

DERECHO DIGITAL Y REGULACIÓN JURÍDICA

— • EN LA ERA TECNOLÓGICA • —



Andrés Fernando García Escobar



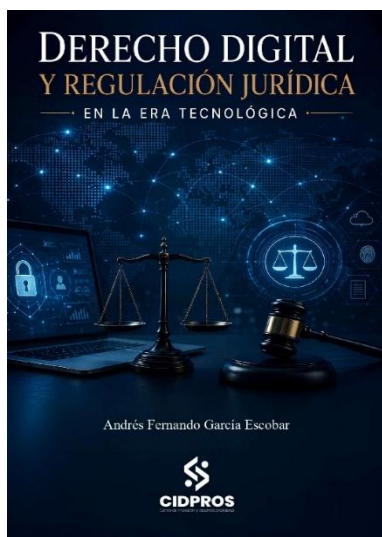
CIDPROS

Centro de innovación y desarrollo profesional

Derecho digital y regulación jurídica en la era tecnológica

Andrés Fernando García Escobar





Datos bibliográficos

ISBN	978-9907-9562-3-8
Título del libro	Derecho digital y regulación jurídica en la era tecnológica
Autores	Andrés Fernando García Escobar
Editorial	CIDPROS EDITORIAL
Materia	340 - Derecho
Público objetivo	Profesional / académico
Año	2026
Número de edición	1
Tamaño	1.79 Mb
Soporte	Libro digital descargable
Formato	PDF (.pdf)
Idioma	Español
DOI	https://doi.org/10.67166/pardn522
	Hecho en Ecuador / Made in Ecuador

MSc. Andrés Fernando García Escobar

Investigador Independiente

andresfernandogarciaescobar@hotmail.com

<https://orcid.org/0009-0006-6158-9754>

Guayaquil, Guayas, Ecuador.

Semblanza

Andrés Fernando García Escobar (Guayaquil, Ecuador, 29 de octubre de 1983) es un jurista, magistrado y académico ecuatoriano cuya trayectoria se ha distinguido por su firme compromiso con la justicia, la defensa de los derechos humanos y la consolidación del Estado Constitucional de Derechos y Justicia. Su vida profesional se ha orientado al estudio profundo del derecho y a la promoción de una cultura jurídica sustentada en los principios de dignidad humana, legalidad y respeto irrestricto a las garantías fundamentales.



En el ámbito jurisdiccional fue Juez de Familia, Mujer, Niñez y Adolescencia de Guayaquil por 12 años, actualmente se desempeña como Juez de lo Civil, Mercantil, Inquilinato y Relaciones Vecinales del cantón Guayaquil, provincia del Guayas. Desde esta alta responsabilidad pública ha contribuido al fortalecimiento de la administración de justicia, promoviendo una interpretación del derecho inspirada en los valores constitucionales, la seguridad jurídica y la tutela efectiva de los derechos de las personas.

Posee el grado académico de Magíster en Derechos Fundamentales y Justicia Constitucional, Magíster en Derechos Humanos con Mención en Sistemas Internacionales de Protección es Egresado de un Doctorado en Derecho de la Universidad Nacional de Mar del Plata Argentina y cursa una Maestría en Derecho con Mención en Derecho Procesal Penal, formación que ha consolidado su visión garantista del derecho y su permanente interés por el desarrollo del constitucionalismo contemporáneo. Paralelamente, ejerce la docencia universitaria en programas de pregrado y posgrado, donde comparte su experiencia como jurista y magistrado, contribuyendo a la formación de nuevas generaciones de profesionales comprometidos con la ética jurídica, la investigación y el servicio a la sociedad.

Como investigador jurídico ha desarrollado una significativa producción académica reflejada en diversos artículos científicos, entre los que destacan “Derechos de la Naturaleza en el Ecuador: Una vía para garantizar el Buen Vivir”, “Relevancia de las Garantías Constitucionales dentro del Derecho Penal Ecuatoriano: Una aproximación holística de la aplicación penal en el Ecuador” e “Importancia de las Garantías

Constitucionales del ordenamiento Jurídico Ecuatoriano en la protección de los derechos”. Sus aportes evidencian una visión integral del derecho y una profunda preocupación por la vigencia efectiva de las garantías constitucionales dentro del sistema jurídico ecuatoriano.

Por su destacada trayectoria profesional, académica y humana ha recibido importantes reconocimientos, entre ellos el Doctorado Honoris Causa otorgado por la Universidad de Artes y Oficios de México, la distinción de Hijo Ilustre de la Ciudad de Guayaquil concedida por la Junta Cívica de Guayaquil, Fue Declarado Destacado Líder Ecuatoriano por la UNESCO, Defensor de Derechos Humanos por diversas Organizaciones Sociales y posee diversos reconocimientos como Jurista del Año por el Colegio de Abogados del Guayas. Su figura se caracteriza por su vocación de servicio público, su integridad, responsabilidad y liderazgo, cualidades que lo proyectan como un defensor incansable de la justicia, la dignidad humana y el fortalecimiento del orden jurídico en el Ecuador.

AGRADECIMIENTO

A mi padre.

Abogado, cuya memoria inspira esta obra. Ejercicio el Derecho por ti y para honrar el camino que me mostraste. Tu tránsito por este mundo, complejo y humano conoció de ausencias y batallas, pero el amor de un hijo y la venia entre colegas dictan hoy un veredicto de paz sobre el pasado. En la culminación de este tratado, evoco tu recuerdo con profunda nostalgia y gratitud infinita. Gracias por la herencia de esta profesión, papá; este logro es compartido. Que la eternidad te conceda el orgullo de ver tu legado vivo en mis letras.

DEDICATORIA

A mis amadas hijas, Renata y Fernanda.

Dedico esta obra jurídica a sus vidas, con la firme convicción de que el derecho cobra verdadero sentido cuando busca asegurar un futuro de justicia, equidad y dignidad para las nuevas generaciones. Que el rigor científico, el esfuerzo y la disciplina plasmados en estas páginas les sirvan como testimonio vivo del valor inquebrantable del estudio constante y el compromiso con la verdad.

Ustedes son mi mayor orgullo, el motor de mi desarrollo personal y profesional, la razón última por la cual busco, a través de la ciencia del derecho; contribuir a la construcción de un orden social más justo y humano.



El contenido y las ideas expuestas en esta obra se encuentran protegidos por la normativa vigente en materia de propiedad intelectual y constituyen derechos exclusivos de su(s) autor(es).

Todos los derechos reservados © 2026

SINOPSIS

Derecho Digital y regulación jurídica en la era tecnológica es una obra académica que analiza los principales desafíos jurídicos surgidos a partir de la transformación digital y el acelerado avance de las tecnologías contemporáneas. El libro aborda de manera integral temas relacionados con la sociedad de la información, la protección de datos personales, la inteligencia artificial, la ciberseguridad, los delitos informáticos y la justicia digital, destacando la necesidad de adaptar los sistemas jurídicos frente a las nuevas dinámicas tecnológicas. A través de un enfoque crítico y actualizado, la obra examina el impacto de las tecnologías emergentes sobre los derechos fundamentales, la privacidad, la responsabilidad jurídica y la regulación de los entornos virtuales. Asimismo, estudia los mecanismos legales orientados a garantizar seguridad jurídica, transparencia y protección de los ciudadanos dentro del ciberespacio. Esta publicación constituye una herramienta de consulta para estudiantes, investigadores y profesionales interesados en comprender la relación entre Derecho y tecnología en la era digital.

Palabras clave: Derecho Digital, inteligencia artificial, ciberseguridad, delitos informáticos, justicia digital.

SYNOPSIS

Digital Law and Legal Regulation in the Technological Era is an academic work that analyzes the main legal challenges arising from digital transformation and the accelerated advancement of contemporary technologies. The book comprehensively addresses topics related to the information society, personal data protection, artificial intelligence, cybersecurity, cybercrime, and digital justice, highlighting the need to adapt legal systems to new technological dynamics. Through a critical and updated approach, the work examines the impact of emerging technologies on fundamental rights, privacy, legal liability, and the regulation of virtual environments. Likewise, it studies legal mechanisms aimed at guaranteeing legal certainty, transparency, and the protection of citizens within cyberspace. This publication serves as a reference tool for students, researchers, and professionals interested in understanding the relationship between law and technology in the digital era.

Keywords: Digital Law, Artificial Intelligence, Cybersecurity, Cybercrime, Digital Justice.

ÍNDICE

AGRADECIMIENTO	6
DEDICATORIA	7
SINOPSIS	9
SYNOPSIS	10
Introducción.....	13
CAPÍTULO 1 Fundamentos del Derecho Digital y sociedad tecnológica.....	15
1.1 Evolución histórica del Derecho Digital.....	16
1.2 Sociedad de la información y transformación tecnológica.....	19
1.3 Concepto, características y principios del Derecho Digital.....	22
1.4 Impacto de las tecnologías emergentes en el sistema jurídico.....	25
1.5 Derechos fundamentales en entornos digitales	28
1.6 Gobierno electrónico y administración pública digital.....	31
1.7 Retos éticos y jurídicos de la sociedad tecnológica	34
CAPÍTULO 2 Protección de datos personales y privacidad	37
2.1 Concepto y naturaleza jurídica de los datos personales	38
2.2 Principios de protección de datos y privacidad digital	40
2.3 Consentimiento informado y tratamiento de datos personales.....	43
2.4 Derechos ARCO y garantías de los titulares de datos	46
2.5 Regulación internacional y comparada sobre protección de datos.....	50
2.6 Protección de datos en redes sociales y plataformas digitales.....	52
2.7 Transferencia internacional de datos y almacenamiento en la nube	56
2.8 Responsabilidad jurídica por vulneración de datos personales	58
CAPÍTULO 3 Inteligencia artificial y responsabilidad jurídica.....	61
3.1 Concepto y clasificación de la inteligencia artificial.....	62
3.2 Inteligencia artificial y automatización de decisiones.....	64
3.3 Responsabilidad civil y penal derivada del uso de IA.....	67

3.4 Sesgos algorítmicos y discriminación tecnológica.....	71
3.5 Regulación jurídica de la inteligencia artificial en el derecho comparado.....	73
3.6 Desafíos éticos y jurídicos de la inteligencia artificial generativa	76
CAPÍTULO 4 Delitos informáticos y ciberseguridad	79
4.1 Conceptualización y evolución de los delitos informáticos	80
4.2 Tipología de ciberdelitos en entornos digitales	82
4.3 Fraude electrónico, phishing y suplantación de identidad.....	85
4.4 Acceso ilícito, hacking y vulneración de sistemas informáticos	87
4.5 Ciberseguridad y protección de infraestructuras digitales.....	90
4.6 Investigación y persecución penal de delitos informáticos	92
4.7 Cooperación internacional y normativa sobre ciberdelincuencia.....	94
CAPÍTULO 5 Prueba digital y justicia en entornos tecnológicos.....	98
5.1 Concepto y naturaleza jurídica de la prueba digital	99
5.2 Admisibilidad, autenticidad y valoración de la evidencia electrónica	101
5.3 Cadena de custodia en evidencias digitales	103
5.4 Firma electrónica, documentos digitales y validez jurídica	106
5.5 Uso de tecnologías digitales en procesos judiciales	108
5.6 Retos de la justicia digital y debido proceso en entornos tecnológicos.....	111
Bibliografía.....	114

Introducción

La transformación tecnológica de las últimas décadas ha modificado profundamente la manera en que las personas se comunican, trabajan, comercian y ejercen sus derechos dentro de la sociedad contemporánea. El desarrollo acelerado de internet, las plataformas digitales, la inteligencia artificial y los sistemas automatizados ha generado nuevas dinámicas sociales y económicas que trascienden las estructuras tradicionales del Derecho. En este contexto, el Derecho Digital surge como una disciplina jurídica indispensable para regular las relaciones desarrolladas en entornos tecnológicos y garantizar la protección de los derechos fundamentales frente a los desafíos de la era digital.

Actualmente, la digitalización de la información y la expansión de las tecnologías de la comunicación han provocado importantes cambios dentro de la administración pública, el comercio electrónico, la protección de datos personales y los sistemas de justicia. Asimismo, el crecimiento de los delitos informáticos, la vulneración de la privacidad y la utilización masiva de inteligencia artificial evidencian la necesidad de construir marcos regulatorios modernos capaces de responder eficazmente a los riesgos derivados del entorno digital. En consecuencia, los Estados y organismos internacionales enfrentan el reto permanente de equilibrar innovación tecnológica, seguridad jurídica y protección integral de los derechos humanos.

La presente obra, titulada *Derecho Digital y regulación jurídica en la era tecnológica*, tiene como finalidad analizar los principales desafíos jurídicos derivados de la transformación digital contemporánea, abordando de manera integral los fundamentos teóricos, normativos y prácticos del Derecho Digital. A lo largo de sus capítulos se examinan temas relacionados con la sociedad tecnológica, la protección de datos personales, la inteligencia artificial, la ciberseguridad, los delitos informáticos y la utilización de tecnologías digitales dentro de los procesos judiciales. Además, se incorporan reflexiones sobre los retos éticos y jurídicos que surgen frente a la automatización, la gobernanza digital y la protección de derechos fundamentales en entornos virtuales.

El primer capítulo desarrolla los fundamentos conceptuales del Derecho Digital y su relación con la evolución tecnológica y la sociedad de la información. Posteriormente, el segundo capítulo analiza la protección de datos personales y la privacidad digital,

considerando principios jurídicos, derechos ARCO y regulaciones nacionales e internacionales. El tercer capítulo aborda la inteligencia artificial y la responsabilidad jurídica derivada de su utilización, incluyendo aspectos relacionados con automatización, sesgos algorítmicos y regulación comparada. Por su parte, el cuarto capítulo estudia los delitos informáticos y la ciberseguridad como fenómenos centrales dentro de la criminalidad digital contemporánea. Finalmente, el quinto capítulo examina la prueba digital y la justicia tecnológica, destacando la importancia de la evidencia electrónica, la cadena de custodia y el debido proceso en los entornos judiciales digitales.

Esta obra busca contribuir al análisis académico y jurídico de los cambios producidos por la revolución tecnológica, ofreciendo una visión crítica y actualizada sobre los principales desafíos regulatorios de la sociedad digital. Asimismo, pretende servir como material de consulta para estudiantes, docentes, investigadores y profesionales del Derecho interesados en comprender el impacto de las tecnologías emergentes dentro del ordenamiento jurídico contemporáneo. En un mundo cada vez más interconectado y automatizado, resulta indispensable fortalecer el estudio del Derecho Digital como herramienta orientada a garantizar seguridad jurídica, transparencia y protección de los derechos fundamentales en la era tecnológica.



CAPÍTULO 1

**Fundamentos del Derecho Digital y
sociedad tecnológica**

1.1 Evolución histórica del Derecho Digital

El Derecho Digital nace como respuesta a los avances tecnológicos y comunicacionales que comenzaron a expandirse desde la segunda mitad del siglo XX. En un inicio, los sistemas jurídicos tradicionales no contaban con normas específicas para regular fenómenos relacionados con la informática y las telecomunicaciones, por lo que fue necesario adaptar principios del derecho civil, penal y comercial a los entornos electrónicos. Además, el crecimiento del uso de computadoras y sistemas automatizados impulsó la creación de regulaciones vinculadas con la protección de datos, la propiedad intelectual y la contratación electrónica. De esta manera, el desarrollo tecnológico empezó a transformar y modernizar las instituciones jurídicas contemporáneas. (Vargas, 2021; Mendoza et al., 2021).

Durante las décadas de 1980 y 1990, la expansión de Internet transformó significativamente el desarrollo del Derecho Digital, ya que las actividades sociales, económicas y comerciales comenzaron a ejecutarse en entornos virtuales. Esta realidad obligó a los Estados a fortalecer mecanismos jurídicos relacionados con delitos informáticos, comercio electrónico y seguridad de la información. De acuerdo con Cornejo (2023), la globalización digital impulsó la creación de normas internacionales orientadas a garantizar la protección jurídica de los usuarios en entornos virtuales. Asimismo, Arango (2024) sostiene que el surgimiento de la sociedad de la información transformó radicalmente la manera en que el derecho interpreta la territorialidad, la soberanía y la jurisdicción en contextos tecnológicos.

El avance acelerado de las tecnologías digitales permitió la consolidación de nuevas ramas jurídicas vinculadas con protección de datos personales, ciberseguridad y derechos digitales fundamentales. A medida que el intercambio de información electrónica se volvió cotidiano, aumentaron también los riesgos relacionados con vulneración de privacidad, fraude informático y acceso indebido a sistemas digitales. En consecuencia, los sistemas jurídicos comenzaron a incorporar legislaciones especializadas capaces de responder a estas nuevas amenazas tecnológicas. Miranda et al. (2025) indican que la evolución del Derecho Digital se encuentra estrechamente relacionada con la necesidad de equilibrar innovación tecnológica y protección de derechos humanos en entornos virtuales.

La evolución histórica del Derecho Digital también se vincula con el reconocimiento progresivo del acceso a Internet y a las tecnologías de la información como elementos esenciales para el ejercicio de derechos fundamentales. Diversos organismos internacionales comenzaron a considerar la conectividad digital como un componente indispensable para garantizar participación ciudadana, educación, libertad de expresión y acceso a la información. En este sentido, Ramírez (2025) afirma que la digitalización de la sociedad ha generado nuevas formas de ciudadanía digital que requieren protección jurídica especializada. Del mismo modo, Morón et al. (2025) señalan que los Estados contemporáneos enfrentan el desafío de adaptar constantemente sus sistemas normativos frente a la rápida evolución tecnológica global.

En América Latina, el desarrollo del Derecho Digital se fortaleció principalmente a partir de la expansión del comercio electrónico y la necesidad de regular la utilización de tecnologías en instituciones públicas y privadas. Los países latinoamericanos comenzaron a implementar leyes relacionadas con firma electrónica, protección de datos personales y delitos informáticos con el objetivo de fortalecer la seguridad jurídica en medios digitales. Según Ortiz et al. (2025), la modernización normativa en la región ha permitido consolidar mecanismos legales orientados a regular transacciones electrónicas y proteger derechos digitales emergentes. De igual forma, la transformación digital en América Latina exige marcos regulatorios dinámicos y adaptables frente a los cambios tecnológicos permanentes (Chuquicahua et al., 2025).

La aparición de tecnologías emergentes como inteligencia artificial, blockchain, big data y computación en la nube ha ampliado considerablemente el campo de acción del Derecho Digital en el siglo XXI. Estas innovaciones tecnológicas han generado debates jurídicos relacionados con responsabilidad algorítmica, automatización de decisiones y protección de datos masivos. En consecuencia, los sistemas jurídicos contemporáneos han debido desarrollar nuevos enfoques regulatorios para enfrentar desafíos asociados con ética digital y gobernanza tecnológica.

Gamboa et al. (2024) destacan que la evolución tecnológica actual exige la creación de regulaciones flexibles capaces de responder a escenarios digitales complejos y altamente cambiantes. Asimismo, Macías y Espinoza (2024) sostienen que el Derecho Digital se ha consolidado como una disciplina transversal que mantiene relación con diversas áreas del ordenamiento jurídico moderno, debido al impacto creciente de las tecnologías en las relaciones sociales, económicas y jurídicas.

El crecimiento de actividades ilícitas relacionadas con fraude electrónico, robo de identidad, acceso no autorizado a sistemas y ataques informáticos ha impulsado reformas penales especializadas en diversos países. Rafael y Anccasi (2026) manifiestan que la cibercriminalidad constituye uno de los principales retos jurídicos de la era tecnológica debido a la complejidad transnacional de los delitos digitales. De igual manera, Melgar et al. (2026) consideran que la cooperación internacional es un elemento fundamental para fortalecer los mecanismos de investigación, prevención y sanción de conductas ilícitas dentro de los entornos virtuales globalizados, debido a que los delitos digitales suelen superar las fronteras territoriales tradicionales y requieren respuestas jurídicas coordinadas entre distintos Estados.

En Ecuador, la evolución del Derecho Digital ha estado acompañada por reformas legales orientadas a incorporar mecanismos de regulación tecnológica y protección de derechos digitales. La Constitución de la República del Ecuador (2008) reconoce derechos vinculados con privacidad, protección de datos personales y acceso universal a tecnologías de la información. Además, la promulgación de leyes relacionadas con comercio electrónico, protección de datos personales y ciberseguridad refleja el interés estatal por modernizar el marco jurídico frente a los desafíos tecnológicos contemporáneos. Dueñas et al. (2025) señalan que el ordenamiento jurídico ecuatoriano ha experimentado avances significativos en materia digital, aunque aún existen vacíos regulatorios relacionados con inteligencia artificial y gobernanza de datos.

Para concluir, la evolución histórica del Derecho Digital evidencia que el derecho contemporáneo se encuentra en un proceso permanente de adaptación frente a la innovación tecnológica. La consolidación de sociedades digitalizadas ha generado nuevas dinámicas económicas, sociales y culturales que exigen respuestas jurídicas especializadas y multidisciplinarias. En la actualidad, el Derecho Digital no solo regula aspectos técnicos relacionados con Internet y sistemas informáticos, sino que también protege derechos fundamentales dentro de espacios virtuales cada vez más complejos. Corcino et al. (2026) sostienen que el futuro del Derecho Digital dependerá de la capacidad de los sistemas jurídicos para equilibrar innovación tecnológica, seguridad jurídica y protección integral de los derechos humanos en la era digital.

1.2 Sociedad de la información y transformación tecnológica

La sociedad de la información constituye una etapa histórica marcada por el uso masivo de tecnologías digitales para la creación, almacenamiento y transmisión de información a gran escala. Este modelo social se desarrolló como resultado de los avances tecnológicos impulsados por la revolución informática y la expansión mundial de Internet, los cuales transformaron profundamente la comunicación, la economía y las relaciones sociales contemporáneas (Lara y Romero, 2023).

En este contexto, la información adquiere un valor estratégico dentro de las dinámicas económicas, educativas, políticas y culturales contemporáneas. Según Vargas (2021), la transformación tecnológica ha modificado profundamente las formas tradicionales de interacción humana y organización social. Asimismo, Mendoza et al. (2021) sostienen que la digitalización ha generado nuevas estructuras sociales basadas en conectividad, automatización y acceso inmediato a la información.

La expansión de redes digitales permitió la creación de entornos virtuales capaces de conectar personas, instituciones y empresas en tiempo real a nivel global. Esta transformación tecnológica facilitó nuevas modalidades de trabajo, educación y comercio electrónico, modificando significativamente las relaciones sociales tradicionales. Cornejo (2023) afirma que la revolución digital ha generado una nueva lógica de interacción social sustentada en plataformas tecnológicas y sistemas de información automatizados. De igual manera, Arango (2024)) señala que la conectividad digital constituye uno de los principales motores de transformación de las sociedades contemporáneas.

La consolidación de la sociedad digital también ha impulsado importantes cambios en las estructuras económicas mundiales. Actualmente, los datos y la información se consideran recursos estratégicos capaces de generar innovación, competitividad y crecimiento económico. En consecuencia, múltiples sectores productivos han incorporado tecnologías emergentes como inteligencia artificial, big data y computación en la nube para optimizar procesos y aumentar eficiencia. Gamboa et al. (2024) indican que la transformación tecnológica ha provocado la aparición de economías digitales sustentadas en automatización y análisis masivo de datos. Asimismo, Macías y Espinoza (2024)) sostienen que la digitalización empresarial ha redefinido los modelos tradicionales de producción y prestación de servicios.

La expansión de la sociedad de la información también ha transformado profundamente los sistemas educativos y las dinámicas de acceso al conocimiento. Las plataformas virtuales, herramientas colaborativas y recursos digitales han permitido nuevas formas de enseñanza y aprendizaje dentro de entornos tecnológicos globalizados. En este escenario, la educación digital se ha convertido en un componente esencial para el desarrollo de competencias tecnológicas y ciudadanía digital. Ramírez (2025) manifiesta que la transformación tecnológica exige replantear los modelos pedagógicos tradicionales para responder a las necesidades de las nuevas generaciones. Del mismo modo, Miranda et al. (2025) consideran que las tecnologías educativas fortalecen procesos de inclusión y democratización del conocimiento.

No obstante, el avance de la sociedad de la información también ha generado riesgos relacionados con privacidad, protección de datos y vulneración de derechos digitales. La recopilación masiva de información personal por parte de plataformas digitales y sistemas tecnológicos ha incrementado preocupaciones jurídicas y éticas sobre el manejo de datos sensibles. En respuesta a esta problemática, diversos países han implementado regulaciones orientadas a proteger la información personal y garantizar seguridad digital.

El Reglamento General de Protección de Datos (2016) constituye uno de los principales instrumentos internacionales destinados a fortalecer la protección de datos personales dentro de entornos digitales. Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) en Ecuador incorpora mecanismos jurídicos destinados a garantizar el tratamiento adecuado de los datos personales y la protección de los derechos de los ciudadanos dentro del entorno tecnológico.

El crecimiento acelerado de las tecnologías digitales también ha favorecido el incremento de delitos informáticos y amenazas cibernéticas a nivel global. Actividades ilícitas como fraude electrónico, robo de identidad, acceso ilegal a sistemas y ataques informáticos representan desafíos importantes para los sistemas jurídicos contemporáneos. Rafael y Anccasi (2026) sostienen que la cibercriminalidad constituye una de las principales consecuencias negativas derivadas de la expansión tecnológica global.

En este contexto, la Convención sobre Ciberdelincuencia, Convenio de Budapest, (2001) se consolidó como uno de los primeros instrumentos internacionales destinados a fortalecer la cooperación jurídica frente a delitos informáticos. De igual manera, el

Código Orgánico Integral Penal (2014) tipifica infracciones relacionadas con sistemas informáticos y delitos tecnológicos en Ecuador.

La transformación tecnológica también ha generado nuevas discusiones sobre derechos digitales y acceso equitativo a las tecnologías de la información. El acceso a Internet y a herramientas digitales se considera actualmente un elemento esencial para el ejercicio de múltiples derechos fundamentales relacionados con educación, libertad de expresión y participación ciudadana. La Constitución de la República del Ecuador (2008) reconoce el derecho universal al acceso a tecnologías de la información y comunicación como parte de los derechos del Buen Vivir. En este sentido, Morón et al. (2025) señalan que las brechas digitales representan uno de los principales obstáculos para garantizar igualdad tecnológica en sociedades contemporáneas. Jáuregui (2025) agrega que la exclusión digital puede profundizar desigualdades económicas y sociales preexistentes.

Otro aspecto relevante de la sociedad de la información corresponde al crecimiento de plataformas digitales y redes sociales como espacios de interacción social y circulación de contenidos. Estas herramientas tecnológicas han modificado las formas de comunicación interpersonal, participación política y producción cultural en todo el mundo. Sin embargo, también han generado problemáticas relacionadas con desinformación, manipulación algorítmica y difusión masiva de noticias falsas. Chuquichua et al. (2025) afirman que la expansión de redes digitales ha transformado significativamente los mecanismos tradicionales de construcción de opinión pública. Asimismo, Ortiz et al. (2025) consideran que las plataformas tecnológicas poseen un enorme poder de influencia social y política dentro de las sociedades digitales contemporáneas.

La regulación jurídica dentro de la sociedad de la información enfrenta actualmente el desafío de equilibrar innovación tecnológica y protección de derechos fundamentales. Los avances acelerados de tecnologías emergentes dificultan la creación de marcos normativos capaces de responder de manera inmediata a nuevos escenarios digitales. En consecuencia, los sistemas jurídicos requieren desarrollar regulaciones flexibles y dinámicas que permitan adaptarse a la constante evolución tecnológica. Dueñas et al. (2025) sostienen que la gobernanza digital constituye uno de los mayores retos jurídicos del siglo XXI debido a la complejidad global de las tecnologías emergentes. Melgar et al. (2026) agregan que la cooperación internacional resulta indispensable para garantizar seguridad jurídica y protección de derechos en entornos digitales transnacionales.

En resumen, la sociedad de la información y la transformación tecnológica evidencian que las tecnologías digitales se han convertido en componentes esenciales para el funcionamiento de las sociedades modernas. La digitalización de procesos económicos, educativos, administrativos y sociales ha generado nuevas oportunidades de desarrollo, innovación y conectividad global. Sin embargo, también ha planteado desafíos relacionados con privacidad, ciberseguridad, regulación jurídica y protección de derechos humanos en entornos virtuales. Corcino et al. (2026) sostienen que el futuro de la sociedad digital dependerá de la capacidad de los Estados y organismos internacionales para construir modelos regulatorios equilibrados y sostenibles. En este sentido, el Derecho Digital adquiere un papel fundamental dentro de la protección jurídica de las sociedades tecnológicas contemporáneas.

1.3 Concepto, características y principios del Derecho Digital

El Derecho Digital puede entenderse como la rama del Derecho encargada de regular las relaciones, actividades y conflictos que se desarrollan dentro de los entornos tecnológicos contemporáneos. Esta disciplina reúne normas, principios y mecanismos jurídicos orientados a garantizar seguridad jurídica en espacios virtuales caracterizados por el constante intercambio de información y el uso permanente de tecnologías digitales, las cuales influyen directamente en las relaciones sociales, económicas y jurídicas actuales.

Su desarrollo responde a la necesidad de adaptar el ordenamiento jurídico tradicional frente a fenómenos derivados de Internet, inteligencia artificial, comercio electrónico y protección de datos personales. Según Cornejo (2023), el Derecho Digital constituye una respuesta normativa frente a las nuevas dinámicas sociales generadas por la transformación tecnológica global. Asimismo, Vargas (2021) sostiene que esta rama jurídica busca equilibrar innovación tecnológica y protección de derechos fundamentales en entornos digitales.

El concepto de Derecho Digital se encuentra estrechamente relacionado con la evolución de la sociedad de la información y la expansión de las tecnologías de la comunicación. A medida que las actividades humanas migraron hacia espacios virtuales, surgió la necesidad de establecer marcos regulatorios capaces de controlar riesgos tecnológicos y proteger derechos digitales emergentes. En este sentido, el Derecho Digital abarca ámbitos como protección de datos personales, ciberseguridad, delitos informáticos, propiedad intelectual y contratación electrónica. Mendoza et al. (2021) afirman que esta

disciplina posee un carácter transversal debido a su interacción con múltiples áreas del derecho tradicional. Del mismo modo, Arango (2024) considera que el Derecho Digital constituye uno de los pilares regulatorios fundamentales dentro de las sociedades tecnológicas contemporáneas.

Entre las principales características del Derecho Digital destaca su naturaleza dinámica y evolutiva frente a los constantes cambios tecnológicos. A diferencia de otras ramas jurídicas tradicionales, esta disciplina debe adaptarse permanentemente a innovaciones digitales que modifican las relaciones sociales y económicas de manera acelerada. Por ello, las normas digitales requieren flexibilidad suficiente para responder a escenarios tecnológicos complejos y cambiantes. Gamboa et al. (2024) señalan que la velocidad de evolución tecnológica representa uno de los mayores desafíos para los sistemas regulatorios contemporáneos. Asimismo, Macías y Espinoza (2024) indican que el Derecho Digital demanda procesos constantes de actualización normativa y reinterpretación jurídica.

Otra característica esencial del Derecho Digital corresponde a su dimensión global y transnacional. Las actividades desarrolladas dentro de Internet y plataformas digitales suelen superar las fronteras territoriales tradicionales, lo que genera dificultades relacionadas con jurisdicción, competencia y soberanía estatal. Esta situación obliga a fortalecer mecanismos de cooperación internacional y armonización normativa entre distintos países. Según Morón et al. (2025), la globalización tecnológica ha debilitado las limitaciones territoriales clásicas del derecho tradicional. En consecuencia, instrumentos internacionales como la Convención sobre Ciberdelincuencia (2001) buscan fortalecer la cooperación jurídica internacional frente a delitos informáticos y amenazas cibernéticas.

El Derecho Digital también se caracteriza por poseer una fuerte orientación hacia la protección de derechos fundamentales en entornos virtuales. La expansión tecnológica ha generado riesgos relacionados con privacidad, protección de datos, libertad de expresión y acceso a la información, lo que exige mecanismos jurídicos especializados para garantizar seguridad y dignidad humana dentro de espacios digitales. La Constitución de la República del Ecuador (2008) reconoce derechos vinculados con privacidad, acceso universal a tecnologías y protección de información personal. En este contexto, Miranda et al. (2025) sostienen que los derechos digitales representan una extensión contemporánea de los derechos humanos tradicionales. Jáuregui (2025) agrega que la

protección jurídica de la persona constituye uno de los principios esenciales del Derecho Digital moderno.

Entre los principios fundamentales del Derecho Digital destaca el principio de protección de datos personales, orientado a garantizar el tratamiento adecuado, seguro y transparente de la información de los usuarios. Este principio adquiere especial relevancia debido al crecimiento masivo de plataformas digitales capaces de recopilar, almacenar y procesar datos personales a gran escala. El Reglamento General de Protección de Datos (2016) establece estándares internacionales relacionados con consentimiento, transparencia y responsabilidad en el manejo de información personal. Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) regula en Ecuador los mecanismos destinados a proteger privacidad y confidencialidad digital. Ramírez (2025) sostiene que la protección de datos constituye actualmente uno de los ejes centrales de la regulación jurídica tecnológica.

Otro principio relevante dentro del Derecho Digital corresponde al principio de seguridad informática y ciberseguridad. Este principio busca garantizar integridad, disponibilidad y confidencialidad de la información digital frente a amenazas tecnológicas y delitos cibernéticos. El incremento de ataques informáticos, fraudes electrónicos y robo de identidad ha impulsado la creación de mecanismos legales orientados a proteger infraestructuras tecnológicas y sistemas digitales. Rafael y Ancasi (2026) afirman que la ciberseguridad representa un componente indispensable para garantizar confianza dentro de entornos digitales contemporáneos. De igual forma, el Código Orgánico Integral Penal (2014) incorpora disposiciones relacionadas con delitos informáticos y protección de sistemas tecnológicos en Ecuador.

El principio de neutralidad tecnológica constituye otra base fundamental del Derecho Digital contemporáneo. Este principio establece que las normas jurídicas deben aplicarse de manera independiente respecto al tipo específico de tecnología utilizada, evitando regulaciones limitadas a herramientas tecnológicas concretas que puedan quedar obsoletas rápidamente. Gracias a este enfoque, los sistemas jurídicos pueden adaptarse de forma más eficiente a la constante innovación tecnológica. Dueñas et al. (2025) sostienen que la neutralidad tecnológica permite construir marcos regulatorios flexibles y sostenibles frente a la transformación digital permanente. Del mismo modo, Ortiz et al. (2025) consideran que este principio favorece estabilidad jurídica y continuidad normativa en escenarios tecnológicos dinámicos.

Finalmente, el Derecho Digital se consolida actualmente como una disciplina jurídica indispensable dentro de las sociedades tecnológicas modernas debido a su función reguladora y protectora frente a los desafíos derivados de la digitalización global. La complejidad de fenómenos relacionados con inteligencia artificial, plataformas digitales, protección de datos y cibercriminalidad exige sistemas normativos capaces de equilibrar innovación tecnológica y garantía de derechos fundamentales. Corcino et al. (2026) sostienen que el futuro del Derecho Digital dependerá de la capacidad estatal e internacional para desarrollar regulaciones adaptables y efectivas frente a escenarios digitales emergentes. En este sentido, Melgar et al. (2026) concluyen que la consolidación de sociedades digitales requiere marcos jurídicos sólidos orientados a fortalecer seguridad, transparencia y protección integral de los ciudadanos.

1.4 Impacto de las tecnologías emergentes en el sistema jurídico

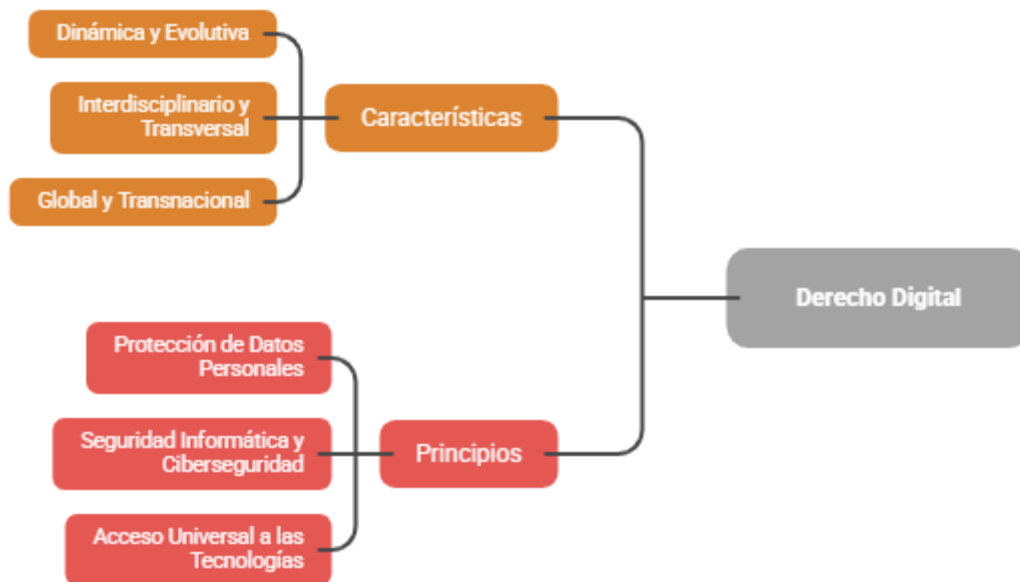
El Derecho Digital es una rama jurídica especializada que regula las relaciones sociales, económicas y tecnológicas desarrolladas en entornos digitales. Su aparición surge como respuesta al crecimiento de Internet, la automatización y las tecnologías de la información y comunicación. Asimismo, esta disciplina aborda temas relacionados con protección de datos personales, comercio electrónico, ciberseguridad y delitos informáticos. Además, busca garantizar la protección de los derechos digitales dentro de la sociedad contemporánea. Según Cajahuanca (2025), el Derecho Digital representa una respuesta normativa frente a los desafíos generados por la transformación tecnológica global. Asimismo, Jiménez y Pincay (2024) sostienen que esta disciplina adquiere relevancia debido al impacto de las tecnologías digitales sobre los derechos constitucionales y la sociedad contemporánea.

El concepto de Derecho Digital también se encuentra vinculado con la regulación jurídica de los espacios virtuales y el uso responsable de tecnologías digitales dentro de la sociedad de la información. A medida que las actividades humanas migran hacia plataformas digitales, resulta indispensable establecer normas que garanticen seguridad jurídica y protección de derechos fundamentales en entornos tecnológicos. Cornejo (2023) señala que la modernización tecnológica obliga a los Estados a replantear mecanismos regulatorios tradicionales para responder a nuevas dinámicas sociales y económicas. Del mismo modo, Vargas (2021) considera que la implementación del

gobierno digital refleja la necesidad de fortalecer estructuras jurídicas capaces de responder a la evolución tecnológica contemporánea.

Figura 1

Derecho Digital: Regulación y Desafíos



Entre las principales características del Derecho Digital destaca su naturaleza dinámica y evolutiva. Esta rama jurídica se encuentra en constante transformación debido al desarrollo acelerado de nuevas tecnologías como inteligencia artificial, blockchain, computación en la nube y big data. Por ello, las regulaciones digitales requieren mecanismos flexibles que permitan adaptarse rápidamente a escenarios tecnológicos emergentes. Gamboa et al. (2024) afirman que los sistemas jurídicos contemporáneos enfrentan importantes desafíos relacionados con la protección de derechos constitucionales dentro de entornos digitales. Asimismo, Macías y Espinoza (2024) sostienen que el derecho moderno debe evolucionar continuamente para garantizar protección efectiva frente a los cambios tecnológicos permanentes.

Otra característica esencial del Derecho Digital corresponde a su carácter interdisciplinario y transversal. Esta disciplina interactúa con diversas áreas jurídicas tradicionales como derecho civil, penal, administrativo, constitucional e internacional, debido a que los fenómenos tecnológicos afectan múltiples dimensiones sociales y económicas. Además, requiere conocimientos técnicos relacionados con informática, telecomunicaciones y sistemas digitales para comprender adecuadamente los riesgos tecnológicos contemporáneos. Mendoza (2024) sostiene que la regulación jurídica de la

privacidad digital demanda enfoques multidisciplinarios capaces de integrar perspectivas tecnológicas y jurídicas. Del mismo modo, Rivera y Maldonado (2023) consideran que la protección de derechos digitales requiere mecanismos regulatorios especializados frente a las amenazas derivadas del entorno virtual.

El Derecho Digital posee una dimensión global y transnacional, debido a que muchas actividades realizadas en Internet superan las fronteras territoriales tradicionales. Esta realidad genera desafíos relacionados con jurisdicción, soberanía estatal y cooperación internacional frente a delitos informáticos y conflictos digitales. Por ello, los Estados han promovido acuerdos internacionales orientados a fortalecer la regulación tecnológica y la seguridad jurídica en el ciberespacio. La Convención sobre Ciberdelincuencia (2001) representa uno de los principales instrumentos internacionales para combatir los delitos informáticos mediante cooperación jurídica internacional. Muñiz (2023) destaca la importancia estratégica de la diplomacia tecnológica en las relaciones internacionales actuales.

Uno de los principios fundamentales del Derecho Digital corresponde al principio de protección de datos personales, orientado a garantizar privacidad, confidencialidad y control sobre la información individual dentro de plataformas tecnológicas. El crecimiento del intercambio masivo de datos digitales ha incrementado la necesidad de establecer mecanismos legales capaces de proteger la información personal frente a usos indebidos. El Reglamento General de Protección de Datos (2016) establece estándares internacionales relacionados con consentimiento, transparencia y responsabilidad en el tratamiento de datos personales. Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) fortalece en Ecuador la protección jurídica de la información digital. Ojeda y Suárez (2025) sostienen que la protección de datos personales constituye actualmente un auténtico derecho humano digital.

Otro principio relevante del Derecho Digital es el principio de seguridad informática y ciberseguridad, cuyo objetivo consiste en proteger sistemas tecnológicos frente a amenazas digitales, accesos ilegales y ataques informáticos. La expansión de delitos cibernéticos ha generado preocupación mundial respecto a vulnerabilidad de infraestructuras digitales y riesgos asociados con robo de información o fraude electrónico. El Código Orgánico Integral Penal (2014) incorpora disposiciones relacionadas con delitos informáticos dentro del ordenamiento jurídico ecuatoriano. Rafael y Anccasi (2026) consideran que el fortalecimiento del gobierno digital requiere

sistemas robustos de seguridad tecnológica capaces de garantizar confianza y estabilidad institucional. Asimismo, Melgar et al. (2026) destacan la importancia de implementar estrategias digitales seguras dentro de la administración pública contemporánea.

El principio de acceso universal a las tecnologías de la información también constituye una base esencial del Derecho Digital moderno. Este principio busca garantizar igualdad de oportunidades dentro de la sociedad digital, permitiendo que todas las personas puedan acceder a herramientas tecnológicas y participar activamente dentro de entornos virtuales. La Constitución de la República del Ecuador (2008) reconoce el acceso a tecnologías de la información como parte de los derechos relacionados con comunicación y participación ciudadana. Chuquicahua et al. (2025) sostienen que la transformación digital de las instituciones públicas debe desarrollarse bajo principios de inclusión y accesibilidad tecnológica. Del mismo modo, Ramírez (2025) afirma que el gobierno abierto fortalece transparencia y participación democrática mediante herramientas digitales.

Para finalizar, el Derecho Digital se consolida como una disciplina jurídica indispensable dentro de las sociedades contemporáneas debido a su función reguladora frente a los desafíos tecnológicos actuales. La creciente digitalización de procesos económicos, administrativos y sociales exige marcos normativos capaces de proteger derechos fundamentales, fortalecer seguridad jurídica y garantizar equilibrio entre innovación y regulación. Dueñas et al. (2025) sostienen que los derechos fundamentales deben reinterpretarse constantemente frente a los cambios tecnológicos contemporáneos. En este contexto, Corcino et al. (2026) consideran que la modernización digital del Estado requiere sistemas jurídicos sólidos capaces de responder de manera eficiente a las nuevas dinámicas tecnológicas globales.

1.5 Derechos fundamentales en entornos digitales

Los derechos fundamentales en entornos digitales constituyen garantías jurídicas orientadas a proteger la dignidad, libertad y privacidad de las personas dentro de espacios tecnológicos y virtuales. El crecimiento acelerado de Internet y las tecnologías de la información ha generado nuevos escenarios donde los derechos humanos tradicionales deben adaptarse a dinámicas digitales complejas. En este contexto, la protección jurídica adquiere especial relevancia frente a riesgos relacionados con vulneración de privacidad, uso indebido de datos y restricciones al acceso a la información. Como sostienen Benlonch y Sarrión (2022) la era digital plantea importantes desafíos constitucionales

debido a la constante transformación tecnológica y sus efectos sobre los derechos fundamentales. Asimismo, la Constitución de la República del Ecuador (2008) reconoce derechos vinculados con privacidad, comunicación y acceso universal a tecnologías digitales.

Uno de los principales derechos fundamentales dentro de los entornos digitales corresponde al derecho a la protección de datos personales. Este derecho busca garantizar que la información privada de las personas sea tratada de manera segura, transparente y legítima por instituciones públicas y privadas. El crecimiento de plataformas digitales y sistemas automatizados ha incrementado la recopilación masiva de datos personales, generando preocupación respecto a posibles vulneraciones de privacidad. Aguilar et al. (2022) afirman que la protección de datos personales constituye una necesidad esencial dentro de las sociedades tecnológicas contemporáneas. Del mismo modo, Ojeda y Suárez (2025) consideran que la protección de datos debe reconocerse como un auténtico derecho humano digital debido a su importancia para preservar la dignidad y autonomía individual.

La regulación jurídica relacionada con protección de datos personales ha adquirido gran relevancia en múltiples sistemas normativos internacionales y nacionales. El Reglamento General de Protección de Datos (2016) establece principios relacionados con consentimiento, transparencia y responsabilidad en el tratamiento de información digital. En Ecuador, la Ley Orgánica de Protección de Datos Personales (2021) fortalece mecanismos destinados a garantizar confidencialidad y seguridad de la información personal. Según Rovira y Robles (2023), la promulgación de esta normativa representa un avance significativo dentro de la protección jurídica digital ecuatoriana. Asimismo, Molina y Pachano (2025) sostienen que la aplicación efectiva de estas regulaciones resulta indispensable para garantizar derechos fundamentales en entornos tecnológicos.

Otro derecho fundamental relevante dentro de los entornos digitales corresponde al derecho a la privacidad e intimidad personal. Las tecnologías digitales permiten almacenar, monitorear y compartir grandes cantidades de información relacionada con la vida privada de las personas, lo que incrementa riesgos asociados con vigilancia y exposición indebida de datos sensibles. Lara y Romero (2023) señalan que la libertad de expresión dentro de medios digitales debe coexistir con el respeto al derecho a la privacidad e intimidad personal. Asimismo, Rivera y Maldonado (2023) sostienen que las vulneraciones de privacidad representan uno de los principales problemas jurídicos

derivados de la expansión tecnológica contemporánea. En este escenario, el Derecho Digital busca equilibrar acceso a la información y protección de la vida privada dentro de plataformas virtuales.

El derecho al acceso universal a las tecnologías de la información también constituye un derecho fundamental dentro de la sociedad digital contemporánea. La conectividad y el acceso a herramientas tecnológicas permiten ejercer otros derechos relacionados con educación, participación ciudadana y libertad de información. La Constitución de la República del Ecuador (2008) reconoce el acceso a tecnologías de la información y comunicación como parte de los derechos del Buen Vivir. En este sentido, Jiménez y Pincay (2024) sostienen que los derechos digitales representan una extensión moderna de los derechos constitucionales tradicionales frente a la sociedad de la información. Asimismo, Chuquicahua et al. (2025) consideran que la implementación del gobierno digital debe desarrollarse bajo principios de inclusión tecnológica y accesibilidad universal.

Dentro de los entornos digitales también adquiere relevancia el derecho a la seguridad informática y protección frente a delitos cibernéticos. El crecimiento de ataques informáticos, robo de identidad y fraudes electrónicos ha generado preocupación respecto a la vulnerabilidad de usuarios y sistemas tecnológicos. Por ello, los Estados han incorporado normas orientadas a fortalecer mecanismos de prevención y sanción frente a actividades ilícitas desarrolladas en Internet. El Código Orgánico Integral Penal (2014) tipifica delitos relacionados con acceso ilegal a sistemas y vulneración de información digital. Además, la Convención sobre Ciberdelincuencia (2001) fortalece la cooperación internacional frente a amenazas tecnológicas globales. Como señalan Rafael y Anccasi (2026), la seguridad digital constituye un elemento esencial para garantizar confianza y estabilidad dentro de sociedades digitalizadas.

En términos finales, los derechos fundamentales en entornos digitales evidencian la necesidad de construir sistemas jurídicos capaces de responder eficazmente a los desafíos tecnológicos contemporáneos. La evolución constante de herramientas digitales obliga a reinterpretar derechos tradicionales bajo nuevas dinámicas sociales y tecnológicas. Dueñas et al. (2025) sostienen que el análisis jurisprudencial contemporáneo demuestra la necesidad de fortalecer mecanismos constitucionales de protección frente a riesgos digitales emergentes. Asimismo, Macías y Espinoza (2024) consideran que la evolución del derecho constitucional moderno depende de su capacidad para garantizar protección

efectiva de los derechos humanos dentro de la era tecnológica. En consecuencia, el Derecho Digital se consolida como una herramienta indispensable para preservar dignidad, libertad y seguridad jurídica en las sociedades contemporáneas.

1.6 Gobierno electrónico y administración pública digital

El gobierno electrónico constituye una estrategia de modernización estatal basada en la incorporación de tecnologías de la información y comunicación dentro de los procesos administrativos y de prestación de servicios públicos. Su principal finalidad consiste en mejorar eficiencia, transparencia y accesibilidad mediante plataformas digitales que faciliten la interacción entre ciudadanos e instituciones públicas. Este modelo transforma las estructuras tradicionales de gestión pública al integrar herramientas tecnológicas orientadas a optimizar procedimientos y fortalecer la participación ciudadana. Según Vargas (2021) el gobierno digital representa un mecanismo fundamental para modernizar las funciones estatales y fortalecer la eficiencia institucional. Asimismo, Arango (2024) sostiene que la digitalización administrativa permite mejorar significativamente la calidad de los servicios públicos ofrecidos a la ciudadanía.

El desarrollo del gobierno electrónico surge como respuesta a la necesidad de adaptar las administraciones públicas frente a los avances tecnológicos y las nuevas exigencias sociales derivadas de la sociedad de la información. La implementación de plataformas digitales facilita la automatización de trámites, reducción de tiempos administrativos y simplificación de procedimientos burocráticos. Además, fortalece el acceso ciudadano a información pública y servicios gubernamentales mediante herramientas digitales accesibles desde diferentes espacios geográficos. Cornejo (2023) afirma que la modernización de la gestión pública requiere procesos permanentes de innovación tecnológica capaces de responder a las demandas contemporáneas. De igual forma, Mendoza et al. (2021) consideran que el gobierno abierto y digital fortalece la comunicación entre Estado y ciudadanía.

Una de las principales características del gobierno electrónico corresponde a la utilización de sistemas digitales interconectados para optimizar la gestión administrativa y garantizar mayor eficiencia institucional. Las plataformas virtuales permiten almacenar, procesar y compartir información de manera rápida y segura, facilitando la toma de decisiones dentro de organismos públicos. Además, el uso de tecnologías digitales contribuye a disminuir costos operativos y mejorar la productividad estatal. Chuquicahua et al. (2025) sostienen

que los modelos de gobierno digital permiten optimizar significativamente los procesos administrativos en entidades públicas. Asimismo, Corcino et al. (2026) consideran que la transformación digital fortalece eficiencia y calidad dentro de la administración pública contemporánea.

El gobierno electrónico también desempeña un papel fundamental en el fortalecimiento de la transparencia y lucha contra la corrupción dentro de las instituciones públicas. La digitalización de procesos administrativos facilita el acceso ciudadano a información gubernamental, reduce discrecionalidad y fortalece mecanismos de control social. En consecuencia, las plataformas tecnológicas contribuyen a generar mayor confianza ciudadana respecto a las actuaciones estatales. Bonilla (2025) señala que las herramientas digitales constituyen mecanismos eficaces para promover transparencia y combatir prácticas corruptas dentro de la administración pública. Del mismo modo, Ortiz et al. (2025) afirman que el gobierno electrónico fortalece la rendición de cuentas y mejora la supervisión de la gestión estatal.

Otro aspecto importante relacionado con la administración pública digital corresponde a la participación ciudadana mediante herramientas tecnológicas. Las plataformas virtuales permiten que los ciudadanos accedan a información pública, realicen trámites electrónicos y participen activamente dentro de procesos administrativos y democráticos. Esto fortalece principios relacionados con inclusión, transparencia y acceso universal a los servicios estatales. Ramírez (2025) sostiene que el gobierno abierto favorece la construcción de sociedades más participativas y democráticas mediante el uso de tecnologías digitales. Asimismo, Jáuregui (2025) considera que la transformación digital estatal contribuye significativamente a mejorar las relaciones entre ciudadanía e instituciones públicas.

Sin embargo, el desarrollo del gobierno electrónico también plantea desafíos relacionados con protección de datos personales y seguridad informática. La gestión masiva de información digital dentro de instituciones públicas incrementa riesgos asociados con vulneración de privacidad, filtración de datos y ataques cibernéticos. Por ello, resulta indispensable implementar mecanismos jurídicos y tecnológicos orientados a garantizar confidencialidad y protección de la información ciudadana. La Ley Orgánica de Protección de Datos Personales (2021) establece principios destinados a regular el tratamiento adecuado de información digital en Ecuador. Asimismo, Aguilar et al. (2022)

sostienen que la protección de datos constituye un componente esencial dentro de la administración pública digital contemporánea.

La seguridad informática representa otro elemento fundamental dentro de los procesos de gobierno electrónico debido al incremento de amenazas cibernéticas y delitos informáticos dirigidos contra infraestructuras digitales estatales. El uso de tecnologías digitales dentro de instituciones públicas requiere sistemas robustos de protección capaces de garantizar integridad y disponibilidad de la información gubernamental. La Convención sobre Ciberdelincuencia (2001) fortalece la cooperación internacional frente a delitos tecnológicos y amenazas digitales globales. Rafael y Anccasi (2026) afirman que la modernización digital del Estado debe acompañarse de estrategias eficaces de ciberseguridad institucional. Asimismo, Melgar et al. (2026) consideran que la transformación tecnológica pública depende directamente de la capacidad estatal para garantizar seguridad digital.

La administración pública digital también enfrenta desafíos relacionados con brecha tecnológica y acceso desigual a herramientas digitales dentro de diferentes sectores sociales. Aunque las plataformas electrónicas facilitan múltiples servicios públicos, no todos los ciudadanos poseen acceso adecuado a Internet o competencias digitales suficientes para utilizar estas herramientas. Esta situación puede generar exclusión y limitar el ejercicio efectivo de derechos ciudadanos dentro de entornos digitales. Morón et al. (2025) sostienen que la modernización tecnológica estatal debe desarrollarse bajo principios de inclusión y accesibilidad universal. Del mismo modo, Miranda et al. (2025) consideran que el gobierno electrónico debe garantizar igualdad de oportunidades para todos los ciudadanos independientemente de sus condiciones socioeconómicas.

En resumen, el gobierno electrónico y la administración pública digital constituyen elementos fundamentales dentro de los procesos contemporáneos de modernización estatal y transformación tecnológica. La incorporación de herramientas digitales permite fortalecer eficiencia administrativa, transparencia institucional y participación ciudadana dentro de sociedades cada vez más conectadas. Sin embargo, también exige mecanismos jurídicos sólidos capaces de proteger derechos fundamentales, garantizar seguridad informática y reducir brechas tecnológicas. Según Cajahuanca (2025), las ciencias jurídicas desempeñan un papel esencial dentro de la regulación de los procesos digitales contemporáneos. En consecuencia, el Derecho Digital se consolida como una disciplina

indispensable para garantizar el adecuado funcionamiento de la administración pública en la era tecnológica.

1.7 Retos éticos y jurídicos de la sociedad tecnológica

La sociedad tecnológica contemporánea enfrenta múltiples retos éticos y jurídicos derivados del acelerado desarrollo de herramientas digitales y sistemas automatizados. El crecimiento de Internet, inteligencia artificial, plataformas virtuales y procesamiento masivo de datos ha transformado profundamente las relaciones sociales, económicas y políticas, generando nuevas problemáticas relacionadas con privacidad, seguridad y protección de derechos fundamentales. En este contexto, los sistemas jurídicos deben adaptarse constantemente para responder a escenarios digitales complejos y dinámicos (Cajahuanca, 2025; Forero, 2023). Además, la transformación tecnológica exige mecanismos regulatorios capaces de equilibrar innovación, desarrollo económico y respeto por los derechos humanos dentro de entornos virtuales.

Uno de los principales retos éticos de la sociedad tecnológica corresponde al tratamiento masivo de datos personales y la vulneración potencial del derecho a la privacidad. Las plataformas digitales recopilan grandes cantidades de información relacionada con hábitos, preferencias y actividades de los usuarios, lo que incrementa riesgos asociados con vigilancia, comercialización indebida de datos y exposición de información sensible. Según Mendoza (2024), la regulación jurídica de la privacidad digital constituye uno de los desafíos más importantes dentro de las sociedades tecnológicas contemporáneas. Asimismo, Rivera y Maldonado (2023) sostienen que las vulneraciones a la intimidad representan una problemática creciente derivada del uso intensivo de tecnologías digitales.

Otro desafío relevante se relaciona con la necesidad de garantizar protección efectiva de los derechos fundamentales dentro de entornos digitales globalizados. La expansión tecnológica ha generado conflictos entre libertad de expresión, acceso a la información y protección de la intimidad personal, especialmente en redes sociales y plataformas virtuales. Además, la difusión masiva de información falsa y discursos de odio plantea importantes debates éticos y jurídicos sobre límites y responsabilidades dentro de Internet (Lara y Romero, 2023; Rodas et al., 2025). En este sentido, el Derecho Digital debe desarrollar mecanismos capaces de garantizar equilibrio entre derechos individuales y seguridad colectiva dentro de los espacios tecnológicos contemporáneos.

La inteligencia artificial y la automatización también representan importantes retos éticos para las sociedades actuales debido a los riesgos relacionados con decisiones automatizadas, discriminación algorítmica y falta de transparencia tecnológica. Muchas plataformas digitales utilizan sistemas automatizados capaces de influir en decisiones laborales, financieras y administrativas sin supervisión humana suficiente. Como afirman Macías y Espinoza (2024) el derecho contemporáneo enfrenta la necesidad de reinterpretar principios jurídicos tradicionales frente a los cambios tecnológicos acelerados. Del mismo modo, Muñiz (2023) considera que la gobernanza tecnológica internacional debe incorporar principios éticos orientados a proteger dignidad, igualdad y derechos humanos dentro de la era digital.

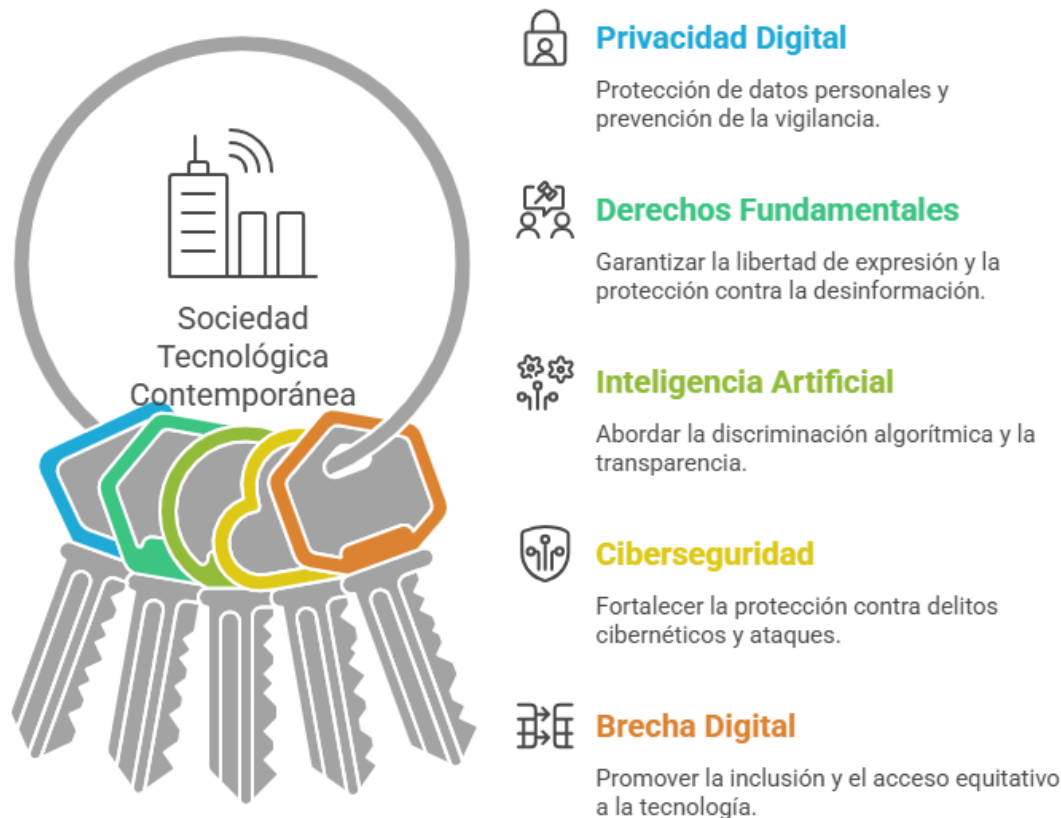
La ciberseguridad constituye otro de los grandes desafíos jurídicos y éticos de la sociedad tecnológica moderna. El incremento de delitos informáticos, ataques cibernéticos y robo de información digital amenaza tanto a ciudadanos como a instituciones públicas y privadas. En consecuencia, los Estados han impulsado regulaciones orientadas a fortalecer la seguridad informática y proteger infraestructuras digitales estratégicas (Convención sobre Ciberdelincuencia, 2001; Código Orgánico Integral Penal (COIP), 2014). Además, la cooperación internacional resulta indispensable para combatir amenazas tecnológicas transnacionales que afectan estabilidad institucional y seguridad de los sistemas digitales globales.

Otro reto importante corresponde a la brecha digital y desigualdad en el acceso a las tecnologías de la información. Aunque la digitalización ha generado múltiples oportunidades de desarrollo, millones de personas aún enfrentan limitaciones económicas, educativas y tecnológicas que dificultan su participación dentro de la sociedad digital. Esta situación puede profundizar desigualdades sociales y restringir el ejercicio efectivo de derechos fundamentales relacionados con educación, comunicación y acceso a servicios públicos. Según Jáuregui (2025), la modernización tecnológica del Estado debe desarrollarse bajo principios de inclusión y accesibilidad universal. Asimismo, Chuquicahua et al. (2025) sostienen que el gobierno digital solo puede consolidarse plenamente cuando existe igualdad de acceso a herramientas tecnológicas y conectividad digital.

Por último, los retos éticos y jurídicos de la sociedad tecnológica evidencian la necesidad de fortalecer marcos regulatorios capaces de responder eficazmente a la rápida evolución digital contemporánea. La transformación tecnológica continuará generando nuevos

escenarios jurídicos relacionados con inteligencia artificial, plataformas digitales, automatización y protección de derechos fundamentales. Por ello, resulta indispensable construir sistemas normativos flexibles, éticos y multidisciplinarios orientados a garantizar seguridad jurídica y protección integral de las personas dentro de los entornos virtuales (Dueñas et al., 2025; Gamboa et al., 2024). En este contexto, el Derecho Digital adquiere un papel esencial como herramienta jurídica destinada a regular responsablemente la sociedad tecnológica moderna.

Figura 2
Desafíos de la Socienda tecnológica





CAPÍTULO 2

Protección de datos personales y privacidad

2.1 Concepto y naturaleza jurídica de los datos personales

La protección de los datos personales constituye uno de los pilares fundamentales dentro del Derecho Digital contemporáneo, debido a que la información relacionada con las personas ha adquirido un valor estratégico en la sociedad tecnológica. En la actualidad, múltiples actividades cotidianas implican la recopilación, almacenamiento y tratamiento de datos mediante plataformas digitales, redes sociales, aplicaciones móviles y sistemas automatizados. Por esta razón, surge la necesidad de establecer mecanismos jurídicos que regulen el uso adecuado de dicha información y garanticen el respeto a los derechos fundamentales de los ciudadanos. En este contexto, los datos personales representan un elemento esencial dentro de la relación entre tecnología, privacidad y seguridad jurídica (Aguilar et al., 2022)

Los datos personales comprenden toda información que permite identificar directa o indirectamente a una persona natural, mediante elementos como nombres, números de identificación, direcciones electrónicas o datos biométricos. Asimismo, el avance de las tecnologías de análisis masivo de datos ha incrementado las posibilidades de identificación digital a través de hábitos y patrones de comportamiento. Frente a ello, la regulación jurídica busca proteger la dignidad humana y prevenir el uso indebido de la información dentro de los entornos digitales. Según Aguilar et al. (2022), la protección de datos personales constituye una garantía necesaria frente al incremento del tratamiento automatizado de información en la sociedad contemporánea.

Asimismo, la naturaleza jurídica de los datos personales se encuentra estrechamente vinculada con los derechos fundamentales relacionados con la intimidad, privacidad y autodeterminación informativa. Esto significa que las personas deben mantener control sobre el acceso, uso y difusión de su información personal, especialmente cuando esta es tratada por entidades públicas o privadas. En este sentido, el derecho a la protección de datos no solo protege información aislada, sino también la capacidad de cada individuo para decidir sobre el manejo de sus datos dentro de los sistemas tecnológicos actuales. De esta manera, el tratamiento de datos personales debe realizarse bajo principios de legalidad, transparencia y consentimiento informado (Becerra et al., 2024).

Por otra parte, el crecimiento de la economía digital ha convertido a los datos personales en recursos estratégicos para empresas, gobiernos y plataformas tecnológicas, los cuales son utilizados para crear perfiles de usuarios y personalizar servicios digitales. No

obstante, esta situación también ha incrementado riesgos relacionados con vigilancia masiva, comercialización indebida de información y vulneraciones a la privacidad. Frente a ello, los sistemas jurídicos modernos han desarrollado normativas destinadas a limitar el uso abusivo de los datos y fortalecer la protección de los derechos de los titulares de la información. Como señala Bonilla (2025), la expansión de las tecnologías digitales exige nuevas formas de regulación que equilibren innovación tecnológica y protección de derechos fundamentales.

De igual manera, la doctrina jurídica reconoce que los datos personales poseen una naturaleza dual, debido a que representan simultáneamente un derecho fundamental y un activo económico. Por un lado, los datos forman parte de la esfera personal de cada individuo y requieren protección constitucional; mientras que, por otro lado, poseen valor comercial dentro de los mercados digitales y tecnológicos. Esta doble dimensión ha generado importantes debates sobre los límites del tratamiento de datos y las responsabilidades de quienes administran información personal. En consecuencia, el Derecho Digital busca establecer mecanismos que permitan compatibilizar el desarrollo tecnológico con la protección efectiva de la privacidad de las personas (Rodas et al., 2025).

En relación con el ámbito normativo, diversos instrumentos internacionales han reconocido la importancia jurídica de la protección de datos personales. Entre ellos destacan el Reglamento General de Protección de Datos de la Unión Europea (Reglamento del Parlamento Europeo y del Consejo, 2016) y múltiples legislaciones nacionales orientadas a fortalecer los derechos digitales de los ciudadanos. Estas normas establecen principios relacionados con el consentimiento, finalidad, minimización de datos, confidencialidad y responsabilidad proactiva. Además, promueven obligaciones específicas para las instituciones encargadas del tratamiento de información personal. Según Martínez et al. (2024), la evolución normativa internacional refleja la creciente preocupación por garantizar la seguridad y privacidad de los datos en entornos digitales cada vez más complejos.

En el caso ecuatoriano, la protección de datos personales adquirió especial relevancia con la promulgación de la Ley Orgánica de Protección de Datos Personales (2021), la cual reconoce derechos relacionados con el acceso, rectificación, eliminación y oposición al tratamiento de información personal. Esta normativa busca fortalecer la seguridad jurídica en el uso de tecnologías digitales y garantizar que las instituciones públicas y

privadas actúen bajo parámetros de responsabilidad y transparencia. Asimismo, establece principios orientados a proteger la dignidad humana frente a posibles vulneraciones derivadas del uso indebido de datos personales. En consecuencia, Ecuador se incorpora progresivamente a las tendencias internacionales de regulación digital (Ley Orgánica de Protección de Datos Personales, 2021).

De igual forma, la protección de datos personales mantiene una relación directa con el desarrollo de nuevas tecnologías como la inteligencia artificial, el big data y el internet de las cosas. Estas herramientas permiten recopilar grandes volúmenes de información y procesarlos mediante algoritmos automatizados capaces de influir en decisiones sociales, económicas y políticas. Debido a ello, los riesgos asociados a la manipulación y utilización de datos se incrementan considerablemente, especialmente cuando no existen mecanismos adecuados de supervisión jurídica. Por esta razón, resulta indispensable fortalecer las políticas de ciberseguridad y promover una cultura digital basada en el respeto a la privacidad y los derechos fundamentales (Constante y López, 2025).

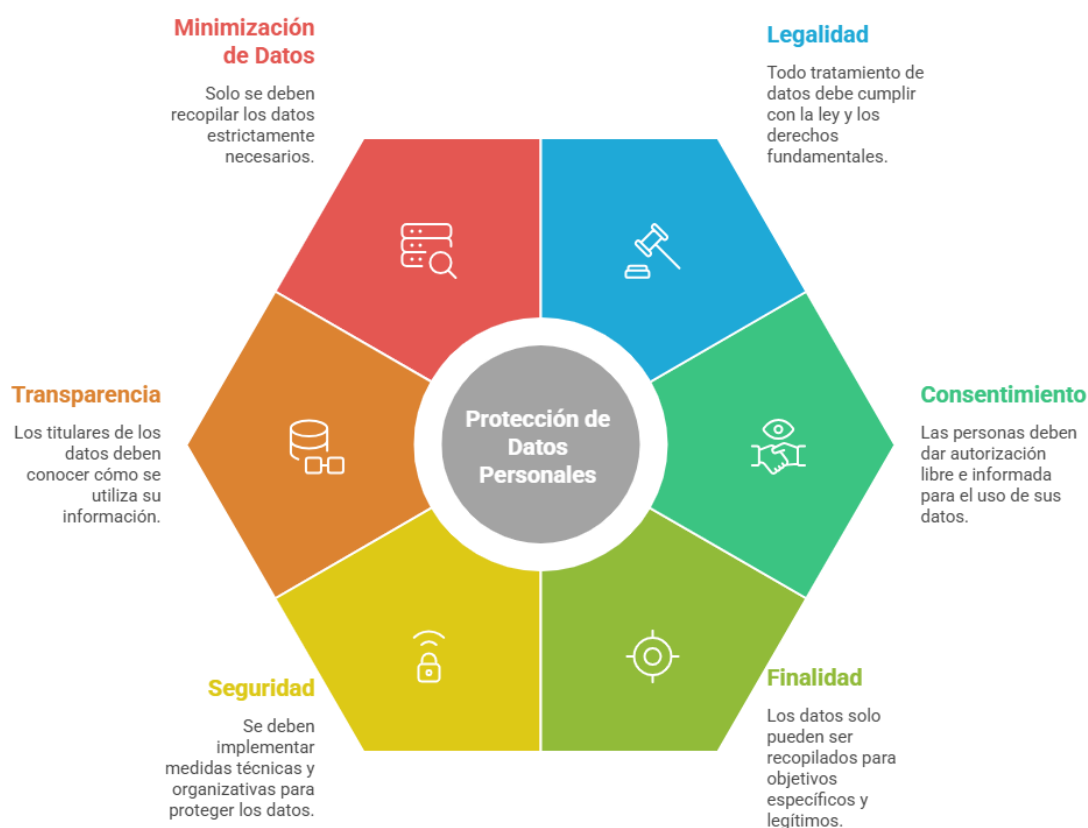
En conclusión, la naturaleza jurídica de los datos personales demuestra que la información constituye uno de los bienes más sensibles dentro de la sociedad tecnológica actual. La expansión de los entornos digitales ha transformado la manera en que las personas interactúan, trabajan y acceden a servicios, generando nuevos desafíos para el Derecho y las instituciones encargadas de garantizar la protección de derechos fundamentales. En este escenario, la regulación de los datos personales no solo representa una necesidad jurídica, sino también una condición esencial para promover confianza, seguridad y equilibrio entre innovación tecnológica y dignidad humana. Por ello, la protección de datos continuará consolidándose como uno de los principales ejes del Derecho Digital contemporáneo (Giler, 2023).

2.2 Principios de protección de datos y privacidad digital

La protección de datos personales y la privacidad digital se sustentan en una serie de principios jurídicos que orientan el tratamiento adecuado de la información dentro de los entornos tecnológicos. Estos principios buscan garantizar que los datos de las personas sean recopilados, almacenados y utilizados de manera legítima, transparente y segura, evitando prácticas abusivas o vulneraciones a los derechos fundamentales. En la actualidad, el incremento del uso de plataformas digitales y sistemas automatizados ha generado mayores riesgos relacionados con la difusión indebida de información personal.

Por ello, las normativas nacionales e internacionales han incorporado principios orientados a fortalecer la seguridad jurídica y proteger la dignidad humana en la sociedad digital (Ley Orgánica de Protección de Datos Personales, 2021).

Figura 3
Principios de Protección de Datos



Uno de los principios más importantes es el principio de legalidad, el cual establece que todo tratamiento de datos personales debe realizarse conforme a la ley y respetando los derechos fundamentales de los titulares de la información. Este principio implica que ninguna entidad pública o privada puede recopilar o utilizar datos personales sin una base jurídica válida que legitime dicho tratamiento. Además, exige que las actividades relacionadas con el manejo de información sean claras y estén sujetas a supervisión normativa. Según Gutiérrez (2022), el reconocimiento de los datos personales como un derecho humano obliga a los Estados a establecer mecanismos legales eficaces para garantizar su protección frente a posibles vulneraciones digitales.

Asimismo, el principio de consentimiento constituye una garantía esencial dentro de la privacidad digital, debido a que reconoce el derecho de las personas a decidir sobre el uso de su información personal. Este principio determina que el titular de los datos debe

otorgar autorización libre, específica, informada e inequívoca antes de que sus datos sean tratados por terceros. De esta manera, se fortalece la autodeterminación informativa y se limita el tratamiento arbitrario de información en entornos tecnológicos. En consecuencia, las organizaciones deben proporcionar información clara sobre las finalidades y condiciones del tratamiento de datos personales (Rovira y Robles, 2023).

Por otra parte, el principio de finalidad establece que los datos personales únicamente pueden ser recopilados para objetivos determinados, legítimos y explícitos. Esto significa que la información no puede ser utilizada posteriormente para propósitos incompatibles con aquellos para los cuales fue obtenida inicialmente. Dicho principio busca evitar el uso indiscriminado de datos y fortalecer la confianza de los ciudadanos en los sistemas digitales. Además, promueve prácticas responsables dentro de instituciones públicas y privadas que manejan información personal. Como señalan Aguilar et al. (2022), la delimitación de finalidades específicas constituye un elemento fundamental para garantizar transparencia y protección efectiva de datos personales en Ecuador.

De igual manera, el principio de seguridad exige que quienes administran datos personales implementen medidas técnicas, organizativas y jurídicas destinadas a prevenir accesos no autorizados, pérdida de información o vulneraciones digitales. Actualmente, las amenazas relacionadas con ciberataques, filtraciones de datos y delitos informáticos representan uno de los principales desafíos dentro de la protección de la privacidad digital. Debido a ello, las organizaciones deben adoptar mecanismos de ciberseguridad que permitan garantizar la confidencialidad e integridad de la información almacenada. En este sentido, la protección de datos personales no depende únicamente de normas jurídicas, sino también de estrategias tecnológicas eficaces (Rivera y Maldonado, 2023).

Igualmente, el principio de transparencia dispone que los titulares de los datos deben conocer cómo, por qué y para qué se recopila y utiliza su información personal. Este principio fortalece la confianza en los servicios digitales y promueve relaciones más equilibradas entre ciudadanos, empresas e instituciones públicas. Además, implica la obligación de informar sobre políticas de privacidad, tiempos de conservación de datos y posibles transferencias de información a terceros. Según Martínez et al. (2024), la transparencia constituye un componente indispensable para garantizar el ejercicio efectivo de derechos relacionados con el habeas data y la protección de datos personales dentro del ordenamiento jurídico ecuatoriano.

Por otro lado, el principio de minimización de datos establece que únicamente deben recopilarse aquellos datos estrictamente necesarios para cumplir la finalidad prevista. Esto permite reducir riesgos asociados al almacenamiento excesivo de información y limita posibles vulneraciones a la privacidad de los usuarios. En la práctica, este principio obliga a las organizaciones a evaluar constantemente la pertinencia y necesidad de los datos recopilados dentro de plataformas digitales y sistemas tecnológicos. Además, favorece una gestión responsable de la información en el contexto de la transformación digital y el gobierno electrónico (Reglamento General de Protección de Datos, 2016).

Para concluir, los principios de protección de datos y privacidad digital representan herramientas esenciales para garantizar el respeto de los derechos fundamentales en la sociedad tecnológica contemporánea. La expansión de las tecnologías digitales y la creciente circulación de información personal han generado nuevos desafíos jurídicos relacionados con la seguridad, confidencialidad y control de datos. Frente a este escenario, los principios de legalidad, consentimiento, finalidad, seguridad, transparencia y minimización permiten establecer límites al tratamiento de información y fortalecer la confianza ciudadana en los entornos digitales. Por ello, la protección de datos personales se consolida como uno de los principales retos del Derecho Digital moderno (Molina y Pachano, 2025)

2.3 Consentimiento informado y tratamiento de datos personales

El consentimiento informado es un principio esencial en la protección de datos personales y la privacidad digital, ya que permite que las personas mantengan control sobre el uso de su información. El crecimiento de plataformas digitales y sistemas automatizados ha incrementado la recopilación masiva de datos por parte de instituciones públicas y privadas. Frente a ello, el consentimiento garantiza la autonomía y la autodeterminación informativa de los ciudadanos, permitiendo además que conozcan las finalidades y condiciones del tratamiento de sus datos personales. (Ley Orgánica de Protección de Datos Personales, 2021).

Desde una perspectiva jurídica, el consentimiento informado puede entenderse como la manifestación libre, específica, inequívoca e informada mediante la cual una persona autoriza el tratamiento de sus datos personales. Este consentimiento debe otorgarse de manera voluntaria, sin presiones ni mecanismos engañosos que afecten la decisión del titular de la información. Asimismo, resulta indispensable que las entidades responsables

expliquen de forma clara los objetivos, riesgos y alcance del tratamiento de datos personales. Según Rovira y Robles (2023), el consentimiento informado representa un elemento esencial para garantizar transparencia y legitimidad en el manejo de información personal dentro del entorno digital ecuatoriano.

Por otra parte, el tratamiento de datos personales comprende todas aquellas operaciones relacionadas con la recopilación, almacenamiento, organización, modificación, transferencia y eliminación de información personal. Estas actividades pueden realizarse tanto de manera manual como automatizada mediante herramientas tecnológicas y sistemas digitales. Debido al crecimiento exponencial de las tecnologías de información, el tratamiento de datos se ha convertido en una actividad permanente dentro de múltiples sectores económicos, sociales y gubernamentales. Sin embargo, esta situación también ha incrementado los riesgos relacionados con vulneraciones a la privacidad y usos indebidos de información personal (Aguilar et al., 2022).

Asimismo, uno de los principales requisitos del consentimiento informado es que el titular de los datos tenga acceso a información clara y comprensible sobre el uso de su información personal. Esto implica que las políticas de privacidad y los términos de uso no deben redactarse mediante lenguaje ambiguo o excesivamente técnico que dificulte la comprensión del usuario. Además, las organizaciones tienen la obligación de informar sobre la finalidad del tratamiento, el tiempo de conservación de los datos y los posibles destinatarios de la información recopilada. De esta manera, se fortalece la transparencia y se promueve una relación más equilibrada entre usuarios y entidades digitales. Como señalan Jiménez y Pincay (2024) la protección de los derechos digitales exige mecanismos claros que permitan a los ciudadanos ejercer control efectivo sobre su información personal.

De igual manera, el consentimiento informado debe cumplir determinadas características para ser considerado válido dentro del marco jurídico. En primer lugar, debe ser libre, lo cual significa que no puede obtenerse mediante coerción o condicionamientos indebidos. En segundo lugar, debe ser específico, es decir, relacionado con finalidades concretas y determinadas. Finalmente, debe ser informado e inequívoco, garantizando que el titular comprende plenamente el alcance del tratamiento de datos. Estas condiciones buscan evitar prácticas abusivas y fortalecer la protección de la privacidad digital en el contexto de la transformación tecnológica actual (Reglamento General de Protección de Datos, 2016).

En el ámbito digital, el consentimiento informado enfrenta diversos desafíos derivados de la complejidad tecnológica y el uso masivo de plataformas virtuales. Muchas veces los usuarios aceptan políticas de privacidad sin leer completamente las condiciones relacionadas con el tratamiento de sus datos personales (Lara y Romero, 2023). Esto provoca que numerosas empresas recopilen información sensible sin que exista una comprensión real sobre el alcance de dicha autorización. Además, el uso de algoritmos y herramientas de inteligencia artificial permite procesar grandes volúmenes de datos con fines comerciales, estadísticos o publicitarios. Frente a esta situación, se vuelve indispensable fortalecer la educación digital y promover mecanismos de protección más efectivos para los usuarios.

Por otro lado, el tratamiento de datos personales debe regirse por principios jurídicos orientados a garantizar el respeto de los derechos fundamentales. Entre estos principios destacan la legalidad, finalidad, proporcionalidad, seguridad y confidencialidad. Dichos principios limitan el uso arbitrario de información y obligan a las organizaciones a implementar medidas adecuadas de protección de datos. Asimismo, establecen responsabilidades para las entidades encargadas del tratamiento de información personal, especialmente cuando se producen filtraciones o vulneraciones de seguridad digital. En este contexto, la regulación jurídica busca equilibrar el avance tecnológico con la protección efectiva de la privacidad de las personas (Machuca et al., 2022).

En relación con el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (2021) establece obligaciones específicas para las instituciones públicas y privadas encargadas del tratamiento de información. Entre estas obligaciones se encuentran garantizar el consentimiento del titular, implementar medidas de seguridad y respetar los derechos de acceso, rectificación y eliminación de datos personales. Además, la normativa reconoce la importancia de proteger información sensible relacionada con salud, orientación política, datos biométricos y otros elementos vinculados con la esfera íntima de las personas. Según Giler (2023), el habeas data constituye una garantía fundamental dentro del sistema jurídico ecuatoriano para proteger la privacidad y controlar el tratamiento de información personal.

De igual forma, el consentimiento informado posee especial relevancia dentro de sectores como la salud, la educación y los servicios financieros, debido a que estas áreas manejan grandes cantidades de información sensible. Por ejemplo, en las historias clínicas digitales resulta indispensable garantizar que los pacientes conozcan el uso y

almacenamiento de sus datos médicos. Asimismo, en las plataformas educativas virtuales se recopilan datos relacionados con rendimiento académico, hábitos de aprendizaje y actividad digital de los estudiantes. En consecuencia, las instituciones deben adoptar mecanismos de seguridad y protocolos éticos que protejan adecuadamente la privacidad de los usuarios (Ojeda y Suárez, 2025).

Además, el avance de tecnologías emergentes como el big data y la inteligencia artificial ha transformado la manera en que se procesan los datos personales. Actualmente, numerosos sistemas automatizados son capaces de recopilar información de comportamiento, preferencias y ubicación de los usuarios para elaborar perfiles digitales detallados (Zambrano L. , 2024). Aunque estas herramientas generan beneficios relacionados con personalización y eficiencia, también incrementan riesgos asociados con vigilancia masiva y discriminación algorítmica. Por ello, el consentimiento informado adquiere mayor importancia como mecanismo de control jurídico frente al tratamiento automatizado de datos personales dentro de la economía digital.

Como cierre, el consentimiento informado y el tratamiento de datos personales representan elementos esenciales dentro de la protección de la privacidad digital y los derechos fundamentales en la sociedad contemporánea. El crecimiento de las tecnologías digitales exige fortalecer las normativas jurídicas y promover prácticas responsables relacionadas con el manejo de información personal. Asimismo, resulta necesario fomentar una cultura de transparencia, seguridad y respeto por la autodeterminación informativa de los ciudadanos. En este escenario, el consentimiento informado se consolida como una herramienta indispensable para garantizar equilibrio entre innovación tecnológica, desarrollo digital y protección de la dignidad humana (Rodas et al., 2025).

2.4 Derechos ARCO y garantías de los titulares de datos

Los derechos ARCO constituyen uno de los mecanismos más importantes dentro de la protección de datos personales y la privacidad digital, debido a que permiten a los ciudadanos mantener control sobre el tratamiento de su información personal. La denominación ARCO hace referencia a los derechos de acceso, rectificación, cancelación y oposición, los cuales garantizan que toda persona pueda conocer, modificar, eliminar o limitar el uso de sus datos dentro de sistemas públicos y privados. Estos derechos se desarrollan como respuesta al crecimiento del tratamiento automatizado de información

en la sociedad tecnológica contemporánea. Además, representan una manifestación del derecho fundamental a la autodeterminación informativa y la protección de la dignidad humana. En consecuencia, los derechos ARCO se consolidan como pilares esenciales dentro del Derecho Digital moderno (Ley Orgánica de Protección de Datos Personales, 2021).

En primer lugar, el derecho de acceso permite que los titulares de los datos conozcan qué información personal poseen las entidades públicas o privadas, así como las finalidades para las cuales está siendo utilizada. Este derecho garantiza transparencia en el tratamiento de datos y fortalece la confianza de los ciudadanos dentro de los entornos digitales. Asimismo, posibilita que las personas verifiquen la legalidad del tratamiento de su información y detecten posibles irregularidades relacionadas con el uso indebido de datos personales. Según Giler (2023), el ejercicio del *habeas data* constituye una garantía fundamental que permite a los ciudadanos acceder y controlar la información almacenada sobre ellos dentro de bases de datos públicas y privadas.

Por otra parte, el derecho de rectificación faculta a los titulares para corregir datos inexactos, incompletos o desactualizados que puedan afectar sus derechos e intereses. Este derecho resulta especialmente importante dentro de sistemas digitales automatizados, debido a que errores en la información pueden generar consecuencias negativas relacionadas con acceso a servicios, historial financiero o reputación digital. Además, las entidades responsables del tratamiento de datos tienen la obligación de actualizar la información cuando el titular solicite modificaciones justificadas. En este sentido, la rectificación contribuye a garantizar veracidad y calidad en el manejo de datos personales dentro de la sociedad digital (Zambrano L. , 2024).

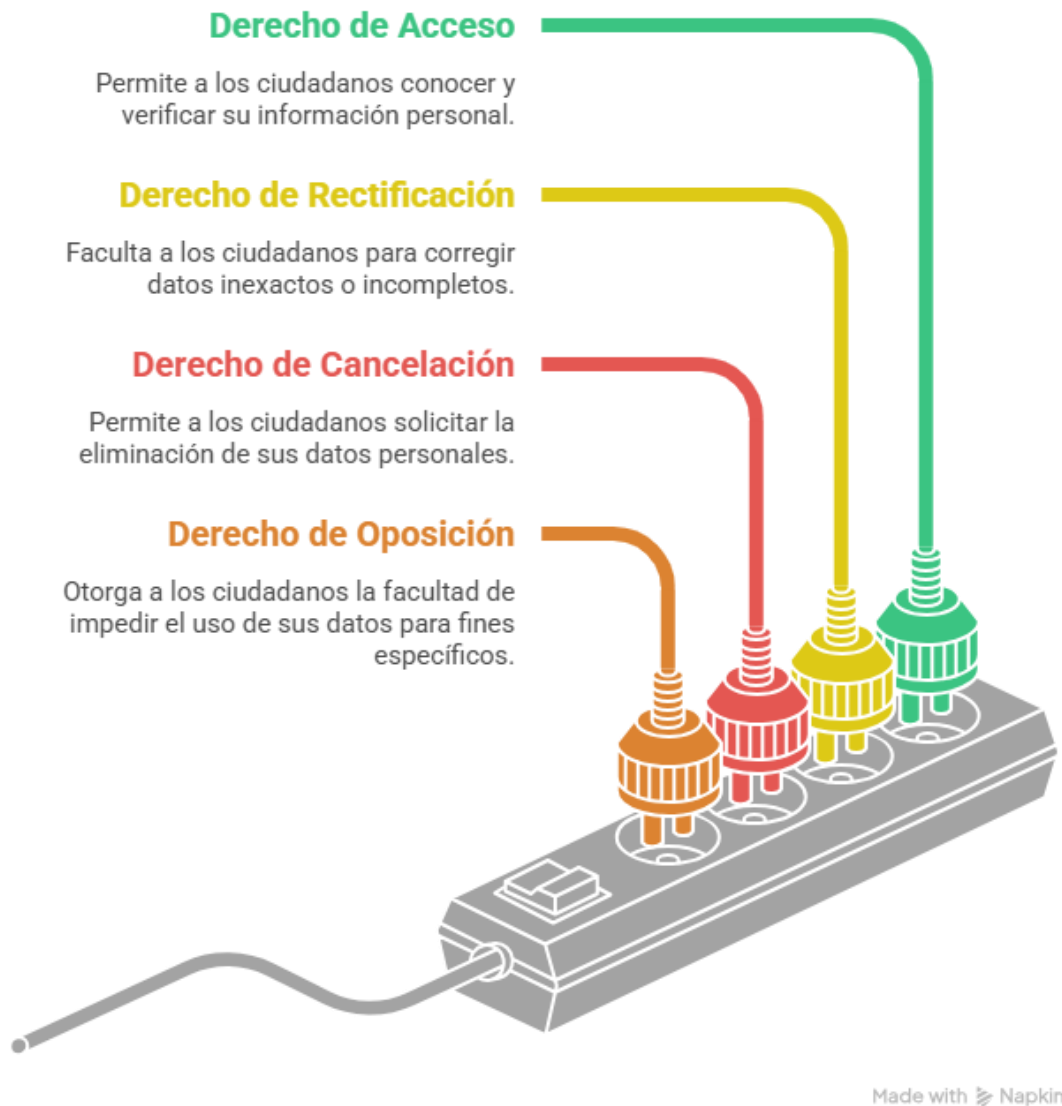
Asimismo, el derecho de cancelación permite que las personas soliciten la eliminación de sus datos personales cuando estos ya no sean necesarios o exista un tratamiento indebido de la información. Este derecho busca evitar la conservación excesiva de datos y disminuir riesgos relacionados con filtraciones, accesos no autorizados y vulneraciones a la privacidad digital. Además, fortalece el principio de minimización de datos y fomenta una gestión responsable de la información personal dentro de los entornos tecnológicos. Como señalan Martínez et al. (2024), la cancelación de datos constituye una herramienta jurídica indispensable para garantizar protección efectiva frente al tratamiento desproporcionado de información personal dentro del ordenamiento jurídico ecuatoriano.

De igual manera, el derecho de oposición otorga a los titulares la facultad de impedir que sus datos personales sean utilizados para determinadas finalidades, especialmente aquellas relacionadas con publicidad, perfilamiento o decisiones automatizadas. Este derecho adquiere gran relevancia dentro de la economía digital actual, debido al uso masivo de algoritmos y herramientas tecnológicas capaces de analizar hábitos, preferencias y comportamientos de los usuarios. En consecuencia, el derecho de oposición permite equilibrar el desarrollo tecnológico con la protección de la privacidad y los derechos fundamentales de las personas (Reglamento General de Protección de Datos, 2016).

Además de los derechos ARCO, los titulares de datos personales cuentan con diversas garantías jurídicas orientadas a proteger su información frente a posibles vulneraciones digitales. Entre estas garantías destacan el derecho a la confidencialidad, la seguridad de la información y la protección frente al acceso no autorizado a datos personales. Asimismo, las legislaciones modernas establecen obligaciones específicas para las entidades responsables del tratamiento de datos, incluyendo medidas de ciberseguridad, protocolos de transparencia y mecanismos de notificación ante incidentes de seguridad informática. Según Guanín (2024) el habeas data no solo protege la intimidad de las personas, sino que también fortalece el control ciudadano sobre la circulación de información dentro de los sistemas digitales contemporáneos.

Figura 4

Derechos ARCO y Protección de Datos



En conclusión, los derechos ARCO y las garantías de los titulares de datos representan instrumentos esenciales para la protección de la privacidad y la seguridad jurídica dentro de la sociedad tecnológica actual. El crecimiento de las plataformas digitales y el tratamiento masivo de información personal han generado nuevos desafíos relacionados con vigilancia, comercialización de datos y vulneraciones a la intimidad. Frente a este escenario, los derechos de acceso, rectificación, cancelación y oposición permiten fortalecer la autodeterminación informativa y promover relaciones más equilibradas entre ciudadanos, empresas e instituciones públicas. Por ello, la protección efectiva de los datos personales constituye uno de los principales retos del Derecho Digital contemporáneo (Molina y Pachano, 2025)

2.5 Regulación internacional y comparada sobre protección de datos

La regulación internacional sobre protección de datos personales ha adquirido gran relevancia dentro del contexto de la sociedad digital contemporánea, debido al crecimiento exponencial del intercambio de información mediante plataformas tecnológicas y redes globales. Actualmente, los datos personales circulan constantemente entre diferentes países, lo que ha generado la necesidad de establecer marcos jurídicos internacionales capaces de garantizar la privacidad y seguridad de los ciudadanos. En este escenario, múltiples organismos internacionales y sistemas jurídicos han desarrollado normativas orientadas a regular el tratamiento de datos personales y proteger los derechos fundamentales relacionados con la intimidad y la autodeterminación informativa. Por ello, la cooperación internacional resulta esencial para enfrentar los desafíos derivados de la globalización tecnológica y el uso masivo de información digital.

Uno de los instrumentos más importantes en materia de protección de datos es el Reglamento General de Protección de Datos de la Unión Europea, conocido como RGPD (Reglamento del Parlamento Europeo y del Consejo, 2016). Esta normativa constituye uno de los modelos regulatorios más influyentes a nivel mundial, debido a que establece principios rigurosos relacionados con consentimiento, transparencia, minimización de datos y responsabilidad proactiva. Además, reconoce derechos específicos para los titulares de los datos, incluyendo acceso, rectificación, eliminación y oposición al tratamiento de información personal. Según Benlonch y Sarrión (2022) la regulación europea representa un referente internacional en la defensa de los derechos fundamentales frente a los desafíos jurídicos derivados de la era digital.

Asimismo, el RGPD incorpora mecanismos relacionados con responsabilidad empresarial y sanciones administrativas para aquellas organizaciones que incumplen las disposiciones sobre protección de datos personales. Esto ha impulsado que numerosas empresas internacionales adopten políticas más estrictas de privacidad y seguridad digital. Además, la normativa europea exige que las entidades informen claramente sobre las finalidades del tratamiento de datos y obtengan consentimiento válido de los usuarios antes de recopilar información personal. En consecuencia, el modelo europeo se ha convertido en una referencia para múltiples legislaciones nacionales en América Latina y otras regiones del mundo (Reglamento General de Protección de Datos, 2016).

Por otra parte, diversos países latinoamericanos han desarrollado marcos normativos orientados a fortalecer la protección de datos personales dentro de sus sistemas jurídicos. Estas regulaciones buscan armonizar estándares internacionales con las necesidades particulares de cada Estado, especialmente frente al crecimiento de la economía digital y el gobierno electrónico (Ojeda y Suárez, 2025). En muchos casos, las legislaciones latinoamericanas han incorporado principios relacionados con legalidad, consentimiento, finalidad y confidencialidad de la información personal. Además, han reconocido mecanismos constitucionales como el habeas data para garantizar el control ciudadano sobre el tratamiento de sus datos personales.

En el caso ecuatoriano, la promulgación de la Ley Orgánica de Protección de Datos Personales (2021) representó un avance significativo dentro del desarrollo normativo nacional en materia de privacidad digital. Esta normativa establece obligaciones específicas para las instituciones encargadas del tratamiento de datos y reconoce derechos fundamentales relacionados con acceso, rectificación, cancelación y oposición. Asimismo, incorpora estándares internacionales orientados a fortalecer la seguridad jurídica y la transparencia dentro de los entornos digitales. Según Rovira y Robles (2023), la legislación ecuatoriana refleja una creciente adaptación de los sistemas jurídicos nacionales frente a los desafíos tecnológicos contemporáneos y la necesidad de proteger la información personal de los ciudadanos.

De igual forma, la regulación comparada demuestra que la protección de datos personales no constituye únicamente un problema tecnológico, sino también una cuestión relacionada con derechos humanos y garantías constitucionales. En numerosos países, la privacidad digital ha sido reconocida como un derecho fundamental vinculado con la dignidad humana y la libertad individual. Esto ha generado que tribunales constitucionales y organismos internacionales desarrollen criterios jurisprudenciales destinados a limitar el tratamiento abusivo de información personal. Además, se ha fortalecido la idea de que los ciudadanos deben mantener control sobre sus datos dentro de plataformas digitales y sistemas automatizados (Lara y Romero, 2023).

Por otro lado, la cooperación internacional en materia de ciberseguridad y protección de datos resulta indispensable para enfrentar delitos informáticos y vulneraciones transnacionales de privacidad. Instrumentos como el Convenio de Budapest sobre ciberdelincuencia han promovido mecanismos de colaboración entre Estados para combatir actividades ilícitas relacionadas con acceso indebido a sistemas informáticos y

uso ilegal de información personal. Estas iniciativas internacionales buscan fortalecer capacidades institucionales y establecer estándares comunes frente a amenazas digitales que trascienden fronteras nacionales. Como señalan Cajahuanca (2025), las ciencias jurídicas enfrentan actualmente el desafío de adaptar sus estructuras tradicionales a fenómenos tecnológicos globales que requieren respuestas normativas coordinadas.

Asimismo, la regulación internacional y comparada evidencia la importancia de implementar principios éticos y jurídicos en el desarrollo de tecnologías emergentes como inteligencia artificial, big data e internet de las cosas. Estas herramientas permiten recopilar y procesar grandes volúmenes de información personal mediante algoritmos automatizados, lo que incrementa riesgos relacionados con discriminación, vigilancia masiva y pérdida de privacidad (Constante y López, 2025). Debido a ello, múltiples organismos internacionales han promovido recomendaciones orientadas a garantizar transparencia algorítmica, protección de derechos digitales y responsabilidad en el tratamiento automatizado de datos personales.

A manera de conclusión, la regulación internacional y comparada sobre protección de datos demuestra que la privacidad digital constituye uno de los principales retos jurídicos de la sociedad tecnológica actual. El crecimiento de los flujos globales de información y el desarrollo acelerado de tecnologías digitales exigen marcos normativos sólidos capaces de garantizar equilibrio entre innovación y protección de derechos fundamentales. En este contexto, las experiencias internacionales permiten identificar buenas prácticas y fortalecer los sistemas nacionales de protección de datos personales. Por ello, la cooperación jurídica internacional y la armonización normativa continuarán desempeñando un papel fundamental dentro del desarrollo del Derecho Digital contemporáneo (Molina y Pachano, 2025).

2.6 Protección de datos en redes sociales y plataformas digitales

La protección de datos personales en redes sociales y plataformas digitales constituye uno de los principales desafíos jurídicos de la sociedad tecnológica contemporánea, debido al crecimiento masivo del intercambio de información en entornos virtuales. Actualmente, millones de usuarios comparten diariamente fotografías, videos, datos biométricos, ubicaciones y preferencias personales mediante aplicaciones y redes sociales. Esta situación ha generado preocupaciones relacionadas con privacidad, seguridad informática y uso indebido de información personal por parte de empresas tecnológicas y terceros no

autorizados. En consecuencia, la regulación jurídica busca establecer mecanismos que permitan garantizar el respeto de los derechos fundamentales dentro de los espacios digitales. Según Rivera y Maldonado (2023), la vulneración del derecho a la privacidad se ha intensificado considerablemente con el desarrollo de plataformas digitales y redes sociales en Ecuador.

Las redes sociales recopilan grandes cantidades de información personal mediante procesos automatizados de almacenamiento y análisis de datos. Estas plataformas utilizan información relacionada con hábitos de navegación, intereses, ubicación geográfica y comportamiento digital de los usuarios para personalizar contenidos y estrategias publicitarias. Sin embargo, muchas veces las personas desconocen el alcance real del tratamiento de sus datos y las implicaciones derivadas de aceptar políticas de privacidad extensas y complejas. Además, el uso de algoritmos y herramientas de inteligencia artificial incrementa la capacidad de perfilamiento digital y vigilancia masiva dentro de internet (Reglamento General de Protección de Datos, 2016).

Asimismo, la privacidad digital se encuentra estrechamente vinculada con el derecho a la intimidad y la protección de la dignidad humana en los entornos virtuales. Las publicaciones realizadas en redes sociales pueden exponer aspectos sensibles de la vida personal, familiar y profesional de los usuarios, generando riesgos relacionados con discriminación, extorsión, robo de identidad y ciberacoso. Por ello, resulta indispensable que las plataformas digitales implementen políticas de seguridad y mecanismos transparentes de tratamiento de información personal. Según Lara y Romero (2023), el equilibrio entre libertad de expresión y derecho a la privacidad constituye uno de los principales retos jurídicos derivados del desarrollo de la comunicación digital contemporánea.

Por otra parte, uno de los principales problemas relacionados con las plataformas digitales es la recopilación excesiva de datos personales sin un consentimiento plenamente informado. En numerosas ocasiones, los usuarios aceptan condiciones de uso sin comprender cómo serán utilizados sus datos ni qué terceros tendrán acceso a dicha información. Esta situación limita la autodeterminación informativa y favorece prácticas de comercialización masiva de datos dentro de la economía digital. Además, las empresas tecnológicas pueden transferir información personal entre diferentes países, dificultando el control jurídico sobre el tratamiento de datos y la protección efectiva de la privacidad (Molina y Pachano, 2025).

De igual manera, las plataformas digitales enfrentan constantes amenazas relacionadas con ciberataques y vulneraciones de seguridad informática. Las filtraciones masivas de datos personales representan uno de los riesgos más graves para la privacidad digital, debido a que pueden comprometer información financiera, médica y personal de millones de usuarios. Frente a ello, las organizaciones tecnológicas tienen la obligación de implementar sistemas de ciberseguridad que permitan prevenir accesos no autorizados y garantizar confidencialidad en el tratamiento de información. Según Gonzalo et al. (2025) las buenas prácticas de protección de datos deben incluir protocolos técnicos y organizativos destinados a fortalecer la seguridad de la información en entornos digitales.

Además, las redes sociales poseen una gran influencia dentro de la formación de opiniones públicas, relaciones sociales y dinámicas económicas contemporáneas. Debido a ello, la utilización indebida de datos personales puede afectar no solo la privacidad individual, sino también procesos democráticos y derechos colectivos. Casos relacionados con manipulación algorítmica, difusión de noticias falsas y utilización política de datos personales han demostrado la necesidad de fortalecer mecanismos regulatorios dentro del ámbito digital. En consecuencia, la protección de datos personales adquiere relevancia no únicamente desde una perspectiva individual, sino también social y democrática (Becerra et al., 2024).

En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (2021) establece principios y obligaciones aplicables al tratamiento de información dentro de plataformas digitales y redes sociales. Esta normativa reconoce derechos relacionados con acceso, rectificación, eliminación y oposición al tratamiento de datos personales, fortaleciendo la protección jurídica de los usuarios frente a posibles vulneraciones digitales. Asimismo, impone responsabilidades específicas a las entidades encargadas del manejo de información personal, especialmente en relación con transparencia y consentimiento informado. Según Gutiérrez (2022), el reconocimiento de la protección de datos como derecho humano exige mecanismos eficaces que permitan controlar el tratamiento de información dentro de la sociedad digital ecuatoriana.

Por otro lado, el avance tecnológico ha permitido el desarrollo de nuevas plataformas digitales basadas en inteligencia artificial, reconocimiento facial y análisis predictivo de comportamiento. Estas herramientas incrementan la capacidad de recopilación y procesamiento de datos personales mediante sistemas automatizados capaces de identificar patrones y preferencias de los usuarios. Aunque estas tecnologías ofrecen

ventajas relacionadas con personalización y eficiencia, también generan preocupaciones sobre vigilancia permanente y pérdida progresiva de privacidad. En consecuencia, resulta necesario establecer límites éticos y jurídicos que regulen el uso responsable de tecnologías emergentes dentro de los entornos digitales (Jiménez y Pincay, 2024)

Asimismo, la educación digital desempeña un papel fundamental dentro de la protección de datos en redes sociales y plataformas virtuales. Muchas vulneraciones a la privacidad ocurren debido al desconocimiento de los usuarios sobre riesgos relacionados con publicación de información sensible, configuración de privacidad y uso de aplicaciones digitales (Bonilla, 2025). Por ello, resulta indispensable promover programas de alfabetización digital orientados a fortalecer capacidades relacionadas con seguridad informática y protección de datos personales. Además, la formación ciudadana en materia digital contribuye a desarrollar un uso más responsable y consciente de las tecnologías contemporáneas.

De igual forma, las empresas tecnológicas y administradores de plataformas digitales deben asumir responsabilidades éticas relacionadas con el tratamiento de datos personales de sus usuarios. Esto implica implementar políticas claras de privacidad, garantizar transparencia en el uso de información y adoptar medidas efectivas de protección frente a amenazas cibernéticas. Además, deben respetar principios relacionados con minimización de datos, confidencialidad y consentimiento informado. Según Aguilar et al. (2022), la protección de datos personales requiere no solo regulación jurídica, sino también compromiso institucional y responsabilidad tecnológica frente a los riesgos derivados del entorno digital.

En síntesis, la protección de datos en redes sociales y plataformas digitales representa uno de los principales retos del Derecho Digital contemporáneo. El crecimiento acelerado de la tecnología y la constante circulación de información personal exigen mecanismos jurídicos capaces de equilibrar innovación tecnológica, libertad de comunicación y protección de derechos fundamentales (Giler, 2023). En este contexto, resulta indispensable fortalecer normativas, sistemas de ciberseguridad y políticas educativas orientadas a garantizar privacidad y seguridad dentro de los espacios virtuales. Por ello, la protección de datos personales continuará consolidándose como un elemento esencial para el desarrollo responsable de la sociedad digital moderna.

2.7 Transferencia internacional de datos y almacenamiento en la nube

La transferencia internacional de datos y el almacenamiento en la nube permiten la circulación global de información mediante plataformas y servicios digitales, facilitando el acceso y procesamiento remoto de datos. No obstante, esta dinámica también genera desafíos relacionados con privacidad, soberanía digital y protección de derechos fundamentales. Frente a ello, los sistemas jurídicos modernos han impulsado regulaciones orientadas a controlar la circulación transfronteriza de datos y garantizar seguridad digital. Según Muñiz (2023), la transformación tecnológica global exige nuevas estrategias jurídicas y diplomáticas capaces de responder a los desafíos derivados del intercambio internacional de información digital.

La transferencia internacional de datos personales ocurre cuando información relacionada con una persona es enviada, almacenada o procesada fuera del país donde fue recopilada originalmente. Este proceso puede producirse mediante plataformas digitales, redes sociales, servicios financieros, aplicaciones móviles o sistemas de computación en la nube. Además, muchas compañías tecnológicas operan mediante infraestructuras globales que distribuyen información en centros de datos ubicados en distintas regiones del mundo. Según Aguilar et al. (2022), el crecimiento de la economía digital y la globalización tecnológica han incrementado considerablemente los riesgos asociados con el tratamiento transfronterizo de datos personales, especialmente en materia de privacidad y seguridad informática.

Asimismo, el almacenamiento en la nube permite guardar información en servidores remotos administrados por proveedores tecnológicos especializados, facilitando acceso flexible y reducción de costos operativos para empresas e instituciones. Esta modalidad tecnológica ofrece ventajas relacionadas con eficiencia, escalabilidad y disponibilidad permanente de información digital. Sin embargo, también genera preocupaciones sobre control de los datos, acceso por terceros y vulnerabilidad frente a ataques cibernéticos. Debido a ello, las organizaciones deben adoptar medidas técnicas y jurídicas orientadas a garantizar confidencialidad, integridad y disponibilidad de la información almacenada en entornos virtuales (Mendoza H. , 2024).

Por otra parte, uno de los principales problemas relacionados con la transferencia internacional de datos es la diferencia entre los niveles de protección jurídica existentes en cada país. Mientras algunas naciones cuentan con normativas estrictas sobre

privacidad y protección de datos personales, otras poseen regulaciones limitadas o insuficientes para garantizar derechos digitales. Esta situación puede provocar que la información transferida quede expuesta a usos indebidos, vigilancia masiva o tratamiento arbitrario por parte de entidades extranjeras. En consecuencia, numerosos sistemas jurídicos han establecido requisitos específicos para autorizar transferencias internacionales de datos únicamente hacia países que garanticen niveles adecuados de protección (Reglamento General de Protección de Datos, 2016)

De igual manera, la protección jurídica de los datos almacenados en la nube requiere mecanismos de seguridad informática capaces de prevenir accesos no autorizados y vulneraciones digitales. Los ciberataques dirigidos contra servidores y plataformas tecnológicas pueden comprometer información sensible relacionada con identidad, finanzas, salud o actividad profesional de los usuarios. Frente a ello, las empresas proveedoras de servicios en la nube deben implementar protocolos avanzados de cifrado, autenticación y gestión de riesgos tecnológicos. Según Gonzalo et al. (2025), las buenas prácticas de protección de datos personales exigen fortalecer continuamente las medidas de ciberseguridad dentro de los entornos digitales y sistemas de almacenamiento virtual.

En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (2021) incorpora disposiciones relacionadas con transferencia internacional de datos y responsabilidades de quienes realizan tratamiento de información fuera del territorio nacional. La normativa establece que las transferencias internacionales deben respetar principios de legalidad, consentimiento y seguridad, garantizando que los datos personales reciban niveles adecuados de protección. Además, reconoce la importancia de implementar mecanismos de supervisión y control frente al uso de servicios digitales globales. Según Molina y Pachano (2025), el fortalecimiento del marco normativo ecuatoriano resulta indispensable para enfrentar los desafíos derivados del almacenamiento digital y la circulación internacional de información personal.

En definitiva, la transferencia internacional de datos y el almacenamiento en la nube constituyen elementos esenciales dentro del funcionamiento de la economía digital y la sociedad tecnológica contemporánea. Aunque estas herramientas ofrecen importantes beneficios relacionados con conectividad, innovación y eficiencia operativa, también generan riesgos significativos para la privacidad y seguridad de la información personal. En este contexto, resulta necesario fortalecer marcos regulatorios internacionales, promover cooperación jurídica entre Estados e implementar políticas tecnológicas

responsables orientadas a proteger los derechos fundamentales de los ciudadanos. Según Cajahuanca (2025), las ciencias jurídicas enfrentan actualmente el desafío de adaptar sus estructuras tradicionales frente a fenómenos tecnológicos globales que transforman permanentemente las dinámicas de tratamiento y circulación de datos personales.

2.8 Responsabilidad jurídica por vulneración de datos personales

La responsabilidad jurídica por vulneración de datos personales se ha convertido en uno de los temas más importantes del Derecho Digital contemporáneo, debido al aumento de filtraciones de información, accesos no autorizados y uso indebido de datos en entornos tecnológicos. Actualmente, instituciones públicas y privadas manejan grandes volúmenes de información personal que pueden verse afectados por fallas de seguridad o prácticas negligentes. Frente a ello, los sistemas normativos modernos han establecido mecanismos de responsabilidad destinados a proteger la privacidad y garantizar reparación ante vulneraciones digitales. Según Zambrano et al. (2024), el incumplimiento de las obligaciones relacionadas con protección de datos personales puede generar importantes consecuencias civiles y jurídicas para las organizaciones responsables del tratamiento de información.

La vulneración de datos personales puede producirse mediante diversas conductas, entre ellas accesos ilegítimos a sistemas informáticos, filtraciones masivas de información, pérdida de archivos digitales o difusión no autorizada de datos sensibles. Asimismo, los riesgos aumentan considerablemente debido al uso masivo de tecnologías digitales y plataformas virtuales que recopilan información de millones de usuarios. En consecuencia, las organizaciones deben implementar medidas técnicas y administrativas orientadas a prevenir incidentes de seguridad y garantizar confidencialidad en el tratamiento de datos personales. Según Gonzalo et al. (2025), las buenas prácticas de protección de datos requieren mecanismos permanentes de supervisión, ciberseguridad y control institucional que permitan minimizar riesgos relacionados con vulneraciones digitales.

Asimismo, la responsabilidad jurídica derivada de vulneraciones de datos personales puede manifestarse en diferentes ámbitos, incluyendo responsabilidad civil, administrativa e incluso penal. La responsabilidad civil surge cuando el tratamiento indebido de información ocasiona daños materiales o morales a los titulares de los datos, quienes pueden exigir reparación e indemnización. Por otro lado, la responsabilidad

administrativa implica sanciones impuestas por autoridades competentes debido al incumplimiento de normas relacionadas con privacidad y seguridad de la información. Además, determinadas conductas pueden constituir delitos informáticos cuando existe acceso ilícito, manipulación fraudulenta o comercialización ilegal de datos personales (Código Orgánico Integral Penal (COIP), 2014)

De igual manera, la responsabilidad jurídica de las entidades encargadas del tratamiento de datos se encuentra vinculada con el cumplimiento de principios relacionados con legalidad, transparencia, consentimiento y seguridad informática. Esto significa que las organizaciones deben adoptar medidas preventivas destinadas a proteger información personal frente a amenazas tecnológicas y accesos no autorizados. Además, tienen la obligación de informar oportunamente sobre incidentes de seguridad que puedan comprometer datos de los usuarios. Según Rovira y Robles (2023), la promulgación de la Ley Orgánica de Protección de Datos Personales (2021) en Ecuador fortaleció las obligaciones de las instituciones públicas y privadas respecto al tratamiento responsable de información personal dentro del entorno digital.

Por otra parte, el avance de tecnologías como inteligencia artificial, big data y almacenamiento en la nube ha incrementado los riesgos asociados con vulneraciones de privacidad y uso indebido de información personal. Muchas plataformas digitales recopilan grandes cantidades de datos relacionados con hábitos de navegación, ubicación, preferencias y comportamiento de los usuarios. Cuando estos sistemas presentan fallas de seguridad o son utilizados de manera negligente, los titulares de los datos pueden sufrir afectaciones relacionadas con robo de identidad, fraude financiero o exposición indebida de información sensible. Frente a ello, resulta indispensable fortalecer mecanismos regulatorios y protocolos de ciberseguridad orientados a prevenir incidentes digitales (Mendoza H. , 2024).

En el ámbito internacional, múltiples legislaciones han desarrollado estándares orientados a establecer responsabilidad frente al tratamiento indebido de datos personales. El Reglamento General de Protección de Datos de la Unión Europea, por ejemplo, incorpora sanciones económicas significativas para las empresas que incumplen obligaciones relacionadas con privacidad y protección de información. Asimismo, exige la implementación de medidas técnicas adecuadas y la notificación inmediata de vulneraciones de seguridad que afecten datos personales. Según Benlonch y Sarrión

(2022), los sistemas regulatorios contemporáneos buscan equilibrar innovación tecnológica y protección efectiva de los derechos fundamentales dentro de la era digital.

En el caso ecuatoriano, la Ley Orgánica de Protección de Datos Personales (2021) establece obligaciones específicas para responsables y encargados del tratamiento de información. Entre estas obligaciones destacan garantizar confidencialidad, aplicar medidas de seguridad y respetar los derechos de acceso, rectificación, cancelación y oposición de los titulares de los datos. Además, la normativa contempla mecanismos sancionatorios aplicables cuando se producen incumplimientos relacionados con tratamiento indebido de información personal. Según Gutiérrez (2022), la protección de datos personales debe entenderse como un derecho humano que requiere estructuras normativas sólidas capaces de garantizar responsabilidad efectiva frente a vulneraciones digitales.

Asimismo, la responsabilidad jurídica no solo recae sobre grandes empresas tecnológicas, sino también sobre instituciones educativas, entidades financieras, organismos públicos y cualquier organización que administre datos personales. Todas estas entidades poseen el deber de implementar políticas internas de protección de datos y capacitar a su personal en materia de privacidad y seguridad informática. Además, deben desarrollar protocolos de respuesta rápida frente a incidentes relacionados con filtraciones o accesos indebidos a información sensible. En consecuencia, la cultura organizacional relacionada con protección de datos se convierte en un elemento esencial para prevenir responsabilidades jurídicas dentro del entorno digital contemporáneo (Molina y Pachano, 2025).

Para finalizar, la responsabilidad jurídica por vulneración de datos personales representa una herramienta fundamental para garantizar el respeto de los derechos digitales y fortalecer la confianza dentro de la sociedad tecnológica actual. El crecimiento constante del intercambio de información mediante plataformas digitales exige mecanismos regulatorios eficaces capaces de prevenir abusos y sancionar conductas que afecten privacidad y seguridad de los ciudadanos (Machuca et al., 2022). En este contexto, la implementación de medidas preventivas, sistemas de ciberseguridad y marcos normativos adecuados resulta indispensable para proteger la información personal frente a amenazas digitales. Por ello, la responsabilidad jurídica continuará consolidándose como uno de los principales pilares dentro del desarrollo del Derecho Digital contemporáneo.



CAPÍTULO 3

**Inteligencia artificial y
responsabilidad jurídica**

3.1 Concepto y clasificación de la inteligencia artificial

La inteligencia artificial representa uno de los avances tecnológicos más importantes de la sociedad digital contemporánea, debido a que permite que los sistemas informáticos desarrollen tareas asociadas al razonamiento, aprendizaje y toma de decisiones humanas. Su incorporación en ámbitos administrativos, económicos, jurídicos y sociales ha generado nuevas dinámicas de interacción tecnológica y desafíos regulatorios. Según Cajahuanca (2025), señala que las ciencias jurídicas deben adaptarse al crecimiento acelerado de las tecnologías inteligentes, mientras Jiménez y Pincay (2024) sostienen que el Derecho debe fortalecer mecanismos de protección frente a los riesgos derivados de la automatización y el procesamiento masivo de información.

Desde una perspectiva conceptual, la inteligencia artificial puede entenderse como el conjunto de sistemas tecnológicos diseñados para simular procesos cognitivos humanos mediante algoritmos y modelos computacionales avanzados. Dichos sistemas poseen la capacidad de analizar datos, identificar patrones y ejecutar acciones automatizadas con distintos niveles de autonomía. En este sentido, Muñiz (2023) explica que la transformación digital ha impulsado una nueva etapa de desarrollo tecnológico basada en la automatización inteligente y el uso masivo de datos. De igual manera, Forero (2023) señala que la expansión de herramientas digitales basadas en algoritmos modifica profundamente las relaciones sociales, económicas y jurídicas dentro de la era digital, generando nuevos desafíos regulatorios para los Estados.

Por otra parte, la clasificación de la inteligencia artificial puede realizarse considerando distintos criterios técnicos y funcionales. Una de las divisiones más conocidas diferencia entre inteligencia artificial débil e inteligencia artificial fuerte. La IA débil se encuentra diseñada para ejecutar tareas específicas, como asistentes virtuales, sistemas de recomendación o motores de búsqueda, mientras que la IA fuerte busca reproducir capacidades cognitivas humanas de manera integral. Según Cornejo (2023), la modernización tecnológica ha incrementado el uso de sistemas automatizados en múltiples instituciones públicas y privadas, permitiendo una mayor eficiencia en la gestión de procesos. Además, Melgar et al. (2026) afirman que las nuevas tecnologías inteligentes contribuyen significativamente a la optimización administrativa mediante la automatización de tareas complejas y repetitivas.

Asimismo, otra clasificación importante distingue la inteligencia artificial reactiva, la inteligencia artificial con memoria limitada, la teoría de la mente y la inteligencia artificial autoconsciente. La IA reactiva únicamente responde a estímulos inmediatos sin almacenar experiencias previas, mientras que los sistemas con memoria limitada pueden utilizar datos históricos para mejorar sus respuestas. En relación con ello, Vargas (2021), manifiesta que el desarrollo del gobierno digital depende cada vez más de tecnologías capaces de procesar grandes cantidades de información de manera automatizada. Del mismo modo, Jáuregui (2025) considera que la transformación digital del Estado exige la incorporación progresiva de sistemas inteligentes orientados a mejorar la eficiencia y la toma de decisiones institucionales.

En el ámbito jurídico, la clasificación de la inteligencia artificial adquiere especial relevancia debido a los diferentes niveles de riesgo que presentan los sistemas automatizados. Algunas herramientas de IA poseen funciones de asistencia básica, mientras que otras pueden influir directamente en decisiones relacionadas con derechos fundamentales, seguridad o acceso a servicios públicos. Por ello, Benlonch y Sarrión (2022) advierten que las tecnologías digitales generan tensiones importantes respecto a la protección de los derechos fundamentales dentro de los entornos virtuales. De igual manera, Dueñas et al. (2025) sostienen que los sistemas tecnológicos modernos deben desarrollarse respetando principios constitucionales vinculados con la dignidad humana, la igualdad y la protección jurídica de las personas.

Además, la inteligencia artificial también puede clasificarse según su nivel de aprendizaje y autonomía. En este sentido, existen sistemas basados en aprendizaje supervisado, aprendizaje no supervisado y aprendizaje profundo o deep learning, los cuales permiten mejorar continuamente el rendimiento de las máquinas mediante redes neuronales artificiales. Según Miranda et al. (2025), la implementación de tecnologías digitales avanzadas fortalece los procesos de eficiencia y transparencia dentro de las instituciones modernas. Igualmente, Morón et al. (2025) destacan que las herramientas tecnológicas inteligentes representan uno de los principales mecanismos de modernización administrativa y transformación digital en la actualidad (Morón et al., 2025).

Como resultado final, el avance de la inteligencia artificial evidencia la necesidad de construir marcos regulatorios capaces de equilibrar innovación tecnológica y protección jurídica. Aunque la IA ofrece importantes beneficios en productividad, automatización y

gestión de información, también plantea riesgos relacionados con discriminación algorítmica, vulneración de datos personales y falta de transparencia en la toma de decisiones automatizadas. En consecuencia, Cajahuanca (2025) afirma que el Derecho debe evolucionar constantemente para responder a los desafíos derivados de las tecnologías emergentes. Asimismo, Jiménez y Pincay (2024) consideran que los derechos digitales constituyen una garantía esencial frente al impacto de las nuevas tecnologías dentro de la sociedad de la información.

3.2 Inteligencia artificial y automatización de decisiones

La inteligencia artificial ha transformado los procesos de toma de decisiones dentro de la sociedad digital contemporánea, ya que diversas instituciones públicas y privadas utilizan sistemas automatizados para analizar grandes volúmenes de información de manera rápida y eficiente. Estos mecanismos se basan en algoritmos y modelos predictivos que permiten reemplazar parcialmente la intervención humana en determinadas actividades. Según Muñiz (2023), la expansión tecnológica ha generado nuevas dinámicas de interacción entre los sistemas digitales y la gestión institucional, modificando progresivamente la estructura tradicional de los procesos administrativos y jurídicos.

Asimismo, la automatización de decisiones mediante inteligencia artificial se encuentra presente en ámbitos como la banca, la salud, la educación, el comercio electrónico y la administración pública. Estos sistemas permiten optimizar tiempos, reducir errores operativos y aumentar la eficiencia organizacional mediante el procesamiento automatizado de datos. En relación con ello, Cornejo (2023) sostiene que la modernización de la gestión pública depende en gran medida de la incorporación de herramientas tecnológicas capaces de agilizar procedimientos y mejorar la capacidad de respuesta institucional. Además, Melgar et al. (2026) consideran que la transformación digital fortalece la eficiencia administrativa al permitir una gestión automatizada más precisa y organizada dentro de las instituciones contemporáneas.

Figura 5

¿Cómo implementar la inteligencia artificial de manera responsable?



Por otra parte, los sistemas de inteligencia artificial funcionan a través de algoritmos que recopilan, procesan e interpretan información con el objetivo de identificar patrones y generar resultados automatizados. Estos algoritmos pueden aprender mediante experiencias previas gracias al uso de técnicas de aprendizaje automático o machine learning. Según Vargas (2021), el desarrollo del gobierno digital requiere tecnologías avanzadas que faciliten la automatización de procesos y la gestión eficiente de datos dentro del aparato estatal. En consecuencia, la IA se convierte en una herramienta estratégica para fortalecer la productividad y mejorar los servicios ofrecidos a la ciudadanía.

Sin embargo, la automatización de decisiones también genera importantes desafíos jurídicos y éticos relacionados con la transparencia y la responsabilidad de los sistemas inteligentes. En muchos casos, las decisiones emitidas por algoritmos pueden resultar difíciles de comprender para los usuarios debido a la complejidad técnica de los modelos computacionales utilizados. En este sentido, Jiménez y Pincay (2024) afirman que el crecimiento acelerado de las tecnologías digitales obliga a replantear mecanismos de protección jurídica frente a los riesgos derivados de la automatización tecnológica. Del mismo modo, Benlonch y Sarrión (2022) advierten que las nuevas tecnologías pueden afectar derechos fundamentales cuando las decisiones automatizadas carecen de supervisión humana adecuada.

Además, uno de los principales problemas asociados a la inteligencia artificial consiste en la posible existencia de sesgos algorítmicos dentro de los sistemas automatizados.

Dichos sesgos pueden originarse por errores en la programación, datos incompletos o información discriminatoria utilizada durante el entrenamiento de los algoritmos. Como consecuencia, determinadas personas o grupos sociales podrían verse perjudicados por decisiones automatizadas injustas o desproporcionadas. Por ello, Dueñas et al. (2025) sostienen que el desarrollo tecnológico debe garantizar el respeto de los principios constitucionales relacionados con la igualdad, la dignidad humana y la no discriminación dentro de los entornos digitales.

De igual manera, la automatización de decisiones plantea desafíos importantes en materia de protección de datos personales y privacidad digital. Los sistemas de inteligencia artificial requieren grandes cantidades de información para funcionar correctamente, lo que implica riesgos relacionados con el tratamiento masivo de datos sensibles. En relación con ello, Aguilar et al. (2022) manifiestan que la protección de datos personales constituye uno de los principales retos jurídicos de la sociedad digital contemporánea, especialmente frente al crecimiento acelerado de tecnologías automatizadas. Asimismo, Mendoza (2024) señala que el entorno digital exige mecanismos regulatorios capaces de proteger eficazmente la privacidad y los derechos de los usuarios frente al uso intensivo de información personal.

En el ámbito de la administración pública, la inteligencia artificial permite automatizar procedimientos relacionados con atención ciudadana, gestión documental, seguridad informática y análisis de información gubernamental. Estas herramientas contribuyen a fortalecer la eficiencia institucional y optimizar recursos estatales. Según Miranda et al. (2025), el gobierno electrónico mejora la transparencia y la eficacia administrativa mediante la implementación de tecnologías digitales avanzadas. Además, Chuquicahua et al. (2025) consideran que los modelos de gobierno digital representan mecanismos fundamentales para modernizar la gestión pública y mejorar la calidad de los servicios ofrecidos por el Estado.

No obstante, la utilización de sistemas automatizados en funciones públicas y privadas requiere mecanismos de control jurídico que permitan supervisar las decisiones emitidas por inteligencia artificial. La ausencia de regulación específica podría generar escenarios de inseguridad jurídica, especialmente cuando las decisiones automatizadas afectan derechos fundamentales de las personas. En este contexto, Gamboa et al. (2024) sostienen que las garantías constitucionales cumplen un papel esencial en la tutela de los derechos

frente a las nuevas tecnologías digitales. Por ello, resulta indispensable que los Estados desarrollen marcos normativos orientados a garantizar transparencia, supervisión humana y rendición de cuentas en el uso de inteligencia artificial.

Para concluir, la relación entre inteligencia artificial y automatización de decisiones evidencia la necesidad de equilibrar innovación tecnológica y protección jurídica dentro de la sociedad digital. Aunque los sistemas inteligentes ofrecen importantes ventajas relacionadas con eficiencia, rapidez y optimización de procesos, también generan riesgos asociados con discriminación, privacidad y responsabilidad legal. En consecuencia, Cajahuanca (2025) afirma que las ciencias jurídicas deben adaptarse constantemente a los cambios tecnológicos emergentes mediante regulaciones modernas y mecanismos efectivos de protección de derechos. De esta manera, la inteligencia artificial podrá desarrollarse de forma responsable y compatible con los principios fundamentales del Estado de Derecho.

3.3 Responsabilidad civil y penal derivada del uso de IA

El avance de la inteligencia artificial ha generado importantes debates jurídicos relacionados con la responsabilidad civil y penal derivada del uso de sistemas automatizados. La incorporación de herramientas inteligentes en actividades económicas, administrativas y sociales ha incrementado el riesgo de daños materiales, morales y vulneraciones de derechos fundamentales ocasionados por decisiones automatizadas. Frente a ello, surge la necesidad de determinar quién debe asumir responsabilidad jurídica por los perjuicios causados por la inteligencia artificial. Según Cajahuanca (2025), el crecimiento acelerado de las tecnologías digitales obliga al Derecho a desarrollar nuevos mecanismos regulatorios capaces de responder a los desafíos contemporáneos vinculados con la automatización y el uso de algoritmos inteligentes.

Desde la perspectiva civil, la responsabilidad derivada del uso de inteligencia artificial se relaciona con la obligación de reparar daños ocasionados por sistemas automatizados. Estos daños pueden producirse como consecuencia de errores de programación, fallos técnicos, decisiones discriminatorias o uso indebido de información personal. En consecuencia, la responsabilidad puede recaer sobre desarrolladores, fabricantes, propietarios o usuarios de los sistemas inteligentes, dependiendo de las circunstancias específicas del caso. Forero (2023) sostiene que el entorno digital contemporáneo ha

transformado profundamente las relaciones jurídicas tradicionales, generando nuevos conflictos vinculados con el uso de plataformas y tecnologías automatizadas.

Asimismo, uno de los principales desafíos de la responsabilidad civil en inteligencia artificial consiste en determinar el nexo causal entre la actuación del sistema automatizado y el daño producido. A diferencia de otros mecanismos tecnológicos convencionales, muchos sistemas de IA poseen capacidades de aprendizaje autónomo que dificultan identificar con precisión el origen del error o la decisión perjudicial. En este sentido, Zambrano et al. (2024) afirman que el incumplimiento de normas relacionadas con el tratamiento y protección de datos puede generar importantes consecuencias civiles dentro del entorno digital. Además, Mendoza (2024) considera que la regulación jurídica de la privacidad y de las tecnologías digitales requiere mecanismos claros de atribución de responsabilidad frente a vulneraciones ocasionadas por herramientas tecnológicas avanzadas.

Por otra parte, la inteligencia artificial también plantea importantes desafíos en materia de responsabilidad penal, especialmente cuando los sistemas automatizados son utilizados para ejecutar conductas ilícitas o facilitar actividades delictivas. La utilización de IA en fraudes informáticos, manipulación de datos, ciberataques o vulneración de sistemas digitales representa una preocupación creciente dentro de los ordenamientos jurídicos modernos. Según el Código Orgánico Integral Penal (2014), las conductas relacionadas con delitos informáticos y vulneraciones tecnológicas pueden generar sanciones penales cuando afectan derechos protegidos por la legislación ecuatoriana.

Además, la utilización de inteligencia artificial dentro de entornos digitales incrementa el riesgo de afectaciones relacionadas con la privacidad y el tratamiento indebido de datos personales. Los sistemas inteligentes procesan grandes volúmenes de información para ejecutar funciones automatizadas, lo que puede derivar en vulneraciones de confidencialidad o acceso no autorizado a información sensible. Aguilar et al. (2022) sostienen que la protección de datos personales constituye uno de los principales desafíos jurídicos de la era digital, especialmente frente al crecimiento de tecnologías automatizadas basadas en análisis masivo de información. Del mismo modo, Rivera y Maldonado (2023) advierten que las tecnologías digitales pueden afectar gravemente el derecho a la privacidad cuando no existen controles adecuados sobre el uso de datos personales dentro de plataformas tecnológicas.

En relación con ello, la responsabilidad penal derivada del uso de IA también involucra problemas relacionados con la autoría y culpabilidad. Debido a que los sistemas inteligentes pueden actuar con cierto grado de autonomía, resulta complejo establecer si la conducta ilícita debe atribuirse exclusivamente al programador, al operador del sistema o al usuario final. Por esta razón, Benlonch y Sarrión (2022) manifiestan que los derechos fundamentales enfrentan importantes tensiones frente al crecimiento de tecnologías digitales capaces de influir directamente en decisiones humanas y procesos sociales. En consecuencia, los sistemas jurídicos deben adaptar sus criterios tradicionales de imputación penal a los nuevos escenarios tecnológicos contemporáneos.

De igual manera, el uso de inteligencia artificial en sectores sensibles como salud, transporte, seguridad y administración pública incrementa la necesidad de establecer controles normativos estrictos sobre el funcionamiento de los sistemas automatizados. Un error algorítmico dentro de estos ámbitos podría ocasionar daños de gran magnitud, afectando incluso derechos fundamentales de las personas. En este contexto, Gamboa et al. (2024) consideran que las garantías constitucionales cumplen un papel esencial en la protección de los ciudadanos frente a posibles abusos tecnológicos y vulneraciones derivadas del entorno digital. Por ello, la supervisión humana continúa siendo un elemento indispensable dentro del uso responsable de inteligencia artificial.

Asimismo, el desarrollo de marcos regulatorios internacionales evidencia la preocupación global respecto a la responsabilidad derivada del uso de tecnologías inteligentes. Diversos organismos internacionales han impulsado principios orientados a garantizar transparencia, seguridad, ética y respeto de derechos humanos dentro de la implementación de inteligencia artificial. Según Muñoz (2023), la diplomacia tecnológica y la cooperación internacional constituyen mecanismos fundamentales para enfrentar los desafíos jurídicos y políticos asociados con la transformación digital contemporánea. En consecuencia, la regulación de la IA requiere una coordinación constante entre innovación tecnológica y protección jurídica.

Por otra parte, la responsabilidad civil y penal vinculada con inteligencia artificial también se relaciona con la obligación de implementar medidas preventivas orientadas a reducir riesgos tecnológicos. Las empresas e instituciones que utilizan sistemas automatizados deben garantizar procesos de supervisión, actualización y evaluación permanente de los algoritmos empleados. Gonzalo et al. (2025) afirman que las buenas

prácticas relacionadas con protección de datos y seguridad digital constituyen mecanismos esenciales para prevenir vulneraciones dentro de los entornos tecnológicos modernos. De esta manera, la prevención jurídica adquiere una importancia fundamental en el uso adecuado de inteligencia artificial.

Además, el principio de transparencia representa uno de los elementos más relevantes para determinar responsabilidades derivadas de decisiones automatizadas. Los usuarios tienen derecho a conocer cómo funcionan los sistemas de inteligencia artificial y cuáles son los criterios utilizados para emitir determinadas decisiones. En este sentido, Jiménez y Pincay (2024) sostienen que los derechos digitales requieren mecanismos efectivos de protección frente a la opacidad tecnológica y los riesgos derivados de la automatización. Asimismo, Dueñas et al. (2025) consideran que el respeto a los derechos fundamentales debe prevalecer frente a cualquier forma de innovación tecnológica implementada dentro de la sociedad digital.

Como cierre, la responsabilidad civil y penal derivada del uso de inteligencia artificial constituye uno de los principales desafíos jurídicos de la era tecnológica. Aunque la IA ofrece importantes beneficios relacionados con eficiencia, productividad y automatización de procesos, también genera riesgos asociados con daños, discriminación, vulneración de datos y conductas ilícitas. Por ello, resulta indispensable que los sistemas jurídicos desarrollen marcos regulatorios modernos capaces de garantizar seguridad jurídica, transparencia y protección efectiva de derechos fundamentales frente al uso creciente de tecnologías inteligentes dentro de la sociedad contemporánea.

Tabla 1
Responsabilidad jurídica derivada del uso de inteligencia artificial

Tipo de responsabilidad	Situación relacionada con IA	Posible consecuencia jurídica	Ejemplo
Responsabilidad civil	Daños ocasionados por decisiones automatizadas	Reparación e indemnización	Error en diagnóstico médico automatizado

Tipo de responsabilidad	Situación relacionada con IA	Posible consecuencia jurídica	Ejemplo
Responsabilidad penal	Uso de IA para actividades ilícitas	Sanción penal	Fraude digital mediante deepfakes
Responsabilidad administrativa	Incumplimiento de normas digitales	Multas y sanciones institucionales	Uso indebido de datos personales
Responsabilidad ética	Discriminación algorítmica	Vulneración de derechos fundamentales	Exclusión automatizada en procesos laborales
Responsabilidad tecnológica	Fallos técnicos o errores algorítmicos	Afectación de usuarios y sistemas	Accidente causado por vehículo autónomo

Nota. Elaboración propia a partir del análisis de la responsabilidad civil y penal derivada del uso de inteligencia artificial en entornos digitales.

3.4 Sesgos algorítmicos y discriminación tecnológica

El desarrollo de la inteligencia artificial ha permitido optimizar múltiples procesos dentro de la sociedad digital; sin embargo, también ha generado preocupaciones relacionadas con los sesgos algorítmicos y la discriminación tecnológica. Los sistemas automatizados toman decisiones mediante algoritmos entrenados con grandes volúmenes de información, los cuales pueden contener errores, prejuicios o patrones discriminatorios. Como consecuencia, determinadas personas o grupos sociales podrían verse afectados injustamente por decisiones automatizadas en ámbitos como empleo, educación, seguridad o acceso a servicios digitales. Según Cajahuanca (2025), las innovaciones tecnológicas actuales plantean importantes desafíos jurídicos relacionados con la protección de derechos y la regulación de sistemas inteligentes dentro de la era digital.

Asimismo, los sesgos algorítmicos pueden originarse durante distintas etapas del desarrollo de los sistemas de inteligencia artificial. En algunos casos, los problemas

surgen debido a bases de datos incompletas o desequilibradas; mientras que, en otros, los errores se producen por fallas en la programación o por decisiones humanas incorporadas dentro del diseño del algoritmo. En este contexto, Benlonch y Sarrión (2022) sostienen que las tecnologías digitales contemporáneas generan tensiones significativas respecto al respeto de los derechos fundamentales, especialmente cuando los sistemas automatizados afectan principios de igualdad y no discriminación.

Por otra parte, la discriminación tecnológica puede manifestarse de manera directa o indirecta dentro de los entornos digitales. La discriminación directa ocurre cuando el sistema utiliza variables relacionadas con género, etnia, edad o condición social para emitir decisiones desfavorables; mientras que la discriminación indirecta se presenta cuando los algoritmos producen resultados excluyentes aparentemente neutrales. Dueñas et al. (2025) afirman que el respeto a la dignidad humana y a los principios constitucionales debe prevalecer frente al desarrollo e implementación de nuevas tecnologías digitales. En consecuencia, la supervisión jurídica de los sistemas inteligentes resulta indispensable para garantizar igualdad y protección de derechos fundamentales.

Además, uno de los principales problemas asociados a los sesgos algorítmicos consiste en la falta de transparencia dentro de los procesos automatizados. Muchas herramientas de inteligencia artificial funcionan mediante modelos complejos cuya lógica interna resulta difícil de comprender incluso para sus desarrolladores. Esta situación limita la capacidad de las personas para cuestionar o impugnar decisiones automatizadas que puedan resultar discriminatorias. En relación con ello, Jiménez y Pincay (2024) consideran que los derechos digitales deben garantizar mecanismos efectivos de protección frente a los riesgos derivados de la automatización tecnológica y el uso masivo de algoritmos en la sociedad contemporánea.

De igual manera, la discriminación tecnológica puede afectar gravemente derechos relacionados con privacidad, acceso a oportunidades y libertad individual. En determinados casos, los sistemas inteligentes utilizados en plataformas digitales recopilan y analizan información personal para clasificar o perfilar usuarios, generando posibles exclusiones injustificadas. Aguilar et al. (2022) sostienen que el tratamiento masivo de datos personales representa uno de los mayores retos jurídicos dentro del entorno digital, especialmente cuando la información es utilizada mediante sistemas automatizados sin controles adecuados. Además, Rivera y Maldonado (2023) advierten que la vulneración

de la privacidad constituye una problemática creciente dentro de la era digital debido al uso intensivo de tecnologías inteligentes y plataformas virtuales.

En el ámbito institucional, los sesgos algorítmicos también generan riesgos relacionados con la administración pública y la prestación de servicios estatales. La implementación de inteligencia artificial en procesos gubernamentales puede contribuir a mejorar la eficiencia administrativa; no obstante, la ausencia de mecanismos de supervisión podría ocasionar decisiones injustas o excluyentes para determinados ciudadanos. Según Gamboa et al. (2024), las garantías constitucionales cumplen un papel fundamental en la protección de los derechos frente a posibles vulneraciones derivadas del uso de tecnologías digitales. Por esta razón, resulta necesario establecer controles regulatorios orientados a garantizar transparencia, equidad y responsabilidad en el funcionamiento de sistemas automatizados.

En definitiva, los sesgos algorítmicos y la discriminación tecnológica representan uno de los principales desafíos éticos y jurídicos de la inteligencia artificial dentro de la sociedad contemporánea. Aunque estas tecnologías ofrecen importantes beneficios relacionados con automatización, eficiencia y análisis de información, también pueden reproducir desigualdades sociales existentes cuando no son diseñadas adecuadamente (Rodas et al., 2025). En consecuencia, resulta indispensable desarrollar marcos regulatorios y principios éticos que promuevan sistemas de inteligencia artificial transparentes, inclusivos y respetuosos de los derechos fundamentales, garantizando así un uso responsable y equitativo de la tecnología en la era digital.

3.5 Regulación jurídica de la inteligencia artificial en el derecho comparado

La regulación jurídica de la inteligencia artificial constituye uno de los principales desafíos del Derecho contemporáneo debido al acelerado crecimiento de las tecnologías digitales y su impacto en múltiples ámbitos sociales. Actualmente, diversos países y organismos internacionales han impulsado iniciativas orientadas a establecer normas capaces de controlar el desarrollo y utilización de sistemas inteligentes. Estas regulaciones buscan equilibrar innovación tecnológica, protección de derechos fundamentales y seguridad jurídica frente a los riesgos derivados de la automatización. Según Cajahuanca (2025), las ciencias jurídicas enfrentan la necesidad de adaptarse constantemente a los cambios tecnológicos mediante marcos normativos modernos que respondan adecuadamente a las nuevas dinámicas digitales.

Asimismo, la Unión Europea representa uno de los principales referentes internacionales en materia de regulación de inteligencia artificial. Sus propuestas normativas se orientan a clasificar los sistemas de IA según niveles de riesgo, estableciendo obligaciones específicas para tecnologías consideradas de alto impacto. En este contexto, el Reglamento General de Protección de Datos (2016) ha servido como antecedente importante para fortalecer mecanismos de protección relacionados con privacidad, tratamiento de datos y transparencia digital. Además, Mendoza (2024) sostiene que la regulación jurídica del entorno digital requiere instrumentos normativos sólidos que permitan garantizar derechos fundamentales frente al crecimiento de tecnologías automatizadas.

Por otra parte, países como Estados Unidos han desarrollado un enfoque regulatorio más flexible basado principalmente en principios éticos, autorregulación empresarial y supervisión sectorial. Este modelo prioriza la innovación tecnológica y el desarrollo competitivo de empresas dedicadas a la inteligencia artificial. Sin embargo, también ha generado debates relacionados con la insuficiencia de controles jurídicos frente a posibles vulneraciones de derechos. En relación con ello, Forero (2023) afirma que la expansión de las tecnologías digitales y de los sistemas automatizados obliga a replantear los mecanismos tradicionales de regulación dentro del entorno jurídico contemporáneo.

De igual manera, diversos países latinoamericanos han comenzado a incorporar discusiones relacionadas con la regulación de inteligencia artificial dentro de sus agendas legislativas y políticas públicas. Aunque la mayoría de los Estados de la región aún no cuentan con leyes específicas sobre IA, existen avances relacionados con protección de datos personales, gobierno digital y derechos digitales. Según Jiménez y Pincay (2024), los desafíos jurídicos de la sociedad de la información exigen la creación de mecanismos regulatorios orientados a proteger a las personas frente al impacto de las tecnologías emergentes. En consecuencia, América Latina enfrenta el reto de fortalecer sus marcos normativos para responder adecuadamente a la transformación digital contemporánea.

En el caso ecuatoriano, la regulación vinculada con inteligencia artificial se encuentra relacionada principalmente con normas constitucionales y disposiciones sobre protección de datos personales, privacidad y derechos digitales. La Constitución de la República del Ecuador (2008) reconoce derechos fundamentales vinculados con intimidad, acceso a la información y protección de datos, los cuales adquieren gran relevancia frente al uso de

sistemas automatizados. Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) establece principios orientados a garantizar el tratamiento adecuado de información dentro del entorno digital.

Además, la regulación comparada evidencia que uno de los principales objetivos jurídicos consiste en garantizar transparencia y supervisión humana dentro de los sistemas de inteligencia artificial. Muchos países consideran necesario que las decisiones automatizadas puedan ser explicadas y revisadas para evitar arbitrariedades o discriminación tecnológica. Benlonch y Sarrión (2022) sostienen que las nuevas tecnologías digitales generan importantes tensiones respecto a la protección de derechos fundamentales, especialmente cuando los sistemas automatizados afectan principios relacionados con igualdad, privacidad y dignidad humana. Por ello, la transparencia algorítmica se ha convertido en un principio esencial dentro de las propuestas regulatorias internacionales.

Asimismo, el derecho comparado demuestra que la regulación de inteligencia artificial no solo aborda aspectos tecnológicos, sino también consideraciones éticas y sociales vinculadas con responsabilidad, discriminación y control de riesgos. Diversos organismos internacionales promueven principios relacionados con seguridad, equidad, protección de derechos humanos y uso responsable de sistemas inteligentes. En este sentido, Muñiz (2023) afirma que la cooperación internacional y la diplomacia tecnológica constituyen herramientas fundamentales para enfrentar los desafíos globales derivados de la transformación digital y la expansión de tecnologías emergentes.

Por otra parte, la implementación de regulaciones sobre inteligencia artificial enfrenta dificultades relacionadas con la velocidad del avance tecnológico y la complejidad técnica de los sistemas automatizados. Muchas normas jurídicas tradicionales resultan insuficientes para responder a problemas derivados de algoritmos autónomos, aprendizaje automático y procesamiento masivo de datos. Debido a ello, varios países han optado por desarrollar marcos regulatorios flexibles capaces de adaptarse continuamente a la evolución tecnológica. Además, Dueñas et al. (2025) consideran que los principios constitucionales deben mantenerse como eje fundamental en cualquier proceso de regulación tecnológica, garantizando siempre la protección efectiva de los derechos humanos frente a la innovación digital.

De manera final, la regulación jurídica de la inteligencia artificial en el derecho comparado evidencia la necesidad de construir sistemas normativos modernos, dinámicos y compatibles con los desafíos de la sociedad digital. Aunque cada país adopta enfoques distintos según sus prioridades políticas, económicas y tecnológicas, existe un consenso creciente respecto a la importancia de establecer límites jurídicos claros para el uso de sistemas inteligentes. En consecuencia, el desarrollo de marcos regulatorios internacionales y nacionales representa un elemento esencial para garantizar que la inteligencia artificial evolucione de manera ética, transparente y respetuosa de los derechos fundamentales dentro del contexto global contemporáneo.

3.6 Desafíos éticos y jurídicos de la inteligencia artificial generativa

La inteligencia artificial generativa representa uno de los avances tecnológicos más innovadores de la era digital debido a su capacidad para crear textos, imágenes, audios, videos y otros contenidos de manera automatizada. Estas herramientas utilizan modelos avanzados de aprendizaje automático entrenados con grandes volúmenes de información para producir resultados similares a las creaciones humanas. Sin embargo, el crecimiento acelerado de esta tecnología también ha generado importantes desafíos éticos y jurídicos relacionados con privacidad, autoría, responsabilidad y protección de derechos fundamentales. Según Cajahuanca (2025), las innovaciones tecnológicas actuales exigen una constante adaptación del Derecho frente a los nuevos escenarios digitales y automatizados.

Asimismo, uno de los principales desafíos éticos de la inteligencia artificial generativa se relaciona con la difusión de información falsa o manipulada. Las herramientas de IA pueden producir contenidos altamente realistas que dificultan distinguir entre información auténtica y material alterado digitalmente. Esta situación incrementa los riesgos de desinformación, manipulación mediática y afectación de la confianza pública dentro de la sociedad digital. En este contexto, Jiménez y Pincay (2024) sostienen que el desarrollo de tecnologías digitales debe estar acompañado de mecanismos jurídicos orientados a proteger los derechos de las personas frente a posibles abusos tecnológicos.

Por otra parte, la inteligencia artificial generativa también plantea problemas relacionados con la propiedad intelectual y los derechos de autor. Muchos sistemas inteligentes son entrenados utilizando obras, textos, imágenes y contenidos creados por terceros sin autorización expresa, lo que genera debates sobre titularidad y uso legítimo de la

información. En consecuencia, resulta complejo determinar quién posee los derechos sobre las creaciones generadas mediante inteligencia artificial. Forero (2023) afirma que las tecnologías digitales han modificado profundamente las relaciones jurídicas tradicionales, especialmente en ámbitos relacionados con producción de contenidos y regulación del entorno digital contemporáneo.

Además, la utilización de inteligencia artificial generativa implica importantes riesgos vinculados con privacidad y protección de datos personales. Estas herramientas requieren enormes cantidades de información para funcionar correctamente, incluyendo datos obtenidos de plataformas digitales, redes sociales y otros entornos virtuales. En relación con ello, Aguilar et al. (2022) manifiestan que la protección de datos personales constituye uno de los principales retos jurídicos de la era digital debido al crecimiento de tecnologías capaces de recopilar y procesar información masiva de los usuarios. Del mismo modo, Mendoza (2024) considera que los sistemas tecnológicos actuales deben garantizar mecanismos eficaces de protección de privacidad frente al uso intensivo de datos dentro del entorno digital.

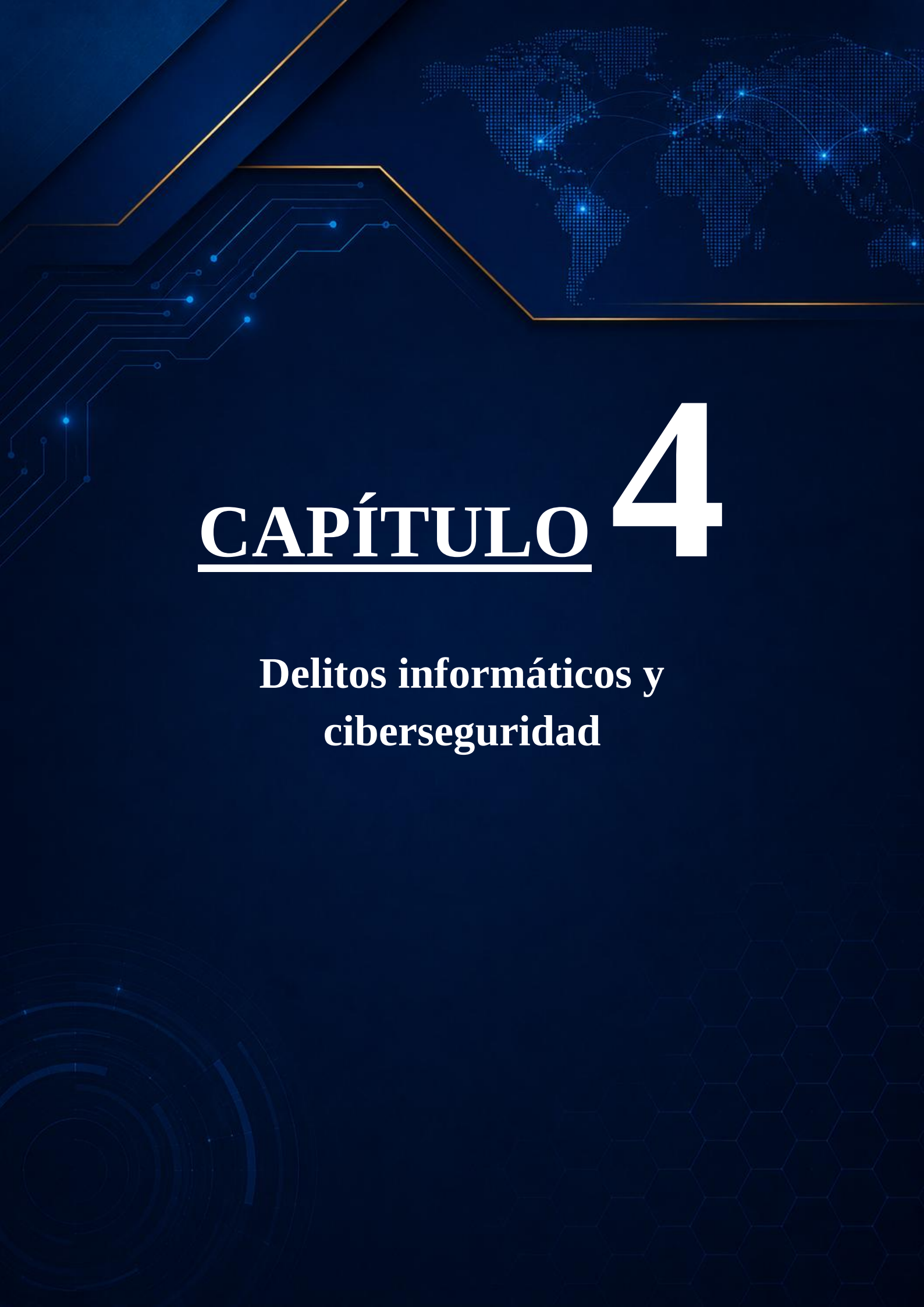
De igual manera, otro desafío importante consiste en la posible generación de contenidos discriminatorios o sesgados por parte de los sistemas de inteligencia artificial generativa. Debido a que estos modelos aprenden a partir de datos previamente existentes, pueden reproducir prejuicios sociales, culturales o ideológicos presentes dentro de las bases de entrenamiento. Como consecuencia, podrían generarse respuestas ofensivas, excluyentes o contrarias a principios de igualdad y dignidad humana. Benlonch y Sarrión (2022) advierten que las tecnologías digitales contemporáneas generan tensiones significativas respecto a la protección de los derechos fundamentales dentro de los entornos virtuales y automatizados.

Asimismo, la inteligencia artificial generativa plantea desafíos relacionados con responsabilidad jurídica frente a daños ocasionados por contenidos automatizados. En muchos casos, resulta difícil determinar quién debe responder cuando una herramienta de IA genera información falsa, vulnera derechos o produce consecuencias perjudiciales para terceros. Esta problemática se vuelve aún más compleja debido al carácter autónomo y dinámico de los sistemas inteligentes. En este sentido, Dueñas et al. (2025) sostienen que la protección constitucional de los derechos fundamentales debe mantenerse como

prioridad frente al desarrollo e implementación de tecnologías emergentes dentro de la sociedad digital contemporánea.

Por otra parte, el uso masivo de inteligencia artificial generativa también genera preocupaciones éticas relacionadas con el impacto social y laboral de la automatización. La capacidad de producir contenidos de manera rápida y automatizada podría transformar significativamente profesiones vinculadas con redacción, diseño, educación, comunicación y producción audiovisual. En consecuencia, surgen debates relacionados con desplazamiento laboral, dependencia tecnológica y pérdida de autenticidad en la producción intelectual humana. Además, Muñiz (2023) considera que la transformación digital contemporánea exige reflexionar sobre los efectos políticos, sociales y culturales derivados del avance acelerado de tecnologías inteligentes en el contexto global.

A manera de conclusión, los desafíos éticos y jurídicos de la inteligencia artificial generativa evidencian la necesidad de desarrollar marcos regulatorios modernos capaces de equilibrar innovación tecnológica y protección de derechos fundamentales. Aunque estas herramientas ofrecen importantes beneficios relacionados con creatividad, automatización y acceso a la información, también generan riesgos vinculados con privacidad, discriminación, responsabilidad y desinformación. Por ello, resulta indispensable promover principios éticos, transparencia algorítmica y supervisión humana dentro del desarrollo de tecnologías generativas, garantizando así un uso responsable y compatible con los valores fundamentales del Estado de Derecho en la era digital.



CAPÍTULO 4

Delitos informáticos y ciberseguridad

4.1 Conceptualización y evolución de los delitos informáticos

La conceptualización de los delitos informáticos ha evolucionado de manera significativa conforme las tecnologías digitales se han incorporado a la vida cotidiana y a los sistemas de gestión pública y privada. Inicialmente, estas conductas se asociaban únicamente con el acceso no autorizado a sistemas computacionales; sin embargo, actualmente comprenden actividades mucho más complejas, como el fraude electrónico, el robo de identidad, la manipulación de datos y los ataques cibernéticos dirigidos contra infraestructuras digitales. En este contexto, la expansión del entorno virtual ha obligado al Derecho a replantear sus mecanismos de protección y control frente a nuevas formas de criminalidad tecnológica. Según Cajahuanca (2025), las ciencias jurídicas enfrentan importantes desafíos para adaptarse a las innovaciones digitales y garantizar respuestas eficaces ante los riesgos tecnológicos contemporáneos.

Asimismo, los delitos informáticos pueden definirse como aquellas conductas ilícitas que utilizan medios tecnológicos, sistemas informáticos o redes digitales para afectar bienes jurídicos protegidos, tales como la privacidad, el patrimonio, la información o la seguridad pública. Estas infracciones poseen características particulares debido a su rapidez de ejecución, dificultad de rastreo y alcance transnacional. Además, el anonimato que ofrecen algunas plataformas digitales incrementa la complejidad de la investigación penal y del juzgamiento de los responsables. En consecuencia, el fenómeno de la ciberdelincuencia se ha convertido en una preocupación constante para los Estados y organismos internacionales (Convención sobre Ciberdelincuencia, 2001).

Por otra parte, el avance de la digitalización y del gobierno electrónico ha incrementado la dependencia de sistemas tecnológicos dentro de las instituciones públicas y privadas. Esta transformación, aunque favorece la eficiencia administrativa y el acceso a servicios digitales, también genera nuevas vulnerabilidades frente a ataques informáticos y filtraciones de información sensible. De acuerdo con Vargas (2021), la implementación del gobierno digital requiere mecanismos sólidos de seguridad informática para prevenir riesgos asociados al manejo masivo de datos y plataformas electrónicas. En este sentido, la ciberseguridad adquiere una función esencial dentro de las políticas estatales orientadas a proteger la información y garantizar la continuidad de los servicios digitales.

Del mismo modo, la evolución de los delitos informáticos se encuentra estrechamente relacionada con el desarrollo de internet y de las tecnologías de comunicación global. En las primeras etapas de la informática, los ataques se limitaban principalmente a sabotajes internos o accesos ilegales básicos; no obstante, en la actualidad existen estructuras criminales organizadas que operan mediante ransomware, phishing, malware y espionaje digital. Estas conductas afectan no solo a individuos, sino también a empresas, entidades financieras e incluso gobiernos. Por ello, la comunidad internacional ha impulsado instrumentos jurídicos orientados a fortalecer la cooperación entre Estados y combatir la ciberdelincuencia de manera coordinada (Código Orgánico Integral Penal (COIP), 2014).

En el caso ecuatoriano, la regulación de los delitos informáticos ha tenido un desarrollo progresivo a partir de la incorporación de normas relacionadas con el comercio electrónico, la protección de datos y la seguridad digital. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Asamblea Nacional del Ecuador, 2002) estableció uno de los primeros marcos legales vinculados al uso de tecnologías digitales dentro del país. Posteriormente, el COIP incorporó diversas figuras penales relacionadas con el acceso ilícito a sistemas informáticos, la interceptación ilegal de datos y la vulneración de información electrónica. Según Jiménez y Pincay (2024), el crecimiento de la sociedad de la información exige que los sistemas jurídicos evolucionen constantemente para responder adecuadamente a los nuevos escenarios digitales.

De igual manera, la protección de datos personales se ha convertido en uno de los elementos centrales dentro del estudio de los delitos informáticos. El uso indebido de información privada mediante plataformas digitales puede generar graves afectaciones a derechos fundamentales como la intimidad, la dignidad y la autodeterminación informativa. En consecuencia, las legislaciones modernas han fortalecido mecanismos de tutela jurídica frente a prácticas ilícitas relacionadas con la manipulación y comercialización de datos personales. La Ley Orgánica de Protección de Datos Personales (2021) constituye un avance importante dentro del ordenamiento jurídico ecuatoriano para prevenir vulneraciones derivadas del entorno digital (Rovira y Robles, 2023).

Además, la globalización tecnológica ha provocado que muchos delitos informáticos trasciendan las fronteras nacionales, dificultando la identificación y sanción de los responsables. Los ciberdelincuentes pueden operar desde diferentes países utilizando

herramientas de anonimización y redes internacionales que complican las investigaciones judiciales. Por esta razón, la cooperación internacional y el intercambio de información entre organismos especializados son fundamentales para enfrentar eficazmente estas amenazas. En este escenario, la Convención de Budapest representa uno de los principales instrumentos internacionales orientados a armonizar las legislaciones y fortalecer la lucha contra la ciberdelincuencia (Convención sobre Ciberdelincuencia, 2001).

Por último, la evolución de los delitos informáticos evidencia que la tecnología, además de ofrecer beneficios para la sociedad, también genera riesgos jurídicos y sociales que requieren respuestas normativas actualizadas. La transformación digital ha modificado las formas tradicionales de criminalidad y ha obligado a replantear conceptos relacionados con la prueba, la jurisdicción y la responsabilidad penal en entornos virtuales. En consecuencia, la ciberseguridad y la regulación jurídica de las conductas informáticas ilícitas constituyen desafíos prioritarios dentro del Derecho Digital contemporáneo. Como sostiene Cajahuanca (2025), la adaptación de las ciencias jurídicas frente a la innovación tecnológica resulta indispensable para garantizar la protección efectiva de los derechos en la era digital.

4.2 Tipología de ciberdelitos en entornos digitales

La tipología de los ciberdelitos en entornos digitales comprende una amplia variedad de conductas ilícitas que afectan sistemas informáticos, redes de comunicación y datos personales. Estas infracciones han aumentado considerablemente debido al crecimiento de internet y de las plataformas tecnológicas utilizadas en actividades cotidianas, financieras y administrativas. Además, los ciberdelitos se caracterizan por su capacidad de ejecutarse de manera remota, rápida y con altos niveles de anonimato. En consecuencia, los Estados han debido fortalecer sus marcos normativos para responder a las nuevas amenazas digitales. Según Cajahuanca (2025), la transformación tecnológica contemporánea exige una actualización constante de las ciencias jurídicas frente a las nuevas modalidades delictivas desarrolladas en el ciberespacio.

Uno de los principales tipos de ciberdelitos corresponde al acceso ilícito a sistemas informáticos, también conocido como hacking. Esta conducta consiste en ingresar sin autorización a plataformas digitales, servidores o redes privadas con el propósito de obtener información, alterar datos o vulnerar medidas de seguridad. Asimismo, este tipo de delito puede utilizarse como medio para ejecutar otras actividades ilícitas, como

espionaje digital o fraude electrónico. Debido a ello, la legislación penal ha incorporado sanciones específicas relacionadas con la intrusión informática y la manipulación ilegal de sistemas tecnológicos (Código Orgánico Integral Penal (COIP), 2014).

Por otra parte, el phishing constituye una de las modalidades de ciberdelito más frecuentes dentro de los entornos digitales actuales. Este mecanismo fraudulento consiste en engañar a las personas mediante correos electrónicos, páginas falsas o mensajes digitales con el objetivo de obtener información confidencial, claves bancarias o datos personales. Además, el incremento de las transacciones electrónicas ha facilitado la expansión de este tipo de fraude a nivel mundial. En este contexto, Gutiérrez (2022) señala que la protección de los datos personales representa una necesidad fundamental dentro del entorno digital, debido al creciente riesgo de vulneraciones relacionadas con el uso indebido de información privada.

Asimismo, los delitos relacionados con malware y ransomware han adquirido gran relevancia dentro de la cibercriminalidad moderna. El malware incluye programas maliciosos diseñados para dañar sistemas informáticos, robar información o controlar dispositivos sin autorización del usuario. En cambio, el ransomware bloquea archivos o sistemas completos y exige un pago económico para restablecer el acceso a la información. Estas prácticas afectan tanto a personas particulares como a instituciones públicas y privadas, generando pérdidas económicas y riesgos para la seguridad digital. En consecuencia, la ciberseguridad se ha convertido en un elemento esencial para prevenir ataques informáticos y proteger infraestructuras tecnológicas críticas (Convención sobre Ciberdelincuencia, 2001).

De igual forma, los delitos contra la privacidad y la protección de datos personales forman parte de las tipologías más relevantes dentro de los ciberdelitos contemporáneos. Estas conductas incluyen la obtención ilegal de información privada, la difusión no autorizada de datos y el uso indebido de bases de datos digitales. Además, la masificación de redes sociales y plataformas virtuales ha incrementado los riesgos de exposición de información sensible. Según Rivera y Maldonado (2023), la vulneración del derecho a la privacidad en la era digital constituye uno de los principales desafíos jurídicos para los sistemas de protección de derechos fundamentales en Ecuador.

Por otro lado, dentro de los entornos digitales también se encuentran los delitos relacionados con la falsificación electrónica y el fraude informático. Estas conductas comprenden la alteración de documentos digitales, la manipulación de sistemas de pago y la realización de transacciones fraudulentas mediante medios tecnológicos. A su vez, el uso de identidades falsas y mecanismos de suplantación digital facilita la ejecución de estas actividades ilícitas. Debido a ello, los ordenamientos jurídicos modernos han incorporado disposiciones específicas para regular la autenticidad de los mensajes electrónicos y garantizar la seguridad de las operaciones digitales (Asamblea Nacional del Ecuador, 2002).

En síntesis, la evolución de las tecnologías digitales ha permitido que los ciberdelitos adopten modalidades cada vez más complejas y sofisticadas. La interconexión global y la dependencia tecnológica han ampliado las oportunidades para la comisión de conductas ilícitas mediante plataformas digitales y sistemas automatizados. En consecuencia, resulta indispensable fortalecer los mecanismos de prevención, cooperación internacional y educación en ciberseguridad para reducir los riesgos asociados a la criminalidad informática. Como sostienen Jiménez y Pincay (2024), el Derecho Digital enfrenta el desafío permanente de adaptarse a las transformaciones tecnológicas y garantizar la protección efectiva de los derechos en la sociedad de la información.

Tabla 2
Clasificación de los principales ciberdelitos en entornos digitales

Tipo de ciberdelito	Descripción	Objetivo principal
Hacking o acceso ilícito	Ingreso no autorizado a sistemas informáticos	Vulnerar seguridad y obtener información
Phishing	Obtención fraudulenta de datos mediante engaño digital	Robar credenciales y datos bancarios
Malware	Programas maliciosos que dañan dispositivos o sistemas	Alterar o controlar sistemas informáticos

Tipo de ciberdelito	Descripción	Objetivo principal
Ransomware	Secuestro de información mediante bloqueo de archivos	Exigir pagos económicos
Fraude informático	Manipulación digital para obtener beneficios ilícitos	Obtener dinero o ventajas ilegales
Suplantación de identidad	Uso indebido de identidad digital ajena	Engañar o cometer fraudes
Delitos contra la privacidad	Obtención o difusión ilegal de datos personales	Vulnerar confidencialidad

Nota. Elaboración propia con base en las principales tipologías de ciberdelitos desarrolladas en los entornos digitales contemporáneos.

4.3 Fraude electrónico, phishing y suplantación de identidad

El fraude electrónico constituye una de las formas más frecuentes de ciberdelincuencia dentro de los entornos digitales contemporáneos. Este tipo de delito se desarrolla mediante el uso de plataformas tecnológicas, sistemas informáticos o medios electrónicos con la finalidad de obtener beneficios económicos ilícitos a través del engaño. Además, el crecimiento del comercio electrónico y de las transacciones digitales ha incrementado significativamente las oportunidades para la comisión de estas conductas. En consecuencia, tanto usuarios como instituciones financieras enfrentan riesgos constantes relacionados con la manipulación de información y el acceso indebido a recursos económicos. Según Cajahuanca (2025), el desarrollo acelerado de las tecnologías digitales ha generado nuevos escenarios jurídicos vinculados a delitos cometidos mediante herramientas informáticas.

Asimismo, el phishing representa una modalidad específica de fraude electrónico que consiste en obtener datos confidenciales mediante técnicas de engaño digital. Generalmente, los ciberdelincuentes utilizan correos electrónicos, enlaces falsos o sitios web fraudulentos que aparentan pertenecer a entidades legítimas, como bancos o

instituciones públicas. De esta manera, inducen a las víctimas a proporcionar contraseñas, números de tarjetas o información personal sensible. Además, el phishing se ha sofisticado con el uso de mensajes personalizados y plataformas automatizadas que dificultan su detección. Por ello, la seguridad informática y la educación digital se han convertido en mecanismos fundamentales para prevenir este tipo de ataques (Convención sobre Ciberdelincuencia, 2001).

Por otra parte, la suplantación de identidad constituye otra de las prácticas ilícitas más comunes dentro del ámbito digital. Esta conducta ocurre cuando una persona utiliza de manera indebida los datos personales o perfiles electrónicos de otra con el propósito de cometer fraudes, acceder a servicios o afectar la reputación de la víctima. Además, las redes sociales y plataformas virtuales han facilitado la creación de identidades falsas que permiten ejecutar actividades delictivas con mayor facilidad. En este contexto, Gutiérrez (2022) sostiene que la protección de datos personales representa un derecho fundamental cuya vulneración puede generar graves consecuencias jurídicas y sociales en la era digital.

De igual forma, el fraude electrónico y la suplantación de identidad afectan directamente derechos relacionados con la privacidad, la intimidad y la seguridad de la información. Los delincuentes digitales suelen aprovechar vulnerabilidades tecnológicas o errores humanos para acceder ilegalmente a datos personales almacenados en sistemas informáticos. Como resultado, las víctimas pueden sufrir pérdidas económicas, daños reputacionales y exposición indebida de información sensible. Debido a ello, los sistemas jurídicos modernos han incorporado mecanismos normativos orientados a garantizar la protección de los datos personales y sancionar las conductas ilícitas relacionadas con su uso indebido (Ley Orgánica de Protección de Datos Personales, 2021).

Además, la expansión del gobierno digital y de los servicios electrónicos ha incrementado la necesidad de fortalecer la ciberseguridad institucional frente a ataques de fraude y robo de identidad. Las entidades públicas y privadas almacenan grandes cantidades de información que puede convertirse en objetivo de ciberdelincuentes interesados en manipular datos o cometer delitos financieros. Según Vargas (2021), el desarrollo del gobierno digital requiere implementar medidas de seguridad tecnológica capaces de proteger la integridad de la información y garantizar la confianza de los usuarios en los servicios electrónicos. En consecuencia, la prevención del fraude digital se ha transformado en una prioridad dentro de las políticas públicas y empresariales.

Por otro lado, las consecuencias jurídicas derivadas del phishing y de la suplantación de identidad han impulsado la actualización de las legislaciones penales en diversos países. Actualmente, muchas normativas contemplan sanciones específicas relacionadas con el acceso ilícito a sistemas, el robo de información y las estafas electrónicas. En Ecuador, el Código Orgánico Integral Penal incorpora disposiciones orientadas a sancionar conductas vinculadas con delitos informáticos y vulneraciones a la seguridad digital. Además, la cooperación internacional resulta indispensable debido al carácter transnacional de estas actividades ilícitas y a la complejidad de rastrear a los responsables (Código Orgánico Integral Penal (COIP), 2014).

Como resultado final, el fraude electrónico, el phishing y la suplantación de identidad reflejan cómo la criminalidad ha evolucionado paralelamente al desarrollo tecnológico y a la digitalización global. Estas conductas afectan no solo a individuos, sino también a empresas, instituciones financieras y organismos estatales, comprometiendo la confianza en los entornos digitales. Por ello, resulta fundamental promover una cultura de prevención basada en la educación tecnológica, la protección de datos y el fortalecimiento de mecanismos de ciberseguridad. Como señalan Rivera y Maldonado (2023), la vulneración de la privacidad y de la información personal constituye uno de los principales riesgos jurídicos presentes en la sociedad digital contemporánea.

4.4 Acceso ilícito, hacking y vulneración de sistemas informáticos

El acceso ilícito a sistemas informáticos constituye una de las conductas más representativas dentro de los delitos informáticos contemporáneos. Esta práctica consiste en ingresar sin autorización a redes, plataformas o dispositivos tecnológicos con la finalidad de obtener información, alterar datos o vulnerar mecanismos de seguridad digital. Además, el crecimiento de la conectividad global y de los servicios electrónicos ha incrementado las oportunidades para la comisión de este tipo de infracciones. En consecuencia, los sistemas jurídicos han debido incorporar regulaciones específicas orientadas a sancionar las conductas relacionadas con intrusiones informáticas y ataques cibernéticos. Según Cajahuanca (2025), la transformación digital ha generado nuevos desafíos legales asociados a la protección de sistemas tecnológicos y datos electrónicos.

Asimismo, el hacking se refiere al conjunto de técnicas utilizadas para acceder, manipular o intervenir sistemas informáticos sin autorización legítima. Aunque originalmente el término se relacionaba con conocimientos avanzados de programación y exploración

tecnológica, actualmente suele asociarse con actividades ilícitas orientadas al robo de información o sabotaje digital. Además, los hackers emplean herramientas sofisticadas que permiten vulnerar redes corporativas, plataformas financieras y bases de datos gubernamentales. Debido a ello, la ciberseguridad se ha convertido en un componente esencial dentro de la protección de infraestructuras digitales y servicios electrónicos (Convención sobre Ciberdelincuencia, 2001).

Por otra parte, la vulneración de sistemas informáticos afecta directamente la confidencialidad, integridad y disponibilidad de la información digital. Cuando un sistema es comprometido mediante accesos ilícitos, pueden producirse alteraciones de datos, pérdida de información o interrupciones en servicios tecnológicos esenciales. Además, estas acciones pueden tener repercusiones económicas, sociales y jurídicas tanto para personas particulares como para instituciones públicas y privadas. En este contexto, Vargas (2021), sostiene que la consolidación del gobierno digital requiere implementar mecanismos eficaces de protección informática para garantizar la seguridad de la información y fortalecer la confianza ciudadana en los servicios tecnológicos.

De igual manera, uno de los métodos más comunes utilizados en el hacking es la explotación de vulnerabilidades presentes en programas, redes o dispositivos electrónicos. Los ciberdelincuentes identifican fallos de seguridad para obtener acceso indebido a sistemas protegidos y ejecutar acciones ilegales de manera remota. Asimismo, el uso de malware, spyware y programas automatizados facilita el control no autorizado de equipos informáticos y la extracción de datos sensibles. En consecuencia, las organizaciones deben mantener actualizadas sus herramientas de protección y desarrollar protocolos permanentes de prevención frente a amenazas digitales (Código Orgánico Integral Penal (COIP), 2014).

Además, el acceso ilícito a sistemas informáticos puede vincularse con otros delitos tecnológicos, como el fraude electrónico, la suplantación de identidad o el espionaje digital. En muchos casos, los hackers obtienen información financiera, credenciales personales o datos confidenciales que posteriormente son utilizados para actividades fraudulentas. Por ello, las vulneraciones informáticas no solo afectan la seguridad tecnológica, sino también derechos fundamentales relacionados con la privacidad y la protección de datos personales. Según Gutiérrez (2022), el tratamiento indebido de datos

en entornos digitales evidencia la necesidad de fortalecer las garantías jurídicas orientadas a proteger la información de los ciudadanos frente a riesgos tecnológicos.

En el ámbito institucional, los ataques informáticos contra entidades públicas representan una amenaza significativa para la estabilidad de los servicios digitales y la administración estatal. La digitalización de procesos gubernamentales ha permitido mejorar la eficiencia administrativa; sin embargo, también ha incrementado la exposición de sistemas críticos a ciberataques. Asimismo, los ciberdelincuentes pueden afectar plataformas relacionadas con salud, educación, seguridad o gestión financiera pública. Frente a esta realidad, la implementación de políticas de ciberseguridad y protocolos de respuesta inmediata resulta indispensable para reducir vulnerabilidades y garantizar la continuidad operativa de los sistemas tecnológicos (Arango, 2024).

Por otro lado, la vulneración de sistemas informáticos también genera importantes desafíos probatorios y procesales dentro del Derecho Penal. Las investigaciones relacionadas con hacking suelen requerir conocimientos técnicos especializados para identificar rastros digitales, recuperar información y determinar la autoría de los hechos. Además, muchas de estas conductas poseen carácter transnacional, ya que los ataques pueden originarse desde diferentes países utilizando redes internacionales y mecanismos de anonimización. En consecuencia, la cooperación jurídica internacional y el intercambio de información entre organismos especializados resultan fundamentales para combatir eficazmente la ciberdelincuencia (Convención sobre Ciberdelincuencia, 2001).

De igual forma, la protección de datos personales adquiere especial relevancia frente a los riesgos derivados del hacking y de los accesos ilegales a plataformas digitales. Las filtraciones masivas de información pueden comprometer datos financieros, historiales médicos y registros personales de millones de usuarios. Como resultado, las legislaciones modernas han fortalecido mecanismos jurídicos orientados a garantizar la confidencialidad y seguridad de la información digital. Según Rovira y Robles (2023), la promulgación de la Ley Orgánica de Protección de Datos Personales (2021) en Ecuador representa un avance importante para enfrentar las amenazas relacionadas con el uso indebido de información privada en entornos tecnológicos.

Para concluir, el acceso ilícito, el hacking y la vulneración de sistemas informáticos reflejan la complejidad de los riesgos existentes dentro de la sociedad digital

contemporánea. El desarrollo tecnológico ha permitido mejorar la comunicación y la gestión de información; sin embargo, también ha favorecido nuevas formas de criminalidad que afectan derechos fundamentales y la seguridad de las infraestructuras digitales. Por ello, resulta imprescindible fortalecer la educación en ciberseguridad, actualizar los marcos normativos y promover mecanismos internacionales de cooperación frente a amenazas tecnológicas. Como señalan Jiménez y Pincay (2024) el Derecho Digital debe evolucionar constantemente para responder a los desafíos jurídicos derivados de la sociedad de la información y de las transformaciones tecnológicas actuales.

4.5 Ciberseguridad y protección de infraestructuras digitales

La ciberseguridad constituye uno de los pilares fundamentales para la protección de las infraestructuras digitales dentro de la sociedad tecnológica contemporánea. Su objetivo principal consiste en prevenir, detectar y responder ante amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en sistemas informáticos. Además, el incremento de servicios digitales y plataformas electrónicas ha generado una mayor dependencia tecnológica tanto en el sector público como privado. En consecuencia, la seguridad informática se ha convertido en una prioridad estratégica para garantizar el funcionamiento adecuado de las infraestructuras digitales. Según Vargas (2021), el fortalecimiento del gobierno digital requiere implementar mecanismos sólidos de protección tecnológica capaces de reducir riesgos asociados a ataques cibernéticos.

Asimismo, las infraestructuras digitales comprenden el conjunto de redes, servidores, bases de datos y sistemas tecnológicos que permiten el funcionamiento de servicios esenciales dentro de una sociedad digitalizada. Estas infraestructuras sostienen actividades relacionadas con salud, educación, banca, comercio electrónico, telecomunicaciones y administración pública. Debido a ello, cualquier vulneración informática puede generar graves consecuencias económicas y sociales. Además, la creciente interconectividad global ha incrementado la exposición de estos sistemas a amenazas provenientes del ciberespacio. Por esta razón, la protección de infraestructuras críticas constituye una necesidad indispensable dentro de las políticas nacionales de seguridad tecnológica (Convención sobre Ciberdelincuencia, 2001).

Por otra parte, la ciberseguridad implica la aplicación de medidas técnicas, jurídicas y organizativas destinadas a prevenir accesos ilícitos y ataques informáticos. Entre estas

medidas se encuentran el uso de firewalls, sistemas de autenticación, cifrado de datos y monitoreo permanente de redes digitales. Asimismo, las organizaciones deben desarrollar protocolos internos orientados a gestionar incidentes tecnológicos y minimizar vulnerabilidades. En este contexto, Cajahuanca (2025) sostiene que las ciencias jurídicas y tecnológicas deben trabajar de manera conjunta para responder eficazmente a los riesgos derivados de la transformación digital y de la expansión del entorno virtual.

De igual forma, uno de los principales riesgos que enfrentan las infraestructuras digitales corresponde a los ataques de malware y ransomware. Estas amenazas permiten a los ciberdelincuentes bloquear sistemas, alterar archivos o sustraer información confidencial mediante programas maliciosos diseñados para vulnerar la seguridad informática. Además, este tipo de ataques puede afectar tanto a usuarios individuales como a grandes instituciones financieras o gubernamentales. En consecuencia, las estrategias de ciberseguridad deben incluir mecanismos preventivos orientados a fortalecer la resiliencia digital y garantizar la recuperación rápida de los sistemas afectados (Código Orgánico Integral Penal (COIP), 2014).

Además, la protección de datos personales representa un componente esencial dentro de la ciberseguridad contemporánea. El almacenamiento masivo de información en plataformas digitales ha incrementado los riesgos relacionados con filtraciones, robo de identidad y uso indebido de datos sensibles. Por ello, las legislaciones modernas han fortalecido mecanismos normativos dirigidos a garantizar la privacidad y la seguridad de la información de los ciudadanos. Según Rovira y Robles (2023), la promulgación de la Ley Orgánica de Protección de Datos Personales (2021) en Ecuador constituye un avance significativo para enfrentar las amenazas derivadas del tratamiento indebido de datos en entornos digitales.

En el ámbito institucional, la ciberseguridad también desempeña un papel fundamental dentro de los procesos de gobierno electrónico y modernización administrativa. Las entidades públicas utilizan plataformas digitales para gestionar trámites, almacenar información y brindar servicios a la ciudadanía. Sin embargo, esta transformación tecnológica incrementa la exposición de los sistemas estatales frente a ataques informáticos y vulneraciones de seguridad. Debido a ello, resulta indispensable implementar políticas públicas orientadas a fortalecer la protección de las infraestructuras

digitales y garantizar la continuidad operativa de los servicios electrónicos (Arango, 2024).

Por otro lado, la capacitación y concienciación de los usuarios constituyen elementos esenciales dentro de las estrategias de ciberseguridad. Muchas vulneraciones informáticas ocurren debido a errores humanos relacionados con el uso inadecuado de contraseñas, enlaces fraudulentos o correos electrónicos maliciosos. Asimismo, el phishing y otras modalidades de fraude digital aprovechan la falta de conocimientos tecnológicos para engañar a las víctimas y acceder a información confidencial. En consecuencia, promover la educación digital y las buenas prácticas informáticas permite reducir considerablemente los riesgos asociados a los ataques (Gonzalo et al., 2025).

Figura 6
Pilares de la Ciberseguridad



4.6 Investigación y persecución penal de delitos informáticos

La investigación y persecución penal de los delitos informáticos constituye uno de los mayores desafíos dentro del Derecho Penal contemporáneo debido a la complejidad técnica y transnacional de estas conductas ilícitas. Los ciberdelitos suelen ejecutarse mediante redes digitales, plataformas electrónicas y sistemas informáticos que dificultan la identificación inmediata de los responsables. Además, el anonimato que ofrece internet permite que muchos delincuentes operen desde diferentes jurisdicciones utilizando herramientas tecnológicas avanzadas. En consecuencia, los sistemas judiciales han debido adaptar sus mecanismos de investigación para responder eficazmente a las nuevas

modalidades de criminalidad digital. Según Cajahuanca (2025), las ciencias jurídicas enfrentan importantes retos relacionados con la adaptación normativa y procesal frente al crecimiento de los entornos tecnológicos.

Asimismo, la investigación de delitos informáticos requiere la utilización de técnicas especializadas orientadas a la obtención y preservación de evidencia digital. Este tipo de prueba comprende archivos electrónicos, registros de acceso, correos digitales, direcciones IP y datos almacenados en dispositivos tecnológicos. Sin embargo, debido a la facilidad con la que la información digital puede ser modificada o eliminada, resulta indispensable aplicar procedimientos técnicos adecuados para garantizar su autenticidad e integridad. En este contexto, la cooperación entre peritos informáticos, fiscales y organismos especializados se convierte en un elemento esencial dentro de los procesos penales relacionados con ciberdelitos (Código Orgánico Integral Penal (COIP), 2014).

Por otra parte, uno de los principales obstáculos en la persecución penal de delitos informáticos radica en el carácter transnacional de estas conductas. Los ciberdelincuentes pueden ejecutar ataques desde distintos países, utilizar servidores internacionales y ocultar su identidad mediante sistemas de anonimización digital. Debido a ello, las investigaciones requieren mecanismos de cooperación jurídica internacional orientados al intercambio de información y asistencia técnica entre Estados. Además, instrumentos internacionales como la Convención sobre Ciberdelincuencia han permitido fortalecer estrategias coordinadas para combatir la criminalidad informática a nivel global (Convención sobre Ciberdelincuencia, 2001).

De igual manera, la persecución penal de los delitos informáticos implica importantes desafíos relacionados con la protección de derechos fundamentales. Durante las investigaciones digitales, las autoridades deben garantizar el respeto a la privacidad, confidencialidad y protección de datos personales de los ciudadanos. Asimismo, las diligencias relacionadas con acceso a dispositivos electrónicos o monitoreo de comunicaciones deben realizarse conforme a los principios de legalidad y proporcionalidad. Según Gutiérrez (2022), el tratamiento de datos personales dentro de los entornos digitales exige mecanismos jurídicos equilibrados que permitan proteger los derechos humanos sin obstaculizar la investigación de conductas ilícitas.

Además, el avance de las tecnologías digitales ha obligado a los organismos de investigación criminal a modernizar sus capacidades técnicas y operativas. Actualmente, las unidades especializadas en ciberdelitos utilizan herramientas de análisis forense digital, rastreo electrónico y monitoreo de redes para identificar actividades ilícitas en el ciberespacio. Sin embargo, la rápida evolución tecnológica genera la necesidad de capacitación constante para fiscales, jueces y agentes investigadores encargados de enfrentar nuevas modalidades de criminalidad informática. En consecuencia, el fortalecimiento institucional constituye un factor indispensable para garantizar investigaciones eficientes y respuestas penales adecuadas frente a los ciberdelitos (Arango, 2024).

Por otro lado, la preservación de la cadena de custodia representa un aspecto fundamental dentro de los procesos de investigación digital. La evidencia electrónica debe recopilarse, almacenarse y analizarse mediante procedimientos técnicos rigurosos que aseguren su validez jurídica durante el proceso penal. Además, cualquier alteración indebida de la información digital puede comprometer la eficacia probatoria y afectar el desarrollo de la investigación judicial. Por ello, los sistemas procesales modernos han incorporado protocolos especializados para el manejo de evidencia informática y documentos electrónicos (Asamblea Nacional del Ecuador, 2002).

Como cierre, la investigación y persecución penal de los delitos informáticos exige una respuesta integral basada en cooperación internacional, actualización normativa y fortalecimiento tecnológico de las instituciones judiciales. La expansión de la criminalidad digital demuestra que los métodos tradicionales de investigación resultan insuficientes frente a las nuevas amenazas presentes en el ciberespacio. Por ello, es indispensable promover mecanismos especializados orientados a proteger la seguridad informática y garantizar la efectiva aplicación de la justicia en entornos digitales. Como sostienen Jiménez y Pincay (2024), el Derecho Digital debe evolucionar constantemente para responder a los desafíos jurídicos derivados de la sociedad tecnológica y de la transformación digital contemporánea.

4.7 Cooperación internacional y normativa sobre ciberdelincuencia

La cooperación internacional constituye uno de los mecanismos más importantes para enfrentar la ciberdelincuencia dentro de la sociedad digital contemporánea. Los delitos informáticos poseen un carácter transnacional debido a que pueden ejecutarse desde

diferentes países mediante redes tecnológicas globales, lo que dificulta la identificación y sanción de los responsables. Además, los ciberdelincuentes utilizan herramientas de anonimización y servidores internacionales para ocultar su ubicación y evitar la persecución penal. En consecuencia, los Estados han debido fortalecer estrategias conjuntas orientadas al intercambio de información y asistencia jurídica internacional. Según Cajahuanca (2025), la transformación digital exige respuestas jurídicas coordinadas frente a los nuevos desafíos tecnológicos presentes en el ciberespacio.

Asimismo, uno de los principales instrumentos internacionales en materia de ciberdelincuencia es la Convención sobre Ciberdelincuencia, conocida también como Convenio de Budapest. Este tratado internacional establece lineamientos comunes para la tipificación de delitos informáticos, la cooperación judicial y la obtención de evidencia digital entre los Estados participantes. Además, promueve mecanismos de asistencia mutua para facilitar investigaciones relacionadas con accesos ilícitos, fraude informático y ataques contra sistemas tecnológicos. Debido a ello, la Convención de Budapest se ha convertido en un referente fundamental dentro de la regulación internacional de los delitos informáticos (Convención sobre Ciberdelincuencia, 2001).

Por otra parte, la cooperación internacional permite fortalecer la capacidad de respuesta de los sistemas judiciales frente a amenazas tecnológicas complejas. Muchos delitos informáticos involucran múltiples jurisdicciones debido a que los servidores, víctimas y responsables pueden encontrarse ubicados en distintos países. En consecuencia, las investigaciones requieren intercambio rápido de información digital, coordinación entre organismos especializados y mecanismos eficaces de asistencia jurídica recíproca. En este contexto, Arango (2024) sostiene que la modernización tecnológica de las instituciones públicas exige también fortalecer la seguridad digital y los sistemas de cooperación internacional frente a riesgos cibernéticos.

De igual forma, la normativa internacional sobre ciberdelincuencia busca armonizar las legislaciones nacionales para evitar vacíos jurídicos que puedan ser aprovechados por organizaciones criminales. Algunos países poseen regulaciones avanzadas sobre delitos informáticos, mientras que otros mantienen marcos normativos limitados o desactualizados. Esta desigualdad normativa dificulta la persecución efectiva de conductas ilícitas realizadas mediante plataformas digitales. Por ello, los organismos internacionales han impulsado estándares comunes orientados a garantizar una respuesta

penal más uniforme frente a la criminalidad informática (Código Orgánico Integral Penal (COIP), 2014).

Además, la protección de datos personales representa un elemento esencial dentro de la cooperación internacional en materia de ciberseguridad. Las investigaciones relacionadas con delitos informáticos suelen implicar el tratamiento de grandes volúmenes de información digital y datos sensibles de los usuarios. En consecuencia, los Estados deben garantizar que los procedimientos de intercambio de información respeten los derechos fundamentales relacionados con la privacidad y la protección de datos. Según Rovira y Robles (2023), la consolidación de marcos normativos sobre protección de datos resulta indispensable para enfrentar los riesgos derivados del entorno digital y de las nuevas formas de criminalidad tecnológica.

Por otro lado, las organizaciones internacionales también han promovido estrategias orientadas al fortalecimiento de capacidades técnicas para combatir la ciberdelincuencia. Estas iniciativas incluyen programas de capacitación, asistencia tecnológica y desarrollo de unidades especializadas en investigación digital. Asimismo, la cooperación internacional favorece el intercambio de buenas prácticas relacionadas con ciberseguridad, protección de infraestructuras críticas y manejo de evidencia electrónica. Debido a ello, la colaboración entre Estados y organismos multilaterales resulta esencial para enfrentar amenazas cibernéticas cada vez más sofisticadas y complejas (Protección de la información y de los datos, 2009)

En el caso ecuatoriano, la regulación de los delitos informáticos ha evolucionado mediante la incorporación de disposiciones relacionadas con comercio electrónico, protección de datos y seguridad digital. El Código Orgánico Integral Penal (2014) contempla diversas figuras delictivas vinculadas con accesos ilícitos, fraude electrónico y vulneración de sistemas informáticos. Además, Ecuador ha fortalecido progresivamente sus mecanismos de cooperación internacional para enfrentar amenazas relacionadas con la ciberdelincuencia y el uso indebido de tecnologías digitales. En este sentido, la adaptación normativa resulta indispensable para responder adecuadamente a los riesgos derivados de la globalización tecnológica (Asamblea Nacional del Ecuador, 2002).

Asimismo, la evolución constante de las tecnologías digitales obliga a actualizar permanentemente las normativas relacionadas con ciberseguridad y ciberdelincuencia. El desarrollo de inteligencia artificial, computación en la nube y plataformas automatizadas

ha generado nuevas modalidades de ataques informáticos que superan muchas regulaciones tradicionales. Por ello, los Estados deben promover reformas jurídicas flexibles y adaptables que permitan responder eficazmente a escenarios tecnológicos cambiantes. Según Jiménez y Pincay (2024), el Derecho Digital enfrenta desafíos permanentes relacionados con la necesidad de garantizar seguridad jurídica dentro de una sociedad caracterizada por la rápida transformación tecnológica.

En síntesis, la cooperación internacional y la normativa sobre ciberdelincuencia representan herramientas esenciales para garantizar la seguridad del entorno digital y la protección de los derechos fundamentales. La naturaleza global de los delitos informáticos exige respuestas coordinadas basadas en intercambio de información, armonización legislativa y fortalecimiento institucional. Asimismo, la consolidación de políticas internacionales de ciberseguridad contribuye a prevenir ataques tecnológicos y fortalecer la confianza en los sistemas digitales. Como sostiene Cajahuanca (2025), la evolución tecnológica contemporánea obliga a los sistemas jurídicos a desarrollar estrategias integrales capaces de responder eficazmente a los desafíos del ciberespacio y de la criminalidad digital.



CAPÍTULO 5

**Prueba digital y justicia en
entornos tecnológicos**

5.1 Concepto y naturaleza jurídica de la prueba digital

La prueba digital constituye uno de los elementos más relevantes dentro de los procesos judiciales contemporáneos, debido al crecimiento de las tecnologías de la información y la comunicación en la sociedad actual. En este contexto, la información generada mediante dispositivos electrónicos, plataformas digitales y sistemas informáticos ha adquirido valor probatorio dentro de las controversias civiles, penales y administrativas. Además, la evolución tecnológica ha provocado que los operadores jurídicos deban adaptar los mecanismos tradicionales de valoración de la prueba a nuevos escenarios digitales. Según Cajahuanca (2025), las ciencias jurídicas enfrentan actualmente importantes desafíos derivados de la transformación digital y de la incorporación constante de nuevas herramientas tecnológicas dentro del ámbito judicial.

Asimismo, la naturaleza jurídica de la prueba digital se relaciona con la capacidad que tienen los datos electrónicos para demostrar hechos relevantes dentro de un proceso judicial. Dichos elementos pueden manifestarse mediante correos electrónicos, registros informáticos, mensajes instantáneos, archivos multimedia, bases de datos o documentos electrónicos. En consecuencia, el Derecho Digital ha debido establecer principios orientados a garantizar autenticidad, integridad y conservación de la evidencia electrónica. En este sentido, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Asamblea Nacional del Ecuador, 2002) reconoce la validez jurídica de los mensajes de datos y de los documentos electrónicos dentro del ordenamiento jurídico ecuatoriano.

Por otra parte, la prueba digital posee características particulares que la diferencian de los medios probatorios tradicionales, ya que puede ser fácilmente modificada, alterada o eliminada si no se aplican mecanismos adecuados de preservación. Debido a ello, la cadena de custodia digital adquiere especial relevancia dentro de las investigaciones tecnológicas y procesos judiciales relacionados con delitos informáticos. Además, los sistemas de almacenamiento y recuperación de datos requieren procedimientos técnicos especializados que permitan garantizar la confiabilidad de la información presentada ante los tribunales. Desde esta perspectiva, Cornejo (2023) sostiene que la modernización de la gestión pública y judicial exige la incorporación de mecanismos tecnológicos capaces de fortalecer la seguridad y transparencia de la información digital.

De igual manera, la incorporación de pruebas digitales dentro de los procesos judiciales se encuentra vinculada con la protección de derechos fundamentales como la privacidad, la intimidad y la protección de datos personales. Esto ocurre porque gran parte de la evidencia electrónica contiene información sensible de las personas, lo cual obliga a los Estados a establecer límites jurídicos para su obtención y utilización. En efecto, la Constitución de la República del Ecuador (2008) reconoce el derecho a la protección de datos personales y a la intimidad como garantías fundamentales dentro del entorno digital. En consecuencia, la obtención ilícita de evidencia electrónica puede afectar derechos constitucionales y provocar la nulidad procesal de la prueba (Rivera y Maldonado, 2023).

En relación con ello, la autenticidad constituye uno de los principios esenciales de la prueba digital, debido a que permite verificar que la información presentada no ha sido alterada desde su creación o almacenamiento. Para lograrlo, se utilizan mecanismos como firmas electrónicas, certificados digitales, sellos de tiempo y sistemas criptográficos. Además, los peritajes informáticos cumplen una función fundamental al momento de determinar la legitimidad y procedencia de la evidencia electrónica presentada dentro de un juicio. Según Asamblea Nacional del Ecuador (2002) los mensajes de datos conservan valor probatorio siempre que exista certeza sobre su integridad y accesibilidad posterior.

Por consiguiente, la valoración judicial de la prueba digital requiere no solo conocimientos jurídicos, sino también criterios técnicos especializados que permitan interpretar adecuadamente la información electrónica. En muchos casos, los jueces dependen de informes periciales informáticos para comprender el funcionamiento de sistemas digitales complejos y determinar la validez de la evidencia presentada. Además, la cooperación entre profesionales del Derecho y expertos tecnológicos se ha convertido en una necesidad dentro de los procesos judiciales modernos. En este sentido, Jiménez y Pincay (2024) afirman que los derechos digitales y los nuevos entornos tecnológicos obligan al sistema jurídico a replantear sus métodos tradicionales de análisis probatorio.

Por otro lado, la expansión de los delitos informáticos ha incrementado considerablemente la utilización de pruebas digitales dentro de las investigaciones penales. Conductas como el acceso ilícito a sistemas, fraude electrónico, phishing, ciberacoso y robo de datos requieren evidencia tecnológica para demostrar la existencia de la infracción y la participación de los responsables. Además, la Convención sobre Ciberdelincuencia (2001) establece mecanismos de cooperación internacional orientados

a facilitar la obtención y preservación de evidencia electrónica en investigaciones transnacionales. De esta manera, la prueba digital se convierte en un instrumento esencial para combatir la criminalidad tecnológica en la actualidad.

En términos finales, la consolidación de la justicia digital y de los procesos judiciales electrónicos ha fortalecido la importancia de la prueba digital dentro del sistema jurídico contemporáneo. Actualmente, numerosos procedimientos judiciales incorporan audiencias virtuales, expedientes electrónicos y plataformas digitales para la gestión procesal, lo cual incrementa la producción y utilización de evidencia tecnológica. Además, la transformación digital del Estado exige marcos normativos actualizados que permitan garantizar seguridad jurídica, transparencia y protección de derechos fundamentales en los entornos tecnológicos. Desde esta perspectiva, Jáuregui (2025) considera que la modernización digital de las instituciones públicas representa uno de los principales retos para los sistemas jurídicos contemporáneos.

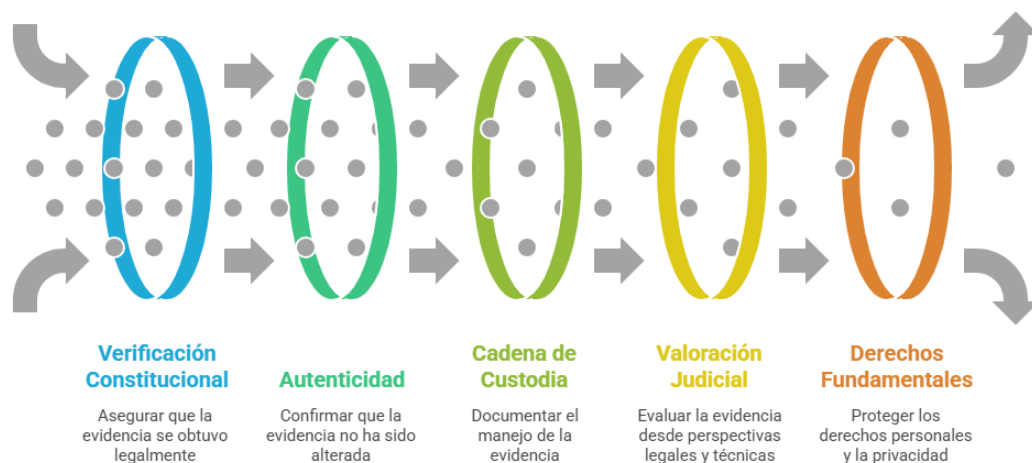
5.2 Admisibilidad, autenticidad y valoración de la evidencia electrónica

La admisibilidad de la evidencia electrónica constituye uno de los aspectos más importantes dentro de los procesos judiciales en entornos tecnológicos, debido a que determina si la información digital puede ser incorporada válidamente como medio probatorio. En este contexto, los jueces deben verificar que la obtención de la evidencia haya respetado las garantías constitucionales y los procedimientos legales establecidos. Además, resulta indispensable comprobar que los datos electrónicos mantengan relación directa con los hechos controvertidos dentro del proceso. Según Gamboa et al. (2024), la tutela efectiva de los derechos constitucionales exige que toda actuación probatoria respete principios de legalidad, debido proceso y seguridad jurídica en el entorno digital.

Asimismo, la autenticidad de la evidencia electrónica representa un requisito esencial para garantizar que la información presentada no haya sido alterada, manipulada o falsificada. Debido a la facilidad con la que los archivos digitales pueden modificarse, los sistemas judiciales requieren mecanismos técnicos que permitan verificar la integridad de los datos electrónicos. En consecuencia, las firmas electrónicas, certificados digitales y sellos de tiempo cumplen una función fundamental dentro de la validación probatoria. En este sentido, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) reconoce que los mensajes de datos poseen eficacia jurídica siempre que se pueda demostrar su autenticidad e integridad.

Por otra parte, la cadena de custodia digital adquiere especial importancia dentro de la valoración de la evidencia electrónica, ya que permite documentar cada etapa relacionada con la obtención, almacenamiento, traslado y análisis de los datos informáticos. De esta manera, se garantiza que la evidencia no haya sufrido alteraciones durante el proceso investigativo o judicial. Además, los procedimientos técnicos deben ser ejecutados por personal especializado que cuente con conocimientos en informática forense y manejo de sistemas tecnológicos. Desde esta perspectiva, Cajahuanca (2025) sostiene que la transformación digital del Derecho obliga a incorporar estándares técnicos y jurídicos más rigurosos para preservar la validez de la prueba electrónica.

Figura 7
Proceso de Admisibilidad de Evidencia Electrónica



De igual forma, la valoración judicial de la evidencia electrónica implica analizar tanto los aspectos jurídicos como los elementos técnicos relacionados con la producción de la prueba digital. Esto significa que los jueces deben considerar la procedencia de la información, los métodos utilizados para su obtención y la confiabilidad de los sistemas tecnológicos involucrados. Además, los informes periciales informáticos se convierten en herramientas esenciales para interpretar archivos, registros y datos digitales complejos. En consecuencia, la cooperación entre expertos tecnológicos y operadores jurídicos resulta indispensable para garantizar decisiones judiciales fundamentadas y objetivas (Martínez et al., 2024).

En relación con ello, los derechos fundamentales desempeñan un papel determinante en la admisibilidad de la evidencia electrónica, especialmente cuando se encuentran involucrados datos personales o información sensible. La obtención ilegal de mensajes

privados, historiales de navegación o conversaciones digitales puede vulnerar derechos relacionados con la intimidad y la protección de datos personales. Por esta razón, los sistemas judiciales deben aplicar criterios de proporcionalidad y legalidad antes de admitir este tipo de pruebas dentro de un proceso. Según Guanín (2024) el hábeas data constituye una garantía constitucional orientada a proteger la intimidad y el control sobre la información personal en los entornos digitales.

Por consiguiente, la evolución tecnológica ha generado nuevos desafíos respecto a la conservación y almacenamiento de la evidencia electrónica dentro de los procesos judiciales. Actualmente, gran parte de la información digital se encuentra alojada en servidores remotos, servicios en la nube y plataformas internacionales, lo cual dificulta su preservación y recuperación. Además, la naturaleza transnacional de los sistemas digitales obliga a fortalecer los mecanismos de cooperación jurídica internacional para garantizar el acceso legítimo a la información requerida. En este sentido, la Convención sobre Ciberdelincuencia (2001) establece procedimientos orientados a facilitar la recopilación y preservación internacional de evidencia electrónica en investigaciones penales.

Como cierre, la consolidación de la justicia digital ha incrementado significativamente la relevancia de la evidencia electrónica dentro de los sistemas judiciales contemporáneos. La implementación de expedientes electrónicos, audiencias virtuales y plataformas digitales de gestión procesal ha transformado la forma en que se produce y valora la prueba dentro de los tribunales. Además, los avances tecnológicos exigen marcos normativos flexibles y actualizados que permitan responder adecuadamente a las nuevas formas de interacción digital. Desde esta perspectiva, Jiménez y Pincay (2024) afirman que los derechos digitales y la sociedad de la información demandan una reinterpretación constante de los principios jurídicos tradicionales frente a los nuevos escenarios tecnológicos.

5.3 Cadena de custodia en evidencias digitales

La cadena de custodia en evidencias digitales constituye un procedimiento fundamental dentro de los procesos judiciales modernos, debido a que garantiza la conservación, integridad y autenticidad de la información electrónica utilizada como medio probatorio. Este mecanismo permite documentar de manera detallada cada etapa relacionada con la obtención, manipulación, almacenamiento y análisis de los datos digitales. Además, su

correcta aplicación evita alteraciones, pérdidas o manipulaciones que puedan afectar la validez de la evidencia presentada ante las autoridades judiciales. Según Cajahuanca (2025), la transformación tecnológica del Derecho exige procedimientos especializados que aseguren confiabilidad y seguridad jurídica en el manejo de información digital.

Asimismo, la cadena de custodia digital inicia desde el momento en que la evidencia electrónica es identificada y recolectada por las autoridades competentes. En esta etapa, resulta indispensable aplicar protocolos técnicos adecuados para evitar modificaciones involuntarias en los archivos o dispositivos informáticos. Además, cada actuación debe registrarse de manera precisa, indicando fecha, hora, responsables y métodos utilizados durante la obtención de la información. En este sentido, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) reconoce la necesidad de preservar la integridad y autenticidad de los mensajes de datos dentro de los procedimientos jurídicos.

Por otra parte, uno de los principales desafíos de la cadena de custodia digital radica en la naturaleza intangible y fácilmente modificable de la información electrónica. A diferencia de la evidencia física tradicional, los archivos digitales pueden ser alterados en segundos mediante herramientas tecnológicas simples, lo cual incrementa el riesgo de manipulación indebida. Debido a ello, las investigaciones informáticas requieren procedimientos especializados de informática forense orientados a proteger la integridad de los datos. Desde esta perspectiva, Cornejo (2023) sostiene que la modernización tecnológica de las instituciones públicas debe incorporar mecanismos de seguridad capaces de garantizar transparencia y confiabilidad en la gestión digital.

De igual manera, los peritos informáticos desempeñan una función esencial dentro de la cadena de custodia de evidencias digitales, ya que son responsables de aplicar técnicas científicas para la recuperación, análisis y preservación de los datos electrónicos. Además, estos especialistas deben utilizar herramientas certificadas y metodologías reconocidas internacionalmente que permitan asegurar la confiabilidad de la prueba digital. En consecuencia, los informes periciales constituyen elementos clave para demostrar ante el juez que la evidencia no ha sufrido alteraciones durante el proceso investigativo. Por ello, la capacitación técnica de los operadores judiciales resulta indispensable para fortalecer la administración de justicia tecnológica (Martínez et al., 2024).

En relación con ello, la cadena de custodia también se vincula directamente con la protección de derechos fundamentales como la privacidad, la intimidad y la protección de datos personales. Muchas evidencias digitales contienen información sensible relacionada con comunicaciones privadas, historiales de navegación o datos personales almacenados en dispositivos electrónicos. Por esta razón, las autoridades deben actuar bajo criterios de legalidad, proporcionalidad y autorización judicial para evitar vulneraciones constitucionales. Según Guanín (2024), el hábeas data constituye una garantía orientada a proteger el control de las personas sobre su información dentro de los entornos tecnológicos y digitales.

Por consiguiente, la documentación adecuada de cada etapa de la cadena de custodia resulta indispensable para garantizar la validez procesal de la evidencia electrónica. Esto implica registrar de manera detallada quién tuvo acceso a la información, qué procedimientos se aplicaron y en qué condiciones fue almacenada la evidencia digital. Además, cualquier irregularidad dentro de este procedimiento puede generar dudas sobre la autenticidad de la prueba y afectar su admisibilidad dentro del proceso judicial. En consecuencia, la trazabilidad de la información se convierte en un elemento esencial para preservar la seguridad jurídica en las investigaciones tecnológicas (Rivera y Maldonado, 2023).

Por otro lado, el crecimiento de los delitos informáticos ha incrementado la importancia de la cadena de custodia en investigaciones relacionadas con fraude electrónico, acceso ilícito a sistemas, robo de datos y ciberdelincuencia. En estos casos, las autoridades deben actuar rápidamente para evitar la pérdida o destrucción de la información digital relevante para el proceso penal. Además, la cooperación internacional resulta necesaria cuando la evidencia se encuentra almacenada en servidores ubicados fuera del territorio nacional. En este sentido, la Convención sobre Ciberdelincuencia (2001) establece mecanismos de colaboración internacional destinados a facilitar la preservación y obtención de evidencia electrónica en investigaciones transnacionales.

De igual forma, la evolución tecnológica ha generado nuevos retos relacionados con el almacenamiento en la nube, dispositivos móviles y plataformas digitales de comunicación. Actualmente, gran parte de la información relevante para las investigaciones judiciales se encuentra distribuida en entornos virtuales que requieren procedimientos técnicos más complejos para su preservación. Además, la volatilidad de

ciertos datos digitales obliga a las autoridades a aplicar medidas inmediatas para asegurar la conservación de la evidencia. Según Jiménez y Pincay (2024), los derechos digitales y los nuevos escenarios tecnológicos demandan una constante actualización normativa y técnica dentro de los sistemas de justicia contemporáneos.

Para concluir, la cadena de custodia en evidencias digitales representa una garantía esencial para asegurar transparencia, confiabilidad y legalidad dentro de los procesos judiciales tecnológicos. Su correcta aplicación permite fortalecer la confianza en la administración de justicia y garantizar que la información electrónica presentada conserve valor probatorio ante los tribunales. Además, el desarrollo de protocolos especializados y estándares internacionales contribuye a mejorar la eficacia de las investigaciones digitales y la protección de derechos fundamentales. De esta manera, la consolidación de la justicia digital requiere mecanismos sólidos capaces de responder adecuadamente a los desafíos derivados de la sociedad tecnológica contemporánea.

5.4 Firma electrónica, documentos digitales y validez jurídica

La firma electrónica y los documentos digitales representan elementos fundamentales dentro de la transformación tecnológica de los sistemas jurídicos contemporáneos, debido a que permiten realizar actos jurídicos mediante medios electrónicos con plena validez legal. Gracias al desarrollo de las tecnologías de la información, numerosas actividades administrativas, comerciales y judiciales se ejecutan actualmente en entornos digitales, lo cual ha impulsado la necesidad de establecer mecanismos que garanticen autenticidad, integridad y seguridad jurídica. Además, estos instrumentos facilitan la modernización de los procedimientos públicos y privados mediante la reducción de tiempos y costos operativos. Según Vargas (2021), el gobierno digital constituye una herramienta esencial para fortalecer la eficiencia institucional y promover la transformación tecnológica del Estado.

Asimismo, la firma electrónica puede definirse como un conjunto de datos electrónicos asociados a un documento digital que permite identificar al firmante y manifestar su voluntad respecto del contenido del documento. Este mecanismo tecnológico cumple funciones similares a la firma manuscrita tradicional, pero incorpora sistemas criptográficos y certificados digitales orientados a garantizar mayor seguridad en las transacciones electrónicas. Además, la utilización de firmas electrónicas fortalece la confianza en las comunicaciones digitales y en la ejecución de actos jurídicos

electrónicos. En este sentido, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) reconoce expresamente la validez jurídica y eficacia probatoria de la firma electrónica en el Ecuador.

Por otra parte, los documentos digitales constituyen soportes electrónicos que contienen información susceptible de ser almacenada, transmitida o reproducida mediante sistemas tecnológicos. Estos documentos pueden presentarse en diferentes formatos, tales como contratos electrónicos, correos electrónicos, certificados digitales, expedientes judiciales o archivos multimedia. Debido a ello, los sistemas jurídicos modernos han debido adaptar sus normas tradicionales para reconocer la equivalencia funcional entre documentos físicos y electrónicos. Desde esta perspectiva, Arango (2024) sostiene que la digitalización administrativa y gubernamental exige mecanismos normativos capaces de garantizar seguridad y eficiencia dentro de los procesos tecnológicos contemporáneos.

De igual manera, la validez jurídica de los documentos digitales depende principalmente de la posibilidad de demostrar autenticidad, integridad y disponibilidad de la información contenida en ellos. Esto significa que debe existir certeza respecto a la identidad del emisor y a la inexistencia de alteraciones posteriores en el documento electrónico. Además, los sistemas de certificación digital y las entidades acreditadas desempeñan un papel fundamental dentro de este proceso de validación tecnológica. En consecuencia, la utilización de mecanismos criptográficos fortalece la confianza jurídica en las operaciones realizadas mediante plataformas digitales (Corcino et al., 2026).

En relación con ello, la firma electrónica también posee una importante función probatoria dentro de los procesos judiciales, ya que permite acreditar la autoría y aceptación de actos jurídicos celebrados electrónicamente. Esto resulta especialmente relevante en contratos digitales, trámites administrativos y procedimientos judiciales virtuales, donde la evidencia tecnológica adquiere gran relevancia. Además, los jueces deben valorar la autenticidad de las firmas electrónicas mediante peritajes técnicos y certificados digitales emitidos por entidades autorizadas. Según Jiménez y Pincay (2024), la expansión de los derechos digitales y de la sociedad de la información obliga a replantear constantemente los mecanismos tradicionales de validación jurídica.

Por consiguiente, la implementación de documentos digitales y firmas electrónicas también se encuentra vinculada con la protección de datos personales y la privacidad de

los usuarios. Gran parte de las transacciones electrónicas involucran información sensible que debe ser protegida frente a accesos no autorizados, fraudes o vulneraciones informáticas. Debido a ello, los Estados han desarrollado marcos normativos orientados a garantizar la seguridad de la información digital y la protección de derechos fundamentales en entornos tecnológicos. En este contexto, la Ley Orgánica de Protección de Datos Personales (2021) establece principios y obligaciones relacionadas con el tratamiento seguro de datos dentro de sistemas digitales y electrónicos.

Por otro lado, el avance de la justicia digital ha incrementado significativamente el uso de documentos electrónicos dentro de los procedimientos judiciales modernos. Actualmente, numerosos tribunales utilizan expedientes digitales, notificaciones electrónicas y audiencias virtuales como parte de la modernización de la administración de justicia. Esto ha permitido agilizar trámites judiciales y facilitar el acceso a los servicios jurídicos mediante plataformas tecnológicas. Sin embargo, también han surgido desafíos relacionados con la ciberseguridad, la conservación documental y la autenticidad de la información procesal. Según Jáuregui (2025), la modernización digital del Estado requiere sistemas tecnológicos confiables que garanticen transparencia, eficiencia y seguridad jurídica en las actuaciones públicas.

A manera de conclusión, la consolidación de la firma electrónica y de los documentos digitales refleja la creciente adaptación del Derecho a las exigencias de la sociedad tecnológica contemporánea. La transformación digital de las relaciones jurídicas ha generado nuevas dinámicas económicas, administrativas y judiciales que requieren marcos normativos flexibles y actualizados. Además, la seguridad tecnológica y la protección de derechos fundamentales continúan siendo elementos esenciales dentro de la regulación de los entornos digitales (Becerra et al., 2024). De esta manera, la validez jurídica de los documentos electrónicos y de las firmas digitales se ha convertido en un pilar fundamental para garantizar confianza y eficacia en las interacciones tecnológicas modernas

5.5 Uso de tecnologías digitales en procesos judiciales

El uso de tecnologías digitales en los procesos judiciales ha transformado significativamente la administración de justicia en los últimos años, debido a la necesidad de modernizar los sistemas judiciales y garantizar mayor eficiencia procesal. Actualmente, herramientas como expedientes electrónicos, audiencias virtuales,

notificaciones digitales y plataformas de gestión judicial permiten agilizar trámites y facilitar el acceso a los servicios jurídicos. Además, estas tecnologías contribuyen a reducir costos operativos y tiempos procesales dentro de los tribunales. Según Jáuregui (2025), la modernización digital del Estado constituye uno de los principales mecanismos para optimizar la gestión pública y fortalecer la eficiencia institucional.

Asimismo, la implementación de plataformas judiciales electrónicas ha permitido que numerosos procedimientos puedan desarrollarse de manera virtual, especialmente en contextos donde el acceso físico a las instituciones resulta limitado. Las audiencias telemáticas, por ejemplo, facilitan la participación de jueces, abogados, fiscales y partes procesales mediante sistemas de videoconferencia. Además, estas herramientas han fortalecido la continuidad del servicio judicial frente a situaciones de emergencia o restricciones de movilidad. En este sentido, Corcino et al. (2026) sostienen que la transformación digital de las instituciones públicas favorece procesos más ágiles, transparentes y eficientes dentro de la administración estatal.

Por otra parte, el expediente judicial electrónico representa uno de los avances más relevantes dentro de la justicia digital, debido a que permite almacenar, organizar y consultar información procesal mediante sistemas informáticos seguros. Gracias a ello, las actuaciones judiciales pueden realizarse de forma más rápida y ordenada, reduciendo el uso de documentos físicos y mejorando la trazabilidad de los procesos. Además, los sistemas digitales facilitan el acceso remoto a información judicial para las partes procesales autorizadas. Desde esta perspectiva, Vargas (2021) considera que el gobierno digital constituye una herramienta fundamental para fortalecer la transparencia y eficiencia dentro de las instituciones públicas y judiciales.

De igual manera, las tecnologías digitales han fortalecido la utilización de evidencia electrónica dentro de los procesos judiciales contemporáneos. Actualmente, correos electrónicos, mensajes instantáneos, registros informáticos y documentos digitales son utilizados frecuentemente como medios probatorios dentro de litigios civiles, administrativos y penales. Sin embargo, esta situación también ha generado la necesidad de establecer mecanismos especializados para garantizar autenticidad, integridad y preservación de la información electrónica. En consecuencia, los sistemas judiciales requieren procedimientos técnicos y jurídicos adecuados para valorar correctamente este tipo de evidencia (Martínez et al., 2024; Zambrano L. , 2024).

Figura 8
Transformación Digital de la Justicia



En relación con ello, la incorporación de tecnologías digitales dentro de la justicia también plantea desafíos vinculados con la protección de datos personales y la seguridad de la información. Los expedientes judiciales suelen contener datos sensibles relacionados con la intimidad y privacidad de las personas, por lo cual resulta indispensable aplicar medidas de ciberseguridad que eviten accesos no autorizados o filtraciones de información. Además, las plataformas judiciales deben garantizar confidencialidad, disponibilidad e integridad de los datos procesales. Según Molina y Pachano (2025), la protección de datos personales constituye uno de los principales retos jurídicos dentro del entorno digital ecuatoriano.

Por consiguiente, el uso de tecnologías digitales también exige una constante capacitación de jueces, fiscales, abogados y servidores judiciales en materias relacionadas con informática jurídica y herramientas tecnológicas. La correcta utilización de plataformas digitales y sistemas electrónicos requiere conocimientos técnicos que permitan garantizar un adecuado desarrollo de las actuaciones procesales. Además, la brecha digital puede afectar el acceso igualitario a la justicia cuando ciertos sectores de la población carecen de recursos tecnológicos o conectividad adecuada. En este contexto, Jiménez y Pincay (2024) afirman que la expansión de la sociedad de la información obliga a replantear constantemente las estructuras jurídicas tradicionales frente a los nuevos escenarios digitales.

En resumen, la consolidación de la justicia digital refleja el proceso de adaptación del sistema jurídico a las exigencias de la sociedad tecnológica contemporánea (Constante y

López, 2025). La incorporación de herramientas digitales dentro de los procesos judiciales ha permitido fortalecer principios como celeridad, eficiencia y acceso a la justicia, aunque también ha generado nuevos desafíos normativos y tecnológicos. Además, la evolución constante de las tecnologías obliga a los Estados a actualizar permanentemente sus marcos regulatorios y sistemas de seguridad informática. De esta manera, el uso de tecnologías digitales en la administración de justicia representa una transformación estructural que continuará redefiniendo el funcionamiento de los sistemas judiciales modernos.

5.6 Retos de la justicia digital y debido proceso en entornos tecnológicos

La justicia digital representa una de las transformaciones más importantes dentro de los sistemas jurídicos contemporáneos, debido a la incorporación de tecnologías digitales en las actuaciones judiciales y administrativas. Este proceso ha permitido agilizar trámites, fortalecer la gestión procesal y facilitar el acceso remoto a los servicios judiciales. Sin embargo, también ha generado importantes desafíos relacionados con la protección de derechos fundamentales y las garantías procesales. Según Jáuregui (2025), la modernización tecnológica del Estado exige mecanismos capaces de equilibrar eficiencia administrativa y seguridad jurídica dentro de los entornos digitales.

Asimismo, uno de los principales retos de la justicia digital consiste en garantizar el debido proceso dentro de procedimientos desarrollados mediante plataformas tecnológicas. Esto implica asegurar que todas las partes procesales puedan ejercer adecuadamente su derecho a la defensa, presentar pruebas y participar en igualdad de condiciones durante las actuaciones judiciales. Además, las audiencias virtuales y expedientes electrónicos requieren sistemas tecnológicos confiables que permitan evitar interrupciones o limitaciones en la comunicación procesal. En este sentido, Gamboa et al. (2024) sostienen que la tutela efectiva de derechos constitucionales depende del respeto integral a las garantías procesales dentro de cualquier actuación judicial.

Por otra parte, la brecha digital constituye un problema relevante dentro de la implementación de la justicia tecnológica, ya que no todas las personas poseen acceso adecuado a internet, dispositivos electrónicos o conocimientos informáticos suficientes para interactuar con plataformas judiciales digitales. Esta situación puede generar desigualdades procesales y limitar el acceso efectivo a la justicia para determinados grupos sociales. Además, las dificultades tecnológicas pueden afectar especialmente a

personas en situación de vulnerabilidad o residentes en zonas con baja conectividad. Desde esta perspectiva, Corcino et al. (2026) consideran que la transformación digital de las instituciones públicas debe acompañarse de políticas orientadas a garantizar inclusión y accesibilidad tecnológica.

De igual manera, la protección de datos personales y la ciberseguridad representan desafíos fundamentales dentro de la justicia digital. Los sistemas judiciales almacenan información sensible relacionada con procesos penales, civiles y administrativos, lo cual exige mecanismos robustos de protección frente a accesos no autorizados, filtraciones o ataques informáticos. Además, la vulneración de información judicial puede afectar gravemente derechos relacionados con la intimidad, privacidad y seguridad jurídica de las personas. En consecuencia, los Estados deben implementar protocolos tecnológicos orientados a garantizar confidencialidad, integridad y disponibilidad de los datos procesales (Molina y Pachano, 2025; Ojeda y Suárez, 2025).

En relación con ello, la utilización de inteligencia artificial y sistemas automatizados dentro de los procesos judiciales también plantea importantes cuestionamientos éticos y jurídicos. Actualmente, algunas plataformas tecnológicas utilizan algoritmos para clasificar expedientes, gestionar información procesal o apoyar decisiones administrativas dentro de los tribunales. Sin embargo, el uso de estas herramientas puede generar riesgos asociados con discriminación algorítmica, falta de transparencia y ausencia de control humano suficiente. Según Jiménez y Pincay (2024), la expansión de los derechos digitales obliga a replantear constantemente los límites jurídicos y éticos del uso de tecnologías automatizadas dentro del sistema judicial.

Por consiguiente, otro reto importante radica en la autenticidad y valoración de las pruebas digitales dentro de los procesos judiciales electrónicos. La facilidad con la que ciertos archivos electrónicos pueden ser alterados o manipulados exige protocolos rigurosos para garantizar integridad y confiabilidad de la evidencia tecnológica. Además, los jueces requieren conocimientos especializados y apoyo técnico pericial para interpretar adecuadamente determinados elementos probatorios digitales. En este contexto, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) establece principios orientados a garantizar la validez jurídica y eficacia probatoria de los documentos electrónicos dentro del ordenamiento ecuatoriano.

En conclusión, la consolidación de la justicia digital exige una constante actualización normativa y tecnológica que permita responder adecuadamente a las nuevas dinámicas de la sociedad de la información. La evolución permanente de las tecnologías obliga a los sistemas jurídicos a desarrollar marcos regulatorios flexibles capaces de proteger derechos fundamentales sin limitar los beneficios de la innovación digital. Además, resulta indispensable fortalecer la capacitación tecnológica de jueces, fiscales, abogados y servidores judiciales para garantizar una adecuada administración de justicia en entornos digitales. De esta manera, el debido proceso en contextos tecnológicos se convierte en un elemento esencial para preservar legitimidad, transparencia y seguridad jurídica dentro de la justicia contemporánea.

Bibliografía

- Aguilar, M., Gordillo, D., Paredes, J., y León, G. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 10(Especial 1). <https://observatorio.anec.cu/uploads/064cd32a-1023-4201-9326-e386e3290528.pdf>
- Arango, N. (2024). Gobierno Electrónico y Gestión Administrativa. *Revista de Climatología Edición Especial Ciencias Sociales*, 24, 57. <https://doi.org/10.59427/rcli/2024/v24cs.56-65>
- Asamblea Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Registro Oficial Suplemento 557. Ministerio de Telecomunicaciones y de la Sociedad de la Información: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf>
- Becerra, A., Chang, C., Rea, M., Vargas, E., Colon, E., y Romero, H. (2024). Intimidad y protección de datos personales en historias clínicas digitales: análisis desde una perspectiva jurisprudencial. *Sinergia Académica*, 7(4), 411-427. <https://sinergiaacademica.com/index.php/sa/article/view/342/698>
- Benlonch, C., y Sarrión, J. (2022). Los derechos fundamentales ante las aporías de la era digital. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*(46), 3-28. <https://doi.org/10.22201/ijj.24484881e.2022.46.17046>
- Bonilla, J. (2025). Las plataformas digitales como herramientas anticorrupción: democracia, tecnología y transparencia en la era digital. *Universitá Ciencia*, 13(36), 116-131. <https://doi.org/10.5281/zenodo.15121041>
- Cajahuanca, G. (2025). Ciencias jurídicas en la era digital: revisión sistemática sobre innovaciones y desafíos legales actuales. *Revista Tribunal*, 5(12), 43-58. <https://doi.org/10.59659/revistatribunal.v5i12.192>
- Chuquicahua, W., Irigoyen, J., Guerrero, A., y Carrión, G. (2025). Modelo de gobierno digital para optimizar la gestión administrativa en una entidad pública. *Universidad y Sociedad*, 17(5), e5376-e5376. <https://rus.ucf.edu.cu/index.php/rus/article/view/5376>

- Código Orgánico Integral Penal (COIP)*. (2014). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Constante, O., y López, D. (2025). El alcance del derecho de la protección de datos de carácter personal. Análisis de la sentencia n. 2064-14-ep/21. *Revista Ciencia y Educación* , 6(9.3), 128-146. <https://doi.org/10.5281/zenodo.18123700>
- Constitución de la República del Ecuador*. (2008). https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
- Convención sobre Ciberdelincuencia*. (2001). Convenio de budapest: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Corcino, L., Cerafin, V., y Gonzales, J. (2026). Gobierno electrónico para la optimización de procesos en la administración pública: una revisión sistemática. *Revista InveCom/ISSN en línea: 2739-0063* , 6(3), 1-11. <https://doi.org/10.5281/zenodo.17479024>
- Cornejo, C. (2023). Modernización e implementación de la nueva gestión pública. Una revisión sistemática. *Revista de Climatología Edición Especial Ciencias Sociales* , 23, 73. <https://doi.org/10.59427/rcli/2023/v23cs.72-85>
- Dueñas, R., Ochoa, W., Ponce, Y., Vargas, G., y Aráuz, G. (2025). Análisis jurisprudencial de derechos fundamentales en el tenor del derecho constitucional. *Revistalexenlace* , 2(1), 10-19. <https://doi.org/10.63644/mb1ny291>
- Forero, L. (2023). La era digital y el derecho de la competencia: una mirada a los desafíos de la regulación. *Via Iuris*(35), 51-72. <https://doi.org/10.37511/viaiuris.n35a8>
- Gamboa, A., Gutiérrez, D., y García, Á. (2024). Garantías y Tutela de Derechos Constitucionales en el Ecuador. *Tesla Revista Científica* , 4(1), e368-e368. <https://doi.org/https://doi.org/10.55204/trc.v4i1.e368>
- Giler, P. (2023). La garantía jurisdiccional del hábeas data y sus implicaciones en Ecuador. Una aproximación al tratamiento normativo y jurisprudencial. *Ciencia Latina Revista Científica Multidisciplinar* , 7(3), 5064-5080. https://doi.org/10.37811/cl_rcm.v7i3.6534

- Gonzalo, S., Proaño, G., y Castro, F. (2025). Buenas prácticas para la protección de datos personales. *Noesis. Revista Electrónica de Investigación*, 7(2). <https://doi.org/10.35381/noesisin.v7i2.618>
- Guanín, O. (2024). El habeas data como garantía de protección al derecho a la intimidad. *Revista Científica de Ciencias Humanas y Sociales RECIHYS* , 2(1), 20-25. <https://doi.org/10.24133/recihys.v2i1.3472>
- Gutiérrez, J. (2022). Los datos personales en el Ecuador como un derecho humano una necesidad de mejoramiento en su regulación. *Revista Jurídica Crítica y Derecho* , 3(5), 53-66. <https://doi.org/10.29166/cyd.v3i5.3950>
- Jáuregui, P. (2025). El impacto del gobierno digital en la modernización del estado: revisión sistemática. *Revista Científica" Visión de Futuro"*, 29(1), 87-106. <https://www.redalyc.org/journal/3579/357980396007/357980396007.pdf>
- Jiménez, A., y Pincay, S. (2024). Derechos Digitales y Constitución: Retos Jurídicos ante la Sociedad de la Información. *Ciencia Latina: Revista Multidisciplinar*, 8(1), 8249-8264. https://doi.org/10.37811/cl_rcm.v8i1.10150
- Lara, H., y Romero, C. (2023). El alcance del derecho a la libertad de expresión frente al derecho privacidad e intimidad personal. *KIRIA: Revista Científica Multidisciplinaria* , 1(2), 69-82. <https://doi.org/10.53877/t0eb4x18>
- Ley Orgánica de Protección de Datos Personales*. (2021). Registro Oficial Suplemento 459.: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf>
- Machuca, S., Vinueza, N., Sampedro, C., y Santillán, A. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251. http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt
- Macías, J., y Espinoza, L. (2024). Evolución y desafíos del derecho constitucional en la protección de los derechos humanos en Ecuador. *Revista 593 Digital Publisher CEIT* , 9(5), 854-867. <https://doi.org/10.33386/593dp.2024.5.2684>

- Martínez, O., Freire, E., y Alzate, L. (2024). Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano. *European Public & Social Innovation Review* , 9, 1-21. <https://doi.org/10.31637/epsir-2024-1842>
- Melgar, K., Coronel, L., Ramírez, E., García, J., y Merino, J. (2026). Transformación digital en la gestión pública: Impacto de las nuevas tecnologías en la eficiencia administrativa. *Impulso, Revista de Administración*, 6(13), 110-127. <https://doi.org/10.59659/impulso.v.6i13.227>
- Mendoza, H. (2024). Regulación jurídica de la privacidad en el entorno digital y sus desafíos actuales. *Innova Science Journal*, 2(1), 28-40. <https://doi.org/10.63618/omd/i>
- Mendoza, J., Cobo, E., y Boza, J. (2021). La gestión pública y el gobierno abierto como herramienta de comunicación. *Universidad y Sociedad*, 13(S2), 583-590. <https://rus.ucf.edu.cu/index.php/rus/article/view/2359>
- Miranda, D., Tingo, M., Zamora, C., y Zamora, D. (2025). Impacto del gobierno electrónico en la eficiencia y transparencia de la gestión pública. *Revista Veritas de Difusão Científica* , 6(1), 659-682. <https://doi.org/10.61616/rvdc.v6i1.426>
- Molina, K., y Pachano, A. (2025). La protección de datos personales en el entorno digital ecuatoriano: análisis crítico del marco normativo y su aplicación práctica. *Sociedad & Tecnología* , 8(S3), 1053-1066. <https://doi.org/10.51247/st.v8iS3.350>
- Morón, A., Vértiz, P., Jara, O., Cornelio, R., y Rojas, R. (2025). Herramientas para la modernización de la gestión pública: una revisión sistemática. *Revista InveCom*, 6(2), 2. <https://dialnet.unirioja.es/servlet/articulo?codigo=10327108>
- Muñiz, M. (2023). Diplomacia tecnológica para la era digital. *Revista CIDOB d'Afers Internacionals*(134), 91-102. <https://doi.org/10.24241/rcai.2023.134.2.91>
- Ojeda, Z., y Suárez, C. (2025). El derecho a la protección de datos personales:¿ un derecho humano digital? *Ius Comitiālis*, 8(16), 151-166. <https://iuscomitialis.uaemex.mx/article/view/26625/19917>
- Ortiz, Z., Soto, R., y Ureña, P. (2025). Gobierno electrónico y la lucha contra la corrupción en la gestión pública: una revisión sistemática. *Revista Impulso* , 5(11), 72-87. <https://doi.org/10.59659/impulso.v.5i11.131>

- Protección de la información y de los datos.* (2009).
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>
- Rafael, W., y Anccasi, R. (2026). Gobierno digital y modernización del Estado: Una revisión bibliométrica. *Acta Peruana de Ciencias Sociales y Humanidades*, 2(1).
<https://apcsh-journal.org/index.php/apcsh/article/view/28>
- Ramírez, R. (2025). Gobierno abierto y transparencia en la administración pública: Revisión de buenas prácticas en América Latina. *Innovarium International Journal*, 3(2), 1-13. <https://revinde.org/index.php/innovarium/article/view/58>
- Reglamento del Parlamento Europeo y del Consejo.* (2016). (UE) 2013/679:
<https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- Reglamento General de Protección de Datos.* (2016). (RGPD): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Rivera, Y., y Maldonado, L. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. *Polo del Conocimiento* , 8(10), 982-1009.
<https://doi.org/10.23857/pc.v8i10.6172>
- Rodas, J., Alomoto, M., y Alvarado, L. (2025). El derecho a la información frente al derecho a la intimidad de los funcionarios públicos. *Revista Lex* , 8(29), 658-672.
<https://doi.org/10.33996/revistalex.v9i28.309>
- Rovira, Z., y Robles, L. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. *Revista Polo del Conocimiento*, 8(8), 1355-1373.
<https://polodelconocimiento.com/ojs/index.php/es/article/view/5908>
- Vargas, C. (2021). El gobierno digital y su implementación en el estado. *Ciencia Latina Revista Científica Multidisciplinar*, 5(6), 13767-13777.
https://doi.org/10.37811/cl_rcm.v5i6.1356
- Zambrano, J., Sasintuña, J., y Jarara, P. (2024). Responsabilidad civil por el incumplimiento de la normativa de protección de datos personales. *USFQ Law Review* , 11(2). <https://doi.org/10.18272/ulr.v1i2.3370>

Zambrano, L. (2024). Ámbito de operatividad del derecho al hábeas data como Acción de Garantía Constitucional en Ecuador. *Polo del Conocimiento: Revista científico-profesional* , 9(1), 2741-2763. <https://doi.org/10.23857/pc.v9i1.7385>



CIDPROS

Centro de innovación y desarrollo profesional

ISBN: 978-9907-9562-3-8



9 789907 956238