www.jstor.org/stable/1340732

Unión Europea. (2022). Decisión (UE) 2022/2481 por la que se establece el programa estratégico de la Década Digital para 2030. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022D2481

Unión Internacional de Telecomunicaciones (ITU). (2024). Global Cybersecurity Index 2024. https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx

United Nations Human Rights Council. (2024). Privacy in the digital age (Resolutions 54/21, 55/3). https://www.ohchr.org/en/privacy-in-the-digital-age

United Nations Office on Drugs and Crime (UNODC). (2024). Cybercrime. https://www.unodc.org/unodc/en/cybercrime/index.html

United Nations Office on Drugs and Crime (UNODC). (2025). What to know about cybercrime in

2025. https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html

United Nations Office on Drugs and Crime. (2024). United Nations Convention against Cybercrime. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

UNODC. (2018). Cybercrime Module 7: Sovereignty and Jurisdiction. https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html

UNODC. (2024). United Nations Convention against Cybercrime.

UNODC. (2024). United Nations Convention against Cybercrime. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

Usercentrics. (2025). Global Data Privacy Laws: Your 2025 Guide (GDPR, CCPA, More). https://usercentrics.com/guides/data-privacy/data-privacy-laws/

Van Hoecke, M. (2024). Comparative Law and Legal Methodology. https://scholar.google.com/citations?user=h5MY380AAAAJ&hl=nl

Waldron, J. (2010). The Harm in Hate Speech. Harvard University Press. https://www.tandfonline.com/doi/full/10.1080/03906701.2022.2133406

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Prberkeley.edu/record/1180013?ln=en

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity.

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press. https://www.politybooks.com/bookdetail?book_slug=cybercrime--the-transformation-of-crime-in-the-information-age--second-edition--9780745639727

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Routledge.

Wiener, N. (1949). Cibernética o el control y comunicación en animales y máquinas. https://es.wikipedia.org/wiki/Cibern%C3%A9tica_(libro)

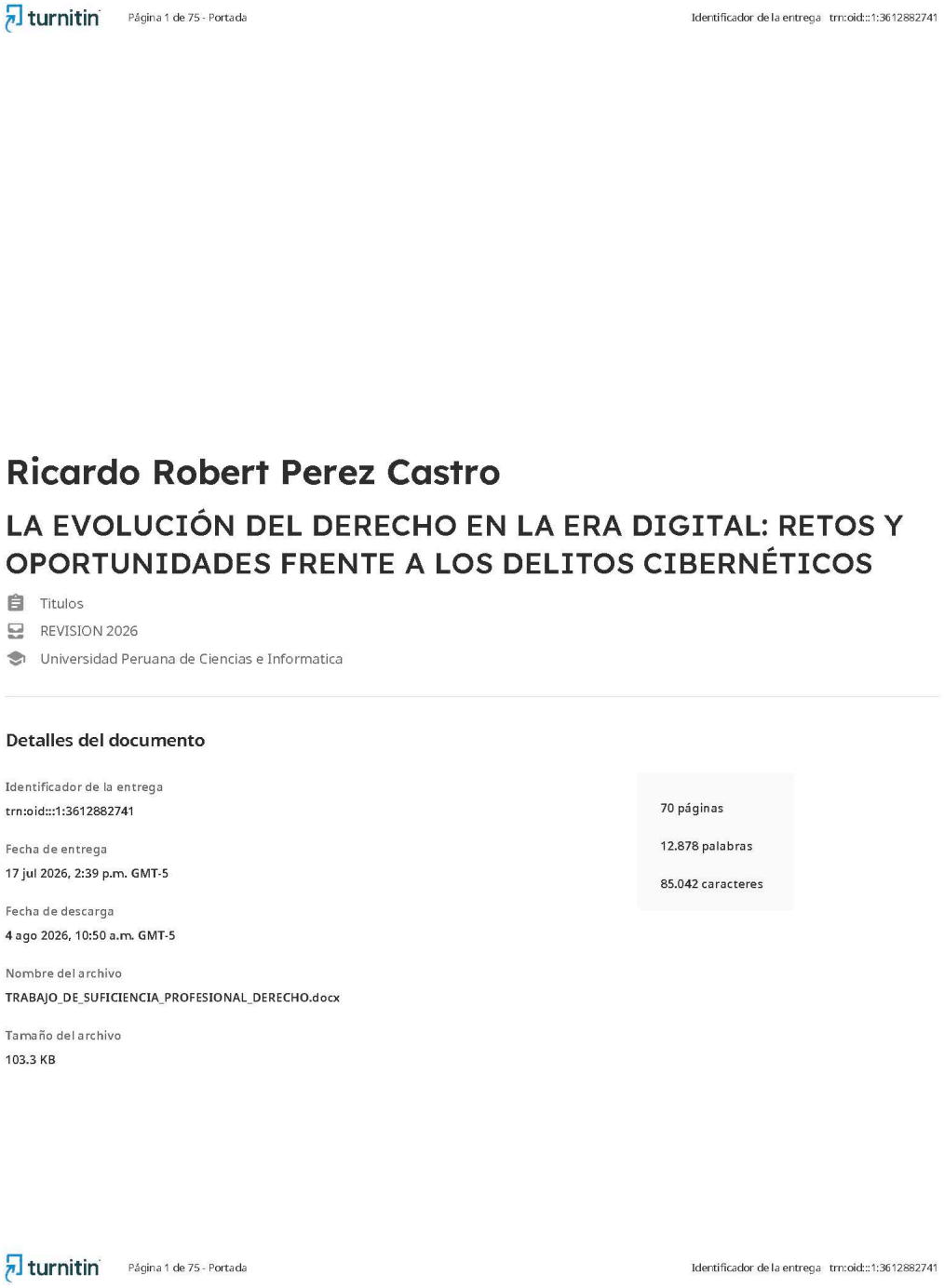
Winner, L. (1986). The Whale and the Reactor: A Search for Limits in an Age of High Technology. University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/W/bo3637992.html

Ziccardi, G. (2013). Il diritto dell'informatica. Giuffrè Editore.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs. https://www.pu781610395694/

ANEXOS

Anexo 1.- Evidencia de similitud digital



13% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

13% Fuentes de Internet
8% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

turnitin Página 2 de 75 - Descripción general de integridad Identificador de la entrega trn:oid::1:3612882741

Fuentes principales

13% Fuentes de Internet
8% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Internet	
repositorio.upci.edu.pe		3%
2	Trabajos del estudiante	
Universidad Peruana de Ciencias e Informatica		<1%
3	Publicación	
"Dinámicas socioambientales, legales y económicas en la triple frontera Madre d...		<1%
4	Trabajos del estudiante	
Universidad Internacional de la Rioja		<1%
5	Internet	
diposit.ub.edu		<1%
6	Trabajos del estudiante	
Universidad Europea de Madrid		<1%
7	Internet	
www.informatica-juridica.com		<1%
8	Trabajos del estudiante	
Integración Blackboard		<1%
9	Internet	
www.trendtic.cl		<1%
10	Internet	
repositorio.uia.ac.cr:8080		<1%
11	Trabajos del estudiante	
Universidad Mariano Gálvez de Guatemala		<1%

turnitin Página 3 de 75 - Descripción general de integridad Identificador de la entrega trn:oid::1:3612882741

12	Internet	
www.gobernacion.gob.mx		<1%
13	Publicación	
"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derech...		<1%
14	Internet	
www.scribd.com		<1%
15	Trabajos del estudiante	
Universidad Anahuac México Sur		<1%
16	Trabajos del estudiante	
Universidad Privada Antenor Orrego 2025		<1%
17	Internet	
dokumen.pub		<1%
18	Internet	
dspace.ceu.es		<1%
19	Internet	
repositorio.21.edu.ar		<1%
20	Internet	
themisdata.net		<1%
21	Publicación	
María Mercedes Barreno Salinas. "The Right to Privacy in the Digital Age", VISUAL...		<1%
22	Internet	
cdn.www.gob.pe		<1%
23	Internet	
dspaceapi.live.udesa.edu.ar		<1%
24	Internet	
www.dch.unne.edu.ar		<1%
25	Internet	
www.ismsforum.es		<1%

26	Trabajos del estudiante	
Pathfinder Enterprises		<1%
27	Internet	
fastercapital.com		<1%
28	Internet	
www.dykinson.com		<1%
29	Internet	
www.hrw.org		<1%
30	Internet	
derechoshumanos.mainel.org		<1%
31	Internet	
octaedro.com		<1%
32	Internet	
www.ucm.es		<1%
33	Trabajos del estudiante	
Blackboard		<1%
34	Publicación	
"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derech...		<1%
35	Trabajos del estudiante	
Corporación Universitaria Minuto de Dios,UNIMINUTO		<1%

turnitin Página 5 de 75 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3612882741

Anexo 2.- Autorización de publicación en repositorio

UPCI
Universidad Peruana de Ciencias e Informática

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: PEREZ CASTRO

DNI: 08419544 Correo electrónico: ricardoprpc@gmail.com

Domicilio: KIKIJANA 535-A

Teléfono fijo: _____ Teléfono celular: 960 972 276

2.- IDENTIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS

Facultad / Carrera: DERECHO Y CIENCIAS POLÍTICAS

Tipo: Trabajo de Suficiencia Profesional (X) Tesis ( )

Título del Trabajo de Suficiencia Profesional / Tesis:

La evolución del derecho en la era digital: Retos y oportunidades frente a los delitos cibernéticos.

3.- OBTENER:

Título Profesional (X)

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
(X) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 17 días del mes de Julio de 2026.

FIRMA

HUELLA