Laura Marcela Franco Mateus

Hacia un marco legal para la sociedad digital

Tesis para optar al título de Doctora en Derecho Público

Universidad Santo Tomás

Seccional Tunja

Director

Sergio Luis Mondragón Duarte. Phd.

2026

Resumen

La Quinta Revolución Industrial (5RI) está generando transformaciones profundas en lo social, lo económico, lo político y lo jurídico, cambiando también la manera en que la tecnología interactúa con los derechos fundamentales. La convergencia de tecnologías disruptivas crea entornos digitales interconectados y complejos, que avanzan tan rápido que el derecho tradicional no alcanza a seguirles el paso. Esto representa un reto especialmente fuerte para el constitucionalismo actual, porque derechos como la intimidad, el habeas data, la igualdad, la libertad de expresión y el debido proceso empiezan a verse expuestos a nuevos riesgos y tensiones.

En el caso colombiano, estas dificultades aparecen en fenómenos como la vigilancia masiva, la discriminación basada en algoritmos, la difusión de desinformación, el debilitamiento de la privacidad o incluso la afectación de garantías procesales cuando se usa inteligencia artificial para tomar decisiones judiciales, administrativas o empresariales. Tecnologías emergentes, como el metaverso, la tokenización de activos o las identidades digitales sintéticas, siguen funcionando sin reglas claras, lo que limita la capacidad del Estado para proteger a las personas y da lugar a respuestas tardías y más correctivas que preventivas.

Aunque la Constitución de 1991 ofrece un catálogo amplio de derechos, los llamados "derechos digitales" no tienen un reconocimiento autónomo ni una definición precisa. La regulación que existe en protección de datos, comercio electrónico y ciberseguridad es dispersa, tiene vacíos importantes y a menudo reacciona después del daño. La jurisprudencia ha avanzado en temas clave como la intimidad digital, la libertad de expresión en redes y el habeas data, pero todavía no contamos con un marco integral capaz de enfrentarse a los desafíos propios de la 5RI. Esto evidencia la necesidad de un constitucionalismo digital más coherente, actualizado y capaz de anticipar riesgos.

En este contexto, la investigación plantea un modelo de constitucionalismo digital para Colombia. No se propone crear una nueva categoría de derechos fundamentales a través de una reforma constitucional, porque reconocer un conjunto amplio y cambiante de "derechos digitales" no solo sería difícil, sino también conceptualmente inestable. En lugar de eso, se plantea fortalecer el marco constitucional actual mediante una interpretación más clara de cómo los derechos existentes deben aplicarse en entornos tecnológicos, y acompañarlo de una propuesta legislativa que desarrolle estos criterios sin pretender elevarlos al rango constitucional.

Los objetivos del trabajo se orientan a revisar la evolución histórica del constitucionalismo hasta llegar a su enfoque digital, analizar el impacto de las nuevas tecnologías sobre los derechos en Colombia, estudiar experiencias comparadas como el GDPR, la AI Act y la Carta de Derechos Digitales de España, diseñar un modelo de constitucionalismo digital adaptado al país y, finalmente, estructurar una propuesta normativa que fortalezca la soberanía de los datos, la transparencia algorítmica y la gobernanza tecnológica. Esta propuesta busca ser una ley de desarrollo y no una norma que cree derechos fundamentales nuevos.

La investigación adopta un enfoque cualitativo, con momentos descriptivos, analíticos y propositivos. Se inicia con un diagnóstico doctrinal, normativo y jurisprudencial, continúa con el análisis de riesgos y vacíos y termina con el diseño del modelo y su correspondiente propuesta legislativa, siempre en coherencia con la Constitución.

El principal aporte es un modelo de constitucionalismo digital que no pretende inventar derechos nuevos, sino aclarar cómo deben protegerse los existentes cuando se ejercen en entornos digitales. Se fundamenta en la dignidad humana, la eficacia de los derechos, la transparencia de los algoritmos, la soberanía de los datos y la responsabilidad diferenciada entre el Estado, las plataformas digitales y quienes desarrollan tecnología. Incluye mecanismos para anticipar riesgos, como el fortalecimiento del habeas data digital, el control de decisiones automatizadas y la supervisión de tecnologías de alto riesgo.

La propuesta legislativa plantea lineamientos y obligaciones para los actores del ecosistema digital, armonizando la experiencia colombiana con referentes internacionales, pero sin copiar modelos ni asumir que existe un catálogo autónomo de derechos digitales. Académicamente, el trabajo contribuye al debate sobre constitucionalismo digital y aporta a la línea de Derecho Público y Digital. En lo social, ofrece herramientas de protección frente a los riesgos de la transformación tecnológica. En lo institucional, genera productos como publicaciones, ponencias y actividades de formación.

En síntesis, la investigación identifica un vacío importante del ordenamiento colombiano: la falta de un marco de constitucionalismo digital que permita proteger los derechos en escenarios altamente tecnológicos. El modelo propuesto ofrece una arquitectura jurídica preventiva, coherente con la Constitución y centrada en la dignidad humana, que prepara al país para enfrentar con mayor claridad los retos de la Quinta Revolución Industrial.

Palabras claves: Constitucionalismo digital, Quinta Revolución Industrial, Derechos digitales, Transformación digital, Tecnologías emergentes.

Abstract

The Fifth Industrial Revolution (5IR) is generating profound social, economic, political, and legal transformations, also changing how technology interacts with fundamental rights. The convergence of disruptive technologies creates interconnected and complex digital environments that are advancing so rapidly that traditional law cannot keep pace. This represents a particularly significant challenge for current constitutionalism, because rights such as privacy, data protection, equality, freedom of expression, and due process are beginning to face new risks and tensions.

In the Colombian case, these difficulties manifest in phenomena such as mass surveillance, discrimination based on algorithms, the spread of disinformation, the erosion of privacy, and even the undermining of procedural guarantees when artificial intelligence is used to make judicial, administrative, or business decisions. Emerging technologies, such as the metaverse, asset tokenization, and synthetic digital identities, continue to operate without clear regulations, limiting the State's capacity to protect individuals and leading to delayed and more corrective than preventive responses. Although the 1991 Constitution offers a broad catalog of rights, so-called “digital rights” lack autonomous recognition and a precise definition. Existing regulations on data protection, e-commerce, and cybersecurity are fragmented, contain significant gaps, and often react only after harm has occurred. Jurisprudence has made progress on key issues such as digital privacy, freedom of expression online, and habeas data, but we still lack a comprehensive framework capable of addressing the challenges of the Fifth Industrial Revolution (5IR). This highlights the need for a more coherent, up-to-date digital constitutionalism capable of anticipating risks.

In this context, this research proposes a model of digital constitutionalism for Colombia. It does not propose creating a new category of fundamental rights through constitutional reform, because recognizing a broad and evolving set of “digital rights” would not only be difficult but also conceptually unstable. Instead, the proposal aims to strengthen the current constitutional framework through a clearer interpretation of how existing rights should be applied in technological environments, accompanied by a legislative proposal that develops these criteria without seeking to elevate them to constitutional status.

The objectives of this work are to review the historical evolution of constitutionalism leading to its digital focus, analyze the impact of new technologies on rights in Colombia, study comparative experiences such as the GDPR, the AI Act, and Spain's Charter of Digital Rights, design a model of digital constitutionalism adapted to the country, and finally, structure a regulatory proposal that strengthens data sovereignty, algorithmic transparency, and technological governance. This proposal seeks to be a development law, not a regulation that creates new fundamental rights.

The research adopts a qualitative approach, with descriptive, analytical, and propositional phases. It begins with a doctrinal, normative, and jurisprudential diagnosis, continues with an analysis of risks and gaps, and concludes with the design of the model and its corresponding legislative proposal, always in accordance with the Constitution.

The main contribution is a model of digital constitutionalism that does not seek to invent new rights, but rather to clarify how existing rights should be protected when exercised in digital environments. It is based on human dignity, the effectiveness of rights, the transparency of algorithms, data sovereignty, and the differentiated responsibility of the State, digital platforms, and technology developers. It includes mechanisms to anticipate risks, such as strengthening digital habeas data, controlling automated decisions, and supervising high-risk technologies.

The legislative proposal establishes guidelines and obligations for actors in the digital ecosystem, harmonizing Colombian experience with international benchmarks, but without simply copying models or assuming the existence of an autonomous catalog of digital rights. Academically, the work contributes to the debate on digital constitutionalism and supports the field of Public and Digital Law. Socially, it offers tools for protection against the risks of technological transformation. Institutionally, it generates outputs such as publications, presentations, and training activities.

In summary, the research identifies a significant gap in the Colombian legal system: the lack of a digital constitutional framework to protect rights in highly technological environments. The proposed model offers a preventive legal architecture, consistent with the Constitution and centered on human dignity, which prepares the country to face the challenges of the Fifth Industrial Revolution with greater clarity.

Keywords: Digital Constitutionalism, Fifth Industrial Revolution, Digital Rights, Digital Transformation, Emerging Technologies.

Tabla de contenido

Resumen 2

Abstract 4

Agradecimientos 16

Dedicatoria 17

Introducción 19

TÍTULO I: EL CONSTITUCIONALISMO Y SU SIGNIFICACIÓN Y EVOLUCIÓN HISTÓRICA. 24

1. Tipos de Constitucionalismo. 25

1.1. Constitucionalismo clásico: surgimiento y bases. 26

1.2. El neoconstitucionalismo: delimitaciones conceptuales. 29

1.2.1. Contexto histórico del neoconstitucionalismo y causas de su surgimiento 33

1.2.2. Europa de la posguerra: el laboratorio del Estado constitucional 34

1.2.3. El giro interpretativo y la crisis del positivismo 37

1.2.4. América Latina: transición democrática y constitucionalismo garantista 39

1.2.5. Fundamentos teóricos y filosóficos del Neoconstitucionalismo. 42

1.2.6. La supremacía material de la Constitución 46

1.2.7. Reglas y principios: un nuevo paradigma normativo 49

1.2.8. Ponderación y argumentación jurídica 52

1.2.9. Moral y crítica democrática 54

1.3. La Constitución como carta de valores 58

1.3.1. El juez constitucional como garante moral 61

1.4. Tensiones y críticas al componente moral 63

1.5. Difusión latinoamericana: transformación del neoconstitucionalismo en Latinoamérica actualmente. 66

1.5.1. Neoconstitucionalismo en Colombia. 68

1.5.2. Contexto histórico y transformaciones sociales 71

TÍTULO II: EL FENOMENO DE DIGITALIZACIÓN Y EL LA EVOLUCIÓN DE LA QUINTA REVOLUCIÓN INDUSTRIAL. 75

2. Historia de las revoluciones industriales. 75

2.1. Primera Revolución Industrial 78

2.2. Segunda Revolución Industrial 82

2.3. Tercera Revolución Industrial 86

2.4. Cuarta Revolución Industrial 89

2.5. Quinta Revolución Industrial 92

2.6. Nuevas tecnologías de la quinta revolución industrial 95

2.7. Digitalización 101

2.7.1. La expansión de Internet y la sociedad en red: infraestructuras tecnológicas transaccionales. 104

2.7.2. La concentración del poder tecnológico en poderes privados globales 'Big Tech'. 107

2.7.3. Sistemas algorítmicos autónomos: la creación de 'Sociedades algorítmicas'. 115

2.8. Evolución de la sociedad tecnológica y su enfoque interdisciplinario 120

2.9. Tecnologías emergentes en la quinta revolución industrial y su impacto jurídico 123

2.9.1. Big Data 123

2.10. Inteligencia Artificial 133

2.10.1. Clases de inteligencia artificial 137

2.10.2. Riesgos de la IA en el Estado de derecho. 141

2.7 Blockchain y tokenización. 150

2.8 Metaverso 154

2.8.1 Efectos del metaverso en los seres humanos 156

2.8.2 Aspectos Controversiales 158

2.9 Transhumanismo Y Poshumanismo 159
2.10 Transhumanismo y Bioética 163
2.11 Sintiencia Digital 166
2.12 Las Personas Ciborg 168
TÍTULO III. CONSTITUCIONALISMO DIGITAL. 174
3. Delimitaciones doctrinales y aparición. 174
3.1. La insuficiencia del marco constitucional clásico 179
3.2.1. Principios y características del constitucionalismo digital 182
3.2.2. Extensión de la supremacía constitucional al ciberespacio 184
3.3. Protección frente a poderes privados globales 184
3.3.1. Reconocimiento de nuevos derechos digitales 185
3.3.2. Dimensión transnacional y gobernanza cooperativa 186
3.3.3. Normativa y jurisprudencia destacada 187
3.3.4. Desafíos y proyección hacia el constitucionalismo del derecho digital 189
3.4. Inserción del constitucionalismo digital en Latinoamérica. 192
3.4.1. México. 193
3.4.2. Chile. 194
3.4.3. Brasil. 195
3.5. Constitucionalismo digital: inserción en Colombia 197
4. Marco constitucional, legal y jurisprudencial colombiano frente a la transformación digital. 200
5. Protección de los derechos fundamentales en entornos digitales 201
5.1. Marco normativo internacional: tratados en la regulación de nuevas tecnologías. 202
5.1.1. Reglamento General de Protección de datos (GDPR). 202
5.1.2. Law Enforcement directive (LED). 204
5.1.3. Declaración europea sobre los derechos y principios digitales para la década digital. 205

5.1.4. AI Act. 207
5.1.5. Derechos fundamentales involucrados y riesgos constitucionales 212
5.2. Principios constitucionales aplicables....214
5.3. Marco legal y normativo de la digitalización en Colombia....215
5.3.1. Introducción a la 'sociedad digital'. 215
5.3.2. Protección y regulación de datos. 216
5.3.3. Decretos 088 y 338 de 2022 218
5.3.4. Ley 2502 de 2025 218
5.3.5. Transformación digital en Colombia 222
5.3.6. Políticas públicas y CONPES 223
5.3.7. Políticas públicas posterior a la constitución de 1991 223
5.3.8. Antecedentes de políticas públicas sobre desarrollo digital en Colombia 232
5.3.9. Plan Nacional de Desarrollo 2022-2026....235
5.3.10. Estrategia Nacional Digital de Colombia 2023-2026 (END 2023-2026) 237
5.4. Jurisprudencia relevante en entornos digitales 243
5.4.1. Protección de datos y privacidad digital....244
5.4.2. Libertad de expresión y redes sociales 246
5.5. Vacíos normativos y desafíos regulatorios 248
5.5.1. Caso 'DAO'. 248
5.5.2. Falta de regulación integral para tecnologías emergentes 254
5.5.3. Brecha entre avance tecnológico y respuesta legal....263
5.5.4. Necesidad de un constitucionalismo digital colombiano....266
TÍTULO IV: RETOS Y DESAFÍOS DEL CONSTITUCIONALISMO DIGITAL COLOMBIANO. 270
6. Retos normativos y legislativo 271

5.1. Posibles mecanismos institucionales y recomendaciones para la regulación en el ámbito digital. 275
5.2. Retos institucionales y socioculturales 279
5.3. Otros desafíos y desarrollos recientes del constitucionalismo digital 280
5.3.1. Impactos sociales y éticos de la digitalización 280
5.3.2. Responsabilidad de plataformas digitales y neutralidad de la red 282
5.3.3. Proyectos de Leyes colombiano de Inteligencia Artificial 283
5.4. Derecho comparado de derechos digitales. 287
TÍTULO V: PROPUESTA NORMATIVA Y MODELO DE CONSTITUCIONALISMO DIGITAL COLOMBIANO. 296
6. Lineamientos para un marco normativo integral de derechos digitales 298
6.1. Diagnóstico crítico del impacto de la digitalización en los derechos fundamentales. 316
6.2. Retos y desafíos del constitucionalismo digital en Colombia 318
6.3. Propuesta de Ley de Constitucionalismo Digital en Colombia 321
6.3.1. Objeto y finalidad de la ley 321
6.3.2. Principios rectores 322
6.3.3. Reconocimiento y protección de los derechos digitales 324
6.3.4. Deberes de las plataformas digitales y los usuarios 327
6.3.5. Proyecto de Ley para la Regulación de Nuevas Tecnologías, Derechos y Obligaciones, Creación de la ANSDIA, entre otros. 330
6.3.6. Parámetros, criterios y lineamientos del proyecto de ley 337
6.4. Modelo de gobernanza para el constitucionalismo digital 341
6.4.1. Organización institucional 343
6.4.2. Gobernanza digital preventiva 343
6.4.3. Sistema de monitoreo y respuesta a ciberamenazas 344
6.5. Estrategia de implementación 344
6.5.1. Fases de implementación 344

6.5.2. Instrumentos normativos y de política pública 346
6.5.3. Mecanismos de control y seguimiento 346
6.6. Impacto esperado 347
6.7. Defensa del proyecto de ley (Doctorando) 349
Conclusiones 352
Referencias Bibliográficas. 361
Referencias bibliográficas jurídicas y resoluciones administrativas. 387
Anexos .....**¡Error! Marcador no definido.**
Proyecto de Ley .....**¡Error! Marcador no definido.**
Socializaciones de resultados.....**¡Error! Marcador no definido.**

Tabla de figuras

Figura 1.Línea de tiempo sobre la evolución industrial 77
Figura 2. Movimientos migratorios a Estados Unidos 83
Figura 3. Proceso de comunicación según el HTTP. 105
Figura 4. Infraestructura digital. 111
Figura 5. Funcionamiento de un algoritmo. 116
Figura 6.Definición de los pilares de Big Data 127
Figura 7. Funcionamiento de la Inteligencia Artificial. 134
Figura 8. Evolución del blockchain 152
Figura 9. Acceso al metaverso. 155
Figura 10. Riesgos según el AI Act. 208
Figura 11. Ejes de la estrategia 238
Figura 12. Consentimiento informado expreso. 276
Figura 13. Flujograma del Proyecto de Ley 340

Tablas

Tabla 1. Conceptos nuevas tecnologías 96
Tabla 2. Unidades básicas de información y tratamiento de datos 124
Tabla 3. La Ciborgización 170
Tabla 4. Derecho comparado sobre constitucionalismo digital 191
Tabla 5. Expedición de las normas frente al marco jurídico. 219
Tabla 6. CONPES últimos 34 años 224
Tabla 7. Políticas públicas sobre desarrollo digital en Colombia 233
Tabla 8. Ejes, objetivos y líneas estratégicas de la END 2023-2026 239
Tabla 9. Comparación normativa internacional sobre Inteligencia Artificial y derechos digitales 285
Tabla 10. Ciberderechos según Warkentin 288
Tabla 11. Derechos digitales según la APC 288
Tabla 12. Derechos de la ciudadanía digital según Bustamente Donas 289
Tabla 13. Derechos digitales según Riofrío Martínez-Villalba 290
Tabla 14. Derechos digitales según Consejo de Europa 290
Tabla 15. Contraste de jurisdicciones en el ambito de derecho digital. 292
Tabla 16. Evolución de normas en algunos países 314

Anexos

Anexo 1. Proyecto de Ley .....**¡Error! Marcador no definido.**

Anexo 2. Socializaciones de resultados……326

Agradecimientos

A lo largo de este camino, me ha tocado soñar en un país donde la educación es un lujo, las oportunidades son limitadas y en un mundo donde, a menudo, el machismo minimiza a la mujer. Como madre soltera, mis agradecimientos son infinitos hacia mis hijas, quienes han sido mi mayor fuente de inspiración y motivación. A mi madre, por su amor incondicional, y a mis tres hermanas, por su apoyo constante.

Agradezco profundamente a ICETEX, que hizo posible este sueño, y a mi director de tesis, por su confianza en mi trabajo, por responder a mis dudas a tiempo y por impulsarme a seguir adelante, incluso en los momentos más difíciles. También a mi alma mater, el lugar donde comencé a soñar con ser abogada y hoy cierro este ciclo alcanzando el sueño de ser doctora.

A mis docentes y compañeros, quienes me mostraron que el Derecho es un campo en constante evolución y me enseñaron a cuestionar, analizar y transformar. Gracias a todos por su apoyo, su paciencia y sus enseñanzas.

Dedicatoria

A todas las mujeres, para que sigan soñando y luchando por hacer realidad sus sueños. Todo comienza en la mente, y ella es el motor que nos impulsa a convertir todo en realidad. Que nunca dejen de creer en su potencial, porque en su interior está la fuerza para lograr lo que se propongan.

Nota De Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Introducción

En el presente trabajo se propone una reconstrucción investigativa sobre las transformaciones tecnológicas del siglo XXI, las cuales han reconfigurado de manera profunda las dinámicas de interacción social, económica, política y jurídica. La Quinta Revolución Industrial (5RI), impulsada por la inteligencia artificial, el Big Data, la robótica avanzada, la biotecnología, la realidad inmersiva y el metaverso, ha generado escenarios inéditos para la protección de los derechos fundamentales. A partir de este panorama, la relación entre el derecho y la tecnología requiere adoptar una perspectiva que evite caer en esencialismos tecnológicos y que, en cambio, privilegie el análisis de las dimensiones sociales de la tecnología, dado que las relaciones sociales evolucionan al compás de la innovación (Balkin, 2015, pp. 59-60).

Estas tecnologías tienen el potencial de transformar profundamente todos los aspectos de la vida en sociedad. Sin embargo, su aparición y proliferación no se desarrolla dentro de los límites de los sistemas organizativos, éticos y regulatorios tradicionales. En la actualidad, la humanidad atraviesa un punto de inflexión que exige nuevos modelos económicos y normativos capaces de sostener el rápido desarrollo tecnológico (Pagallo et al., 2018). Además, la profundización de la interconexión global y la automatización a gran escala que acompañan a estas tecnologías plantean desafíos sin precedentes para el constitucionalismo contemporáneo, especialmente en materia de intimidad, hábeas data, igualdad, libertad de expresión y debido proceso.

El problema de investigación que orienta esta tesis surge precisamente de la tensión existente entre el acelerado cambio tecnológico y la insuficiencia del marco constitucional colombiano para responder a los desafíos propios de la era digital. A pesar de la existencia de normas en materia de protección de datos personales, comercio electrónico y ciberseguridad, estas resultan fragmentarias y de naturaleza mayormente reactiva, sin configurar un régimen integral de derechos digitales. Este panorama normativo incompleto pone de manifiesto la necesidad urgente de formular un modelo de constitucionalismo digital para Colombia que logre articular principios constitucionales, derechos fundamentales y responsabilidades claras para los actores tecnológicos. Por lo tanto, la orientación y pregunta problema que guía esta investigación corresponde a ¿En Colombia es posible adecuar el constitucionalismo digital de forma estandarizada para el refuerzo y protección de derechos humanos frente a los avances de la quinta revolución industrial?

La hipótesis se centra en un análisis comparativo y vivo de la Constitución Política de 1991, la cual es concebida como un pacto fundacional de derechos y garantías, y es el documento fundacional que debe irradiar todas las áreas de aplicación legislativa y judicial. Empero, es válido recordar que la Constitución fue diseñada para un entorno predominantemente analógico, y, en consecuencia, enfrenta tensiones significativas frente a la realidad digital actual. A su vez, es de importancia mencionar la Corte Constitucional, creada a raíz de la Constitución de 1991, la cual ha permitido que la Constitución tenga una aplicación continua, implementando la regla del precedente constitucional y análisis de aspectos formales como casos que implican los actores que se analizarán a lo largo de este documento. El medio ya no se despliega en la realidad de un territorio fijo, sino en la convivencia de un espacio nuevo: los espacios virtuales; en donde la regla imperante corresponde a la actuación de algoritmos autónomos y la circulación transnacional de datos, lo que desemboca en un término conocido como 'sociedades algorítmicas' (San José et al., 2022).

La concurrencia de fenómenos tecnológicos parece desplazar el rol del Estado como garante de seguridad y protección de derechos fundamentales; cuando son actores que no tienen una ubicación o territorial, si quiera, personería jurídica propia. Las preguntas sobre la relación entre las personas físicas y entes de tecnología dejan en claro vacíos normativos; entendiendo los vacíos dentro de la legislación actual, las leyes actuales de tratamiento de datos o leyes sobre vigilancia y transparencia institucional; los vacíos referentes en el trabajo también se analizan desde una perspectiva constitucional, y el papel del Estado de derecho en su poder legislativo para hacer frente a los desarrollos tecnológicos sin menoscabar su importancia y adaptación al entorno.

Una de las problemáticas centrales que atañe a esta tesis corresponde a la ausencia de un reconocimiento formal de los derechos digitales como categoría autónoma. Esta carencia limita la capacidad del Estado para responder de manera eficaz a fenómenos como la vigilancia masiva, la discriminación algorítmica, la expansión de dominio de entidades tecnológicas translaciones o la explotación indiscriminada de datos personales.

Para atender las problemáticas identificadas, el objetivo general de esta tesis es analizar la evolución tecnológica contemporánea y los fenómenos asociados, evaluando su impacto en el Estado de derecho y en la garantía de los derechos fundamentales, con el propósito de desarrollar un modelo de Constitucionalismo Digital para Colombia que fortalezca y actualice la protección de dichos derechos frente a los desafíos de la Quinta Revolución Industrial. Este objetivo se articula mediante la identificación de vacíos normativos y la formulación de una

propuesta legislativa coherente con los riesgos, dinámicas y potencialidades de las tecnologías emergentes.

De este objetivo general se derivan los siguientes objetivos específicos:

1. Analizar la evolución del constitucionalismo, desde sus orígenes hasta la propuesta de un constitucionalismo digital, identificando sus fundamentos teóricos y doctrinales.
2. Examinar los impactos de las tecnologías disruptivas de la Quinta Revolución Industrial sobre los derechos fundamentales en Colombia, evidenciando riesgos y vacíos normativos.
3. Realizar un análisis jurídico y comparado de la normativa nacional e internacional sobre protección de datos, inteligencia artificial y derechos digitales, identificando estándares aplicables.
4. Desarrollar un modelo de constitucionalismo digital colombiano y un proyecto de ley asociado que articulen principios, mecanismos de protección de derechos y responsabilidades de los actores tecnológicos, contribuyendo al fortalecimiento del marco jurídico nacional.

La metodología utilizada será de análisis cualitativo, pues se partirá de la recopilación de bibliografía utilizada para la profundización e investigación de temas específicos relativos a la tecnología; los cuales permitirán dar un alcance más entendible no solo al funcionamiento 'técnico' de las tecnologías, sino como sus dinámicas pueden llegar a causar daño a derechos fundamentales y su inserción para la alineación en el ordenamiento jurídico colombiano. La bibliografía corresponde a artículos científicos y libros que se centran alrededor de este tema, recalcando específicamente "El capitalismo de vigilancia" por Zuboff (2019) entre otros autores que han puesto énfasis en el desarrollo tecnológico, por otro lado, autores como Celeste (2018) y De Gregorio (2022) son pilares fundamentales en la comprensión del Constitucionalismo digital, sus teorías, tesis y comprensión de estos fenómenos se abordarán de forma descriptiva en la primera parte de este trabajo. Sumada a la metodología cualitativa se hará un análisis exhaustivo de regulación internacional (ONU, Comisión Europea) y jurisprudencia internacional (TJUE, Cortes de Estados Unidos) y nacional (Corte Constitucional); finalizando con el análisis de normativa vigente en Colombia al respecto, con

carácter descriptivo, analítico y propositivo. Cabe resaltar que la finalidad del trabajo tiene el fin de desembocar en el diseño y propuesta legislativa, la cual corresponderá a la parte final de este trabajo, después de la ardua y extensiva investigación, comparación y contraste, se buscará ajustar el proyecto de ley sobre protección de derechos fundamentales en la nueva 'era' digital concordando con el contexto colombiano.

La estructura de la tesis se organiza en cinco capítulos interrelacionados, siguiendo un orden progresivo que avanza desde los fundamentos conceptuales hasta la propuesta normativa final.

En el primer capítulo, se abordan las bases teóricas y el recorrido histórico del constitucionalismo, con el fin de comprender su evolución y el surgimiento de nuevas perspectivas frente a la era digital, se hace mención del Constitucionalismo clásico que permitió el surgimiento del neoconstitucionalismo, los contextos históricos que rodearon y moldearon las perspectivas demarcadas en cada una de las corrientes, y la supremacía de la constitución, y como el mismo se difundió en Latinoamérica.

Continuando con el hilo y contexto histórico, en el segundo capítulo se busca centrar el fenómeno de la digitalización, desde los acontecimientos previos en las anteriores revoluciones industriales hasta llegar a lo que conocemos hoy en día como 'digitalización'. Adicionalmente, en este capítulo se navegará la expansión del internet, la protección de datos, y concentración del poder tecnológico en entidades transnacionales; continuando con los sistemas algorítmicos autónomos cuya principal fuente y funcionamiento se dan gracias a 'big data' (Newman y Ángel, 2020). Finalizando con el relativamente reciente (y quizá más impactante) fenómeno tecnológico: la inteligencia artificial (de Oliveira, 2021).

Una vez sentadas las bases tanto del constitucionalismo, como el de la tecnología, es menester que el tercer capítulo haga referencia al constitucionalismo digital. Sus definiciones, cómo el producto y trasegar de la historia constitucional nos ha llevado a este momento (Celeste, 2018), comparando normativas vigentes y actuales, y ejemplos del constitucionalismo digital, su proyección y aplicación en el contexto colombiano. Por ello este capítulo también incluye un análisis normativo y jurisprudencial vigente en Colombia, contrastándolo con referentes internacionales para identificar vacíos, desafíos y oportunidades de mejora.

El capítulo 4 aborda, en específico, los retos y desafíos del constitucionalismo digital, no solamente en el ámbito normativo o legal, sino sus dimensiones sociales y posibles mecanismos de regulación ante las problemáticas desarrolladas en capítulos anteriores.

Para finalizar, el capítulo 5 presenta la propuesta normativa y modelo constitucional digital para Colombia, la propuesta legislativa busca dar respuesta a los vacíos y retos que trae esta ultima revolución industrial.

En términos generales, esta tesis doctoral pretende responder a un vacío normativo sustancial en el país, planteando un modelo integral para la protección de los derechos digitales. El planteamiento combina la teoría constitucional, el análisis jurídico comparado y una propuesta normativa concreta, con la intención de proyectar a Colombia hacia los debates internacionales sobre derechos fundamentales en entornos tecnológicos.

TÍTULO I: EL CONSTITUCIONALISMO Y SU SIGNIFICACIÓN Y EVOLUCIÓN HISTÓRICA.

El constitucionalismo, a lo largo de la historia, ha representado la respuesta jurídica frente a los excesos del poder. Desde la conformación del Estado moderno, la necesidad de imponer límites claros a la autoridad y de garantizar un núcleo irreductible de derechos fundamentales ha impulsado cambios sucesivos en el pensamiento constitucional. Dichas transformaciones no han sido ajenas a las circunstancias históricas, sociales y políticas de cada época y, en tiempos recientes, se han visto intensamente marcadas por el impacto de las innovaciones tecnológicas. Estas han introducido nuevas formas de interacción social y de ejercicio del poder que modifican los marcos tradicionales de regulación.

En el presente, la humanidad enfrenta los retos propios de la denominada Quinta Revolución Industrial, caracterizada por la interconexión digital, el uso masivo de inteligencia artificial, el aprovechamiento del *big data* y el despliegue de plataformas tecnológicas con alcance transnacional. Este escenario plantea desafíos inéditos para la efectividad de los derechos fundamentales, ya que actores privados (en especial las grandes corporaciones tecnológicas) poseen hoy la capacidad de incidir sobre la libertad de expresión, la privacidad y la autodeterminación informativa de millones de personas, a un nivel que incluso puede superar al de algunos Estados (Zuboff, 2019).

Ante tales dinámicas, el constitucionalismo digital emerge como una proyección necesaria de los principios y valores constitucionales hacia el ciberespacio, con el propósito de responder a las tensiones entre poder, derechos y tecnología. De forma complementaria, el denominado constitucionalismo del derecho digital se vislumbra como una etapa posterior (orientada a la creación de un marco normativo integral) que permita enfrentar los riesgos asociados al poder algorítmico y a la gobernanza global de los datos.

Por ello, se hace necesario el análisis histórico del constitucionalismo, el análisis de las bases y principios primigenios y su ubicación en el contexto actual, la delimitación teórica de lo que se entiende por constitucionalismo y su proyección en la modernidad de cara a los retos que enfrenta la digitalización mencionada anteriormente. Teniendo en cuenta la preservación de los derechos fundamentales, en específico, los de legalidad, transparencia y control democrático prevalezcan frente a posibles vulneraciones dadas por el contexto actual del siglo XXI (quinta ola industrial). Adicionalmente, se delimitará lo que se entiende por

constitucionalismo digital, sus repercusiones, antecedentes, al igual que su proyección en el contexto colombiano.

Los retos que afrontan en forma global las instituciones públicas y privadas en el ámbito de automatización, big data e inteligencia artificial serán estudiados de forma correspondiente, a su vez sus respuestas y soluciones en el ámbito internacional. Teniendo en cuenta los retos y desafíos, se analizarán a su vez en el contexto de Colombia, las particularidades en las cuales se aborda la información y cuestiones que corresponden específicamente a la creación de políticas públicas que den respuesta a estos desafíos, garantizando la protección de derechos fundamentales en la era digital.

1. Tipos de Constitucionalismo.

El estudio de los distintos tipos de constitucionalismo resulta esencial para comprender la evolución del pensamiento jurídico y político en torno a la organización del poder y la protección de los derechos fundamentales. Cada etapa del constitucionalismo refleja una respuesta particular a los desafíos históricos, sociales y tecnológicos de su tiempo, configurando un proceso dinámico de adaptación de los principios de libertad, justicia y soberanía. Analizar sus distintas manifestaciones, desde el constitucionalismo clásico hasta las expresiones contemporáneas como el constitucionalismo digital, permite identificar las continuidades y rupturas que han moldeado la noción moderna de Estado de Derecho.

Tener claridad sobre los tipos de constitucionalismo no solo facilita la comprensión de su desarrollo teórico, sino que también permite valorar su vigencia frente a los nuevos escenarios del poder. Mientras el constitucionalismo clásico se centró en limitar la autoridad estatal, los modelos actuales deben enfrentar la compleja realidad del siglo XXI, en la que el poder se dispersa entre actores públicos, privados y tecnológicos. En este contexto, surge la necesidad de repensar la función del derecho constitucional frente a fenómenos como la inteligencia artificial, la gobernanza algorítmica y la circulación global de datos.

Posterior a lo que se conoce como constitucionalismo clásico, a medida que el constitucionalismo avanzaba, surgió la necesidad de que las normas legales fueran más precisas, ya que cualquier supuesto no contemplado en la Constitución no podía ser tramitado por los órganos jurisdiccionales. En este contexto, los Estados comenzaron a adoptar el **neoconstitucionalismo**, que permite superar un positivismo estricto y dotar a la legislación de

mayor flexibilidad y enfoque en la protección de derechos fundamentales (Espinoza & Hidalgo, 2022).

En medio del escenario que deja la digitalización, constitucionalismo adquiere un nuevo papel, presentándose como una evolución necesaria del pensamiento constitucional, al proyectar los valores y principios tradicionales del constitucionalismo hacia los entornos digitales. Se entiende como el conjunto de principios, valores y mecanismos orientados a limitar el poder (estatal o privado) en los espacios digitales, garantizando la protección efectiva de los derechos fundamentales y la preservación de los valores del Estado constitucional en la esfera virtual (Celeste, 2019; Suzor, 2020). Este nuevo paradigma no sustituye las bases del constitucionalismo clásico, sino que las amplía y actualiza para responder a los desafíos derivados de la tecnología, las plataformas globales y la inteligencia artificial.

Por ello, el estudio del constitucionalismo digital no puede desligarse de su raíz histórica. Solo comprendiendo la trayectoria de los modelos constitucionales anteriores es posible dimensionar la magnitud del cambio que supone trasladar los principios del Estado de Derecho al ciberespacio. Así, el análisis de las formas clásicas, liberal, social y contemporánea del constitucionalismo constituye un punto de partida indispensable para fundamentar cualquier propuesta de actualización teórica en el contexto actual.

1.1.Constitucionalismo clásico: surgimiento y bases.

El constitucionalismo clásico constituye la base histórica y doctrinal del derecho constitucional moderno, desarrollado entre los siglos XVII y XVIII como respuesta al absolutismo monárquico europeo. Su propósito fundamental fue limitar el poder del Estado y garantizar las libertades individuales, dando lugar a un Estado liberal de derecho. Este paradigma alcanzó su máxima expresión en dos hitos históricos: la independencia de las trece colonias de Norteamérica en 1776 (que originó la Constitución de 1787) y la Revolución Francesa de 1789 (que consolidó el principio de soberanía popular y la supremacía de la ley) (Ferrajoli, 2001).

En el contexto estadounidense, la Constitución de 1787 y los Federalist Papers (redactados por Alexander Hamilton, James Madison y John Jay) constituyeron el primer esfuerzo sistemático para organizar un poder político limitado y sometido a una Constitución escrita como norma suprema. En Europa, Montesquieu, en El espíritu de las leyes (1748/2003),

sostuvo que la libertad ciudadana solo podía preservarse mediante la división funcional de los poderes del Estado, evitando así la concentración en una sola autoridad.

Desde una perspectiva filosófica, el constitucionalismo clásico se nutrió de la teoría del contrato social. John Locke (1689/1999) defendía que los individuos, al salir del estado de naturaleza, celebraban un pacto para proteger sus derechos a la vida, la libertad y la propiedad, legitimando así un gobierno limitado y controlado por la ley. Jean-Jacques Rousseau (1762/2012), por su parte, introdujo la noción de soberanía popular como fundamento de toda autoridad legítima, afirmando que solo la voluntad general podía generar leyes justas.

Este modelo se estructuró sobre tres pilares fundamentales:

1. Supremacía constitucional, posteriormente sistematizada por Hans Kelsen (1934) al ubicar la Constitución en la cúspide de la pirámide normativa, de la cual depende la validez de todas las normas inferiores.
2. Limitación del poder, garantizada por la separación de poderes y mecanismos de control jurídico y político.
3. Protección de los derechos individuales, principalmente libertades civiles y políticas, aunque con una eficacia más formal que material.

No obstante, el constitucionalismo liberal clásico presentaba importantes limitaciones. Como señala Gina Chávez Vallejo (2017), se sustentaba en un monismo jurídico y en un legicentrismo formalista (donde el Estado era el único productor de derecho y la ley su fuente principal). Esta concepción, que pretendía presentarse como neutral y universal, en realidad reproducía intereses hegemónicos y excluía la pluralidad social y normativa. La globalización, el surgimiento de sociedades cada vez más diversas y las crecientes demandas de democratización en América Latina evidenciaron la necesidad de superar este modelo, impulsando la transición hacia un constitucionalismo plural y participativo (Chávez, 2017).

En este nuevo escenario, el constitucionalismo dejó de verse únicamente como una herramienta de limitación del poder político, para convertirse en un instrumento orientado a la inclusión y al reconocimiento de la diversidad social, cultural y jurídica. La experiencia latinoamericana, especialmente a partir de las reformas constitucionales de finales del siglo XX, demostró que la legitimidad de las constituciones modernas depende tanto de su capacidad para garantizar derechos como de su apertura a las realidades plurales de sus pueblos. De ahí que la noción de “constitucionalismo transformador” adquiera relevancia al proponer que las

constituciones no sean solo marcos normativos, sino proyectos políticos de cambio social, fundados en la justicia material y la participación ciudadana.

Desde una óptica contemporánea, María José Lubertino Beltrán (2019) plantea que el derecho no debe concebirse únicamente como un conjunto de normas limitativas del poder, sino como un mecanismo de armonización social capaz de equilibrar la libertad individual, el bienestar colectivo y la sostenibilidad ambiental. Además, vincula el constitucionalismo con la protección internacional de los derechos humanos, subrayando el papel de las organizaciones no gubernamentales y de los sistemas internacionales en la defensa de la no discriminación, los derechos de los consumidores y la protección del medio ambiente. Esta ampliación del horizonte constitucional redefine las relaciones entre el Estado, la sociedad y el mercado, destacando que la vigencia de los derechos fundamentales trasciende las fronteras nacionales y exige respuestas coordinadas a nivel global (Beltrán, 2019).

En este contexto, el constitucionalismo contemporáneo se enfrenta a la tarea de integrar nuevas dimensiones del poder, particularmente aquellas derivadas de la economía digital, la inteligencia artificial y las redes de comunicación globales. El constitucionalismo ya no puede limitarse al ámbito estatal, pues las estructuras transnacionales de poder condicionan hoy los derechos y las libertades de los individuos. Por ello, el tránsito hacia un constitucionalismo digital implica reconocer que la garantía de los derechos fundamentales debe extenderse al espacio virtual, donde las decisiones algorítmicas, el control de datos y la automatización de procesos pueden incidir directamente sobre la dignidad humana.

Por su parte, Francisco Miguel Mora Sifuentes (2014) profundiza en la transición del legalismo al constitucionalismo al examinar la tensión histórica entre el imperio de la ley y el imperio de la constitución. Según el autor, el legalismo clásico priorizó la libertad negativa y la seguridad jurídica formal (confiando en la ley como única expresión válida del derecho). Sin embargo, la evolución hacia el constitucionalismo moderno puso de manifiesto que la ley debía someterse a la constitución y que los derechos fundamentales requerían mecanismos efectivos de protección. Esta transformación conceptual allanó el camino hacia el neoconstitucionalismo, caracterizado por la fuerza normativa de la constitución, la ponderación de principios y el papel activo de los jueces constitucionales (Sifuentes, 2014).

En síntesis, el estudio de los distintos tipos de constitucionalismo permite comprender la trayectoria de la juridicidad moderna y las diversas formas en que el poder ha sido regulado

a lo largo de la historia. Analizar sus etapas: clásica, liberal, social, plural y digital, no solo ofrece una perspectiva crítica sobre la evolución del Estado de derecho, sino que también habilita una reflexión sobre los desafíos actuales del constitucionalismo en el entorno tecnológico. Así, el constitucionalismo digital no surge como una ruptura con la tradición, sino como su continuidad adaptada a las exigencias de una sociedad interconectada, donde la protección de los derechos fundamentales debe garantizarse tanto en el espacio físico como en el virtual.

Asimismo, el constitucionalismo clásico sentó los cimientos del derecho constitucional contemporáneo:

- La supremacía de la constitución como norma fundante del orden jurídico.
- La división de poderes como técnica de limitación del poder.
- La centralidad de los derechos fundamentales como núcleo del sistema jurídico.

Su formalismo y enfoque estatalista mostraron ser insuficientes para enfrentar la complejidad social y jurídica contemporánea, preparando el terreno para la evolución hacia el neoconstitucionalismo, el constitucionalismo digital y el nuevo constitucionalismo pluralista latinoamericano, donde los derechos fundamentales adquieren eficacia real y dimensión global.

Si bien el constitucionalismo clásico consolidó los cimientos del Estado de derecho moderno, su formalismo legalista y su visión estatalista evidenciaron serios límites frente a las demandas de justicia material, pluralismo social y eficacia de los derechos. La supremacía de la ley y la confianza en la división de poderes no bastaron para evitar abusos de autoridad ni garantizar la vigencia real de las libertades. Esta insuficiencia se hizo más evidente ante la complejidad social y política del siglo XX, donde Estados formalmente legales fueron capaces de sostener regímenes autoritarios y violaciones masivas de derechos humanos. En consecuencia, la sola limitación formal del poder resultó insuficiente para asegurar un orden jurídico justo y eficaz, evidenciando la necesidad de superar un modelo centrado en la ley hacia uno orientado por valores constitucionales y principios garantistas. De esta crisis conceptual y práctica emerge el neoconstitucionalismo, que propone una Constitución con fuerza normativa real, una interpretación basada en principios y ponderación, y un rol judicial activo y vigilante, capaz de convertir la justicia constitucional en una herramienta de transformación y protección efectiva de los derechos fundamentales.

1.2.El neoconstitucionalismo: delimitaciones conceptuales.

La historia del siglo XX demostró con crudeza que la mera existencia de constituciones y leyes no bastaba para evitar los abusos de poder, pues incluso regímenes formalmente legales pudieron sostener estructuras autoritarias y violaciones sistemáticas de los derechos humanos. Esta experiencia histórica generó la necesidad de redefinir la función de la Constitución, transformándola en el centro vinculante del orden jurídico y en un instrumento activo de protección y de transformación social.

El neoconstitucionalismo surge como respuesta crítica a las limitaciones estructurales del constitucionalismo clásico y a la crisis del positivismo legalista, evidenciando que el derecho formal, por sí solo, resulta insuficiente para garantizar la efectividad real de los derechos fundamentales. En este sentido, el neoconstitucionalismo no solo representa una respuesta teórica a las deficiencias del modelo liberal clásico, sino que introduce un cambio de paradigma respecto a la comprensión del derecho, la justicia y el poder. Supone la incorporación de la moral y los valores en la estructura jurídica, reconociendo que el derecho no puede desvincularse de la ética ni de las exigencias de justicia material. Así, la Constitución deja de ser un texto rígido para convertirse en una fuente viva de interpretación dinámica, capaz de adaptarse a los desafíos sociales, políticos y tecnológicos contemporáneos.

Con la Constitución, el concepto de legalidad adquiere un nuevo significado: ya no se trata únicamente de establecer reglas de disciplina, sino que la creación de nuevas leyes queda condicionada por la propia Constitución. Es decir, ninguna norma puede promulgarse si contraviene la Constitución, la cual actúa como límite y marco de referencia para los legisladores (Navarreto Barrero, 2006).

El desarrollo de este constitucionalismo estuvo precedido por numerosos instrumentos y acontecimientos internacionales, como la Carta de las Naciones Unidas (1945), la Declaración Universal de los Derechos Humanos (1948), la Constitución italiana (1948) y la Ley Fundamental de la República Federal Alemana (1948). Estos antecedentes reflejan que las Constituciones cumplen un papel crucial al rechazar toda forma de opresión fascista, promoviendo la separación de poderes, la igualdad entre hombres y mujeres sin distinción de raza o condición social, y garantizando los derechos fundamentales (Ferrajoli, 2010).

El neoconstitucionalismo en una definición jurídico práctica podría definirse como una corriente jurídica que modifica la noción tradicional de Estado de derecho, convirtiéndolo en un Estado Constitucional de derecho, en el que la Constitución no solo limita al poder estatal,

sino que también orienta y condiciona su actuación (Diccionario panhispánico del español jurídico, 2025). Pero más que una definición, el mismo se puede entender de varias formas, puede erigirse como modelo estatal, teoría del derecho o ideología (Prieto, 2001).

Siendo que no está definido o contenido en un solo lineamiento, el neoconstitucionalismo abre el camino hacia nuevas formas de constitucionalismo, como el digital, el ecológico y el intercultural. En un mundo globalizado e interconectado, los principios de dignidad humana, igualdad y libertad deben extenderse más allá del territorio estatal y aplicarse también en los entornos digitales, en la protección del medio ambiente y en el reconocimiento de los pueblos originarios. De este modo, el constitucionalismo contemporáneo se proyecta hacia una dimensión transnacional e interdisciplinaria, donde los derechos fundamentales trascienden las fronteras físicas y deben ser garantizados en espacios virtuales, tecnológicos y ambientales.

El neoconstitucionalismo se distingue por tres ejes doctrinales fundamentales que lo separan del modelo liberal clásico. En primer lugar, la supremacía material de la Constitución, que deja de ser un documento meramente político para convertirse en norma jurídica efectiva y cargada de valores, capaz de irradiar fuerza normativa sobre todo el sistema. En segundo lugar, la centralidad de los derechos fundamentales y los principios constitucionales, que adquieren fuerza normativa plena y guían la interpretación y aplicación del derecho en su conjunto, garantizando la justiciabilidad y la eficacia real de las libertades y garantías. Finalmente, el rol protagónico de los jueces constitucionales, quienes ya no se limitan a aplicar mecánicamente la ley, sino que ponderan principios, ejercen control sobre el legislador y actúan como garantes activos de la justicia constitucional.

A partir de estos pilares, el neoconstitucionalismo ha permitido el fortalecimiento de la justicia constitucional y el empoderamiento de la ciudadanía en la defensa de sus derechos. Instrumentos como las acciones de tutela, los amparos y los mecanismos de control de constitucionalidad han materializado la promesa de un derecho al servicio de la persona, configurando un modelo de democracia sustantiva que supera la mera legalidad formal. Esta tendencia también ha influido en el desarrollo de un constitucionalismo digital garantista, que busca adaptar los principios de libertad, igualdad y privacidad al contexto tecnológico, frente a fenómenos como la vigilancia masiva, la manipulación algorítmica y la concentración del poder informático en manos privadas.

Este modelo ha supuesto avances significativos en la protección de los derechos y en la construcción de una democracia sustantiva, pero también ha suscitado debates críticos. Se cuestiona, por un lado, la judicialización de la política y el riesgo de un "gobierno de jueces", dada la ampliación del poder interpretativo de los tribunales. Por otro, se plantea la tensión entre supremacía judicial y legitimidad democrática, que obliga a los jueces a ejercer autocontención argumentativa y transparencia en la motivación de sus decisiones.

En suma, el neoconstitucionalismo constituye uno de los giros más significativos del derecho contemporáneo, pues no se limita a ser una corriente teórica ni una técnica interpretativa, sino que representa una reconfiguración profunda del papel de la Constitución, los derechos fundamentales y la función judicial en el Estado moderno. En palabras de Alexy (1993), el derecho constitucional actual ya no puede comprenderse sin su dimensión moral, porque la justicia constitucional exige interpretación axiológica, ponderación de principios y argumentación racional como condiciones para la protección efectiva de los derechos.

Pese a estas tensiones, el neoconstitucionalismo ha consolidado una nueva forma de entender el Estado constitucional de derecho, donde el juez se convierte en garante del pacto democrático y la Constitución en una herramienta de transformación social. Este giro implica una redefinición del equilibrio entre poder, derechos y justicia, que resulta indispensable para abordar los desafíos del siglo XXI, especialmente aquellos derivados de la revolución digital, la inteligencia artificial y las desigualdades globales.

En definitiva, el neoconstitucionalismo emerge como la superación crítica del modelo clásico y del positivismo legalista, al evidenciar que la justicia constitucional no puede descansar únicamente en la validez formal de la ley, sino en su capacidad para proteger derechos y garantizar la dignidad humana. Esta reconfiguración del derecho constitucional no surgió de manera espontánea, sino como resultado de procesos históricos concretos que marcaron la segunda mitad del siglo XX. La experiencia de la posguerra europea, con la creación de constituciones cargadas de principios y tribunales constitucionales robustos, y las transiciones democráticas en América Latina, con sus constituciones transformadoras y garantistas, constituyen el escenario donde este paradigma cobró fuerza. Comprender este contexto histórico y doctrinal resulta imprescindible para explicar cómo la necesidad de eficacia real de los derechos y de control efectivo del poder impulsó la evolución hacia un derecho constitucionalizado, axiológico y garantista, que analizaremos en el siguiente apartado.

1.2.1. Contexto histórico del neoconstitucionalismo y causas de su surgimiento

El neoconstitucionalismo no surgió de manera súbita ni como una construcción teórica aislada, sino como una respuesta profunda a las crisis políticas, sociales y jurídicas del siglo XX. Fue la consecuencia de una reflexión colectiva sobre los límites del constitucionalismo clásico y del positivismo legalista, que habían demostrado su incapacidad para garantizar la eficacia real de los derechos fundamentales. Estas insuficiencias se evidenciaron con especial fuerza tras los conflictos bélicos y los regímenes autoritarios que marcaron la primera mitad del siglo pasado, mostrando que el derecho, reducido a una técnica formal, podía coexistir con graves violaciones a la dignidad humana (Ferrajoli, 2001).

En este contexto, las nuevas constituciones democráticas del periodo de posguerra introdujeron la idea de una Constitución con fuerza normativa, que debía orientar todo el orden jurídico y garantizar el respeto efectivo de los derechos fundamentales. No obstante, más que un hecho histórico puntual, el neoconstitucionalismo representa una transformación epistemológica en la manera de concebir el derecho y el poder. Su aparición implicó reconocer que la legitimidad de las normas no podía depender únicamente de su validez formal, sino también de su coherencia con principios éticos universales como la libertad, la igualdad y la justicia (Zagrebelsky, 1995; Alexy, 1993).

Este cambio supuso la superación de la idea del derecho como un sistema cerrado y autosuficiente. El neoconstitucionalismo incorporó la moral y la argumentación como dimensiones esenciales del razonamiento jurídico, afirmando que el juez constitucional debía ponderar valores y principios para alcanzar decisiones justas. Autores como Dworkin (1986) y Prieto Sanchís (2003) resaltan que el derecho no es un conjunto de reglas estáticas, sino un proceso interpretativo que exige razonabilidad, coherencia y fundamentación moral.

En términos estructurales, el neoconstitucionalismo buscó dotar al Estado de herramientas efectivas para limitar el poder y proteger los derechos frente a nuevas formas de dominación, tanto pública como privada. Su importancia radica precisamente en esta capacidad de adaptación: transformar la Constitución en un instrumento vivo que responde a los desafíos de cada época. Así, el neoconstitucionalismo contribuyó a redefinir la relación entre derecho y sociedad, promoviendo una democracia sustantiva que no se limita al cumplimiento formal de las normas, sino que busca la realización material de la justicia.

En América Latina, su recepción estuvo vinculada a los procesos de democratización de finales del siglo XX, donde se adoptaron constituciones con un marcado enfoque garantista y participativo. Sin embargo, más allá de la cronología, lo relevante es que el neoconstitucionalismo latinoamericano asumió la tarea de convertir el texto constitucional en una herramienta de transformación social, orientada a corregir desigualdades y hacer efectivos los derechos. Este enfoque dotó a la Constitución de un valor normativo y pedagógico, situándola como eje de la cultura jurídica y política contemporánea.

En consecuencia, el surgimiento del neoconstitucionalismo debe entenderse no solo como una reacción frente a los abusos del poder, sino como un movimiento de renovación integral del pensamiento jurídico. Supone reconocer que la justicia no puede quedar subordinada a la ley, que la validez requiere legitimidad, y que los derechos fundamentales son el núcleo sustantivo del orden constitucional. Desde esta perspectiva, la Constitución deja de ser una mera carta política y se convierte en una norma suprema vinculante que orienta la interpretación del derecho y guía la actuación estatal.

La relevancia del neoconstitucionalismo en el siglo XXI radica en su vigencia frente a nuevos escenarios de poder. Hoy, las tensiones entre derechos, tecnología y globalización exigen proyectar los valores del constitucionalismo garantista hacia ámbitos emergentes, como el ciberespacio, la inteligencia artificial y la gobernanza de los datos. En esa medida, el constitucionalismo digital puede considerarse una extensión contemporánea del neoconstitucionalismo, al buscar trasladar al entorno tecnológico los principios de dignidad humana, libertad y control del poder.

En síntesis, el neoconstitucionalismo no solo surgió como un resultado histórico, sino como una necesidad ética y política. Su propósito central es asegurar que la Constitución sea un instrumento de justicia real y no un simple marco formal de convivencia. Representa, en última instancia, una apuesta por un derecho con contenido moral, capaz de responder a los desafíos de la sociedad contemporánea, proteger la dignidad humana y garantizar la supremacía efectiva de los derechos en cualquier escenario, físico o digital.

1.2.2. Europa de la posguerra: el laboratorio del Estado constitucional

La Segunda Guerra Mundial dejó al descubierto la profunda fragilidad del modelo positivista y las limitaciones del constitucionalismo clásico. El horror del nazismo y del fascismo demostró que la mera existencia de leyes, parlamentos y procedimientos formales no

bastaba para garantizar la justicia ni para contener el abuso del poder. Regímenes totalitarios lograron mantener una apariencia de legalidad mientras promovían violaciones sistemáticas a los derechos humanos, genocidios y actos de barbarie amparados por normas jurídicas. Esta contradicción puso en evidencia que la validez formal del derecho no siempre coincidía con su legitimidad moral, generando una crisis sin precedentes en la teoría jurídica moderna. Los juristas comenzaron a cuestionar si un derecho que permite la opresión o el exterminio puede considerarse auténtico derecho, lo que llevó a un replanteamiento profundo de los fundamentos del orden jurídico y del papel de la Constitución en la protección de la dignidad humana.

A partir de este escenario, surgió una nueva conciencia sobre la necesidad de construir sistemas jurídicos que no se limitaran a la legalidad formal, sino que incorporaran principios éticos universales como base de su legitimidad. Esta reflexión sentó las bases del neoconstitucionalismo, el cual emergió como respuesta a la crisis del positivismo, proponiendo que la justicia y los derechos fundamentales debían ocupar un lugar central dentro del orden jurídico. El constitucionalismo contemporáneo comenzó entonces a concebir la Constitución no solo como una norma suprema, sino como un texto cargado de valores, principios y garantías que orientan toda la interpretación del derecho. Así, la experiencia trágica de la posguerra impulsó la creación de tribunales constitucionales, declaraciones internacionales de derechos humanos y mecanismos de control judicial que transformaron la relación entre poder, derecho y moralidad, estableciendo las bases de un modelo jurídico más humano, garantista y democrático.

Frente a este escenario, Europa occidental se convirtió en el laboratorio donde se gestó el nuevo paradigma constitucional. Dos textos fundamentales marcaron este giro:

- La Constitución italiana de 1947, que incorporó un amplio catálogo de derechos y principios programáticos vinculantes, estableciendo un Tribunal Constitucional para garantizar su eficacia.

- La Ley Fundamental de Bonn de 1949, que definió a la dignidad humana como núcleo irreductible y colocó a la jurisdicción constitucional como guardiana de los valores del nuevo Estado.

Estas constituciones de posguerra marcaron la transición del Estado legal al Estado constitucional, caracterizado por:

1. La supremacía material de la Constitución sobre la ley.

2. La integración de valores y principios morales al sistema jurídico.

3. La creación de tribunales constitucionales fuertes como garantes efectivos de los derechos fundamentales.

Como señala Guastini (2013), este proceso implicó la constitucionalización del derecho, en la que toda norma inferior encuentra su validez en la conformidad con la Constitución, generando un efecto de irradiación normativa que transforma al derecho en un sistema axiológico y garantista. Esta transformación significó un cambio estructural en la forma de concebir el orden jurídico: la Constitución dejó de ser una carta política programática para convertirse en una norma vinculante con fuerza normativa directa. El principio de supremacía constitucional pasó de ser una declaración teórica a constituirse en un criterio efectivo de validez, interpretación y aplicación de todas las normas del sistema. Así, el derecho comenzó a organizarse jerárquicamente en torno a los valores constitucionales, como la dignidad humana, la igualdad, la libertad y la justicia, los cuales adquirieron un carácter normativo y no meramente retórico. Este proceso también conllevó una expansión del control de constitucionalidad y una reinterpretación del papel del juez, quien dejó de ser un mero aplicador mecánico de la ley para convertirse en garante de los principios fundamentales que orientan la totalidad del sistema jurídico.

Este fue, en consecuencia, el punto de partida teórico y práctico del neoconstitucionalismo europeo, que encontró en la posguerra un terreno fértil para consolidarse como paradigma jurídico y filosófico. La experiencia de la devastación bélica y la creación de nuevas constituciones cargadas de principios, como la Ley Fundamental de Bonn (1949) en Alemania o la Constitución italiana de 1948, marcaron un antes y un después en la historia del derecho. En este contexto, el constitucionalismo adquirió un sentido sustantivo: ya no se trataba solo de limitar el poder, sino de orientar la acción estatal hacia la protección efectiva de los derechos humanos. El derecho dejó de ser un instrumento neutral del Estado para convertirse en un sistema de garantías al servicio de la persona y de la justicia material. Así, la constitucionalización del derecho redefinió los fundamentos mismos de la legalidad y consolidó una nueva cultura jurídica centrada en la primacía de los valores, la fuerza normativa de la Constitución y la integración del derecho interno con el derecho internacional de los derechos humanos.

1.2.3. El giro interpretativo y la crisis del positivismo

Paralelamente al proceso histórico de constitucionalización del derecho, se produjo un giro interpretativo profundo en la teoría jurídica contemporánea, que transformó de manera sustancial la comprensión del derecho, la función de los jueces y el papel de la Constitución. Este cambio se originó en la constatación de que los sistemas jurídicos contemporáneos, impregnados de principios, valores y derechos fundamentales, ya no podían ser comprendidos ni aplicados desde la rigidez del positivismo legalista clásico. Como señala Prieto Sanchís (2003), el nuevo contexto normativo "ha multiplicado los conflictos entre derechos y principios, exigiendo al juez una labor creadora que rebasa el marco tradicional de la subsunción". En consecuencia, la interpretación jurídica dejó de ser un ejercicio técnico de aplicación literal de la ley para convertirse en una actividad argumentativa, ponderativa y axiológica, orientada a garantizar la justicia material y la coherencia con los valores constitucionales.

El positivismo jurídico, en su versión tradicional, había concebido el derecho como un sistema cerrado, completo y autosuficiente, donde las normas derivaban su validez exclusivamente de su procedencia formal. Esta visión, defendida por autores como Kelsen (1934), separaba radicalmente el derecho de la moral y relegaba al juez a un papel subordinado y meramente ejecutor de la voluntad legislativa. Sin embargo, la experiencia del siglo XX, particularmente tras las guerras mundiales y la evidencia de regímenes autoritarios amparados en la legalidad formal, mostró los límites de este modelo. Como advierte Ferrajoli (2001), la tragedia del totalitarismo reveló que la validez formal no basta para garantizar la justicia del derecho ni la protección de los derechos humanos, lo que obligó a repensar las bases mismas de la legitimidad jurídica.

En este contexto, emergió la necesidad de un derecho interpretado a la luz de la Constitución, donde los principios fundamentales actúan como criterios orientadores de toda decisión judicial. La función judicial dejó de ser pasiva: los jueces ya no podían limitarse a aplicar mecánicamente la ley, sino que debían ponderar principios, integrar valores y construir decisiones justificadas racionalmente. Este cambio se tradujo en la consolidación de la argumentación jurídica como herramienta esencial de legitimación judicial. Como sostiene Robert Alexy (1993), los principios constitucionales no son reglas de aplicación automática, sino mandatos de optimización que exigen la ponderación en función de las circunstancias concretas y de la mayor realización posible de los valores en conflicto. De esta manera, la tarea

del juez constitucional se convierte en una labor de equilibrio racional entre derechos y bienes jurídicos, guiada por la coherencia moral y la justificación argumentativa.

Asimismo, el giro interpretativo condujo a la ruptura de la frontera rígida entre derecho y moral defendida por el positivismo clásico. Autores como Ronald Dworkin (1986) sostuvieron que la interpretación jurídica no puede reducirse a la identificación de normas válidas, sino que implica un ejercicio de lectura moral del derecho. Según Dworkin, los jueces deben actuar como "intérpretes integradores" que dan coherencia al sistema jurídico a partir de sus principios morales más profundos, como la equidad, la justicia y la dignidad humana. En esta perspectiva, la legitimidad del derecho no proviene solo de su validez formal, sino de su capacidad para realizar la justicia y proteger efectivamente los derechos fundamentales.

Por su parte, Gustavo Zagrebelsky (1995) enfatiza que la Constitución moderna no puede entenderse únicamente como una norma jurídica superior, sino como un "orden abierto de valores" que orienta la interpretación y aplicación del derecho en todas sus dimensiones. Esto implica reconocer que los jueces, al interpretar la Constitución, no actúan como simples aplicadores de normas, sino como constructores del sentido constitucional, responsables de mantener viva la relación entre derecho y justicia. De este modo, el juez constitucional adquiere un papel político y ético de primer orden, en tanto garante de la supremacía de los derechos frente a los poderes públicos y privados.

Este giro interpretativo consolidó la dimensión moral del derecho constitucional y fortaleció la idea de que la eficacia de la Constitución depende de su aplicación judicial activa, rasgo esencial del neoconstitucionalismo. La Constitución dejó de ser un marco declarativo para convertirse en una norma viva, aplicada y defendida cotidianamente en los tribunales. Así, como plantea Carbonell (2008), el juez constitucional contemporáneo es el verdadero "intérprete último de los derechos", encargado de mantener la coherencia axiológica del sistema jurídico y de asegurar que las normas y políticas públicas respeten los principios fundamentales.

En suma, la crisis del positivismo jurídico y el giro interpretativo que le siguió supusieron una revolución epistemológica en el pensamiento jurídico moderno. El derecho ya no puede entenderse sin referencia a los valores constitucionales que lo legitiman ni sin la intervención activa de los jueces como garantes de la justicia constitucional. Este nuevo paradigma no solo transformó la teoría del derecho, sino que redefinió la relación entre norma,

moral y poder, consolidando el tránsito hacia un modelo jurídico donde la Constitución se erige como el eje material y axiológico de todo el orden jurídico.

1.2.4. América Latina: transición democrática y constitucionalismo garantista

En América Latina, el neoconstitucionalismo encontró un terreno fértil marcado por inestabilidad política, dictaduras militares y violaciones sistemáticas de derechos humanos durante gran parte del siglo XX. La recuperación de la democracia impulsó procesos constituyentes transformadores, que incorporaron derechos de nueva generación, mecanismos de control judicial robustos y apertura al derecho internacional de los derechos humanos.

El contexto latinoamericano fue especialmente propicio para la recepción de las ideas del constitucionalismo garantista, en tanto las nuevas constituciones se convirtieron en instrumentos de reconstrucción democrática, reconciliación nacional y reconfiguración del Estado. Estas reformas no fueron meros ejercicios formales, sino proyectos políticos y éticos que buscaron responder a décadas de exclusión, violencia y desigualdad estructural.

Ejemplos paradigmáticos de este proceso incluyen:

- Colombia (1991): Su Constitución incorporó un amplio catálogo de derechos, la acción de tutela como mecanismo expedito de protección y el bloque de constitucionalidad, integrando normas internacionales como parámetros internos de control.

- Ecuador (2008) y Bolivia (2009): Sus constituciones introdujeron pluralismo jurídico, derechos de la naturaleza y mecanismos de democracia participativa, proyectando un constitucionalismo transformador y garantista.

Aunque América Latina adoptó plenamente el pensamiento político y filosófico del constitucionalismo moderno, lo hizo a través de un proceso propio y distinto del europeo. Si bien Europa sirvió como modelo, la región desarrolló una realidad constitucional particular. La incorporación de instituciones inspiradas en Estados Unidos y Francia, aplicadas en un contexto cultural diferente, produjo resultados muy alejados de los originales, como se observa en la evolución del federalismo y el presidencialismo latinoamericanos.

Asimismo, aunque los nuevos Estados republicanos se definieron como representativos (aun con un sufragio limitado), no llegaron a convertirse en democracias plenas. Las reformas institucionales no fueron acompañadas por cambios equivalentes en las estructuras económicas

y sociales, ni por una verdadera internalización de los principios del constitucionalismo. Por ello, la historia constitucional latinoamericana posterior a la independencia muestra un progresivo distanciamiento del espíritu del constitucionalismo europeo, más allá de lo que indicaran formalmente sus textos constitucionales (Rolla, 2012).

El neoconstitucionalismo no es solo una doctrina, sino una respuesta histórica y teórica a la insuficiencia del derecho formal frente a las demandas de protección efectiva de derechos y control del poder. La posguerra europea demostró la necesidad de un derecho con contenido moral y fuerza vinculante, y América Latina adaptó este modelo como herramienta de reconstrucción democrática y transformación social. Sin embargo, en el contexto latinoamericano, este modelo adquirió un carácter más expansivo y social, vinculado con la idea de un constitucionalismo transformador que no se limita a limitar el poder, sino que busca democratizarlo y redistribuirlo. La Constitución se concibe como una promesa de cambio estructural y justicia material, orientada al logro de condiciones reales de igualdad, inclusión y dignidad.

La experiencia latinoamericana ha sido también un espacio de experimentación institucional. En países como Brasil, Colombia y México, los tribunales constitucionales han desarrollado jurisprudencias creativas que han ampliado el alcance de los derechos sociales, consolidando doctrinas como el "mínimo vital", la "sustitución de la Constitución" o la "doctrina del control de convencionalidad". Estas prácticas judiciales muestran que el constitucionalismo garantista latinoamericano no solo interpreta, sino que también construye el derecho desde una visión comprometida con la justicia sustantiva.

No obstante, su desarrollo plantea desafíos contemporáneos. Entre ellos, la judicialización de la política y el riesgo de un gobierno de jueces, la brecha entre constituciones avanzadas y realidades sociales desiguales, y la necesidad de adaptación a un mundo globalizado y digital, donde la protección de derechos trasciende las fronteras estatales. En la región, el debate sobre los límites del activismo judicial continúa vigente. Mientras algunos lo consideran una forma de justicia emancipadora, otros advierten sobre la posible tensión con la legitimidad democrática y el papel del legislador. Este dilema evidencia que el constitucionalismo garantista debe equilibrar el poder judicial con mecanismos participativos y deliberativos que fortalezcan la democracia constitucional.

El neoconstitucionalismo, en suma, emerge históricamente como una corriente jurídica orientada a garantizar la eficacia y la justicia, proyectándose hacia los retos del constitucionalismo plural y digital del siglo XXI. Como se mencionó anteriormente, sus primeras manifestaciones surgieron en Europa tras la Segunda Guerra Mundial, en un contexto marcado por la reconstrucción institucional y el descrédito del positivismo legalista. La experiencia de los totalitarismos evidenció que la mera obediencia a la ley no bastaba para impedir injusticias, por lo que se impulsó la elaboración de constituciones cargadas de principios y derechos, acompañadas de tribunales constitucionales fuertes. Las constituciones italianas de 1947 y alemana de 1949 se convirtieron así en referentes de este nuevo paradigma, consolidando, como señala Guastini (2013), la idea de un ordenamiento constitucionalizado en el cual toda norma inferior debe ajustarse a los valores y principios de la Constitución.

A partir de este precedente europeo, el neoconstitucionalismo adquirió una relevancia particular en América Latina. En este contexto regional, las democracias emergentes vieron en la Constitución un instrumento clave para enfrentar los legados del autoritarismo, avanzar en procesos de justicia transicional y reparar a las víctimas. Además, las constituciones latinoamericanas incorporaron con mayor fuerza derechos colectivos, ambientales e indígenas, transformando el constitucionalismo en una herramienta no solo jurídica, sino también social y política. Como resultado, la región proyectó una versión más expansiva y garantista del neoconstitucionalismo, adaptada a sus demandas históricas y al propósito de construir un orden jurídico centrado en la dignidad y la protección efectiva de los derechos.

Si bien la influencia del modelo europeo fue decisiva, América Latina lo reinterpretó a partir de su realidad social. Las nuevas constituciones no se limitaron a reproducir estructuras institucionales, sino que las transformaron al incorporar la justicia social, el reconocimiento étnico, los derechos de la naturaleza y la participación ciudadana, elementos ausentes en los constitucionalismos europeos clásicos. De este modo, el neoconstitucionalismo latinoamericano se configuró como una propuesta distintiva, más inclusiva y sensible a la diversidad y desigualdad propias de la región.

Este cambio estructural se acompañó de un giro interpretativo (Pozzolo, 2016), que transformó la función judicial. El juez dejó de ser un mero aplicador mecánico de la ley, para convertirse en intérprete de principios y garante de derechos, con la tarea de resolver conflictos complejos mediante la ponderación y de dotar de eficacia real a la Constitución. La ruptura con el positivismo clásico se materializó, entonces, en tres frentes: epistemológico, al reconocer la

inevitable conexión entre derecho y moral; práctico, al buscar la protección efectiva de los derechos; e institucional, al fortalecer la jurisdicción constitucional como poder garante. Este giro no solo significó un cambio teórico, sino una transformación cultural profunda: los jueces constitucionales pasaron a ser agentes de cambio social, mediadores en conflictos estructurales y defensores de las promesas incumplidas de la democracia.

En América Latina, la expansión del neoconstitucionalismo fue especialmente intensa a partir de las transiciones democráticas de finales del siglo XX. La Constitución colombiana de 1991 marcó un hito regional, incorporando un amplio catálogo de derechos fundamentales, la acción de tutela como mecanismo expedito de protección, y la noción de bloque de constitucionalidad, que integra normas internacionales de derechos humanos como parámetro interno. Posteriormente, las constituciones de Ecuador (2008) y Bolivia (2009) profundizaron esta tendencia, incorporando pluralismo jurídico, derechos de la naturaleza y mecanismos de democracia participativa, consolidando un modelo de Estado constitucional garantista y transformador.

El constitucionalismo garantista latinoamericano, además, introdujo innovaciones teóricas que ampliaron la concepción de los derechos. La noción de "bloque de constitucionalidad" permitió articular el derecho interno con los tratados internacionales, generando un diálogo entre las constituciones nacionales y los sistemas de protección interamericana y universal. Este proceso fortaleció la jerarquía normativa de los derechos humanos y propició una cultura jurídica transnacional en la que la Corte Interamericana de Derechos Humanos se convirtió en fuente obligatoria de interpretación.

Estas reformas evidencian que el constitucionalismo latinoamericano no se limita a reproducir paradigmas europeos, sino que los adapta a sus realidades históricas, culturales y sociales, configurando un modelo propio, dinámico y en permanente evolución. En la actualidad, el reto consiste en proyectar este legado hacia los desafíos del siglo XXI, donde el constitucionalismo garantista deberá dialogar con el constitucionalismo digital, ecológico y global.

1.2.5. Fundamentos teóricos y filosóficos del Neoconstitucionalismo.

El neoconstitucionalismo no puede entenderse únicamente como un hecho histórico o como una técnica interpretativa de la judicatura; es, ante todo, una construcción doctrinal y filosófica que ha redefinido las bases del derecho constitucional en el contexto contemporáneo.

Su desarrollo implica una ruptura con el positivismo jurídico clásico y con el constitucionalismo liberal de corte formalista, en la medida en que sostiene que la validez del derecho no puede quedar limitada a su fuente u origen formal. Desde esta perspectiva, los derechos fundamentales requieren una eficacia material que solo es posible a través de la constitucionalización plena del ordenamiento jurídico. La Constitución pasa a ocupar el centro del sistema normativo y adquiere una fuerza vinculante directa, irradiando su eficacia sobre todas las ramas del derecho (Zagrebelsky, 1995). El resultado es un modelo normativo abierto, dinámico y axiológico, en el que el juez desempeña un papel activo en la concreción de los valores constitucionales y en la garantía efectiva de los derechos.

La Constitución ya no se concibe únicamente como un texto político o un conjunto de reglas procedimentales, sino como un orden normativo cargado de valores y principios. Esta concepción se distancia del positivismo kelseniano, que separaba estrictamente la validez formal del contenido moral de las normas. Para Luigi Ferrajoli (2001), el constitucionalismo contemporáneo supone una revolución garantista en tanto la Constitución fija límites sustantivos al poder político y al legislador, garantizando que toda norma inferior se someta a los principios de justicia, dignidad y derechos fundamentales. A diferencia de los modelos clásicos, donde la Constitución era entendida como una fuente de legitimidad formal, el neoconstitucionalismo plantea que la legitimidad jurídica depende del respeto a los derechos y valores constitucionales, lo que implica que las normas contrarias a estos carecen de validez. Esta transformación ha sido descrita por Prieto Sanchís (2003) como una constitucionalización integral del derecho, donde toda práctica jurídica debe interpretarse a la luz de los principios constitucionales.

Asimismo, esta concepción se articula con una visión moral del derecho, en la que los principios constitucionales actúan como mandatos de optimización, orientando al juez hacia la solución más justa posible dentro de las condiciones fácticas y jurídicas del caso (Alexy, 1993; Dworkin, 1984). En este sentido, la Constitución se convierte en un punto de encuentro entre la normatividad jurídica y la racionalidad práctica, dando lugar a una teoría del derecho que combina validez, eficacia y justicia. Esta perspectiva rompe con el positivismo formalista, que consideraba que la validez de una norma se definía únicamente por su procedencia legítima, y propone que la validez depende también del contenido moral de la norma y de su adecuación a los valores constitucionales.

El neoconstitucionalismo redefine la estructura del sistema jurídico al introducir una jerarquía axiológica donde los principios adquieren fuerza normativa. Los principios dejan de ser simples directrices programáticas y se convierten en normas vinculantes que orientan la interpretación y aplicación del derecho (Atienza y Ruiz Manero, 1996). Ronald Dworkin (1984) fue uno de los primeros en plantear esta ruptura, al sostener que el derecho no es un sistema de reglas sino una práctica interpretativa en la que los principios desempeñan un papel esencial en la decisión judicial. Este planteamiento implica reconocer que los jueces no aplican el derecho de manera mecánica, sino que deben justificar sus decisiones mediante argumentos morales y constitucionales, en un proceso racional y deliberativo que asegure la corrección material de los fallos.

Desde una mirada contemporánea, Habermas (1998) refuerza esta idea al vincular la legitimidad del derecho con la racionalidad comunicativa y el consenso social. Para él, el derecho solo puede ser legítimo cuando su interpretación se somete a la deliberación pública y al principio discursivo, según el cual las normas son válidas si pueden ser aceptadas racionalmente por todos los afectados. De esta manera, el neoconstitucionalismo no solo transforma la estructura del derecho, sino también su dimensión ética y democrática. Esta relación entre derecho y moralidad pública permite comprender que la Constitución no es un límite externo al poder, sino un espacio de construcción colectiva donde se definen los fines de justicia y convivencia social.

El juez constitucional ocupa un lugar central dentro de este paradigma, asumiendo una función activa como garante y constructor del derecho. El modelo tradicional lo concebía como un intérprete pasivo de la ley, mientras que el neoconstitucionalismo lo posiciona como agente de justicia constitucional y protector de los derechos fundamentales. Esta transformación responde a la necesidad de dotar de eficacia real a las normas constitucionales, especialmente en contextos donde las instituciones políticas no logran garantizar los derechos proclamados.

Según Carbonell (2009), esta función judicial activa no constituye un exceso de poder, sino una consecuencia directa de la supremacía constitucional y de la fuerza normativa de los derechos. El juez constitucional no sustituye al legislador, sino que completa el proceso de juridificación de la Constitución, asegurando que su contenido normativo tenga efectividad en la vida social. Ferrajoli (2007) sostiene que la jurisdicción constitucional es la garantía suprema del Estado de Derecho, pues limita el poder a través de la justicia.

Esta nueva función del juez exige un alto grado de racionalidad argumentativa y una estructura deliberativa del razonamiento jurídico. Atienza (2006) denomina a este proceso razonamiento jurídico práctico, destacando que la validez de una decisión depende tanto de su coherencia lógica como de su corrección moral. Así, el juez no se limita a aplicar normas, sino que construye el sentido del derecho desde los principios, generando un orden jurídico dinámico y en constante evolución. La justicia constitucional adquiere, en consecuencia, una dimensión pedagógica, orientada a la consolidación de una cultura de los derechos que trasciende los formalismos legales.

El neoconstitucionalismo también incorpora una dimensión axiológica y humanista del derecho, situando la dignidad humana como valor fundante y criterio último de validez. La influencia de pensadores como Nino (1996) y Bobbio (1990) ha permitido comprender que el derecho no puede desvincularse de la ética, pues su finalidad es la realización de la justicia material y la protección efectiva de la persona. En este marco, el Estado de Derecho se reinterpreta como Estado constitucional de justicia, donde la Constitución no solo limita el poder, sino que orienta la acción pública hacia la consecución de fines éticos. Zagrebelsky (2007) advierte que los derechos fundamentales no son solo límites, sino fines de la actividad estatal, en tanto expresan una moral pública compartida que se proyecta en la vida jurídica, política y social.

La incorporación de los valores constitucionales en la interpretación jurídica implica reconocer la existencia de una moral pública compartida, expresada en principios como la igualdad, la libertad, la solidaridad y el pluralismo. Estos valores no son meros ideales políticos, sino criterios normativos que orientan la actuación judicial y legitiman la acción de los poderes públicos. Esta perspectiva ha fortalecido una visión del derecho como sistema abierto de principios y valores, en el que la justicia constitucional actúa como un proceso de diálogo permanente entre la norma, la moral y la sociedad.

En la actualidad, el neoconstitucionalismo se encuentra en expansión conceptual, extendiéndose más allá del ámbito europeo y latinoamericano para incidir en debates globales sobre justicia, sostenibilidad y derechos digitales. La articulación entre derechos humanos, democracia y justicia social constituye su núcleo doctrinal más sólido, pero también su principal desafío. La globalización, la crisis ambiental y el desarrollo tecnológico exigen repensar la función del constitucionalismo frente a derechos emergentes como la privacidad digital, el acceso a la información, la protección de datos personales y la equidad algorítmica.

En este contexto, el constitucionalismo garantista adquiere una dimensión planetaria orientada hacia la construcción de una ética pública global que trascienda las fronteras del Estado-nación (Uprimny, 2011).

El neoconstitucionalismo, en suma, es un proyecto teórico, político y moral que redefine el sentido del derecho en el mundo contemporáneo. Su fundamento radica en la convicción de que la justicia no puede reducirse a la obediencia a la ley, sino que exige una constante relectura axiológica de la Constitución, guiada por la dignidad humana y la racionalidad práctica. A través de esta perspectiva, el derecho deja de ser un instrumento del poder y se convierte en un espacio de emancipación y garantía efectiva de los derechos fundamentales.

1.2.6. La supremacía material de la Constitución

El primer pilar del neoconstitucionalismo es la supremacía material de la Constitución, la cual se erige como el eje vertebrador del sistema jurídico contemporáneo. A diferencia del constitucionalismo clásico, que concebía la Constitución únicamente como una norma de organización del poder político o como una carta de principios generales, el paradigma neoconstitucional le otorga fuerza normativa plena, transformándola en un instrumento jurídico directamente aplicable y en una fuente de legitimidad sustantiva. Esta concepción implica que la Constitución deja de ser un documento simbólico o declarativo para convertirse en una norma viva, vinculante y operativa que permea todo el ordenamiento jurídico. En consecuencia, su autoridad no se limita al plano formal, sino que abarca el nivel axiológico y material, de modo que toda actuación del Estado debe ser coherente con sus valores y principios estructurales.

La supremacía constitucional se expresa en tres dimensiones esenciales: normativa, axiológica y vinculante. Desde el punto de vista normativo, la Constitución se entiende como una norma jurídica de aplicación directa, capaz de generar efectos sin necesidad de desarrollo legislativo previo. Esta visión fue consolidada por la doctrina del Tribunal Constitucional alemán y por las decisiones de la Corte Constitucional italiana en las décadas posteriores a la Segunda Guerra Mundial, que reconocieron la aplicabilidad inmediata de los derechos fundamentales frente a cualquier autoridad. Como afirma Zagrebelsky (2007), la Constitución moderna es “una norma de normas”, cuya eficacia no depende del legislador, sino de su fuerza jurídica intrínseca. Este carácter normativo implica que toda norma inferior debe adecuarse a

los mandatos constitucionales, y su incumplimiento genera inconstitucionalidad, aun cuando la ley haya sido producida mediante un procedimiento formalmente válido.

En el plano axiológico, la Constitución positiva un conjunto de valores fundamentales como la dignidad humana, la igualdad sustantiva, la libertad y la justicia social, que orientan la interpretación jurídica y actúan como parámetros de corrección normativa. Estos valores no son simples postulados éticos, sino criterios materiales de validez que determinan la legitimidad del derecho. En esta línea, Nino (1992) sostiene que el derecho democrático contemporáneo no puede entenderse sin su dimensión moral, ya que la validez de una norma depende no solo de su origen, sino también de su capacidad para proteger la autonomía y la dignidad de las personas. De esta manera, la supremacía material de la Constitución implica una integración entre derecho y moral constitucional, en la que los principios adquieren fuerza vinculante y orientan la interpretación de todo el sistema jurídico.

La dimensión vinculante y expansiva de la Constitución supone que su autoridad se irradia sobre todo el ordenamiento jurídico. Este efecto de irradiación, como explica Häberle (1997), transforma la Constitución en un marco normativo abierto que influye en la legislación, la administración y la judicatura. El derecho deja de concebirse como un sistema jerárquico cerrado y se convierte en un entramado dinámico en el que todas las normas encuentran su sentido en relación con la Constitución. En este contexto, la labor judicial se redefine: los jueces no solo aplican la ley, sino que garantizan la coherencia constitucional del sistema, asegurando que las decisiones concretas respondan a los valores fundamentales del ordenamiento. Este fenómeno ha consolidado un nuevo modelo de justicia constitucional caracterizado por el control difuso, la ponderación de principios y la expansión del bloque de constitucionalidad.

La supremacía material de la Constitución también implica un cambio en la concepción de la soberanía. Tradicionalmente, el poder constituyente se entendía como un acto fundacional que daba origen al Estado y que se agotaba en la promulgación de la Constitución. Sin embargo, bajo el enfoque neoconstitucional, la soberanía popular se manifiesta de manera permanente a través de la Constitución, que actúa como un pacto vivo entre el Estado y la sociedad. Este planteamiento ha sido desarrollado por Luigi Ferrajoli (2011) y Norberto Bobbio (1995), quienes advierten que la legitimidad democrática no puede reducirse al procedimiento electoral, sino que exige la garantía efectiva de los derechos fundamentales como condición de validez del poder político. Así, el principio de supremacía constitucional se convierte en una

herramienta de control del poder, asegurando que toda manifestación de autoridad se encuentre subordinada a los límites y valores constitucionales.

Asimismo, la Constitución adquiere una función transformadora. No se trata únicamente de una norma de estabilidad institucional, sino de un instrumento de cambio social y político. En América Latina, este carácter transformador ha tenido una relevancia particular, ya que las constituciones de finales del siglo XX —como la colombiana de 1991, la ecuatoriana de 2008 y la boliviana de 2009— incorporaron principios de pluralismo, justicia social y derechos colectivos, ampliando el contenido material de la supremacía constitucional. Como señala Gargarella (2013), estas constituciones no solo reorganizan el poder, sino que redefinen la relación entre Estado, sociedad y derechos, orientando el derecho hacia la inclusión y la equidad. En este sentido, la supremacía material de la Constitución opera como una cláusula de transformación estructural, que condiciona las políticas públicas y redefine los fines del Estado.

El nuevo paradigma también genera tensiones interpretativas. La supremacía constitucional, al incorporar principios de justicia y valores sustantivos, obliga a los operadores jurídicos a adoptar una postura argumentativa y deliberativa. La interpretación constitucional deja de ser una tarea de mera subsunción y se convierte en un proceso de razonamiento práctico en el que deben armonizarse derechos, valores y finalidades públicas. Esta exigencia ha sido subrayada por Manuel Atienza (2005), quien destaca que la argumentación jurídica es el medio por el cual la Constitución adquiere efectividad real, ya que permite justificar las decisiones judiciales en términos de razonabilidad y coherencia moral. En consecuencia, la supremacía material de la Constitución no solo transforma la estructura del derecho, sino también la epistemología jurídica, introduciendo la ética y la deliberación como componentes necesarios de la validez normativa.

En suma, la supremacía material de la Constitución redefine la noción misma de orden jurídico. No se trata únicamente de la norma suprema desde el punto de vista jerárquico, sino del fundamento axiológico y normativo que otorga coherencia al sistema. Su fuerza se manifiesta en la capacidad de irradiar valores, orientar interpretaciones y legitimar decisiones. En el contexto del neoconstitucionalismo, la Constitución deja de ser un texto político para convertirse en un proyecto normativo de justicia, que vincula a todos los poderes públicos y a la sociedad en su conjunto. Este principio no solo asegura la unidad del sistema jurídico, sino

que garantiza su correspondencia con los ideales democráticos y de derechos humanos que constituyen la esencia del Estado constitucional contemporáneo.

1.2.7. Reglas y principios: un nuevo paradigma normativo

El segundo fundamento del neoconstitucionalismo radica en la distinción estructural entre reglas y principios, que constituye uno de los giros más profundos en la teoría jurídica contemporánea. Este planteamiento no se limita a una diferenciación formal, sino que redefine el modo en que se entiende la estructura y la aplicación del derecho. En el modelo positivista clásico, el derecho se concebía como un sistema cerrado de normas compuestas esencialmente por reglas que establecían conductas concretas y que debían aplicarse de manera mecánica a los casos. En cambio, el neoconstitucionalismo asume que las Constituciones modernas están saturadas de principios y valores, lo que exige una nueva lógica interpretativa que no se agota en la subsunción, sino que se amplía hacia la ponderación, la argumentación y la integración axiológica del derecho.

La diferencia entre reglas y principios fue inicialmente planteada por Ronald Dworkin (1977) y desarrollada con precisión analítica por Robert Alexy (1993). Sin embargo, su consolidación teórica se debe al aporte de juristas europeos y latinoamericanos que comprendieron su impacto en la práctica constitucional. Las reglas se caracterizan por su estructura binaria, pues o bien se cumplen o no se cumplen, y cuando entran en conflicto, una de ellas debe ser excluida mediante derogación o inaplicación. Los principios, por su parte, no ordenan una conducta única, sino que establecen mandatos de optimización que orientan a los intérpretes a realizar un valor constitucional en la mayor medida posible, dentro de las condiciones fácticas y jurídicas existentes. En este sentido, los principios no se aplican en términos de todo o nada, sino que se realizan gradualmente, dependiendo del contexto. Esta distinción estructural supone, como afirma Prieto Sanchís (2003), una "transformación copernicana" del derecho, al reconocer que los valores y fines constitucionales poseen fuerza normativa equivalente a la de las reglas legales.

La introducción de los principios como fuente formal y material del derecho tiene consecuencias de gran alcance para la teoría y la práctica jurídica. En primer lugar, modifica la forma de entender la validez normativa. Mientras en el positivismo la validez dependía exclusivamente de la fuente o del procedimiento de producción de la norma, en el modelo neoconstitucional la validez depende también de la compatibilidad material de las disposiciones con los valores constitucionales. En segundo lugar, altera el rol del juez, que deja

de ser un mero aplicador de la ley para convertirse en garante activo de los principios y derechos fundamentales. Esta visión, como señala Peces-Barba (1995), convierte al juez en un intérprete moral del ordenamiento, responsable de armonizar la legalidad con la justicia sustantiva. En consecuencia, el derecho deja de ser un sistema cerrado de reglas para convertirse en un orden abierto de principios que se proyectan sobre toda la práctica jurídica.

La coexistencia de reglas y principios genera un nuevo tipo de conflicto normativo que no puede resolverse mediante los mecanismos tradicionales del positivismo. Mientras que los conflictos entre reglas se resuelven a través de la jerarquía o la cronología, los conflictos entre principios implican colisiones de valores igualmente válidos. En estos casos, el derecho no elimina uno de los principios, sino que busca armonizarlos mediante la ponderación, técnica que permite determinar cuál debe prevalecer en una situación concreta, atendiendo a la intensidad de los derechos en juego y a las circunstancias del caso. Bayón (2000) explica que esta ponderación no implica arbitrariedad, sino un ejercicio racional de argumentación jurídica en el que el juez debe justificar por qué otorga mayor peso a un principio sobre otro, según los fines constitucionales perseguidos. La ponderación, por tanto, introduce una racionalidad práctica que supera la mera aplicación mecánica de normas y exige una fundamentación transparente, coherente y controlable.

La presencia dominante de principios constitucionales ha producido un cambio profundo en la estructura del derecho contemporáneo. Las constituciones actuales están impregnadas de principios como la proporcionalidad, la igualdad, la dignidad humana, la solidaridad o la justicia material, que operan como vectores de interpretación para todo el sistema jurídico. Estos principios no solo regulan la actuación del poder público, sino que orientan la conducta privada y guían la formulación de políticas públicas. En palabras de Aarnio (1997), el derecho se convierte en un "orden discursivo", en el que las normas se interpretan a la luz de los valores compartidos por la comunidad jurídica y política. Así, el paradigma normativo del neoconstitucionalismo no busca desplazar las reglas, sino integrarlas dentro de un marco axiológico que les confiera sentido moral y coherencia estructural.

La incorporación de los principios en el centro del sistema jurídico implica también un cambio epistemológico en la comprensión del derecho. El conocimiento jurídico ya no se limita al análisis lógico-formal de las normas, sino que requiere una comprensión interdisciplinaria que incluya la filosofía, la ética, la política y la teoría de la argumentación. El juez constitucional, en este contexto, se convierte en un intérprete prudencial que debe equilibrar

valores en conflicto mediante razonamientos justificables. Neil MacCormick (2005) denomina a esta forma de razonamiento "racionalidad institucional", destacando que la interpretación constitucional requiere un equilibrio entre la coherencia sistémica del derecho y la sensibilidad moral frente a las consecuencias de las decisiones judiciales. Esta racionalidad práctica permite garantizar que la ponderación no derive en subjetivismo, sino que se sostenga en la estructura argumentativa del derecho como práctica social razonada.

Este nuevo paradigma normativo también plantea una redefinición del concepto de justicia. Si en el positivismo la justicia era externa al derecho, en el neoconstitucionalismo se internaliza en el sistema normativo a través de los principios constitucionales. De este modo, los principios actúan como puentes entre la validez jurídica y la legitimidad moral, asegurando que el derecho sea no solo formalmente válido, sino también sustantivamente justo. Esta concepción ha sido desarrollada por Atienza y Ruiz Manero (2007), quienes sostienen que los principios jurídicos expresan los ideales de justicia y equidad que fundamentan la práctica jurídica y orientan la creación, interpretación y aplicación del derecho. De esta forma, la distinción entre reglas y principios no es meramente técnica, sino ética y política, porque sitúa a los valores constitucionales como el eje que confiere legitimidad al orden jurídico.

Por último, este enfoque implica una transformación en la cultura jurídica. Los operadores del derecho, especialmente los jueces, legisladores y académicos, deben adoptar una actitud argumentativa y deliberativa, conscientes de que toda decisión jurídica tiene un componente axiológico. La supremacía de la Constitución y la presencia de principios vinculantes demandan un compromiso con la coherencia moral y la racionalidad pública. En este sentido, el derecho deja de ser un conjunto de mandatos cerrados y se convierte en un espacio de diálogo entre la ley, la justicia y los derechos humanos. Este modelo no solo fortalece el Estado constitucional de derecho, sino que amplía su horizonte hacia una democracia sustantiva en la que la Constitución actúa como guía permanente para la acción política y jurídica.

En suma, la distinción entre reglas y principios representa un cambio de paradigma que redefine la estructura, la función y la legitimidad del derecho. El neoconstitucionalismo, al incorporar este modelo, propone un sistema normativo más flexible, racional y moralmente fundado, en el que la Constitución se convierte en el centro operativo de la justicia y la interpretación se erige como la herramienta fundamental para garantizar la vigencia real de los derechos fundamentales y los valores democráticos.

1.2.8. Ponderación y argumentación jurídica

El tercer pilar del neoconstitucionalismo es la ponderación, que representa la herramienta interpretativa central para aplicar principios y garantizar la justicia constitucional. Según Alexy (2004), la ponderación sigue tres fases:

1. Identificación de principios en conflicto, por ejemplo, libertad de expresión versus derecho al honor.

2. Asignación de pesos relativos, valorando la importancia de cada principio según las circunstancias fácticas, el impacto social y los valores constitucionales comprometidos.

3. Determinación de la solución proporcional, que maximice la protección de los derechos sin anular completamente al principio que cede en ese caso concreto.

Este método convierte la función judicial en una actividad argumentativa y racional, en la que las decisiones deben justificarse públicamente, reforzando su legitimidad democrática. Como advierte Atienza (2006), la ponderación no equivale a arbitrariedad, sino que representa un ejercicio de racionalidad práctica, especialmente necesario en sociedades pluralistas donde los valores pueden entrar en tensión.

No obstante, este protagonismo judicial plantea desafíos críticos: 1. La discrecionalidad interpretativa puede derivar en decisiones heterogéneas y en inseguridad jurídica. 2. La judicialización de la política puede tensionar la legitimidad democrática, especialmente cuando decisiones de gran impacto social dependen del criterio de tribunales constitucionales.

Los fundamentos teóricos y filosóficos del neoconstitucionalismo reflejan un cambio estructural del derecho:

- La Constitución adquiere fuerza normativa y valor sustantivo.
- Los principios constitucionales se convierten en instrumentos de interpretación y control.
- Los jueces asumen un rol central como garantes activos de los derechos fundamentales.

Este modelo fortalece la democracia sustantiva y la protección de derechos, pero al mismo tiempo genera tensiones con la democracia representativa, pues incrementa la discrecionalidad judicial y el riesgo de un "gobierno de jueces". Su consolidación exige transparencia argumentativa, criterios de autocontención judicial y coherencia institucional, para equilibrar la eficacia de los derechos con la legitimidad del sistema democrático.

En conclusión, los fundamentos teóricos y filosóficos del neoconstitucionalismo revelan un cambio profundo en la concepción del derecho, que pasa de ser un sistema cerrado, formalista y estatalista, propio del constitucionalismo clásico, a convertirse en un ordenamiento abierto, axiológico y garantista, en el que la Constitución ocupa un lugar central como norma viva. Sin embargo, esta reconfiguración estructural no se limita a la incorporación de nuevos mecanismos jurídicos o a la expansión de la función judicial; supone también una transformación cultural del derecho, que exige reconocer la inevitable conexión entre norma y valor, así como la responsabilidad moral del juez en la construcción de la justicia constitucional. Esta dimensión axiológica es, precisamente, la que otorga al neoconstitucionalismo su capacidad de responder a los desafíos sociales y políticos contemporáneos, pero también la que suscita tensiones críticas sobre la legitimidad y los límites del poder judicial. A partir de este punto, resulta imprescindible analizar cómo el componente moral se integra al derecho en este nuevo paradigma, configurando la base ética de la justicia constitucional que será abordada en el siguiente subcapítulo.

En este sentido, el neoconstitucionalismo no solo redefine los pilares estructurales del sistema jurídico, sino que inaugura una nueva racionalidad jurídica en la que la interpretación constitucional se convierte en un ejercicio de responsabilidad ética y política. La centralidad de la Constitución implica que los jueces, los legisladores y los operadores jurídicos asuman un rol deliberativo, orientado a garantizar que las decisiones públicas estén en consonancia con los valores superiores del orden constitucional. Este cambio de paradigma supone una apertura del derecho hacia la argumentación moral y la razonabilidad práctica, donde la legitimidad de las normas no deriva únicamente de su validez formal, sino de su coherencia con los principios de justicia, dignidad y bien común. En consecuencia, el derecho se concibe como una práctica comunicativa y dialógica, en la que la Constitución actúa como horizonte normativo compartido y la interpretación se transforma en un instrumento de construcción democrática. Esta perspectiva reafirma que el neoconstitucionalismo no es simplemente una teoría jurídica,

sino una filosofía pública del derecho orientada a reconciliar legalidad y legitimidad, técnica y ética, forma y justicia.

1.2.9. Moral y crítica democrática

Uno de los elementos que singularizan al neoconstitucionalismo es la incorporación explícita de la dimensión moral dentro de la estructura misma del derecho. Este planteamiento supone una ruptura profunda con el positivismo jurídico clásico, que defendía la separación estricta entre derecho y moral, así como la supuesta neutralidad valorativa del sistema normativo. La experiencia histórica del siglo XX dejó en evidencia que el formalismo legal, por sí solo, no garantiza la justicia: normas revestidas de validez formal fueron utilizadas para sostener regímenes autoritarios y justificar violaciones sistemáticas de derechos humanos.

La introducción de la moral en el ámbito jurídico no implica la disolución de las fronteras entre derecho y ética, sino el reconocimiento de que toda norma jurídica encierra una pretensión de corrección que trasciende la mera validez formal. En este sentido, autores como Ronald Dworkin (1986) sostienen que el derecho no puede entenderse como un sistema cerrado de reglas, sino como una práctica interpretativa que exige al juez buscar la mejor respuesta moral posible dentro del marco constitucional. La interpretación jurídica, por tanto, no se limita a aplicar normas positivas, sino que debe armonizar principios y valores que confieren legitimidad al sistema jurídico.

Esta visión moral del derecho transformó profundamente la función judicial y la naturaleza misma del razonamiento jurídico. Los tribunales constitucionales dejaron de ser órganos de control meramente formal para convertirse en escenarios deliberativos donde se discuten y ponderan los valores fundamentales de la comunidad política. En este contexto, la justicia constitucional se convierte en un espacio de mediación entre el derecho y la moral, en el que la legitimidad de las decisiones depende de su capacidad para justificar racionalmente los principios que las sustentan. Habermas (1998) describe este proceso como una "racionalización comunicativa del derecho", donde la validez normativa se construye a través del diálogo argumentativo y la participación de los ciudadanos en la esfera pública.

La dimensión moral del neoconstitucionalismo también implica un cambio en la concepción de los derechos fundamentales. Estos ya no se entienden como simples límites al poder o como concesiones del Estado, sino como expresiones institucionalizadas de valores morales universales, tales como la dignidad humana, la libertad y la igualdad. La Constitución,

en este marco, actúa como un "código moral político" (Nino, 1994), que orienta la acción estatal y fija los parámetros de legitimidad de toda decisión pública. De este modo, el derecho constitucional deja de ser un conjunto de normas estáticas para convertirse en un proyecto ético de sociedad, orientado al respeto y promoción de los valores compartidos.

Asimismo, el neoconstitucionalismo incorpora la idea de que la moralidad constitucional debe ser aplicada de manera razonable y proporcional, evitando la arbitrariedad judicial. Esto se logra a través del método de ponderación, que permite resolver conflictos entre principios en función de su peso o relevancia en el caso concreto. Como explica Alexy (2003), esta técnica busca garantizar que ningún derecho sea vaciado de contenido, preservando un equilibrio racional entre las distintas exigencias constitucionales. La ponderación, por tanto, no es un acto de subjetividad judicial, sino una forma estructurada de razonamiento moral que traduce los valores constitucionales en decisiones jurídicas concretas.

En América Latina, la incorporación de esta dimensión moral ha tenido una relevancia singular. Las nuevas constituciones de finales del siglo XX no solo ampliaron los catálogos de derechos, sino que también institucionalizaron la justicia como valor supremo y fin del Estado. La jurisprudencia constitucional colombiana, por ejemplo, ha desarrollado una doctrina robusta sobre la dignidad humana como principio fundante del orden jurídico, interpretando los derechos desde una perspectiva humanista y solidaria. La Corte Constitucional ha asumido así una función ética, orientada a garantizar que las normas jurídicas sean coherentes con los valores constitucionales y con los compromisos internacionales en materia de derechos humanos.

La consecuencia más significativa de esta transformación es la consolidación de una cultura constitucional ética, en la que el derecho se concibe como una herramienta de emancipación y justicia social. El neoconstitucionalismo, en su dimensión moral, no pretende moralizar el derecho en términos dogmáticos, sino humanizarlo, devolviéndole su función originaria de proteger la dignidad y el bienestar de las personas. Ello exige un nuevo tipo de jurista, capaz de razonar con principios, deliberar con prudencia y justificar sus decisiones desde una ética pública compartida.

Finalmente, la incorporación de la moral en el derecho no representa una amenaza a la seguridad jurídica, sino un paso evolutivo hacia un modelo más justo, participativo y humanista. La legitimidad del derecho en el siglo XXI no puede descansar únicamente en su

legalidad formal, sino en su capacidad para encarnar los valores que sustentan la convivencia democrática. En este sentido, el neoconstitucionalismo redefine la justicia constitucional como una práctica moral institucionalizada, donde la razón jurídica y la razón ética convergen en la búsqueda de un orden social más equitativo y digno.

El neoconstitucionalismo no se basa en una moral única y rígida, sino en una moral crítica y deliberativa, que se construye dentro de la comunidad política. Siguiendo a Carlos Santiago Nino (1996), la democracia constitucional exige que las decisiones jurídicas y políticas se fundamenten en valores discutidos y compartidos racionalmente, no en convicciones morales privadas o arbitrarias. En este sentido, los principios constitucionales funcionan como instrumentos de moralidad pública que limitan el poder y protegen a las minorías frente a mayorías ocasionales, la interpretación constitucional debe ser coherente con los valores democráticos, asegurando que la protección de derechos no se convierta en imposición moral ajena al consenso social, y la argumentación judicial es la garantía de control democrático al exigir que cada decisión esté justificada en razones públicas y verificables.

El concepto de moral crítica constituye uno de los aportes más significativos del pensamiento neoconstitucionalista, pues busca conciliar la dimensión ética del derecho con el respeto a la pluralidad moral propia de las sociedades contemporáneas. A diferencia de la moral autoritaria, que impone un único código de valores, la moral crítica reconoce la legitimidad del disenso y la diversidad, estableciendo que las normas solo son válidas si pueden ser justificadas racionalmente ante todos los ciudadanos. De este modo, el derecho constitucional se convierte en un espacio deliberativo donde las razones morales son sometidas al escrutinio público, garantizando que la justicia no sea resultado de la imposición, sino del diálogo argumentativo.

Jürgen Habermas (1998) profundiza en esta idea al sostener que la legitimidad democrática surge del proceso comunicativo mediante el cual los ciudadanos deliberan en condiciones de igualdad. Desde su teoría del discurso, la moral crítica no reside en contenidos sustantivos predefinidos, sino en los procedimientos que aseguran la participación libre y racional de todos los implicados. La Constitución, en consecuencia, no es solo una norma jurídica suprema, sino el marco institucional que hace posible esa comunicación racional y que garantiza la vigencia de los derechos como presupuestos del diálogo democrático.

Desde la perspectiva del neoconstitucionalismo garantista de Luigi Ferrajoli (2009), la moral pública constitucional no puede depender de convicciones individuales, religiosas o

ideológicas, sino de principios universalizables que aseguren la igualdad moral de todas las personas. Por ello, los derechos fundamentales se conciben como límites éticos y jurídicos frente al poder político y frente a las mayorías sociales. Este enfoque dota al constitucionalismo de una función crítica: la de someter al escrutinio moral toda decisión que vulnere la dignidad humana o que niegue las condiciones mínimas de libertad y justicia.

En este marco, la moral crítica se presenta como el vínculo entre justicia y democracia. John Rawls (1993), en su propuesta de "consenso traslapado", plantea que una sociedad plural puede sostener una moral política compartida, basada en principios de justicia que trascienden las concepciones particulares del bien. La democracia constitucional, bajo esta óptica, se fortalece cuando los jueces, los legisladores y los ciudadanos interpretan los valores constitucionales desde una racionalidad pública, capaz de integrar la diversidad moral en un horizonte común de respeto y equidad.

La función judicial adquiere, por tanto, un papel central en esta construcción moral. Los jueces constitucionales, al resolver conflictos entre derechos y valores, deben argumentar sus decisiones de manera transparente y razonada, mostrando que sus fallos responden a criterios de justicia reconocibles por todos los ciudadanos. En este punto, la deliberación judicial se convierte en un ejercicio de moral pública, pues traduce los principios constitucionales en decisiones concretas que orientan la conducta del Estado y de la sociedad.

La moral crítica, en el contexto del neoconstitucionalismo, también implica una relectura de la democracia representativa. No se trata de sustituir la voluntad popular por el criterio judicial, sino de garantizar que toda decisión política sea evaluada a la luz de los valores constitucionales. En este sentido, el poder judicial actúa como un foro moral de la comunidad, encargado de preservar la coherencia entre las normas legales y los principios éticos fundamentales. Sin embargo, su legitimidad depende del respeto a la deliberación democrática, de la argumentación racional y de la apertura al diálogo con los otros poderes del Estado.

Roberto Gargarella (2010) destaca que la democracia constitucional debe concebirse como un proceso de interacción entre instituciones y ciudadanía, donde los derechos no son meros límites al poder, sino condiciones para su ejercicio legítimo. La moral crítica, entonces, no se opone a la democracia, sino que la fortalece, porque impide que la mayoría actúe de manera arbitraria o que las minorías sean marginadas del debate público. En esta interacción,

el derecho constitucional asume una dimensión transformadora: no solo regula, sino que orienta éticamente la convivencia política.

En América Latina, la moral crítica ha adquirido especial relevancia en contextos de desigualdad estructural y fragilidad institucional. La jurisprudencia de las cortes constitucionales ha servido para consolidar una moral pública basada en la dignidad, la igualdad material y la solidaridad. Casos emblemáticos sobre derechos de comunidades indígenas, igualdad de género, objeción de conciencia o medio ambiente reflejan cómo los tribunales han actuado como mediadores morales entre el Estado y la sociedad, buscando decisiones que equilibren justicia, pluralismo y deliberación democrática.

No obstante, esta visión plantea desafíos significativos. Uno de ellos es la tensión entre la moral crítica y la soberanía popular: ¿hasta qué punto puede el juez constitucional invalidar decisiones democráticas en nombre de valores morales? Otro es el riesgo de que la moral crítica se convierta en moral dogmática, si las cortes adoptan posturas ideológicas cerradas. Frente a estos riesgos, Habermas propone la idea de un "constitucionalismo discursivo", en el que la legitimidad de las decisiones judiciales depende de su capacidad para sostener un diálogo público continuo, abierto a la crítica y a la revisión racional.

Finalmente, la moral crítica y la democracia constitucional convergen en un mismo propósito: construir un derecho que combine validez jurídica, legitimidad democrática y corrección moral. En el paradigma neoconstitucionalista, el derecho no se justifica por su procedencia formal, sino por su contribución al bienestar colectivo y al respeto de la dignidad humana. De este modo, el neoconstitucionalismo se erige como una teoría del derecho y, al mismo tiempo, como una ética pública que promueve la justicia, la participación y la deliberación en el marco del Estado constitucional contemporáneo.

1.3.La Constitución como carta de valores

El neoconstitucionalismo concibe a la Constitución no solo como una norma suprema del ordenamiento, sino también como una carta de valores que expresa los consensos fundamentales de la comunidad política. En este sentido, los principios constitucionales adquieren fuerza normativa y moral, actúan como mandatos de optimización que obligan a todas las autoridades, incluso al legislador, y constituyen criterios de corrección que permiten

invalidar normas o actos que, aun siendo formalmente legales, contradicen la dignidad humana y los valores superiores.

Esta concepción implica un cambio profundo en la forma de entender el derecho y la función constitucional. La Constitución deja de ser un simple texto legal para convertirse en el núcleo ético del sistema jurídico, donde los valores no son meras declaraciones programáticas, sino fundamentos normativos vinculantes. Así, cada disposición constitucional refleja un compromiso moral con la justicia, la libertad, la igualdad y la dignidad humana, que orienta tanto la creación como la aplicación del derecho.

Autores como Ronald Dworkin (1977) sostienen que los principios son normas con contenido moral incorporado que orientan la interpretación jurídica hacia decisiones correctas, mientras que Robert Alexy (1993) afirma que la Constitución contemporánea es inseparable de su dimensión axiológica, porque sin moral el derecho constitucional pierde legitimidad sustantiva. Desde esta perspectiva, el juez constitucional no se limita a aplicar reglas, sino que debe ponderar valores y principios para alcanzar soluciones coherentes con el espíritu de la Constitución.

La fuerza normativa de los valores constitucionales se traduce en la obligación de que toda autoridad pública interprete y actúe conforme a la dignidad humana, la justicia y el bien común. Este principio se encuentra en la base del Estado social y democrático de derecho, donde la validez de las normas depende no solo de su legalidad formal, sino de su coherencia con los valores superiores del ordenamiento. Así, el derecho se convierte en un instrumento para realizar los ideales morales que la sociedad reconoce como propios.

El carácter valorativo de la Constitución también redefine el papel de la interpretación jurídica. Ya no se trata de un ejercicio mecánico de subsunción, sino de una actividad argumentativa que busca armonizar principios y derechos. La ponderación, en este contexto, es la técnica que permite resolver conflictos de valores de manera racional y proporcional. Alexy explica que los principios son mandatos de optimización cuya aplicación depende de las posibilidades fácticas y jurídicas, por lo que el intérprete debe determinar en cada caso cuál valor debe prevalecer sin anular completamente al otro.

La Constitución, concebida como carta de valores, cumple además una función integradora. Representa el pacto ético-político que une a los ciudadanos bajo una comunidad de principios compartidos. Esta función se manifiesta en la exigencia de que toda acción estatal

y toda política pública se funden en la protección de la dignidad y los derechos fundamentales. Ferrajoli (2007) sostiene que la supremacía de la Constitución radica precisamente en su capacidad para imponer límites morales al poder y garantizar el respeto a las personas como fin y no como medio.

En el contexto latinoamericano, esta visión ha adquirido especial relevancia. Las constituciones de países como Colombia, Ecuador o Bolivia han asumido un enfoque neoconstitucional que otorga centralidad a los valores y principios. En Colombia, por ejemplo, la Corte Constitucional ha construido una sólida doctrina sobre la dignidad humana como principio rector del orden jurídico, señalando que todas las normas deben interpretarse a la luz de ese valor supremo. Ello ha permitido que la jurisprudencia actúe como vehículo para materializar la justicia social, la equidad y el reconocimiento de las diferencias.

La idea de la Constitución como carta de valores también tiene un fuerte contenido pedagógico y cultural. No solo orienta a los operadores jurídicos, sino que educa a la ciudadanía en los principios de convivencia democrática. De esta manera, el constitucionalismo contemporáneo se presenta no como una técnica jurídica, sino como un proyecto ético-político que aspira a moldear la conducta social conforme a ideales de justicia. El derecho deja de ser un conjunto de prohibiciones para convertirse en una herramienta de emancipación, capaz de impulsar transformaciones sociales a partir de valores compartidos.

Finalmente, comprender la Constitución como carta de valores implica reconocer que el derecho no puede desvincularse de la moral pública. Las normas constitucionales son la expresión institucional de los valores fundamentales de la sociedad, y su observancia no depende solo del cumplimiento formal, sino de la adhesión ética de los ciudadanos y de sus gobernantes. Por ello, la legitimidad del orden jurídico se mide por su capacidad para realizar en la práctica los ideales de justicia, libertad y dignidad que la Constitución proclama.

En conclusión, el neoconstitucionalismo eleva la Constitución a la categoría de código moral y jurídico supremo, donde el derecho y la moral se integran para garantizar un orden justo. Los valores constitucionales no son simples aspiraciones retóricas, sino mandatos concretos que orientan la vida jurídica y política del Estado. Así, la Constitución no solo organiza el poder, sino que lo limita, lo humaniza y lo somete al servicio de la persona, consolidando una cultura jurídica basada en la ética y la justicia.

1.3.1. El juez constitucional como garante moral

En este nuevo paradigma, el juez constitucional asume un rol protagónico no solo jurídico, sino también ético. A diferencia del modelo clásico, en el que el juez se limitaba a aplicar la ley, en el neoconstitucionalismo el juez:

- Pondera principios en conflicto, evaluando su peso moral y jurídico.
- Corrige al legislador cuando la ley se aparta de los valores constitucionales.
- Protege activamente los derechos fundamentales, aun frente a omisiones normativas o decisiones políticas inadecuadas.

Esta nueva concepción del juez constitucional redefine la naturaleza misma de la justicia. El juez ya no es un mero ejecutor de la voluntad legislativa, sino un garante de la supremacía constitucional y de los valores que sustentan el orden jurídico. Su papel se amplía desde la aplicación mecánica de normas hacia la defensa activa de la dignidad humana, la igualdad y la justicia material. En este sentido, la función judicial se configura como una tarea de interpretación creativa, orientada por los principios constitucionales y por una sensibilidad ética que busca armonizar el derecho con la moral pública.

Autores como Gustavo Zagrebelsky (1995) sostienen que el juez constitucional se erige en "intérprete de la Constitución viva", es decir, del texto que evoluciona junto con la sociedad y refleja sus aspiraciones éticas y políticas. En consecuencia, el juez no solo resuelve conflictos jurídicos, sino que también participa en la construcción del sentido moral del derecho, garantizando que las decisiones del Estado se mantengan dentro de los límites de la justicia constitucional.

Desde esta perspectiva, la ponderación se convierte en la herramienta esencial para la toma de decisiones judiciales. Robert Alexy explica que, al enfrentar principios en tensión, el juez debe identificar cuál de ellos posee mayor peso en el caso concreto, considerando tanto las circunstancias fácticas como los fines constitucionales comprometidos. Este proceso de razonamiento práctico requiere un ejercicio de racionalidad comunicativa y de justificación argumentativa, que legitima la intervención judicial en cuestiones sensibles de la vida pública.

El rol moral del juez constitucional implica además una función pedagógica. Cada sentencia no solo soluciona un litigio particular, sino que comunica a la sociedad los valores

que la Constitución protege. Así, las decisiones judiciales actúan como instrumentos de educación cívica y de consolidación cultural del constitucionalismo. En el contexto latinoamericano, la jurisprudencia constitucional ha tenido un papel decisivo en la transformación social, al promover la inclusión, la equidad de género, la protección de minorías y la ampliación de los derechos sociales.

Sin embargo, esta expansión del poder judicial plantea también tensiones democráticas. La intervención activa de los jueces en asuntos tradicionalmente reservados al legislador o al Ejecutivo genera el debate sobre la "judicialización de la política". Carlos Santiago Nino (1992) advierte que el juez constitucional debe ejercer su función con prudencia, evitando sustituir la deliberación democrática por decisiones judiciales excesivamente intervencionistas. En este sentido, la legitimidad de la justicia constitucional depende de la calidad de su argumentación y de su fidelidad a los valores y principios del texto constitucional, más que de su poder de veto frente al legislador.

La ética judicial se convierte, entonces, en un elemento central del neoconstitucionalismo. El juez debe ser consciente de la dimensión moral de sus decisiones y de su impacto en la vida colectiva. La imparcialidad, la transparencia y la fundamentación racional son condiciones esenciales para que el ejercicio de la jurisdicción constitucional conserve su legitimidad ante la sociedad. Luigi Ferrajoli (2009) señala que la independencia judicial no puede entenderse como un poder sin límites, sino como una responsabilidad institucional orientada al control de los abusos del poder y a la defensa de los derechos de los más débiles.

En este contexto, la figura del juez constitucional se sitúa en la intersección entre derecho y moral, entre política y justicia. Su tarea consiste en garantizar que el sistema normativo refleje los valores superiores de la Constitución, evitando que la legalidad se convierta en instrumento de injusticia. Este papel no debe confundirse con un activismo judicial desmedido, sino que debe entenderse como la exigencia de coherencia ética en la aplicación del derecho.

Dworkin (1986) propone la idea del "juez Hércules", un magistrado ideal que razona con integridad moral y jurídica, buscando siempre la decisión que mejor exprese los principios de justicia que subyacen al ordenamiento. Aunque esta figura es teórica, simboliza la aspiración

del neoconstitucionalismo: un juez comprometido con la verdad moral del derecho, capaz de interpretar las normas desde la perspectiva de los derechos humanos y de la justicia material.

Por tanto, el juez constitucional no solo controla la legalidad de las normas, sino su moralidad. La invalidez de una ley no se deriva únicamente de su contradicción formal con la Constitución, sino de su incompatibilidad con los valores que esta encarna. Este enfoque rompe definitivamente con el positivismo jurídico tradicional, que reducía la función judicial a la subsunción mecánica de hechos bajo reglas. En el neoconstitucionalismo, el juez actúa como garante de un orden jurídico impregnado de principios y valores, donde la justicia no es una consecuencia accidental, sino el fin mismo del derecho.

La ampliación del papel del juez también transforma la noción de separación de poderes. En lugar de una división rígida, el modelo neoconstitucional propone un equilibrio dinámico entre poderes, en el cual la justicia constitucional sirve como mecanismo de control ético-político. El juez no reemplaza al legislador, sino que lo complementa, asegurando que las decisiones democráticas se mantengan dentro del marco axiológico de la Constitución. De esta manera, el control judicial se convierte en un instrumento de depuración moral del poder político.

La legitimidad del juez constitucional se construye, entonces, sobre tres pilares: la argumentación racional, la fidelidad a los valores constitucionales y la transparencia de sus decisiones. Solo cuando estos elementos confluyen, la intervención judicial se percibe como una defensa de la justicia y no como una usurpación del poder democrático. En consecuencia, la tarea del juez es, al mismo tiempo, jurídica y moral, técnica y humana, racional y ética.

En síntesis, el juez constitucional como garante moral representa la culminación del proyecto neoconstitucionalista: un derecho que no se limita a regular, sino que pretende humanizar el poder. Su misión es preservar la integridad de la Constitución como carta de valores, garantizar la vigencia efectiva de los derechos fundamentales y fortalecer la confianza ciudadana en la justicia. De su prudencia, coherencia y compromiso ético depende, en gran medida, la legitimidad del Estado constitucional contemporáneo.

1.4. Tensiones y críticas al componente moral

La integración de la moral en el derecho constitucional fortalece la justicia sustantiva y contribuye a un modelo jurídico más humano y garantista. Sin embargo, esta relación entre moral y derecho no está exenta de dificultades teóricas ni de riesgos prácticos. El

neoconstitucionalismo, al introducir valores, principios y derechos fundamentales como parámetros de validez normativa, transforma profundamente la estructura del orden jurídico, pero al mismo tiempo suscita interrogantes sobre los límites de la función judicial y la legitimidad democrática de las decisiones basadas en juicios morales.

En primer lugar, uno de los principales cuestionamientos se centra en la subjetividad judicial. La ponderación de principios implica la realización de juicios de valor que, aunque guiados por criterios racionales, dependen en gran medida de la interpretación del juez. Como advierte Alexy (2002), la aplicación de principios constitucionales no puede reducirse a un razonamiento puramente lógico-formal, sino que exige una evaluación de proporcionalidad en la que intervienen factores axiológicos y contextuales. Esta apertura valorativa, si bien enriquece la justicia material, puede también generar incertidumbre respecto a la previsibilidad de las decisiones judiciales y, por ende, afectar la seguridad jurídica. En la práctica, distintos tribunales pueden llegar a conclusiones divergentes frente a problemas análogos, lo que debilita la uniformidad del derecho y la confianza ciudadana en el sistema judicial.

En segundo lugar, emerge la judicialización de la política, fenómeno mediante el cual los jueces asumen un papel protagónico en la resolución de controversias que tradicionalmente correspondían al ámbito del legislador o del ejecutivo. Este desplazamiento del debate democrático hacia los tribunales se justifica en parte por la necesidad de proteger derechos fundamentales cuando los poderes públicos fallan en su garantía. No obstante, como señala Gargarella (2010), el activismo judicial puede transformarse en una forma de "gobierno de jueces", en la medida en que las cortes asumen decisiones de alto impacto político sin una legitimidad electoral directa. El riesgo radica en que, bajo la pretensión de tutelar la Constitución, se sustituya la deliberación pública por la interpretación judicial, debilitando así el principio de soberanía popular.

En tercer lugar, la moral constitucional enfrenta el reto de la dependencia del consenso axiológico. La eficacia del neoconstitucionalismo supone la existencia de ciertos valores compartidos dentro de la comunidad política que sirvan de base para la interpretación constitucional. Sin embargo, en sociedades plurales y fragmentadas, donde coexisten concepciones divergentes del bien común, la función moral del juez puede volverse inestable o incluso conflictiva. Dworkin (1986) propone que el derecho debe entenderse como una práctica interpretativa que busca la mejor justificación moral del orden jurídico, pero tal pretensión presupone un horizonte de valores suficientemente consensuado. Cuando este

consenso se debilita, la decisión judicial puede ser percibida como una imposición ideológica o una interferencia moral ajena al pluralismo democrático.

Estas críticas ponen de relieve que el éxito del neoconstitucionalismo no depende exclusivamente de su diseño normativo, sino también de la calidad de las prácticas judiciales, del rigor argumentativo y del diálogo constante con la sociedad democrática. El juez constitucional, en este contexto, no solo debe aplicar la ley conforme a la Constitución, sino también justificar sus decisiones con razones públicas, accesibles y verificables. La legitimidad moral del derecho se construye, por tanto, a través de una comunicación transparente entre el poder judicial y la ciudadanía, en la que las decisiones sean comprensibles y racionalmente defendibles.

Ahora bien, la articulación entre neoconstitucionalismo y moral ha configurado un derecho constitucional abierto y orientado hacia la justicia sustantiva. Este modelo reconoce que la validez del derecho no se agota en su procedencia formal, sino que debe estar sustentada en su capacidad para proteger derechos, promover la igualdad y salvaguardar la dignidad humana. Tal como sostiene Ferrajoli (2011), el constitucionalismo contemporáneo se funda en la idea de límites al poder y en la existencia de principios superiores que orientan todo el sistema jurídico hacia la realización efectiva de la justicia. En este sentido, la moral constitucional actúa como un criterio de legitimidad y control frente a la arbitrariedad, dotando al derecho de una dimensión ética que lo vincula con los ideales democráticos.

Sin embargo, esta apertura axiológica entraña retos sustantivos. Requiere jueces prudentes, conscientes de su papel dentro del equilibrio de poderes, y una argumentación jurídica sólida que evite la discrecionalidad o la moralización excesiva del derecho. El desafío consiste en mantener un balance cuidadoso entre el activismo judicial, necesario para la defensa de los derechos, y el respeto por el principio democrático, que garantiza la participación ciudadana en la creación del derecho. Como afirma Zagrebelsky (1995), la Constitución no puede ser interpretada como un texto cerrado ni como un mandato moral absoluto; su sentido se construye en el diálogo entre las instituciones y la sociedad, en un proceso permanente de actualización de sus valores fundacionales.

De cómo se gestione este equilibrio dependerá que la moral en el derecho funcione como un instrumento de legitimación y transformación, y no como una justificación de decisiones marcadas por la arbitrariedad o el subjetivismo. El juez constitucional debe, por

tanto, asumir una ética de la responsabilidad, donde cada decisión sea el resultado de una deliberación racional, transparente y abierta al escrutinio público. La ponderación, la proporcionalidad y la argumentación deben operar como garantías de que la moral judicial no se convierta en moral personal.

En definitiva, la dimensión moral del neoconstitucionalismo constituye uno de sus rasgos más característicos y, al mismo tiempo, más debatidos. Su principal aporte consiste en fortalecer la justicia constitucional al vincular la validez normativa con la protección de la dignidad humana y los derechos fundamentales. No obstante, también abre interrogantes sobre los límites del poder judicial, pues la incorporación de la moral al derecho otorga a los jueces un papel central en la configuración del orden jurídico, lo que puede derivar en tensiones con la democracia representativa.

Estas dinámicas son especialmente visibles en América Latina, donde los tribunales constitucionales han adquirido un papel preponderante frente a Estados históricamente débiles y sociedades marcadas por profundas desigualdades. En países como Colombia, Ecuador o Bolivia, las cortes han impulsado transformaciones significativas en materia de derechos sociales, medioambientales y de participación ciudadana. Sin embargo, también han enfrentado críticas por exceder sus competencias o por asumir decisiones de naturaleza eminentemente política. Este contexto revela la doble cara del neoconstitucionalismo: por un lado, su potencial emancipador y garantista; por otro, su vulnerabilidad frente a los riesgos de concentración de poder judicial y la crisis de representación política.

El análisis de la expansión e impacto del neoconstitucionalismo latinoamericano permitirá comprender cómo este paradigma ha actuado simultáneamente como motor de transformación jurídica y social, y como escenario de tensiones democráticas y desafíos institucionales. La moral constitucional, lejos de ser un concepto abstracto, se convierte en un campo de disputa entre distintas concepciones de justicia, legitimidad y poder. De su correcta articulación dependerá que el derecho continúe siendo un instrumento de emancipación y no de imposición moral.

1.5. Difusión latinoamericana: transformación del neoconstitucionalismo en Latinoamérica actualmente.

En América Latina, el neoconstitucionalismo ha supuesto una verdadera transformación en la concepción del derecho constitucional y en la protección de los derechos fundamentales.

A diferencia de la tradición liberal clásica, donde la Constitución era frecuentemente un instrumento formal con escasa eficacia práctica, las reformas constitucionales de finales del siglo XX y comienzos del XXI han impulsado textos extensos y garantistas, con un marcado énfasis en la justiciabilidad de los derechos, la supremacía material de la Constitución y el fortalecimiento de los tribunales constitucionales como actores centrales en el Estado de derecho.

Este fenómeno se evidencia con particular claridad en países como Colombia, Ecuador y Bolivia, que han adoptado constituciones de nueva generación, caracterizadas por la densidad normativa en derechos, la incorporación de principios axiológicos, y la creación de mecanismos judiciales expeditos. Entre ellos, destacan:

- La acción de tutela en Colombia, que ha permitido la protección inmediata de los derechos fundamentales y ha convertido a la Corte Constitucional en un protagonista de la ingeniería institucional, capaz de emitir sentencias estructurales en materia de desplazamiento forzado, salud, acceso a servicios sociales y derechos de comunidades vulnerables.

- La Constitución ecuatoriana de 2008 y la Constitución boliviana de 2009, que consolidan un modelo de Estado constitucional plurinacional y transformador, incorporando derechos de la naturaleza, pluralismo jurídico y mecanismos de democracia participativa y comunitaria, reflejando un constitucionalismo social y multicultural de amplio alcance.

Por tanto, se entiende que el neoconstitucionalismo latinoamericano ha significado un avance sustancial en la consolidación del Estado constitucional garantista, al fortalecer la protección de derechos y dotar de efectividad real a la Constitución. Sin embargo, su futuro dependerá de su capacidad para equilibrar el protagonismo judicial con la legitimidad democrática, cerrar la brecha entre norma y realidad y adaptarse a los desafíos del constitucionalismo digital y transnacional, para así mantener su vigencia como modelo transformador en el siglo XXI.

El neoconstitucionalismo ha transformado la manera en que concebimos el derecho, la Constitución y los derechos fundamentales. Su enfoque garantista y axiológico ha fortalecido la justicia constitucional y ha permitido que la Constitución adquiera eficacia real. No obstante, su éxito doctrinal y práctico plantea dilemas: ¿cómo equilibrar el protagonismo judicial con la

legitimidad democrática? ¿Cómo evitar que el derecho constitucionalizado se convierta en un sistema dependiente de la voluntad judicial?

Estas preguntas explican por qué el neoconstitucionalismo es, al mismo tiempo, un modelo de avance garantista y un laboratorio de tensiones democráticas. Su legado es innegable: ha sido el puente conceptual y normativo hacia el constitucionalismo plural y digital (que buscará responder a los retos de la sociedad global e interconectada del siglo XXI).

Comprender el neoconstitucionalismo exige situarlo en su contexto histórico y social, pues este modelo no nació de la abstracción doctrinal, sino de procesos concretos de reconstrucción institucional y evolución jurídica. La Europa de la posguerra (con sus nuevas constituciones cargadas de principios y mecanismos de control judicial) y la América Latina de finales del siglo XX (con sus transiciones democráticas y constituciones transformadoras) ofrecen el escenario donde este paradigma se consolidó.

En conclusión, el neoconstitucionalismo latinoamericano representa un punto de inflexión en la historia jurídica de la región, al convertir a la Constitución en un instrumento vivo de transformación social y al elevar la protección de los derechos fundamentales a un nivel de exigibilidad real. Su legado es ambivalente: por un lado, ha fortalecido la justicia constitucional, ampliado los espacios de garantía y consolidado un modelo garantista; por otro, ha expuesto tensiones estructurales relacionadas con la judicialización de la política, la discrecionalidad interpretativa y la brecha persistente entre norma y realidad social. Estas tensiones no demeritan sus avances (sino que subrayan la necesidad de un constitucionalismo capaz de equilibrar activismo judicial con legitimidad democrática) y de responder a los desafíos de un mundo globalizado y digital, donde la protección de los derechos ya no se limita al ámbito estatal. Así, el neoconstitucionalismo latinoamericano se erige como laboratorio de innovaciones jurídicas y democráticas, pero también como espacio de debate crítico, cuyo futuro dependerá de su capacidad de adaptación a las transformaciones sociales y tecnológicas del siglo XXI.

1.5.1. Neoconstitucionalismo en Colombia.

Siguiendo la línea ideológica de Comanducci (2022), y en el contexto del neoconstitucionalismo en América Latina, donde figuras como Miguel Carbonell (2007) se destacan como referentes prominentes, el neoconstitucionalismo ideológico no solo describe los avances del proceso de constitucionalización, sino que también los valora positivamente y

promueve su defensa y expansión. En la región, estas ideas encuentran aplicación directa en las constituciones, orientando la interpretación y práctica del Derecho. Comanducci (2022) señala además un consenso entre autores como Alexy, Dworkin y Zagrebelsky, quienes relacionan esta ideología con el positivismo jurídico ideológico: la obligación moral de obedecer la Constitución y las leyes que de ella emanan. Aunque el derecho positivo no establece valores morales de manera explícita, la Constitución y las leyes se conciben para perseguir fines justos, como el orden, la justicia y la paz, de modo que su cumplimiento formal ya implica la práctica de valores positivos. En los sistemas democráticos contemporáneos, el neoconstitucionalismo resalta la relación necesaria entre Derecho y moral, reafirmando la obligación ética de acatar la Constitución y las leyes conforme a ella, lo que lo aproxima a una versión moderna del positivismo ideológico del siglo XIX (García, 2010).

En relación con la influencia central del neoconstitucionalismo en Colombia, se destacan dos concepciones fundamentales y una de sus consecuencias jurisprudenciales más significativas: la interpretación sistemática de la Constitución y la interpretación extensiva de los derechos, lo que ha permitido la creación de derechos fundamentales a través de la jurisprudencia. Aunque las constituciones contemporáneas positivizaron numerosos derechos, la Corte Constitucional ha ampliado este catálogo incorporando derechos fundamentales innominados y estableciendo mecanismos judiciales para su protección directa (García, 2012).

Estas transformaciones reflejan la idea del Estado democrático de derecho de origen alemán, según la cual los derechos sociales y civiles deben integrarse de manera coherente. En Colombia, el capítulo constitucional sobre protección de derechos incluye una "cláusula de derechos innominados" (CP, 1991, art 94), que establece que la enumeración de derechos y garantías no excluye otros inherentes a la persona humana, aunque no estén expresamente reconocidos. Todo derecho constitucional orientado a garantizar la dignidad humana y traducible en derecho subjetivo se considera fundamental, dado que preservar la supremacía de la Constitución implica proteger la igualdad y dignidad de todas las personas (García, 2012).

Es por esto que se da una interpretación sistemática y extensiva de los derechos, la Corte ha identificado y creado derechos fundamentales en sentencias emblemáticas, consolidando su protección en líneas jurisprudenciales estables. Un ejemplo destacado es el derecho al mínimo vital, vinculado directamente con la dignidad humana. Esta doctrina, como señala Rodolfo Arango, representa uno de los aportes más importantes del constitucionalismo colombiano al desarrollo de los derechos fundamentales, especialmente en sociedades con desigualdades

estructurales y deficiencias en los mecanismos democráticos (Corte Constitucional, T-426, 1992)

En el caso colombiano, la Corte Constitucional se consolidó como un referente regional de activismo judicial, mediante decisiones que no solo resolvieron conflictos particulares, sino que también transformaron de manera estructural políticas públicas en áreas como desplazamiento forzado, salud, medio ambiente, derechos de las minorías y equidad de género. Este papel protagónico demostró que la Constitución no era un texto meramente simbólico, sino una herramienta viva para la promoción de la justicia social. En este contexto, el neoconstitucionalismo, al menos en su dimensión vinculada al Derecho Constitucional, se manifiesta cuestionando y modificando paradigmas jurídicos tanto tradicionales como contemporáneos. Este proceso de transformación se impulsa a través de decisiones judiciales y políticas que suelen calificarse como "progresistas" o "liberales" (Páez, 2012).

La interpretación sistemática de la Constitución permite articular el régimen económico con el Estado social de derecho, de manera que se cumpla la obligación de promover la igualdad real mediante la efectividad de los derechos sociales. La tradicional distinción entre derechos prestacionales y no prestacionales resulta insuficiente, ya que incluso las libertades básicas poseen una dimensión prestacional, según la jurisprudencia. Un derecho se considera prestacional cuando permite exigir a los poderes públicos (y en ciertos casos a particulares) una acción específica de dar o hacer, derivada de lo dispuesto en la Constitución. Lo fundamental es que la exigencia asociada al derecho esté orientada a garantizar el valor de igualdad que persigue; de lo contrario, si solo busca la abstención de los poderes públicos, no constituye un derecho constitucional prestacional (García, 2012).

Este activismo judicial garantista ha sido fundamental para llenar vacíos de protección en contextos donde el legislador o el ejecutivo no lograban garantizar eficazmente los derechos. La Corte Constitucional colombiana es, sin duda, uno de los ejemplos paradigmáticos de esta tendencia: sus sentencias estructurales han permitido corregir omisiones históricas del Estado, generando planes integrales de protección de derechos sociales y colectivos, y proyectando a la Constitución como instrumento de transformación real de la sociedad.

Ahora bien, el modelo neoconstitucional Colombiano (y latinoamericano) enfrenta desafíos significativos que ponen en tensión sus avances. En primer lugar, la judicialización excesiva de la política ha desplazado parte del debate democrático hacia los tribunales

(generando críticas sobre un eventual "gobierno de jueces" y la debilitación de los espacios deliberativos propios del parlamento). Este fenómeno, aunque permite respuestas eficaces frente a violaciones de derechos, también plantea riesgos para la legitimidad democrática (en tanto decisiones de alto impacto político y social quedan condicionadas a la interpretación judicial y no al consenso ciudadano).

En segundo lugar, la discrecionalidad judicial se ha incrementado debido al uso amplio de la ponderación y de la interpretación axiológica de los principios constitucionales. Si bien estas herramientas permiten respuestas flexibles ante conflictos complejos, su aplicación sin criterios metodológicos claros puede derivar en inseguridad jurídica y heterogeneidad en las decisiones (debilitando la previsibilidad del derecho).

Un tercer reto reside en la brecha entre constitucionalismo formal y realidad social. A pesar de contar con textos constitucionales avanzados, la eficacia material de los derechos se ve limitada por estructuras de desigualdad persistente, debilidad institucional y corrupción. Así, la Constitución garantista puede convertirse en una promesa incumplida si no se acompaña de políticas públicas efectivas, recursos económicos y fortalecimiento institucional.

1.5.2. Contexto histórico y transformaciones sociales

El constitucionalismo digital no surge como un fenómeno aislado ni repentino, sino como el resultado de un proceso histórico de convergencia entre transformaciones tecnológicas, sociales y jurídicas que han alterado radicalmente las condiciones tradicionales de ejercicio del poder y protección de los derechos fundamentales. La arquitectura sobre la que se construyó el constitucionalismo clásico y luego el neoconstitucionalismo se fundaba en un Estado-nación territorial, en la soberanía territorial y en una estructura jurídica vertical que delimitaba con claridad las relaciones entre poder público y ciudadanía. El constitucionalismo, en su origen, fue un proyecto político y normativo diseñado para limitar el poder del Estado, garantizar la separación de funciones y asegurar la supremacía de la ley como expresión de la voluntad general.

Sin embargo, el tránsito hacia la sociedad digital del siglo XXI transformó profundamente este modelo. El desarrollo de internet, la globalización económica y la revolución de los datos desplazaron el eje del poder desde el Estado hacia actores transnacionales y tecnológicos, capaces de influir en la esfera pública y en la vida privada de los individuos sin mediar estructuras estatales. En palabras de Manuel Castells (2001), vivimos

en una “sociedad red”, donde el poder se ejerce mediante el control de la información y la capacidad de conexión, más que por la coerción física o el control territorial. Esta nueva topología del poder diluye las fronteras tradicionales del constitucionalismo y exige una expansión de sus principios hacia ámbitos no estatales y extraterritoriales.

Desde finales del siglo XX, las tecnologías de la información y la comunicación (TIC) iniciaron un proceso de desmaterialización de la economía, la política y la cultura, modificando las bases mismas de la soberanía. Fenómenos como la globalización financiera, las redes sociales, la inteligencia artificial (IA) y la minería de datos consolidaron un nuevo espacio público digital, en el que las interacciones humanas se rigen por lógicas algorítmicas y plataformas privadas que establecen sus propias reglas. Este contexto ha dado lugar a lo que Shoshana Zuboff (2019) denomina “capitalismo de la vigilancia”, un régimen en el que los datos personales se convierten en recursos económicos y en herramientas de poder capaces de moldear comportamientos sociales y decisiones políticas.

La expansión de este poder informacional y tecnológico ha generado una crisis en las categorías clásicas del derecho constitucional. Conceptos como “autoridad pública”, “jurisdicción territorial” o “sujeto de derecho” adquieren nuevos significados en un entorno donde las normas son reemplazadas por algoritmos, las fronteras se difuminan y las decisiones que afectan derechos fundamentales se toman desde centros de poder privados. En este sentido, De Gregorio (2020) sostiene que la digitalización “ha desestabilizado el equilibrio original del constitucionalismo moderno”, al crear una estructura de poder descentralizada que escapa a los controles democráticos tradicionales.

El constitucionalismo digital, por tanto, emerge como una respuesta garantista ante esta mutación estructural del poder. Su finalidad no es solo adaptar las constituciones a las nuevas tecnologías, sino reafirmar la centralidad de los derechos humanos en un entorno donde las reglas del juego son definidas por corporaciones globales. Como subraya Oreste Pollicino (2021), el constitucionalismo digital implica “la reconstrucción del pacto constitucional en el espacio digital”, un esfuerzo por trasladar los principios de dignidad, igualdad y libertad al ciberespacio, donde los ciudadanos también deben ser reconocidos como titulares de derechos y no meros consumidores o usuarios.

Históricamente, este proceso puede entenderse como una tercera gran fase del constitucionalismo moderno. La primera, el constitucionalismo clásico de los siglos XVIII y

XIX, estableció la supremacía de la ley y los límites al poder absoluto. La segunda, el neoconstitucionalismo del siglo XX, introdujo la fuerza normativa de la Constitución y la centralidad de los derechos fundamentales frente al Estado. Finalmente, el constitucionalismo digital del siglo XXI expande esa lógica hacia las estructuras globales y privadas del poder tecnológico, proponiendo un marco de regulación que combine la protección de derechos, la transparencia algorítmica y la responsabilidad digital.

Este cambio también está marcado por la transformación del sujeto constitucional. En el modelo clásico, el ciudadano era un individuo territorialmente vinculado a un Estado; en el paradigma digital, el sujeto constitucional se redefine como ciudadano digital global, cuyas interacciones, identidades y derechos se despliegan en múltiples espacios virtuales. Floridi (2022) describe esta transición como el paso hacia una "infosfera", donde las personas existen simultáneamente en entornos físicos y digitales, y donde la protección de la privacidad, la identidad y la autonomía requieren nuevas formas de constitucionalismo adaptadas a la vida en red.

A esta evolución se suman nuevas formas de participación política y deliberación pública. Las redes sociales, los movimientos digitales y las plataformas de comunicación han transformado el ejercicio de la ciudadanía, permitiendo la emergencia de una "democracia conectiva" (Bennett & Segerberg, 2013) en la que la acción colectiva se organiza sin mediaciones institucionales. No obstante, esta apertura también ha traído consigo fenómenos de desinformación, manipulación algorítmica y polarización social, que ponen a prueba la capacidad del derecho constitucional para garantizar la veracidad, la igualdad en el debate público y la protección frente a la injerencia digital.

En este escenario, el constitucionalismo digital debe responder a una doble tensión: por un lado, preservar los principios de libertad y pluralismo propios de la democracia constitucional, y por otro, establecer límites normativos al uso de tecnologías que amenazan esos mismos valores. El reto, como advierte Jack Balkin (2018), consiste en "reformular el constitucionalismo como una arquitectura de libertad en un entorno controlado por arquitectos privados". De ahí que el debate actual se centre en la creación de marcos constitucionales globales, como la Carta de Derechos Digitales de la Unión Europea (2021) o los Principios de Gobernanza de Internet de la ONU, que permitan articular la ética tecnológica con los valores universales del derecho constitucional.

En suma, el contexto histórico del constitucionalismo digital evidencia una transición desde un modelo tradicional, centrado en la soberanía estatal, hacia un constitucionalismo de redes caracterizado por la interacción compleja entre actores públicos y privados en entornos transnacionales. La legitimidad del orden jurídico, en este nuevo escenario, se vincula estrechamente con su capacidad para orientar, regular y dotar de sentido humanista a los procesos tecnológicos que estructuran la vida social contemporánea. No se trata de una sustitución del paradigma garantista, sino de su proyección y adaptación: los derechos fundamentales solo pueden preservarse de manera plena si se extienden y aplican eficazmente al espacio digital, donde se disputan hoy ámbitos decisivos de la libertad, la privacidad y la igualdad.

Como anticipo a los capítulos siguientes, conviene advertir que esta evolución del constitucionalismo no puede comprenderse cabalmente sin considerar la creciente concentración de poder en manos de empresas privadas y corporaciones transnacionales, cuya capacidad de influir en la arquitectura normativa de lo digital resulta determinante. Las condiciones de su surgimiento, la naturaleza de este poder y las implicaciones que proyecta sobre la teoría y la práctica constitucional serán examinadas con mayor detalle en los subcapítulos posteriores, donde se analizarán las dinámicas, tensiones y desafíos que este fenómeno plantea para la configuración del constitucionalismo digital en el siglo XXI.

TÍTULO II: EL FENOMENO DE DIGITALIZACIÓN Y EL LA EVOLUCIÓN DE LA QUINTA REVOLUCIÓN INDUSTRIAL.

En el capítulo anterior se destacó la importancia de revisar el desarrollo histórico del constitucionalismo para comprender sus manifestaciones contemporáneas. Esta perspectiva resulta indispensable para abordar el llamado constitucionalismo digital, un modelo que emerge como resultado del proceso de digitalización característico de la quinta revolución industrial. En consecuencia, solo entendiendo la trayectoria histórica del pensamiento constitucional es posible situar adecuadamente este nuevo paradigma.

2. Historia de las revoluciones industriales.

A lo largo del tiempo, la tecnología ha actuado como uno de los motores más influyentes del cambio social y jurídico. Cada innovación ha transformado la forma en que las sociedades producen, se comunican y se organizan políticamente; por ello, ha generado nuevos desafíos para el derecho y, en particular, para el constitucionalismo. Como consecuencia de estas transformaciones, la transición hacia un marco constitucional adaptado a la era digital no puede analizarse sin considerar la profunda incidencia de la tecnología en la formación de los Estados modernos, en la distribución del poder y en la evolución de los derechos humanos. La tecnología, en efecto, no debe verse como un simple instrumento, sino como un componente estructural de los procesos de modernización jurídica.

La humanidad ha atravesado diversas etapas de desarrollo industrial, cada una marcada por innovaciones que han alterado la vida cotidiana y los sistemas de producción. Estos cambios, desde la mecanización hasta la automatización avanzada, han producido repercusiones sociales, económicas y políticas de gran magnitud; como resultado, las instituciones y las normas han debido adaptarse continuamente. El estudio de las revoluciones industriales permite comprender el origen del capitalismo y la globalización, y, en consecuencia, ilumina los antecedentes que dieron paso a la sociedad digital contemporánea. Este recorrido histórico ofrece, por tanto, el marco adecuado para justificar la necesidad de un nuevo paradigma jurídico: el constitucionalismo digital.En la época actual, la sociedad ha experimentado un cambio constante, lo que ha llevado a que la industrialización esté en constante cambio desde la Edad Media, cuando se implementó la teoría del capitalismo y se comenzó a utilizar maquinaria, dando origen al capital, los empresarios y, posteriormente, a la segunda revolución industrial con la integración de nuevas tecnologías (Fernández, 2012).

Por otra parte, las guerras mundiales han contribuido a transformaciones extraordinarias, como la invención de nuevas máquinas, la tecnificación de las empresas manufactureras y el uso de energía hidráulica y eólica para la molienda de granos y aserraderos, entre otros avances. En el ámbito del transporte y su infraestructura, se han dado importantes progresos en la construcción y las instalaciones portuarias. Los navíos y el material rodante para el transporte terrestre han evolucionado desde el uso de animales hasta vehículos automotores y trenes, entre otros (Ferrer, 2022).

Como resumen, con el paso del tiempo, las sociedades han atravesado diversos cambios impulsados por el desarrollo científico y tecnológico, que abarcan desde el dominio del fuego, la práctica agrícola, el trabajo con metales y la navegación, hasta el progreso de la máquina de vapor, la electricidad, la química y la energía nuclear, incluyendo también la electrónica, el desarrollo espacial, la informática, las telecomunicaciones, la biogenética y la creación de nuevos materiales (Ordóñez, 2007). Estos inventos e innovaciones han sido claves en las diferentes etapas de las revoluciones industriales, dejando una huella significativa en la historia de la humanidad. La primera revolución industrial se distinguió por la mecanización de los procesos laborales, mientras que la segunda se definió por la introducción de la automatización, y en la tercera revolución industrial, la robotización emergió como un elemento distintivo.

En la tercera revolución industrial, la investigación científica y tecnológica se sitúa como una prioridad en los procesos de innovación, lo que implica que la ciencia guía el progreso y constituye el fundamento de la evolución humana. Por ejemplo, el avance hacia la integración internacional de los mercados financieros fue posible gracias a los avances tecnológicos en el manejo de la información (Richta, 1970). Por otro lado, la influencia de la tecnología en la economía conlleva cambios en áreas principales como: la economía informacional, la economía de redes y la economía globalizada (Castells, 1999).

Adicionalmente, la cuarta revolución industrial ha impulsado la expansión de tecnologías emergentes que están transformando profundamente la vida social, económica y jurídica. La digitalización, entendida como la conversión de información analógica en datos procesables digitalmente, ha permitido crear, almacenar y transmitir información con una eficiencia sin precedentes. En este escenario, herramientas como la inteligencia artificial (IA), la tokenización, la tecnología blockchain, el Big Data y el metaverso se han consolidado como elementos centrales del proceso de transformación digital. Asimismo, el transhumanismo ha

promovido la búsqueda de mejoras tecnológicas en las capacidades humanas, abriendo interrogantes éticos y jurídicos de gran envergadura (Balaguer Callejón et al., 2023).

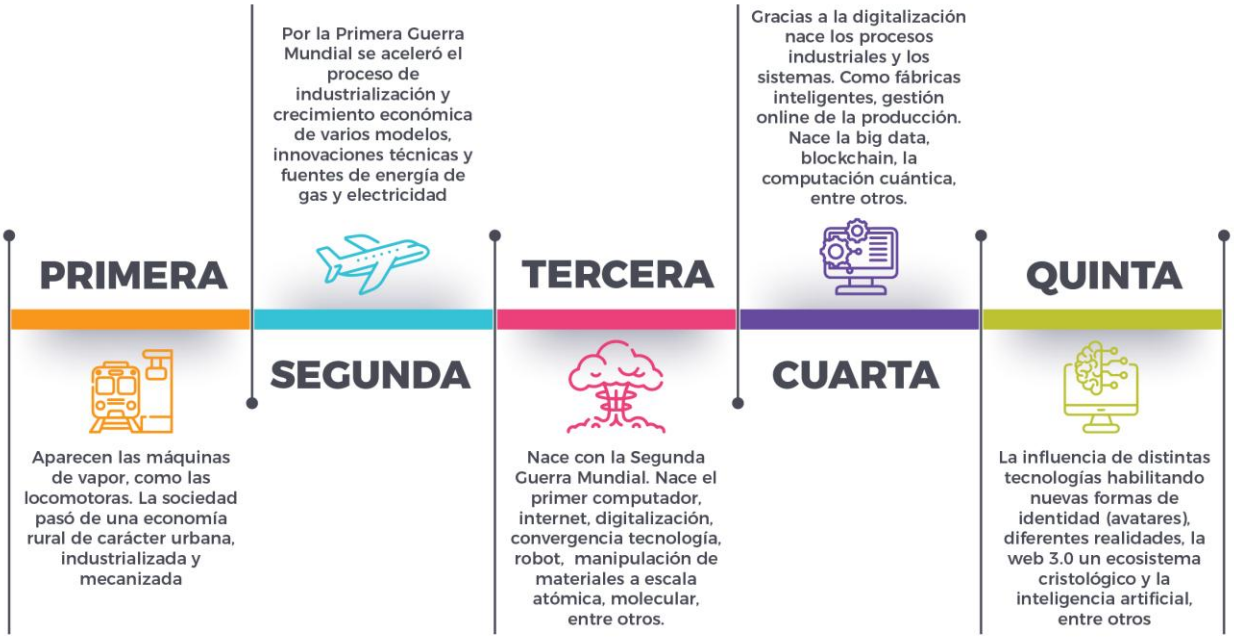
A estos avances se suma la aparición de nuevos actores globales cuya influencia excede las fronteras estatales. Las grandes corporaciones tecnológicas (particularmente las Big Tech o GAFAM) han adquirido un poder económico, informacional y normativo capaz de incidir directamente en la vida pública y privada de millones de personas. Como consecuencia, su presencia reconfigura profundamente la noción clásica de constitucionalismo, que históricamente se había construido sobre la relación entre el Estado y sus ciudadanos. Ahora, estos actores privados participan activamente en la creación de reglas, en la gestión de derechos y en la organización de espacios de interacción digital, lo que obliga a repensar los límites y los sujetos del poder constitucional (Newman y Ángel, 2020).

Con lo anterior, **s**e puede evidenciar que las diferentes revoluciones industriales han variado por circunstancias de la sociedad y en las últimas tres revoluciones han variado de una manera significativa en el que se busca con el uso del internet, los computadores buscan lograr la autonomía de los sistemas a través de la inteligencia artificial como los seres humanos.

A lo largo de la historia, las revoluciones industriales han transformado profundamente la organización social, económica y jurídica de la humanidad. Si bien cada etapa ha estado marcada por innovaciones técnicas, desde la mecanización de la primera revolución industrial hasta la robotización y digitalización de la cuarta, estos avances no han sido neutrales: han generado desigualdades sociales, concentraciones de poder económico y nuevos retos regulatorios para los Estados (Fernández, 2012; Ferrer, 2022; Ordóñez, 2007). La tercera y cuarta revolución industrial evidenciaron que la tecnología no solo impulsa la economía globalizada, sino que también redefine la relación entre los individuos y sus derechos, en especial frente a la automatización, la economía de datos y la interconexión digital (Castells, 1999). Esta evolución histórica demuestra que cada salto tecnológico ha exigido respuestas jurídicas y normativas, y que la actual transición hacia la quinta revolución industrial no es solo un fenómeno técnico, sino un desafío para los marcos constitucionales contemporáneos, que deben adaptarse para garantizar la protección efectiva de los derechos fundamentales en un entorno cada vez más digitalizado.

Figura 1.

Línea de tiempo sobre la evolución industrial



Nota. Elaboración propia (2024).

2.1. Primera Revolución Industrial

Durante el período de la Revolución Industrial británica (1760-1840), se produjeron una serie de avances técnicos significativos, como la invención de las máquinas de vapor. Estos avances transformaron las prácticas laborales, lo que a su vez generó cambios sociales de gran envergadura. Hubo un aumento Notable en la participación laboral de mujeres y niños, que por primera vez en la historia, la población urbana supera a la población rural. Esto se tradujo en matrimonios más tempranos, mayor fertilidad y una mejora en la vida de la población. Sin embargo, la mano de obra se volvió menos especializada y muchos entornos laborales se tornaron insalubres y peligrosos. Las ciudades enfrentaron desafíos como la contaminación, malas condiciones de salubridad y un aumento en la delincuencia (World History Publishing , 2024).

La urbanización no eliminó por completo el sentido de comunidad, ya que se formaron lazos comunitarios en torno a actividades como bandas de fábrica o mina. Sin embargo, la vida en las ciudades, especialmente cerca de las fábricas y minas, se volvió más congestionada y con condiciones de vida precarias. La falta de saneamiento adecuado condujo a la propagación de enfermedades, y las epidemias fueron comunes. Además, la urbanización contribuyó al

aumento de delitos menores, ya que el anonimato en las ciudades ofrecía cierta impunidad a los delincuentes (Coleman, 1992). Ahora bien, desde otras disciplinas algunos estudiosos expresaron sobre esta época como es el economista francés Blanqui (1842), fue uno de los primeros en emplear el término "revolución industrial" en el contexto de los cambios tecnológicos de su época. Se centró particularmente en los efectos sociales provocados de las innovaciones técnicas del siglo XVII, que, según él, habían provocado una "revolución industrial" en Inglaterra, (Blanqui, 1842).

Posteriormente, Friedrich Engels (1820-1895), filósofo alemán y cofundador del materialismo dialéctico y el comunismo moderno junto a Karl Marx, usó extensamente este término en su obra "Sobre las condiciones de la clase obrera en Inglaterra" (1845). Engels, basándose en su estancia en Manchester y en un detallado estudio social y demográfico, describió los duros estilos de vida de los obreros y los bajos salarios, destacando que ambas situaciones habían disminuido en comparación con las de los trabajadores agrícolas y ganaderos de la época. Para Engels, la Revolución Industrial se definía por la combinación de innovaciones en el sector textil y la introducción de la máquina de vapor. La obra de Engels no fue traducida al inglés hasta finales del siglo XIX. Fue el historiador económico Arnold Toynbee (1852-1883) quien popularizó el término en Inglaterra a través de una serie de conferencias en 1881, publicadas póstumamente. No se sabe si Toynbee conocía el trabajo de Engels, y ciertamente no compartía su perspectiva marxista. Sin embargo, es Notable que ambos autores subrayaron secuelas devastadoras y lamentables de la Revolución Industrial para la mayoría de la población británica, llegando a asociar la Revolución Industrial con una catástrofe social (Aibar, 2019).

La Revolución Industrial no solo transformó los medios de producción, sino también las formas de pensamiento y la relación del ser humano con la naturaleza. Este proceso trajo consigo una nueva concepción del tiempo y del trabajo, donde la jornada laboral pasó a ser regulada por la maquinaria y no por los ritmos naturales. Las fábricas impusieron una disciplina estricta, controlando cada minuto de la vida de los obreros. De esta manera, el tiempo dejó de ser una experiencia subjetiva vinculada a los ciclos del día para convertirse en una medida de productividad, lo que significó una profunda transformación cultural.

La mecanización también alteró el paisaje rural, ya que muchas personas abandonaron el campo en busca de empleo en las ciudades. Este fenómeno dio origen a una migración

masiva que transformó la estructura demográfica de Europa. Los pueblos se vaciaron, y las metrópolis industriales crecieron de manera vertiginosa, generando cinturones de pobreza en los suburbios. La concentración de personas en espacios reducidos provocó la proliferación de enfermedades respiratorias y gastrointestinales, lo que derivó en una crisis sanitaria generalizada. Sin embargo, también fue en este contexto donde surgieron los primeros intentos de organización pública en torno a la salud y la educación, impulsados por la necesidad de mantener una fuerza laboral más sana y productiva.

Las ciudades se convirtieron en centros de pobreza, con muchos dependiendo de la caridad de los más afortunados para sobrevivir. Los niños, especialmente, se vieron afectados, con muchos trabajando largas horas en condiciones peligrosas por salarios mínimos. Aunque la urbanización ofrecía a las mujeres más oportunidades laborales y cierta independencia económica, también las exponía a trabajos arduos y mal remunerados. A pesar de los desafíos, la urbanización continuó en ascenso, y para 1880, solo una minoría de la población británica vivía en zonas rurales (Allen, 2009).

De manera paralela, el desarrollo de nuevas tecnologías industriales impulsó la creación de una economía capitalista moderna. El sistema fabril exigía grandes inversiones en maquinaria y materias primas, lo que llevó a la consolidación de la burguesía como clase dominante. Las fábricas se convirtieron en los nuevos templos del progreso, y el trabajo asalariado reemplazó progresivamente al artesanal. Este cambio no solo modificó la estructura económica, sino que redefinió las relaciones sociales y la percepción de la riqueza. La acumulación de capital se erigió como el nuevo ideal de éxito, desplazando los valores tradicionales del trabajo comunitario y artesanal.

En el ámbito laboral, los hombres encontraron nuevas oportunidades en industrias como la minería y la construcción, pero muchos trabajos eran no especializados y se enfrentaban a condiciones laborales peligrosas. Aunque se formaron sindicatos para proteger los derechos de los trabajadores, enfrentaron una fuerte oposición y no incluían a mujeres ni niños (Hobsbawm, 1968). No obstante, este surgimiento nace del dominio de la burguesía, propietaria de los medios de producción y explotadora de la fuerza laboral (obreros industriales y campesinos empobrecidos), impulsó el nacimiento del sindicalismo, el socialismo, el anarquismo y el comunismo (Marx, 1848).

En el plano político, la Revolución Industrial propició un debate sobre los derechos del trabajador y la función del Estado frente al capital. Las ideas de igualdad y justicia social comenzaron a resonar en los movimientos obreros y filosóficos de la época. La precarización

de la clase trabajadora condujo a la formulación de leyes laborales básicas y al cuestionamiento de las prácticas de explotación infantil y femenina. En este contexto, se gestó una nueva conciencia social que más adelante inspiraría las reformas del siglo XX y los principios del constitucionalismo social moderno.

En términos sociales, la Revolución Industrial amplió la brecha entre las clases sociales. Los ricos se enriquecieron aún más, invirtiendo en empresas y capital, mientras que los obreros peleaban por mejorar las condiciones en sus lugares de trabajo. Aunque surgió una clase media urbana, las oportunidades para ascender socialmente eran limitadas para la mayoría. La educación estaba disponible, pero muchos niños trabajaban a tiempo completo en lugar de asistir a la escuela. A pesar de los avances económicos, la desigualdad social y las condiciones de vida precarias persistieron para muchos durante este período de cambio tumultuoso.

Finalmente, la Primera Revolución Industrial puede considerarse el punto de partida de la modernidad tecnológica. Sentó las bases del capitalismo industrial, transformó las estructuras sociales y consolidó la noción de progreso como motor de la historia. Sin embargo, este progreso tuvo un costo humano y ambiental considerable. El uso intensivo del carbón y la contaminación de los ríos marcaron el inicio de la crisis ecológica moderna. Así, este periodo no solo representa un salto económico, sino también un cambio civilizatorio que reconfiguró la manera en que los seres humanos se relacionan con el trabajo, el tiempo y la naturaleza.

Otro de los inventos más significativos en la primera Revolución Industrial incluye la máquina de vapor, los trenes, el bombillo y la máquina de hilar. Es entonces que la máquina de vapor, desarrollada por James Watt en 1768, transformó el calor del carbón en energía mecánica, propiciando la creación de trenes, barcos a vapor y otros mecanismos más eficientes. Los trenes, como símbolo esencial de esta eran, revolucionaron el transporte al reducir drásticamente los tiempos de traslado y conectar regiones distantes. La invención del bombillo a principios del siglo XIX llevó la electricidad a los hogares europeos, reemplazando las luces de gas y combustible y permitiendo una mayor flexibilidad en las horas de trabajo y vida (Mokyr, 1990). Por último, la máquina de hilar aumentó la producción de hilos, crucial para la industria textil en expansión, al permitir un hilado más eficiente en comparación con los manuales tradicionales. Estos avances marcaron un punto de inflexión en la producción y el desarrollo industrial, transformando profundamente la sociedad y la economía de la época (Landes, 1969).

2.2.Segunda Revolución Industrial

La Segunda Revolución Industrial, que tuvo lugar principalmente en el último tercio del siglo XIX, marcó un hito crucial en la historia económica y social del mundo. Esta fase de industrialización estuvo caracterizada debido a una serie de avances tecnológicos y transformaciones estructurales que modificaron radicalmente la elaboración y distribución de bienes (Reche, 2019).

Uno de los aspectos más destacados de la Segunda Revolución Industrial fue el avance en la aplicación de la energía eléctrica y la creación de nuevas fuentes energéticas, como el gas natural y el petróleo. Estas innovaciones permitieron la creación de industrias más eficientes y la expansión de la producción en áreas antes inaccesibles. Además, la optimización de procesos de fabricación y transporte aumentó la productividad y redujo los costos, facilitando la producción a gran escala (AMG Metalmecánica Gallega , 2024).

Otro aspecto crucial de esta revolución fue el desarrollo de nuevas tecnologías, como la maquinaria pesada, los motores de combustión interna y los avances en la industria química. Estas innovaciones transformaron sectores clave de la economía, como la minería, la agricultura y la producción de bienes de consumo (Friedman, 1995).

La Segunda Revolución Industrial también tuvo un profundo impacto en las relaciones laboras y la organización del trabajo. La introducción de nuevas formas de producción, como la línea de ensamblaje, aumentó la demanda de mano de obra y cambió las condiciones de trabajo en las fábricas. Además, el desarrollo del transporte ferroviario y marítimo facilitó el movimiento de trabajadores hacia las áreas industriales, creando nuevas comunidades urbanas y cambiando la estructura social de muchas sociedades (Dominguez, 2023). Sin embargo, uno de los factores más controvertidos de la Segunda Revolución Industrial fue su relación con el imperialismo capitalista. El crecimiento económico impulsado por la industrialización llevó a una intensificación de la competencia entre las potencias industriales por el control de recursos naturales y mercados en todo el mundo. Esto se tradujo en la expansión de los imperios coloniales y la explotación de colonias y países dependientes para garantizar el suministro de materias primas y la apertura de nuevos mercados para los productos manufacturados (Palomo Garrido, 2024).

En cuanto a los cambios demográficos, Estados Unidos experimentó un Notable crecimiento poblacional durante el período mencionado. Por ejemplo, entre 1820 y 1870, su población pasó de 9 millones a 40 millones, y luego, para el año 1900, se aproximó a los 80 millones. Por otro lado, en Europa a principios del siglo XX, la densidad de población era

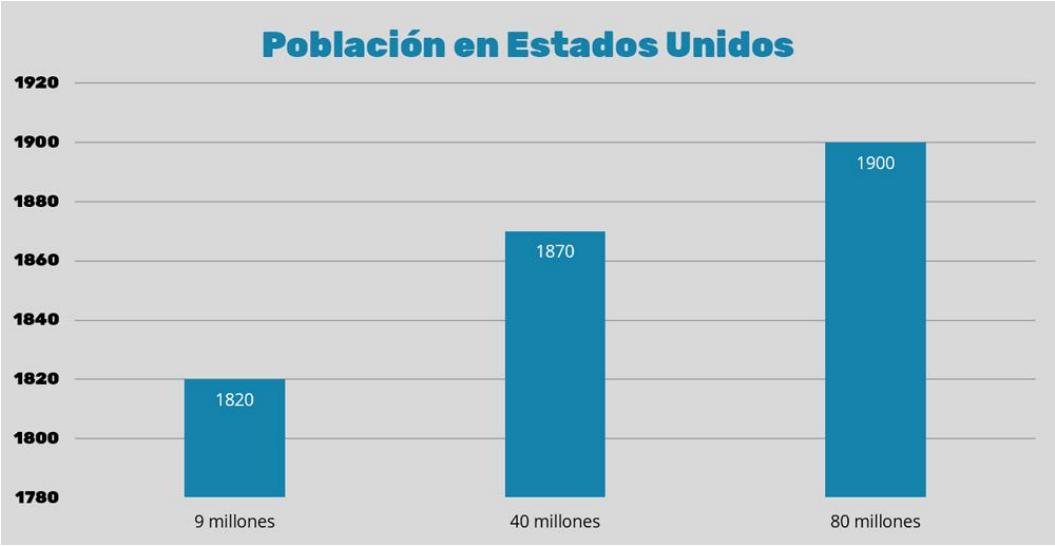
significativamente mayor que en otras regiones, con alrededor de cuarenta habitantes por kilómetro cuadrado, mientras que en Asia esta cifra era la mitad, y en África y América apenas alcanzaba los cuatro habitantes por kilómetro cuadrado (Alcañiz, 2008).

Asimismo, se produjeron considerables movimientos migratorios. A finales del siglo XIX, en las últimas décadas, aproximadamente cinco millones de europeos emigraron principalmente hacia destinos como Estados Unidos, Australia y Nueva Zelanda. De estos, el 60 % tenía origen en Gran Bretaña e Irlanda, mientras que cerca del 30 % procedía de Alemania. Aunque en ciertos países se registraba un crecimiento industrial, este no era suficiente para absorber a la población al ritmo necesario, debido al elevado número de trabajadores desplazados, especialmente agricultores y artesanos, provenientes de lugares con menor productividad.

La segunda revolución industrial fomentó el avance económico y material en Europa occidental y Estados Unidos. El uso del petróleo, junto con la creación del motor de combustión interna, facilitó el comercio de bienes entre las principales potencias industriales, así como con los nuevos territorios colonizados. Al mismo tiempo, los avances en ciencia y tecnología ocurrieron simultáneamente, lo que profundizó tanto los intercambios internacionales en términos económicos como culturales.

Figura 2.

Movimientos migratorios a Estados Unidos



Nota: Adaptado de: Herrera Lima, Fernando F. (2012). La migración a Estados Unidos: una visión del primer decenio del siglo XXI. *Norteamérica, 7*(2), 171-197. Recuperado en 04

de diciembre de 2025, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35502012000200006&lng=es&tlng=es.

Durante el período de transición entre los siglos XIX y XX, tanto el Estado como las instituciones financieras desempeñaron roles significativos como factores clave en el avance de la industrialización. Los Estados que surgieron en este período comenzaron a adoptar una forma incipiente de Estado benefactor, que empezó a prestar atención a cuestiones como la salud y la educación, los precursores de lo que posteriormente se denominaría seguridad social (Flores, 2020).

Además de los empresarios capitalistas, el Estado liberal desempeñó un papel destacado en estas transformaciones en Europa y otras regiones. Los Estados fomentaron la implementación de sistemas de pesos y medidas estandarizados, así como la regulación de las relaciones comerciales, mediante la implementación de nuevos códigos comerciales, como el establecimiento de sociedades anónimas (De Vroey, 2009). Adicionalmente, las considerables necesidades de financiación impulsaron la expansión y profundización de los mercados de valores, donde se negociaban las acciones y obligaciones de estas sociedades anónimas. Asimismo, se promovieron las exportaciones y se adoptaron políticas comerciales basadas en aranceles para proteger las actividades industriales de la competencia de naciones más avanzadas, como Inglaterra, Francia, Alemania y Estados Unidos.

De forma integrada, la evolución en los aspectos económicos, tecnológica, cognitiva, social y política. definió la situación global. Todo esto facilitó la integración de los mercados continentales y transoceánicos, la división internacional del trabajo y la convergencia económica entre los principales países. Este proceso aumentó el poder económico de Alemania y Estados Unidos, lo que condujo a una disputa por la hegemonía territorial y del mercado. En conclusión, la Segunda Revolución Industrial fue lapso de transformación sin precedentes a lo largo de la historia de la economía global. Si bien trajo consigo importantes progresos tecnológicos que han llevado a un aumento en la calidad de vida de numerosas personas, también estuvo marcada por desafíos y conflictos, incluida la exacerbación de la desigualdad económica y el surgimiento del imperialismo capitalista.

En este contexto, surgieron nuevas formas de organización empresarial que consolidaron la economía capitalista moderna. Las grandes corporaciones, conocidas como trusts y monopolios, comenzaron a dominar sectores estratégicos como el acero, la energía y el transporte. Empresas como Standard Oil o General Electric se convirtieron en símbolos del poder industrial y financiero del siglo XX, impulsando la concentración del capital y generando

profundas transformaciones en la dinámica del mercado global. Este proceso marcó el paso del capitalismo competitivo al capitalismo monopolista, donde la libre competencia fue reemplazada por el control y la planificación económica de las grandes industrias.

Del mismo modo, la Segunda Revolución Industrial modificó la estructura social, dando origen a una nueva clase obrera más consciente de sus derechos y de su papel en la producción. El surgimiento de movimientos sindicales organizados, partidos socialistas y asociaciones cooperativas permitió la articulación de luchas colectivas por mejores condiciones laborales, reducción de la jornada de trabajo y reconocimiento de la dignidad del trabajador. Estas conquistas sociales se convirtieron en la base del constitucionalismo social de inicios del siglo XX, que incorporó los derechos laborales dentro del marco legal de los Estados modernos.

En el ámbito cultural, la expansión industrial y el desarrollo de las comunicaciones dieron paso a una nueva mentalidad marcada por la fe en el progreso científico y técnico. El desarrollo de la electricidad, el teléfono y el telégrafo conectó regiones antes aisladas, promoviendo una sensación de modernidad y globalización incipiente. Sin embargo, este mismo proceso intensificó la alienación social, pues el trabajo mecanizado redujo la creatividad individual y transformó al obrero en un simple engranaje del sistema productivo. Así, el progreso técnico convivió con la deshumanización del trabajo y la creciente distancia entre capital y trabajo.

Por otra parte, la carrera industrial alimentó rivalidades imperialistas entre las potencias europeas. La búsqueda de materias primas y nuevos mercados de consumo impulsó la colonización de África y Asia, configurando un mapa geopolítico desigual que consolidó la dependencia económica de los territorios colonizados. Este fenómeno sentó las bases de las tensiones internacionales que desembocarían en la Primera Guerra Mundial, demostrando que el avance tecnológico y la expansión industrial no necesariamente traen consigo estabilidad o justicia global.

Finalmente, puede afirmarse que la Segunda Revolución Industrial representó una síntesis entre el poder de la técnica y la consolidación del capitalismo como sistema hegemónico. La incorporación de la ciencia a la producción, la planificación estatal y la internacionalización del comercio sentaron las bases del mundo contemporáneo. No obstante, las contradicciones sociales y económicas derivadas de este proceso revelaron los límites del progreso sin equidad, anticipando los debates éticos y jurídicos que marcarían el siglo XX y que aún hoy continúan vigentes en la era digital

2.3.Tercera Revolución Industrial

La Tercera Revolución Industrial no solo impulsó una ruptura significativa con la forma tradicional en que se interactúa con la tecnología, sino que también cambiaron de manera fundamental la organización de la economía a nivel mundial y la estructura social en su totalidad.

En primer lugar, la digitalización y la conectividad global facilitaron el surgimiento de nuevos enfoques empresariales y el establecimiento de economías fundamentadas en la información. Empresas como Amazon, Google y Facebook surgieron como gigantes de la industria, aprovechando al máximo las oportunidades que ofrecía Internet para el comercio electrónico, la publicidad digital y las redes sociales (Banco de Desarrollo de América Latina, 2021). Además, la automatización de procesos industriales y la integración de sistemas inteligentes en la producción no solo aumentaron la eficiencia y la productividad, sino que también plantearon desafíos significativos en términos de empleo y distribución de la riqueza. La robotización de la manufactura y la logística, por ejemplo, provocó una disminución en la necesidad de trabajo en algunos sectores, mientras que la demanda de habilidades técnicas y digitales aumentaba en otros (Dominguez, 2023).

En materia energética, el interés por alternativas renovables a los combustibles fósiles ha cobrado relevancia convirtiéndose en una prioridad urgente. El desarrollo de tecnologías solares, eólicas, hidroeléctricas y de biomasa no solo ofreció una respuesta al problema del cambio climático y la contaminación ambiental, sino que también abrió nuevas oportunidades de inversión y desarrollo económico en el sector de las energías renovables (Estenssorio, 2011). Por último, la Tercera Revolución Industrial también planteó importantes desafíos éticos y sociales relacionados con la privacidad de los datos, la desigualdad digital, el impacto ambiental de la tecnología y la diferencia entre países desarrollados y en proceso de desarrollo en referencia al acceso a la tecnología y los recursos digitales.

Es entonces que la Tercera Revolución Industrial transformó radicalmente no solo la interacción con la tecnología, sino también la estructura económica y social global. Este cambio se manifestó en la creación de economías basadas en la información y en la emergencia de nuevos modelos de negocio, liderados por gigantes como Amazon, Google y Facebook. La automatización y digitalización incrementaron la eficiencia, pero también provocaron desafíos en el empleo y la distribución de la riqueza. Además, la transición hacia energías sostenibles se convirtió en un imperativo, abriendo nuevas oportunidades de inversión, mientras que surgieron preocupaciones éticas y sociales relacionadas con la privacidad, la desigualdad

digital y el impacto ambiental. En conjunto, estos cambios redefinieron el panorama económico y social del siglo XXI.

Uno de los elementos centrales de la Tercera Revolución Industrial fue la consolidación de la informática como infraestructura esencial para casi todas las actividades humanas. La aparición del microprocesador en la década de 1970 permitió la miniaturización de los sistemas computacionales y democratizó el acceso a herramientas que antes eran exclusivas de laboratorios o grandes corporaciones. Este avance inauguró una nueva manera de procesar, almacenar y distribuir la información, dando origen a los primeros computadores personales, que se convirtieron en instrumentos transformadores en la educación, la ciencia, la administración pública y los hogares. La posibilidad de realizar cálculos complejos, organizar grandes bases de datos y comunicarse mediante redes electrónicas preparó el terreno para el ecosistema digital contemporáneo.

Asimismo, la convergencia entre informática y telecomunicaciones dio lugar a la expansión acelerada de Internet a partir de los años noventa. La creación de protocolos estandarizados y la infraestructura de fibra óptica permitieron conexiones más rápidas y estables, facilitando la interconexión global de individuos, instituciones y mercados. Esta conectividad produjo una ruptura radical con la lógica industrial anterior, que dependía de la centralización de la producción y la distribución física. Con la digitalización, los bienes intangibles, como software, contenido audiovisual, datos y servicios, comenzaron a dominar la economía, generando nuevas cadenas de valor en sectores antes inexistentes. Internet se convirtió en un recurso estratégico, comparable en importancia histórica a la invención de la imprenta o la llegada de la electricidad.

En este contexto surgió también una transformación profunda en los sistemas educativos y en la producción de conocimiento. Las universidades y centros de investigación adoptaron modelos de enseñanza y aprendizaje asistidos por plataformas digitales, lo que permitió la difusión global del conocimiento científico. La digitalización de las bibliotecas, la creación de repositorios de acceso abierto y la aparición de cursos masivos online revolucionaron los métodos de formación. La información dejó de ser un privilegio restringido para convertirse, potencialmente, en un bien de acceso universal, aunque persistieron brechas de conectividad que afectaron desproporcionadamente a las regiones en desarrollo.

Por otra parte, la Tercera Revolución Industrial introdujo un nuevo paradigma laboral caracterizado por la flexibilización, la deslocalización y la incorporación de tecnologías inteligentes en la gestión organizacional. Las empresas comenzaron a fragmentar sus cadenas

de producción en múltiples territorios, aprovechando ventajas comparativas en costos laborales, infraestructura o políticas fiscales. De este modo, surgió una economía globalizada interdependiente, donde las decisiones de producción dejaron de estar ancladas a un territorio específico. Este fenómeno, conocido como global value chains, transformó la relación entre trabajadores y empleadores, generando tanto oportunidades de crecimiento como riesgos de precarización y desigualdad salarial.

En términos políticos, la expansión de las tecnologías digitales también modificó las formas de participación ciudadana y el funcionamiento de los sistemas democráticos. La comunicación instantánea permitió el surgimiento de movimientos sociales organizados a través de redes digitales, los cuales lograron ejercer presión sobre gobiernos, empresas y organismos internacionales. Sin embargo, esta misma infraestructura abrió la puerta a nuevas amenazas, como la manipulación de la opinión pública mediante campañas de desinformación, el uso político de algoritmos y la vigilancia masiva facilitada por la recolección indiscriminada de datos. La gobernanza global enfrentó así desafíos que las instituciones tradicionales no estaban preparadas para gestionar.

A nivel cultural, la digitalización produjo una transformación profunda en la forma en que las personas construyen identidad, relaciones sociales y sentido de comunidad. La proliferación de redes sociales rediseñó las dinámicas de interacción interpersonal, permitiendo la creación de espacios virtuales donde se producen fenómenos como la hiperconectividad, la inmediatez comunicativa y la exposición constante de la vida privada. Estas plataformas dieron lugar a nuevas formas de sociabilidad, pero también a patologías emergentes como la adicción digital, la ansiedad derivada de la comparación social y la erosión de los espacios de silencio y reflexión, aspectos que autores contemporáneos han explorado a profundidad.

Otro aspecto determinante de esta revolución es la centralidad de los datos como recurso económico. La capacidad para recoger, procesar y analizar información a gran escala dio origen a lo que se conoce como big data, un fenómeno que alteró los modelos de gestión empresarial, las políticas públicas y las prácticas de consumo. Las plataformas comenzaron a recopilar información sobre preferencias, hábitos y comportamientos de los usuarios, generando perfiles predicitivos que permitieron optimizar decisiones comerciales y políticas. Este proceso posicionó a los datos como uno de los activos más valiosos del siglo XXI, comparable al petróleo durante el siglo XX, consolidando lo que algunos autores denominan capitalismo de vigilancia.

En cuanto al impacto ambiental, si bien la digitalización permitió optimizar recursos y reducir ciertos niveles de contaminación, también generó nuevas formas de degradación ecológica. La fabricación de dispositivos electrónicos depende de minerales estratégicos extraídos en condiciones frecuentemente asociadas a conflictos sociales y daños irreversibles al medio ambiente. Además, el consumo energético de los centros de datos y la obsolescencia programada de los dispositivos han producido toneladas de desechos electrónicos, cuya gestión constituye uno de los retos ambientales más significativos de la era digital.

Finalmente, la Tercera Revolución Industrial sentó las bases para el surgimiento de la Cuarta y Quinta Revolución Industrial al establecer una infraestructura digital global que permitió el desarrollo de tecnologías como la inteligencia artificial, la robótica avanzada, la nube, la realidad virtual, el blockchain y el Internet de las cosas. La evolución hacia sociedades interconectadas, automatizadas y centradas en datos ha moldeado un nuevo ecosistema económico, cultural y jurídico que redefine la noción misma de ciudadanía, trabajo, identidad y Estado. Este proceso no solo transformó los cimientos del mundo contemporáneo, sino que abrió interrogantes sobre los límites éticos, políticos y constitucionales de la tecnología, que constituyen el punto de partida para comprender el surgimiento del constitucionalismo digital.

2.4.Cuarta Revolución Industrial

La llegada de la Cuarta Revolución Industrial no puede comprenderse como un fenómeno aislado ni como un simple avance tecnológico, sino como un punto de inflexión histórico que redefine la manera en que las sociedades producen, se organizan y se relacionan. En un escenario global marcado por transformaciones aceleradas, resulta indispensable contextualizar este proceso dentro de la evolución estructural de las revoluciones industriales anteriores y de los cambios culturales, económicos y políticos que dieron lugar a la actual era digital. La emergencia de nuevas tecnologías disruptivas revela no solo un salto cualitativo en la capacidad humana para automatizar y analizar información, sino también la consolidación de un nuevo paradigma civilizatorio que reconfigura las nociones tradicionales de trabajo, ciudadanía, gobernanza y conocimiento. En este sentido, comprender la Cuarta Revolución Industrial implica reconocer su carácter sistémico y transversal, así como su influencia en la manera en que se concibe la interacción entre individuos, instituciones y máquinas inteligentes.

La Cuarta Revolución Industrial tiene profundas raíces en el contexto histórico y social que la precede. Su surgimiento está estrechamente ligado al progreso de la Tercera Revolución Industrial, marcada por la digitalización, la automatización y la globalización de la economía.

A medida que las tecnologías digitales comenzaron a ganar terreno en la segunda mitad del siglo XX, se establecieron los pilares para la revolución tecnológica que se está presenciando hoy.

Históricamente, el avance de la tecnología ha estado intrínsecamente ligado a cambios sociales significativos. Durante la Revolución Industrial del siglo XVIII y XIX, la introducción de la máquina de vapor y la mecanización de la producción transformaron radicalmente la economía y la sociedad, dando lugar a un desplazamiento significativo de personas del campo hacia áreas urbanas, cambios en las relaciones laborales y un aumento en la productividad (Naciones Unidas, 2020). De manera similar, la Tercera Revolución Industrial, impulsada por la informática y las tecnologías de la comunicación, trajo consigo la informatización de los procesos industriales, la aparición de la internet y la globalización de la economía. Esto no solo cambió la forma del trabajo y la comunicación, sino que también alteró la dinámica económica mundial, creando nuevas oportunidades, pero también ampliando la brecha entre países desarrollados y en proceso de desarrollo (Dominguez, 2023).

En este contexto histórico, la Cuarta Revolución Industrial emerge como una continuación de este proceso de transformación tecnológica y social. Sin embargo, lo que la distingue es la velocidad y el alcance de las transformaciones que está provocando. La convergencia de tecnologías digitales, físicas y biológicas está impulsando la creación de sistemas ciber físicos inteligentes que pueden tomar decisiones de manera autónoma, lo que tiene el potencial de alterar fundamentalmente la forma en que se vive y se trabaja (La BBC, 2016).

Desde el punto de vista social, la Cuarta Revolución Industrial plantea importantes desafíos y oportunidades. Por un lado, la automatización y la inteligencia artificial están alterando el panorama laboral, brindando la posibilidad de que muchas tareas sean realizadas por máquinas en lugar de humanos. Esta situación genera dudas respecto al porvenir del empleo y la necesidad de redefinir la educación y la formación profesional para responder a los requerimientos de un entorno laboral que cambia de forma continua (Secretaría de Estrategias Industriales, 2024).

Por otro lado, la digitalización y la conectividad están creando nuevas formas de interacción social y oportunidades para la participación ciudadana. La economía colaborativa, por ejemplo, está permitiendo a las personas compartir recursos y conocimientos de formas antes impensables, mientras que las redes sociales están ampliando nuestras redes de contacto y facilitando la movilización social. En el corazón de la Cuarta Revolución Industrial se

encuentran herramientas tecnológicas como la conectividad del Internet de las cosas (IoT), la inteligencia artificial, el machine learning y la automatización robótica avanzada, la realidad aumentada (RA) y la fabricación aditiva, entre otras. Estas tecnologías están permitiendo la creación de sistemas ciberfísicos inteligentes que pueden comunicarse, colaborar y tomar decisiones de manera autónoma (Dominguez, 2023).

Uno de los factores más relevantes de la Cuarta Revolución Industrial es su impacto en la industria y la economía. Las fábricas inteligentes, por ejemplo, están revolucionando los procesos de fabricación al integrar sistemas de producción totalmente automatizados y conectados. Esto no solo mejora el rendimiento y la eficacia, sino que además posibilita la personalización masiva de productos y la optimización de la cadena de suministro. Además, la Cuarta Revolución Industrial está fomentando el desarrollo de formas innovadoras de emprendimiento y la reconfiguración de diversas industrias. Desde la atención médica hasta la agricultura, pasando por la energía y la movilidad, ninguna industria está quedando al margen de esta revolución. La digitalización y la conectividad están creando oportunidades sin precedentes para el desarrollo innovador y el avance de la economía. No obstante, junto con estas oportunidades también surgen desafíos significativos. La ciberseguridad, por ejemplo, se ha convertido en una preocupación cada vez mayor a medida que aumenta la interconexión de dispositivos y sistemas. Además, existe el riesgo de una mayor desigualdad económica y social si no se abordan adecuadamente los efectos de la automatización y la inteligencia artificial sobre el empleo.

Asimismo, la Cuarta Revolución Industrial es el resultado de una evolución histórica marcada por la interacción entre la tecnología y la sociedad. Su impacto en el mundo moderno es profundo y complejo, y su comprensión requiere un análisis que tenga en cuenta tanto sus aspectos tecnológicos como sus implicaciones sociales y culturales.

De esta manera, la Cuarta Revolución Industrial representa un punto de inflexión en la trayectoria humana, un escenario en el que la innovación tecnológica redefine las nociones tradicionales de productividad, eficiencia y creatividad. Este proceso no solo transforma las estructuras económicas y la manera en que funcionan los mercados, sino que también impulsa la necesidad de modelos educativos más flexibles, políticas públicas innovadoras y marcos normativos capaces de responder a realidades tecnológicas en constante cambio.

Del mismo modo, la expansión de sistemas inteligentes y de plataformas digitales obliga a repensar la relación entre instituciones, ciudadanos y actores tecnológicos globales. La construcción de una sociedad capaz de adaptarse a este nuevo orden exige fortalecer la

alfabetización digital, promover la inclusión tecnológica y garantizar que la innovación no profundice las brechas sociales existentes.

En suma, este fenómeno marca la entrada a una etapa histórica caracterizada por la convergencia de capacidades humanas y digitales en un entorno interconectado, dinámico y en permanente evolución. La Cuarta Revolución Industrial, vista desde esta perspectiva, no solo redefine el presente, sino que configura las bases de las sociedades del futuro, en las que el desarrollo tecnológico deberá ir acompañado de responsabilidad social, ética digital y una visión humanista del progreso.

2.5.Quinta Revolución Industrial

La Quinta Revolución Industrial se configura como un hito histórico que no solo continúa la evolución tecnológica previa, sino que redefine la relación entre seres humanos, máquinas y entornos digitales. En este nuevo ciclo transformador, la tecnología deja de ser únicamente una herramienta de optimización productiva para convertirse en un agente capaz de interactuar, aprender y tomar decisiones de manera autónoma. Este fenómeno invita a reflexionar sobre cómo las sociedades se adaptan a entornos dominados por sistemas inteligentes que influyen en la economía, las dinámicas sociales y los valores democráticos. Comprender esta revolución requiere partir de la premisa de que no se trata únicamente de un avance técnico, sino de una reconfiguración profunda de los modelos de organización social, de las formas de producción y de la estructura misma del poder en un mundo crecientemente automatizado.

El surgimiento de esta etapa también evidencia cómo las transformaciones tecnológicas actuales adquieren un carácter humanocéntrico, orientado no solo a aumentar la capacidad de las máquinas, sino también a mejorar la calidad de vida, fortalecer los sistemas de bienestar y repensar la manera en que los seres humanos interactúan con la inteligencia artificial. Así, la Quinta Revolución Industrial se presenta como una invitación a analizar las implicaciones éticas, políticas y jurídicas derivadas de convivir con sistemas autónomos, en un momento histórico donde los límites entre lo humano, lo digital y lo biológico se vuelven cada vez más difusos.

Esta etapa representa la transformación tecnológica y social que va más allá de las revoluciones industriales anteriores. Su principal característica es la integración entre herramientas digitales, sistemas físicos y avances biotecnológicos, para crear sistemas aún más complejos e interconectados (Dominguez, 2023). A diferencia de las revoluciones industriales

anteriores, que se centraron principalmente en la automatización de la producción, la Quinta Revolución Industrial busca crear sistemas inteligentes con la habilidad de adquirir conocimientos, ajustarse a diferentes contextos y actuar de forma independiente (Universidad en Internet, 2024).

Esta revolución tiene como eje central innovaciones tecnológicas como la inteligencia artificial, el internet de las cosas (IoT), la computación en la nube, la biotecnología y la nanotecnología. Estas tecnologías están transformando radicalmente el modo de vida, las dinámicas laborales y las interacciones sociales de las personas. Por ejemplo, la inteligencia artificial está permitiendo la creación de algoritmos inteligentes que analizan extensos conjuntos de datos y generan respuestas autónomas más rápidas y precisas que los humanos. El IoT está conectando objetos cotidianos a internet, lo que permite la creación de ciudades inteligentes, fábricas automatizadas y sistemas de transporte más eficientes (Gamarra, 2022).

Una de las principales implicaciones de la Quinta Revolución Industrial es su influencia notable en el ámbito laboral. Conforme las máquinas adquieren mayor inteligencia y capacidad para ejecutar funciones que antes solo podían desempeñar los seres humanos, es probable que se vea una reestructuración significativa en la forma del trabajo. Algunos empleos desaparecerán debido a la automatización, mientras que otros surgirán en áreas como la programación, la ingeniería de datos y la ciberseguridad (Carmona, 2023). Además, la Quinta Revolución Industrial plantea importantes desafíos éticos y sociales. Por ejemplo, la creación de sistemas autónomos genera interrogantes en torno a la responsabilidad y la toma de decisiones éticas. ¿Quién es responsable cuando un vehículo autónomo causa un accidente? ¿Cómo se garantiza la privacidad y la seguridad de los datos en un mundo cada vez más conectado? Estos son solo algunos de los muchos dilemas que se desarrollaran a medida que avanza en la nueva era tecnológica. Estos interrogantes seguirán sin ser resueltos debido a que la sociedad sigue en proceso de construcción y reinvención.

Sin embargo, a pesar de los desafíos, la Quinta Revolución Industrial también ofrece enormes oportunidades. Por ejemplo, el desarrollo de tecnologías médicas avanzadas podría llevar a avances significativos en el tratamiento de enfermedades y la mejora de la calidad de vida. Del mismo modo, la digitalización de la economía podría abrir nuevas oportunidades comerciales y el impulso a la generación de puestos de trabajo en industrias en desarrollo (Dominguez, 2023).

Finalmente, la Quinta Revolución Industrial está transformando radicalmente el mundo en el que se vive. Su impacto se sentirá en cada dimensión de la vida cotidiana, incluyendo el

empleo, la formación académica, la atención sanitaria y la sostenibilidad ambiental. Para aprovechar al máximo las oportunidades que ofrece esta nueva era tecnológica, será fundamental adaptarse rápidamente y estar dispuesto a aprender y crecer en un entorno en constante cambio.

La revisión histórica de las revoluciones industriales demuestra que cada salto tecnológico ha transformado de manera estructural la economía, la organización social y la dinámica de los derechos fundamentales. Desde la mecanización y el uso del vapor en la primera revolución industrial, pasando por la automatización y la robotización en la tercera, hasta la digitalización y la interconexión global en la cuarta, todas estas etapas evidencian que el progreso tecnológico nunca ha sido neutro: ha generado oportunidades de desarrollo, pero también profundas desigualdades y nuevos retos regulatorios para los Estados (Fernández, 2012; Ferrer, 2022; Ordóñez, 2007). Esta trayectoria histórica revela que los avances técnicos exigen marcos jurídicos capaces de proteger la dignidad humana y garantizar los derechos fundamentales. En este contexto, la quinta revolución industrial emerge no solo como un cambio tecnológico sin precedentes, sino como un desafío integral para el constitucionalismo contemporáneo, que deberá adaptarse a una sociedad cada vez más digital, interconectada y dependiente de la inteligencia artificial.

En consecuencia, la Quinta Revolución Industrial obliga a replantear los fundamentos de la regulación y del orden constitucional, ya que las tecnologías autónomas, la expansión de la biotecnología y el uso masivo de datos redefinen las fronteras del Estado y su capacidad para garantizar derechos. La interacción constante entre personas y sistemas inteligentes evidencia la necesidad de marcos éticos orientados a proteger la autonomía individual, la privacidad y la equidad en un entorno donde los algoritmos adquieren un papel decisivo en múltiples esferas de la vida.

Asimismo, las transformaciones económicas y sociales de esta revolución exigen que los Estados adopten políticas públicas innovadoras que fomenten la alfabetización digital, la inclusión tecnológica y la adaptación de los sistemas educativos y productivos. Solo de esta manera será posible aprovechar plenamente el potencial de esta nueva etapa histórica sin profundizar las desigualdades existentes ni generar brechas estructurales difíciles de revertir.

Así, la Quinta Revolución Industrial no solo representa un salto tecnológico, sino una oportunidad para reimaginar las relaciones entre humanidad y tecnología bajo un enfoque centrado en los derechos, la sostenibilidad y el bienestar colectivo. La manera en que se gestione esta transición determinará en gran medida la forma del orden social, económico y

jurídico del futuro, reafirmando la importancia de comprender este fenómeno como un proceso complejo, multidimensional y decisivo para el destino de las sociedades contemporáneas.

2.6.Nuevas tecnologías de la quinta revolución industrial

La quinta revolución industrial (5RI) marca una nueva etapa en la historia del desarrollo tecnológico, caracterizada por la integración entre la inteligencia artificial, la robótica avanzada, la conectividad total y la sostenibilidad, con un enfoque centrado en el ser humano. A diferencia de la cuarta revolución industrial, que se enfocó principalmente en la digitalización y la automatización de procesos, la 5RI propone una colaboración activa entre personas y máquinas, potenciando la producción personalizada, la biotecnología y la eficiencia energética (Balaguer Callejón et al., 2023). Este escenario, aunque ofrece oportunidades inéditas para el desarrollo social y económico, también plantea desafíos jurídicos significativos, pues la interconexión de sistemas inteligentes y la ampliación de las capacidades humanas mediante la tecnología generan nuevos riesgos para la privacidad, la seguridad y la autonomía individual. Comprender estas características es esencial para contextualizar el surgimiento del constitucionalismo digital colombiano, que debe adaptarse a esta transformación para garantizar la protección efectiva de los derechos fundamentales en un entorno cada vez más tecnificado.

En pleno debate de la Cuarta Revolución industrial y aparece la quinta revolución industrial producto del desarrollo del metaverso en el año 2023 y la Web 3. Otro aspecto para resaltar es el uso de la información en la sociedad provocará cambios significativos en la forma de vivir. Los avances tecnológicos indican que los seres humanos serán capaces de procesar conocimientos y aplicarlos a nivel individual. Podrá predecir enfermedades y salvar más vidas, de igual forma podrá hacer más, con mayor eficiencia: en ámbitos de desplazamiento y producción, al igual que aumentar el tiempo de vida. Los seres humanos tendrán más recursos a su disposición y vivirán con mayor seguridad (Sergio Arboleda, 2024).

La capacidad de predicción será excepcionalmente precisa, y el cómputo tendrá mayor conocimiento que el ser humano en sí mismo. Esto permitirá comprender mejor los recursos, cómo cuidarlos y explotarlos. Las compañías comprenderán cómo producir y concentrar mayores niveles de riqueza, los Estados podrían ser sustituidos por sistemas de inteligencia artificial o, en su defecto, deberán colaborar estrechamente con ellos. Las formas de dinero físico y digital tenderán a integrarse, haciendo que las operaciones comerciales sean considerablemente más seguras. El comercio electrónico se expandirá hacia mercados

integrados y grandes conglomerados, mientras que la distribución de productos será extremadamente rápida. Habrá una gran demanda de trabajos que hoy no tienen un nombre o forma claros (Sanchez, 2024).

En el ámbito científico, las empresas realizarán mucha más investigación que los institutos académicos y universitarios tradicionales. La ciencia más emocionante, transformadora y fundamental se desarrollará fuera de las universidades, en áreas que hoy ni siquiera existen. Será común que los premios Nobel sean otorgados a personas que trabajan en compañías. En el futuro, podrían ser otorgados a instituciones tecnológicas que actualmente son pequeñas empresas o simplemente una idea en la mente de un niño o adolescente en el tercer mundo (Vargas, 2011).

La educación se personalizará para todos y en todos los niveles. Cada niño podrá tener su propio proceso educativo, tanto colectivo como individual. Las universidades adoptarán sistemas mucho más flexibles y universales, capaces de generar cambios inmediatos y significativos en la sociedad. Si no logran estos objetivos, entonces no serán lo suficientemente revolucionarias. El cambio profundo continuará, y se convertirá en la base de una nueva revolución, caracterizada por cambios exponenciales, que ocurrirán en un tiempo más corto y que se basarán en las primeras cinco revoluciones industriales (Dominguez, 2023). Es por ello, que se debe conocer algunas tecnologías con las que vive cada día el ser humano, con la libertad de su uso y sin restricciones normativas, más allá de las del desarrollador:

Tabla 1.

Conceptos nuevas tecnologías

Concepto	**Significado**
Metaverso:	Un espacio virtual en línea donde los usuarios pueden interactuar en un mundo tridimensional generado por computadora. El metaverso plantea desafíos para la privacidad y la libertad de expresión, ya que los usuarios pueden ser monitoreados y censurados por las empresas que controlan estas plataformas.

Inteligencia artificial	la IA se está utilizando cada vez más en la toma de decisiones en áreas como el empleo, la justicia y la salud. Sin embargo, la IA puede ser sesgada y discriminatoria, lo que plantea desafíos para la igualdad y la no discriminación.
Big data	La recopilación y análisis de grandes cantidades de datos plantea desafíos para la privacidad y la protección de datos personales.
Blockchain:	Una tecnología de registro distribuida que se utiliza para crear sistemas de confianza y transparencia en línea. Blockchain puede ser utilizado para proteger la protección de la información personal y la confidencialidad de los datos.
Teknización:	La creciente integración de la tecnología en la vida cotidiana plantea desafíos para la privacidad y la autonomía personal.
Transhumanismo:	Un movimiento que busca mejorar la condición humana a través de la tecnología. El transhumanismo plantea desafíos éticos y legales en torno a la identidad y la igualdad.
Personas ciborg:	Personas que han integrado tecnología en su cuerpo. Las personas

	ciborg plantean desafíos para la privacidad y la autonomía personal.

Fuente: Elaboración propia (2024).

Nota: Los anteriores conceptos corresponden a los conceptos de las nuevas tecnologías de la quinta revolución industrial.

Como se puede evidenciar, las nuevas tecnologías de la quinta revolución industrial están transformando profundamente la manera de vida, en el trabajo, las relaciones y cuidado de la salud. Esta era tecnológica, marcada debido a la intersección de la inteligencia artificial, la robótica de vanguardia, la biotecnología y la conectividad global, no solo está redefiniendo los procesos productivos y las dinámicas laborales, sino también los vínculos sociales y los sistemas de atención médica. No obstante, este avance vertiginoso trae consigo una serie de desafíos que requieren una atención y consideración cuidadosa. Estos desafíos incluyen la necesidad de actualizar marcos legales y éticos, garantizar la inclusión y equidad en el acceso a estas tecnologías, y abordar las posibles implicaciones sobre la privacidad y seguridad de los datos. Además, es crucial reflexionar sobre el impacto que esta transformación tiene en la sostenibilidad del planeta y el bienestar humano, asegurando que el progreso tecnológico vaya enlazado con el desarrollo social y ambiental.

Estos fenómenos han dado lugar al constitucionalismo digital, entendido como la adaptación de los principios constitucionales a la nueva realidad tecnológica. En Colombia, esta transformación enfrenta desafíos significativos, como la necesidad de revisar y actualizar el marco legal para garantizar la protección de los derechos fundamentales en entornos digitales, reducir la brecha digital que profundiza desigualdades y fortalecer la defensa de la privacidad frente a la masiva recopilación de datos por parte de empresas y del Estado (Orozco, 2023).

La quinta revolución industrial profundiza estos retos al integrar inteligencia artificial, robótica avanzada, biotecnología, metaverso y blockchain, transformando tanto los procesos productivos como las dinámicas sociales. Aunque este avance ofrece oportunidades inéditas para el desarrollo económico, la personalización educativa y la prolongación de la vida humana, también genera riesgos en materia de privacidad, seguridad de los datos, equidad en el acceso y sostenibilidad. Ante esta realidad, la adaptación de los marcos constitucionales y

legales resulta urgente, y el constitucionalismo digital colombiano se presenta como la vía para salvaguardar la dignidad humana, la autonomía individual y la justicia social en una sociedad crecientemente interconectada. Con este panorama, se da paso al estudio de la transformación digital, entendida como la evolución de la sociedad tecnológica, y de su impacto en los derechos fundamentales y en el marco jurídico, eje central del siguiente subcapítulo.

La comprensión interdisciplinaria de la evolución de la sociedad tecnológica permite evidenciar que la digitalización no es un fenómeno aislado, sino un proceso integral que transforma de manera profunda la economía, la cultura, la educación y la política, generando nuevos desafíos para la protección de los derechos fundamentales. Esta mirada holística constituye la base para el análisis de la transformación digital, entendida como la concreción de estos avances tecnológicos en la vida cotidiana, los sistemas productivos y las relaciones sociales. A partir de este punto, el estudio se centrará en examinar cómo la transformación digital impacta directamente en los derechos fundamentales y en los marcos jurídicos, dando paso al análisis crítico que se desarrolla en el siguiente subcapítulo.

La creciente complejidad tecnológica de la quinta revolución industrial evidencia que la humanidad se encuentra ante un punto de inflexión histórico en el que la interacción entre sistemas inteligentes y seres humanos redefine los fundamentos mismos de la organización social. La profundización de tecnologías autónomas capaces de aprender, anticipar comportamientos y tomar decisiones plantea nuevos escenarios que desbordan las categorías jurídicas tradicionales y obligan a repensar no solo la noción de trabajo, sino también los principios de responsabilidad, agencia y control democrático sobre la tecnología. Estos cambios exigen un análisis detallado sobre cómo deben estructurarse los sistemas normativos para garantizar que los avances técnicos respondan a valores constitucionales y no se impongan sin supervisión ni límites adecuados.

De igual forma, se hace evidente que las transformaciones tecnológicas introducen nuevas formas de desigualdad que no se limitan al acceso a dispositivos, sino que penetran en ámbitos como la alfabetización digital, la participación en economías basadas en datos y la capacidad de comprender y cuestionar decisiones algorítmicas. Las sociedades que no logren cerrar estas brechas enfrentarán una redistribución profunda del poder económico y político, concentrado en quienes dominen las infraestructuras tecnológicas, los flujos de datos y los sistemas de inteligencia artificial. En este contexto, la quinta revolución industrial se convierte en un desafío no solo técnico, sino esencialmente democrático y social.

Asimismo, el ritmo acelerado del progreso tecnológico invita a reflexionar sobre la relación entre innovación y sostenibilidad. La masificación de dispositivos, el consumo energético creciente, el uso intensivo de recursos minerales y la expansión de infraestructuras digitales tienen impactos ambientales que deben ser atendidos desde una perspectiva normativa y ética. La transición hacia sistemas inteligentes no puede consolidarse sin paralelamente fortalecer estrategias de economía circular, energías limpias y modelos de innovación que concilien productividad, bienestar humano y preservación del planeta. La revolución tecnológica también demanda una revolución ecológica que permita mitigar los efectos ambientales derivados de esta nueva era.

Al mismo tiempo, el desarrollo de tecnologías biomédicas, neurotecnológicas y genéticas introduce desafíos inéditos para la protección de la identidad, la autonomía corporal y la autodeterminación personal. La posibilidad de integrar dispositivos en el cuerpo humano, manipular información genética o intervenir en procesos cognitivos abre debates urgentes sobre los límites éticos de la mejora humana y la protección del ser humano frente al uso indebido de estas innovaciones. En esta línea, los avances de la quinta revolución industrial obligan a fortalecer marcos de bioética, neuroderechos y protección del cuerpo humano como pilar fundamental del orden constitucional.

En este escenario, adquiere relevancia la creación de mecanismos institucionales capaces de vigilar el desarrollo, implementación y supervisión de tecnologías inteligentes. El Estado deberá consolidar capacidades técnicas que le permitan evaluar algoritmos, auditar sistemas de inteligencia artificial y regular infraestructuras digitales desde un enfoque de derechos humanos. La gobernanza tecnológica no puede limitarse a la regulación convencional, sino que requiere instituciones especializadas, cuerpos técnicos interdisciplinarios y modelos de cooperación internacional que respondan a la globalidad de las plataformas y flujos de datos. Este fortalecimiento institucional es vital para garantizar que la tecnología actúe como herramienta de libertad y no como instrumento de control o exclusión.

En síntesis, la complejidad estructural de la quinta revolución industrial exige una comprensión profunda de sus impactos, riesgos y oportunidades. No se trata únicamente de incorporar nuevas tecnologías, sino de transformar la manera en que se conciben los derechos fundamentales, la democracia, la participación ciudadana y la justicia social en un entorno cada vez más automatizado e interconectado. La necesidad de un marco jurídico robusto, flexible y adaptado a esta nueva realidad se convierte en una condición indispensable para que el progreso

tecnológico se articule con la dignidad humana, la equidad y la sostenibilidad. Así, la revolución tecnológica en curso invita a las sociedades a replantear sus prioridades, fortalecer su estructura normativa y consolidar un enfoque humanocéntrico que asegure que la innovación siga siendo un instrumento al servicio de la humanidad.

2.7. Digitalización

La digitalización constituye uno de los fenómenos más trascendentales de la contemporaneidad, al transformar no solo la economía y la producción, sino también la manera en que las personas perciben, piensa y se relacionan con el mundo. No se trata únicamente de un cambio técnico, sino de una verdadera mutación cultural y ontológica del ser humano. Su relevancia radica en que ha configurado una nueva estructura social y simbólica donde la información se convierte en el recurso más valioso, y donde el poder se ejerce a través del control de datos, algoritmos y plataformas digitales.

Como se ha expuesto en líneas anteriores este espacio nace con la Cuarta Revolución industrial es una tendencia tecnología en la digital en el que las personas mutuas su conducta a la idea de la humanidad digitalmente aumentada. En el contexto de la revolución industrial se traduce cualquier información con un numero en un litado de cifras (Dominguez, 2023).

Ahora bien, en el mundo existe lo digital y lo analógico. En el caso del primero permite traducir en cualquier tipo de información que pueda descomponerse en un listado de cifras, que puede ser veloz, ligero, liviana y además tiene una seguridad al enviarse a su destinatario. En el segundo, se posibilita una representación más compleja y continua de la realidad, pero esta información es lenta, frágil y perecedera. La transición del entorno analógico al digital ha significado, por tanto, un salto cualitativo en la manera de comprender y administrar la información, lo que ha permitido el surgimiento de nuevas formas de comunicación, producción y control social.

La tecnología digital o electrónica, se define como las herramientas, sistemas automatizados, dispositivos y medios utilizados para generar, gestionar o almacenar información. A través de estas tecnologías, es posible comprimir grandes volúmenes de datos en dispositivos de almacenamiento pequeños y portátiles, como móviles, tabletas y computadoras portátiles, lo que facilita su transporte y uso. Además, estas tecnologías agilizan procesos y cálculos, y crean nuevas formas de manipulación de la información, incrementando así la productividad de las personas. Su capacidad para realizar múltiples tareas en menos

tiempo contribuye a simplificar las actividades cotidianas en varios campos, desde el hogar y los negocios hasta la industria, la educación y la medicina. Esto es posible gracias a la optimización de los sistemas y a la provisión de soluciones eficientes para diversos problemas (Montero, 2020).

El propósito principal de la tecnología electrónica es facilitar la vida de las personas en general. Esta tecnología ha impulsado avances significativos en electrodomésticos, teléfonos móviles, televisores, equipos de sonido y muchos otros dispositivos. El impacto más Notable de la tecnología digital ha sido la transformación en la manera en que las personas se comunican, aprenden y trabajan. Estas transformaciones en las formas de vida se han producido sin que muchos se dieran cuenta (The Flash Co. , 2024). O en su defecto generan dependencias por sus productos como son el caso Iphone, youtube, Spotify, Facebook, WhatsApp, Tinder desplegando una simplicidad en la complejidad de la realidad emergente en la superficie (Dominguez, 2023).

Esto se podría llamar como la digitalización de la vida humana que permite empezar a desentrenar los alcances de la condición digital en el que se crea el almacenamiento de bits. Es necesario advertir que la digitalización no solo ocurre en dispositivos, sino que actualmente se puede ver este concepto en la información, puesto que no existe una separación tajante entre la información digital y la realidad. Se podría incluso decir que la condición humana es condición digital. La ausencia de una dimensión temporal en nuestra sociedad transparente y digitalizada deja de lado los hábitos del espíritu, que no pueden adaptarse a las exigencias de la transparencia. El espíritu es lento, porque "se demora en lo negativo y lo trabaja para sí" (Han B.-C. , Hiperculturalidad, 2018). Según Han, "La creciente digitalización de la sociedad ha impulsado la comercialización de la vida humana a tal nivel que ya no existe ningún aspecto de la existencia que escape" (Han, 2022b, p. 39). La constante exposición en la comunicación elimina la singularidad tanto de las personas como de los objetos, reduciéndolos a su valor monetario. El dinero, al permitir que todo sea comparado entre sí, borra cualquier rasgo distintivo" (Han, 2013, p. 11). La sociedad digital centrada en la transparencia transforma todo en un objeto de consumo y convierte cada instante en una extensión del trabajo.

En este sentido, la digitalización puede entenderse como una paradoja: por un lado, libera tiempo, amplía horizontes y conecta al ser humano con una red infinita de información; pero, por otro, lo somete a una lógica de productividad permanente y vigilancia constante. Los dispositivos tecnológicos no solo amplifican las capacidades humanas, sino que también

condicionan comportamientos y moldean subjetividades. La llamada “humanidad aumentada” depende crecientemente de la mediación técnica, lo que plantea nuevos dilemas éticos y jurídicos en torno a la privacidad, la autonomía y el libre desarrollo de la personalidad.

Finalmente, la digitalización provoca una considerable ampliación de las posibilidades del ser humano imaginativas gracias al sistema de relevos que crean los dispositivos conectados en redes, los cuales posibilitan navegar o volar virtualmente hacia espacios y configuraciones humana a las que de otra manera jamás hubieran llegado. Esto además con el COVID -19, hizo que, en muy poco tiempo y casi sin poderlo interiorizar en nuestro día a día de vida genero la necesidad de tener nuestros archivos de manera digital dejando de un tajo la analogía y a tener la costumbre que, en nuestros hogares, trabajo y demás ámbitos a tener la información y nuestra vida en el mundo digitalizado para tener acceso a ella en cualquier momento.

Un caso de éxito fue la transformación brusca de la Rama Judicial en Colombia que desde el año 2010, se venía trabajando el plan estratégico de transformación digital lo que genero reformas de los códigos procesales de cada jurisdicción (penal, laboral, civil entre otros). Sin embargo, a pesar de que estas normas estaban vigentes los despachos judiciales seguían prestado su servicio de manera analógica, es decir, recibir documentos en físico, no se permitía las notificaciones al correo electrónico, el expediente era en físico. Cuando sucedió la pandemia en el año 2020, los despachos tuvieron que reinvertirse expedir el Decreto 806 del 2020, permitir el uso del correo para atender al público, presentar memoriales, crear el expediente digital, notificaciones electrónicas, audiencias entre otras. Es decir que la Rama Judicial tuvo en termino de tres meses la digitalización de sus procesos en cada despacho. Fue tan exitoso que a pensar pasar esta brecha hoy se mantiene a través de la ley 2213 del 2022, el uso de las nuevas herramientas tecnológicas en las actuaciones judiciales.

El estudio de la historia de las revoluciones industriales permite comprender cómo la evolución tecnológica ha transformado de manera progresiva la economía, la sociedad y los marcos jurídicos de los Estados. A lo largo de este subcapítulo se presentará un recorrido por cada una de las revoluciones industriales, desde la primera, marcada por la mecanización, hasta la cuarta, caracterizada por la digitalización y la inteligencia artificial, para identificar los cambios estructurales que cada etapa introdujo en la vida humana y su impacto en los derechos fundamentales. Este análisis histórico no se limita a la descripción de inventos y procesos productivos, sino que busca explicar cómo cada transformación industrial ha generado nuevos

retos sociales y regulatorios, preparando el terreno para la comprensión de la quinta revolución industrial y del constitucionalismo digital en Colombia.

2.7.1. La expansión de Internet y la sociedad en red: infraestructuras tecnológicas transaccionales.

Desde finales del siglo XX, la consolidación de Internet como infraestructura global ha creado un espacio transnacional de interacción sin precedentes, donde personas, empresas y gobiernos interactúan en tiempo real sin las limitaciones físicas que caracterizaron a las sociedades industriales. Castells (1999) denomina a este fenómeno la "sociedad red", caracterizada por la interconexión global, la fluidez de la información y la erosión de las fronteras tradicionales.

Para analizar su interacción y crecimiento, es necesario remontarse a las bases de creación de este fenómeno y su definición. Internet puede definirse como una red global de computadoras interconectadas que se comunican entre sí mediante protocolos técnicos comunes. Su diseño original respondió a la idea de crear un sistema de comunicaciones descentralizado capaz de permitir el intercambio de información entre equipos situados en distintos puntos del mundo. Su desarrollo no fue un evento aislado, sino un proceso progresivo que involucró a investigadores, instituciones y organismos durante varias décadas (Torres, 2016).

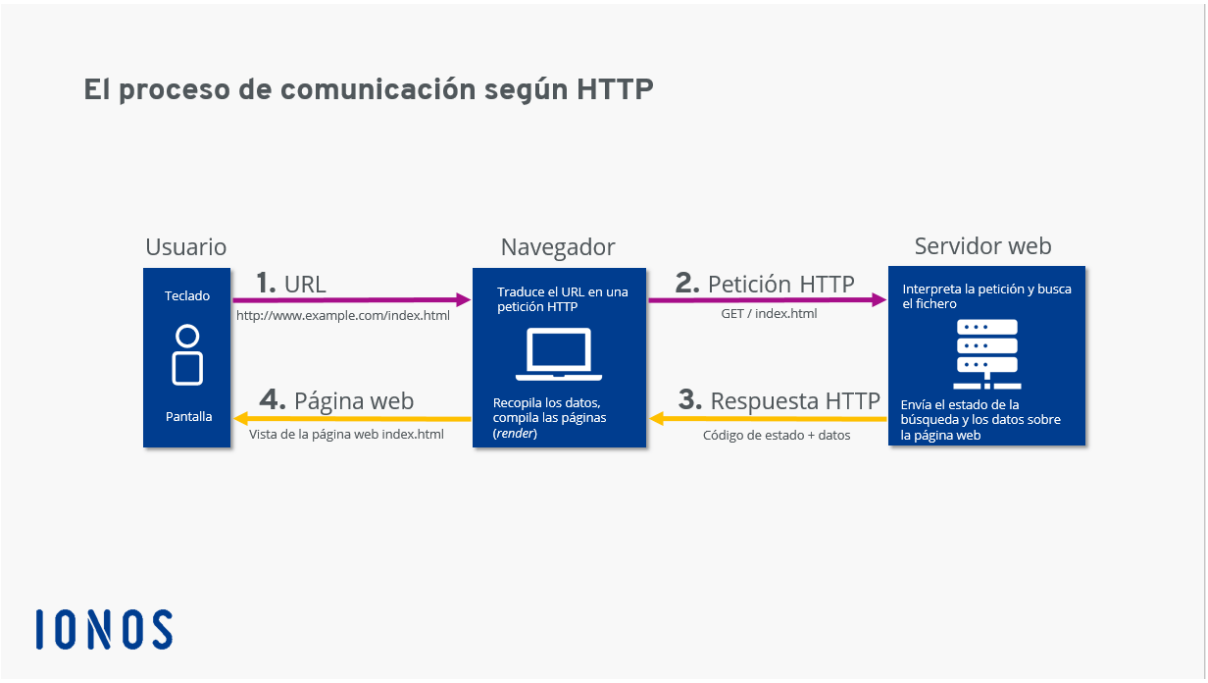
Los primeros antecedentes suelen ubicarse en los experimentos de redes de los años sesenta, especialmente el proyecto ARPANET, financiado por el Departamento de Defensa de los Estados Unidos. Esta red pionera, basada en la conmutación de paquetes, introdujo las bases conceptuales y técnicas que permitirían la posterior expansión de Internet. Con el avance de la tecnología de redes, fueron surgiendo protocolos y estándares que posibilitaron la interconexión de sistemas más amplios y el desarrollo de servicios cada vez más diversos (Aranda, 2004).

Entre esos fundamentos técnicos destacan el Protocolo de Internet (IP), responsable de la identificación y el encaminamiento de los paquetes de datos, y el Protocolo de Control de Transmisión (TCP), encargado de asegurar la fiabilidad en la comunicación entre los usuarios finales. De los 113 nodos que entonces conformaban ARPANET, 68 fueron transferidos a la nueva red militar, mientras que los restantes permanecieron en ARPANET, a la que progresivamente se incorporaron centros de investigación y universidades de diversas partes

del mundo. A pesar de que las fechas de 1969, 1982 y 1983 suelen considerarse hitos en el surgimiento de Internet, lo cierto es que su expansión al ámbito personal no se produjo hasta comienzos de la década de 1990. Esto se debió, en gran medida, al trabajo del británico Tim Berners-Lee, formado en la Universidad de Oxford y posteriormente investigador en el CERN [Laboratorio Europeo de Física de Partículas]. Durante la década de 1980, Berners-Lee comenzó a desarrollar un sistema denominado *Enquire*, destinado a almacenar y recuperar información mediante asociaciones no lineales. A partir de ese proyecto elaboró, en octubre de 1990, el lenguaje HTML [HyperText Markup Language], que permitía combinar texto e imágenes y establecer enlaces entre documentos. Asimismo, creó el primer servidor web y el primer programa cliente WorldWideWeb (Aranda, 2004)

Figura 3.

Proceso de comunicación según el HTTP.



Nota. Adaptado de IONOS (2020). ¿Qué es un HTTP?. IONOS Digital Guide. https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/protocolo-http/.

Finalmente, en 1991 puso a disposición pública sus desarrollos en la red, lo que permitió la emergencia de la World Wide Web. Desde entonces, esta estructura ha experimentado una expansión exponencial desde el punto de vista matemático. En consecuencia, cada página web que consultamos al navegar por Internet es, en esencia, un documento HTML almacenado en un servidor conectado a la WWW. Este acontecimiento daría pie a ideas posteriores, como los

motores de búsqueda, correos electrónicos, y eventualmente APPS (aplicaciones). Este proceso conlleva, inevitablemente, la redefinición de procesos, productos, servicios e incluso modelos de negocio, pero especialmente, en un espacio que transforma su definición de aislado y sectorizado, a ubicuo y dominante, es importante reconocer como el surgimiento de tecnologías como el internet redefinirían los derechos como los conocemos actualmente (Rayón, 2024).

La singularidad de las tecnologías móviles, y en particular del smartphone, no reside únicamente en su portabilidad, tamaño reducido, conectividad o apariencia estética. De hecho, más allá de la pantalla y de los elementos tradicionales de interfaz, estas tecnologías exploran nuevas formas de interacción, que van desde asistentes de voz hasta sensores avanzados, lo que les permite superar los límites de lo visual y táctil. En esencia, lo que realmente define a la tecnología móvil es su capacidad de ubicuidad, es decir, su presencia constante y generalizada que permite superponer de manera continua el contexto digital con la interacción real con el entorno. Así, como dispositivos conectados con funciones de registro (fotos, vídeos, audio, texto), absorben el mundo y lo transforman en múltiples prismas simbólicos: discursos sociales, afectos privados, relatos compartidos o rituales emergentes. Al mismo tiempo, vierten de vuelta esta información sobre el momento, el lugar y la experiencia del usuario, integrando lo simbólico con lo cotidiano (Aguado, 2020).

Por lo tanto, en los dispositivos móviles converge de manera inmediata y ubicua la posibilidad de acceder a contenido, producirlo y compartirlo, así como de interactuar con otros de forma sincrónica o asincrónica. En consecuencia, el smartphone se convierte en la herramienta principal de la interacción contemporánea, donde la ubicuidad digital se revela como su rasgo más definitorio, transformando profundamente la relación del individuo con el espacio, el tiempo y la comunicación social (Aguado, 2020).

Esta transformación tecnológica se inserta en un marco más amplio: la Sociedad de la Información, que comprende mucho más que el simple uso de Internet. Esta sociedad se caracteriza por un entramado complejo de relaciones sociales, económicas y culturales en las que las TIC, a través de diversos dispositivos, herramientas e infraestructuras, facilitan la producción, difusión y gestión de la información. Así, las tecnologías digitales están presentes en numerosas actividades humanas, no solo automatizando procesos dentro de las organizaciones, sino también en tareas de índole personal y social (Cova, 2022)

En este nuevo entorno digital, la soberanía estatal se ve desafiada por actores privados y plataformas tecnológicas que concentran poder informacional y normativo, generando lo que De Gregorio (2021) denomina una "constitucionalización fragmentada del ciberespacio", donde las reglas que rigen la libertad de expresión, la privacidad o la participación política ya no emanan únicamente de los Estados, sino de códigos, algoritmos y condiciones de uso impuestas por corporaciones globales, los cuales se analizarán con detenimiento en la siguiente sección.

2.7.2. La concentración del poder tecnológico en poderes privados globales 'Big Tech'.

En el siglo XXI, las grandes empresas tecnológicas, conocidas como **Big Tech:** Google, Meta (Facebook), Amazon, Apple y Microsoft, entre otras, se han consolidado como poderes *cuasiestatales* (Coroado, 2023). Su influencia global se extiende a sectores como la industria, el comercio, las telecomunicaciones, la educación, los medios y la política. Durante la primera década del siglo, estas compañías pasaron de ser vistas como **"tecnologías de liberación"** a ser señaladas como **"gánsteres digitales"**, dos visiones que reflejan su enorme poder y el impacto ambivalente de sus plataformas y servicios, pues estas empresas controlan la infraestructura, los algoritmos y los datos que median la vida digital de miles de millones de personas, ejerciendo una influencia social y económica comparable a la de los Estados modernos.

Shoshana Zuboff (2019) reconstruye la genealogía de este cambio trascendental en la economía digital. Según su análisis, todo comienza a principios del siglo XXI, cuando los fundadores de Google, Sergey Brin y Larry Page, recurrieron a la publicidad dirigida como estrategia para superar la recesión derivada de la crisis de las empresas punto-com (p. 69). Desde su creación en 1998, el buscador de Google recopilaba grandes cantidades de datos de comportamiento, inicialmente utilizados únicamente para mejorar la experiencia del usuario, optimizando la velocidad, la precisión y servicios gratuitos como la traducción.

Sin embargo, Brin y Page pronto descubrieron que estos datos, combinados con las capacidades analíticas de Google, podían predecir el comportamiento futuro de los usuarios, generando un valor económico enorme, fenómeno que Zuboff denomina "excedente conductual". A partir de este hallazgo, Google y otras grandes empresas de la economía digital —como Facebook, Microsoft, Apple y Amazon— reorientaron sus modelos de negocio siguiendo el "imperativo de extracción", consistente en recopilar la mayor cantidad posible de información sobre la vida de los usuarios para mejorar la capacidad predictiva de sus

algoritmos y optimizar la publicidad. Este proceso marca el surgimiento del capitalismo de vigilancia, un modelo en el que los datos conductuales reemplazan al trabajo como materia prima, generando una nueva forma de explotación capitalista, similar a la apropiación de la fuerza laboral en el capitalismo tradicional.

Las empresas de Big Tech no surgieron como gigantes, sino como startups[1] que desarrollaron plataformas multilaterales (Rochet y Tirole, 2003; Sánchez–Cartas y León, 2021), facilitando interacciones en línea entre compradores y vendedores en áreas como comercio electrónico, búsquedas en Internet y redes sociales. Una vez que una plataforma logra atraer una masa crítica de usuarios en ambos lados del mercado, se activan las externalidades de red, donde un mayor número de vendedores aumenta el valor para los compradores y viceversa, impulsando un crecimiento acelerado. Durante esta etapa, las plataformas optimizan la experiencia del usuario y aprovechan las economías de escala, y a medida que maduran, también pueden beneficiarse de las economías de alcance y de la fidelización de los usuarios debido a los altos costos de cambiar de ecosistema (Gónzalez-Páramo, 2021).

En este contexto, muchas empresas de Big Tech y plataformas de redes sociales ofrecen sus servicios de manera gratuita, lo que permite que miles de millones de personas en todo el mundo accedan fácilmente a sus plataformas. Desde una perspectiva empresarial, este modelo amplía el alcance global de estas compañías y, al mismo tiempo, potencia su principal fuente de ingresos: la publicidad dirigida. Aunque este modelo no es enteramente nuevo —la televisión, la radio y otros medios tradicionales lo han utilizado durante décadas—, las empresas de tecnología y redes sociales cuentan con una ventaja única: la capacidad de recopilar datos de usuarios con rapidez y gran precisión (World affairs council, 2021)

Estos datos de los usuarios, también llamados datos de consumidores o clientes, son extremadamente valiosos para los anunciantes, ya que permiten conocer preferencias personales, demográficas, geográficas y de comportamiento.

La pandemia de COVID-19 aumentó la dependencia de individuos, empresas y Estados soberanos de los servicios ofrecidos por las grandes multinacionales tecnológicas, ya que pudieron responder rápidamente a las necesidades generadas por los confinamientos y la distancia social. A medida que crecieron su valor de mercado e influencia, las empresas de Big

[1] Un startup es una empresa de nueva creación o edad temprana que presenta grandes posibilidades de crecimiento y comercializa productos y servicios a través del uso de las tecnologías de la información y la comunicación (Cámara de Comercio España, 2020).

Tech adquirieron mayor capacidad para intervenir en los ámbitos político, social y económico, desempeñando roles cada vez más relevantes en la política interna y en las relaciones internacionales, llegando incluso a rivalizar con la autoridad de los Estados tradicionales. Aunque la historia muestra ejemplos de compañías con gran poder, como las británicas en la India o Standard Oil (Stoller, 2019), ninguna concentró simultáneamente poder político, económico y geopolítico al nivel que lo hacen las actuales Big Tech (Coroado, 2023).

Además, Big Tech opera transversalmente en múltiples sectores, desde viajes y educación hasta salud y automóviles. Su principal activo es el control de datos y la inteligencia derivada de ellos, lo que les permite reorganizar cadenas de valor completas y superar la ventaja que antes proporcionaba la propiedad física o intelectual. Este dominio digital se ejerce de manera profunda y granular, concentrándose en pocas manos, principalmente en sedes de Estados Unidos y China, generando tensiones que algunos comparan con un "muro de Berlín digital", donde otros países se ven obligados a alinearse con uno de los polos. En este contexto, la transformación digital no solo modifica la estructura de los sectores económicos, sino que también concentra un poder sin precedentes, redefiniendo el control sobre la economía y la sociedad a través del conocimiento y la gestión de los datos (Mangin & Serrano, 2021).

Según el informe *Surveillance Giants* de Amnistía Internacional (2019), Google y Meta han alcanzado un poder sin precedentes sobre la vida de las personas en línea. Estas empresas, junto con las plataformas que poseen —como Facebook, YouTube y WhatsApp— median la manera en que los usuarios buscan y comparten información, participan en debates y se relacionan socialmente, consolidándose como canales fundamentales para la interacción digital global. Por ejemplo, Facebook cuenta con 3,07 mil millones de usuarios activos mensuales, mientras que WhatsApp e Instagram tienen 2 mil millones cada una, lo que sitúa a Meta como propietaria de tres de las cuatro principales plataformas de redes sociales por número de usuarios. YouTube, de Google, registra alrededor de 2,5 mil millones de usuarios activos al mes, y Google Search procesa un estimado de 13,7 mil millones de búsquedas diarias (Amnistía Internacional, 2025).

El poder de mercado de Google y Meta está intrínsecamente ligado a los datos de los usuarios. Sus modelos de negocio se basan en la extracción y acumulación masiva de información, lo que les permite ofrecer contenido y publicidad altamente personalizada a través de prácticas de perfilado. No solo recopilan datos, sino que también los utilizan para inferir nueva información sobre los usuarios. Sus plataformas emplean herramientas avanzadas de

inteligencia artificial y aprendizaje automático que clasifican a los usuarios en categorías muy específicas para fines publicitarios. En gran medida, los servicios de estas empresas son gratuitos para los usuarios porque monetizan nuestros datos (Hutchinson, 2023).

Google recopila información no solo a través de su buscador, sino también mediante su infraestructura de publicidad y el sistema operativo Android, obteniendo datos de búsquedas, navegación, comportamiento en páginas web, ubicación física e incluso interacciones sociales. Meta, de manera similar, monitorea la actividad de usuarios dentro y fuera de sus plataformas, incluyendo personas que no tienen cuenta en sus servicios, mediante acuerdos con terceros. Para maximizar sus ingresos publicitarios, estas compañías buscan ofrecer las mejores predicciones posibles sobre los usuarios, lo que las incentiva a ampliar continuamente la recopilación de datos y a perfeccionar sus algoritmos predictivos. Esto implica expandirse por toda la internet, a nivel global y también en el espacio físico a través de dispositivos inteligentes (Newman y Ángel, 2020).

Parte de esta recopilación se realiza mediante la provisión de servicios a terceros. Por ejemplo, cuando empresas utilizan Google Sign-in, Google Analytics, AdSense o incrustan contenido de YouTube en sus sitios, aceptan compartir información de los usuarios con Google. De manera análoga, los servicios de Meta, como "Login with Facebook", Meta Pixel o los plugins sociales, permiten a la compañía acceder a datos de visitantes de otros sitios web. El poder de mercado de estas empresas se refuerza además mediante adquisiciones estratégicas. Las compras de Meta de Instagram y WhatsApp eliminaron competidores emergentes y expandieron su capacidad de vigilancia sobre distintas formas de comunicación. Google, al adquirir YouTube, Fitbit y tecnologías publicitarias como DoubleClick, consolidó vastas bases de datos en video, salud y publicidad. Por ejemplo, la fusión con Fitbit en 2021 le permitió acceder a datos de salud previamente inaccesibles (Dhingra y Mudgal, 2019)

Finalmente, la dominancia de Meta y Google se ve reforzada por los efectos de red: cuantas más personas utilizan una plataforma, mayor es su valor para los demás, lo que fomenta la permanencia de los usuarios y dificulta que plataformas alternativas ganen tracción. La integración y el cruce de datos de múltiples fuentes profundizan sus capacidades de perfilado y consolidan su poder de mercado en la economía digital (Dhingra y Mudgal, 2019).

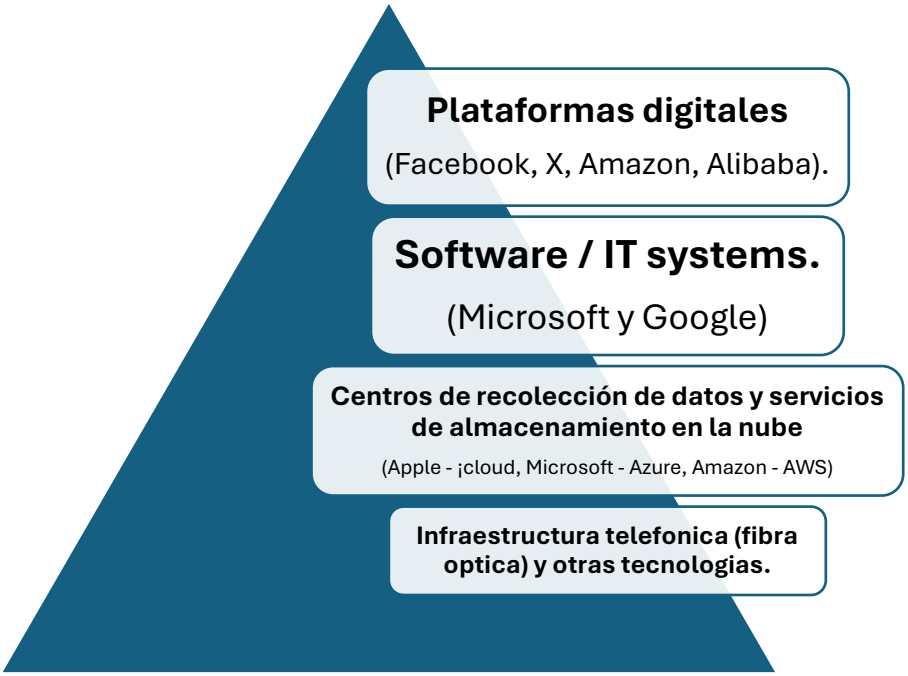
En el estudio de esta dinámica, la socióloga Shoshana Zuboff (2019) ha acuñado el término de "capitalismo de vigilancia", en el que los datos personales se han convertido en la

materia prima de la economía digital. La recolección masiva, análisis algorítmico y monetización de la información de los usuarios no solo genera beneficios económicos, sino también capacidad de predicción y control del comportamiento humano, configurando nuevas asimetrías de poder que el derecho constitucional tradicional no estaba preparado para enfrentar.

Relacionando el concepto de poder disciplinario con las características de las grandes empresas tecnológicas, es posible observar que Big Tech ejerce un poder "anónimo": no se concentra en un individuo específico, pero genera efectos directos sobre los usuarios. Mediante la recolección de datos y el uso del Big Data, estas corporaciones conocen profundamente a sus usuarios, produciendo un poder impersonal y descabezado que influye en comportamientos y decisiones, funcionando como un mecanismo de vigilancia sutil pero efectivo (Mangin & Serrano, 2021).

Figura 4.

Infraestructura digital.



Nota. Infraestructura digital y funcionamiento de almacenamiento de datos, a su vez su transferencia y dinámicas. Adaptado de Ministerio de Asuntos Digitales (2024*). El rol de las Big Tech en la Infraestructura digital.* Gobierno Danés. Copenhague, Dinamarca. https://www.english.digmin.dk/Media/638736628110392217/The%20role%20of%20big%20tech%20as%20digital%20infrastructure.pdf.

Como consecuencia de este poderío aumentado, la red se ha transformado en un nuevo espacio público donde se desarrollan procesos deliberativos, emergen movimientos sociales y se libran disputas políticas que superan los límites del marco jurídico tradicional (Celeste, 2019; Suzor, 2018). No obstante, este entorno digital está lejos de ser neutral. Los algoritmos, la inteligencia artificial y las infraestructuras tecnológicas condicionan las interacciones, determinan qué discursos se vuelven visibles y, en muchos casos, influyen en el alcance efectivo del ejercicio de derechos fundamentales. Por tanto, se observa un desplazamiento del poder normativo hacia lo que Balkin (2018) denomina "nuevas formas de gobernanza privada", en las cuales empresas como Google, Meta o X (antes Twitter) operan, de facto, como autoridades regulatorias.

La tecnología producida por Big Tech se encuentra profundamente imbricada en el funcionamiento cotidiano de las sociedades y economías occidentales. Estas plataformas, por ejemplo, desempeñan un papel clave en las cadenas globales de suministro, facilitan el acceso a recursos esenciales como el trabajo y el financiamiento, fomentan la innovación abierta y posibilitan intercambios descentralizados (Acquier et al., 2017; Montalban et al., 2019; Rikap, 2022). En consecuencia, su elevado nivel de integración vuelve especialmente compleja cualquier iniciativa regulatoria, ya que imponer restricciones podría generar repercusiones significativas tanto en el crecimiento de las economías nacionales como en la dinámica de la economía global.

A pesar de que los legisladores y gobiernos poseen una tradición en la supervisión de corporaciones poderosas con estructuras oligopólicas, las denominadas 'Big Tech' representan un desafío particularmente complejo por varias razones. En primer lugar, estas empresas dependen poco de activos físicos (Murcia y Suddaby, 2024). A diferencia de los ferrocarriles, las compañías de telecomunicaciones y otros monopolios históricos, las tecnológicas cuentan con escasos activos tangibles y presentan costos relativamente bajos en capital humano (Fernandez et al., 2020). Esta cualidad les permite que no están vinculadas a un territorio específico, lo que les otorga la capacidad de trasladarse con facilidad hacia jurisdicciones con marcos regulatorios más favorables, evitando así impuestos y otras formas de supervisión (Allevato y Pastor-Merchante, 2021). Adicionalmente, estas empresas innovan a un ritmo extremadamente acelerado y, con frecuencia, en ámbitos que los reguladores no alcanzan a comprender plenamente. Por esta razón, las iniciativas regulatorias suelen responder a problemas pasados en lugar de anticipar los que surgirán en el futuro (March et al., 2000).

Quizás el mayor desafío a la hora de regular a Big Tech radica en que los intereses de estas empresas y de los Estados que las supervisan se entrelazan de una manera que no se había observado con otros oligopolios. Las compañías tecnológicas funcionan como motores de la innovación y, como señala Teece (2023), aunque generan enormes beneficios, reinvierten la mayor parte de ellos en investigación y desarrollo (I+D). En concreto, la intensidad promedio de I+D de Big Tech en 2018 superó el 10% de sus ingresos totales, mientras que el promedio en las demás empresas del S&P 500 rondaba el 4,5% (Teece, 2023). Por este motivo, el gobierno estadounidense reduce significativamente su necesidad de financiar directamente la investigación y el desarrollo a nivel nacional. Esta situación resulta particularmente relevante para los países occidentales que compiten por la supremacía tecnológica frente a naciones orientales como China e India (Vergne, 2020).

Sin embargo, la sola mención de este poderío ha sido aumentado y cimentado con base en sociedades algorítmicas, las cuales tienen una tracción esencialmente para el funcionamiento de las tecnologías actuales. Las mismas a pesar de mantener una estructura técnica y matemática, están forjadas por seres humanos con intereses concretos, los cuales juegan un papel fundamental en la transformación y evolución del constitucionalismo y la perspectiva de los derechos y su vulneración por agentes, que, en un principio, no solían afectar los derechos fundamentales directamente. En la siguiente sección se dará explicación a los sistemas algorítmicos autónomos, y como su evolución varia la sociedad actual.

2.7.2.1.Recolección de datos por compañías de Big Tech.

Los tratamientos de datos realizados por las Empresas Multinacionales Basadas en Datos (EMNBD) operan bajo recolección de datos, y sus patrones de recolección personal suelen ser bastante homogéneos. Las compañías recurren a múltiples herramientas tecnológicas que permiten rastrear de manera amplia y detallada la interacción del usuario con sus servicios. Entre ellas se encuentran las *cookies* propias o de terceros, los identificadores de anuncios utilizados en dispositivos móviles, las etiquetas de píxel insertas en páginas web o correos electrónicos, los kits de desarrollo de software incorporados en aplicaciones, el almacenamiento web local, las cachés de aplicaciones, los registros automáticos de los servidores y las direcciones URL de seguimiento que permiten conocer la procedencia del tráfico. Empresas como Apple, Google, Tinder, Netflix y Microsoft clasifican las cookies siguiendo la Guía de Cookies de la Cámara Internacional de Comercio del Reino Unido, destacando las cookies estrictamente necesarias, de análisis, de funcionalidad, publicitarias y

de interacción social, mientras que otras empresas incluyen clasificaciones adicionales como cookies permanentes o de sesión. Aunque algunas compañías, como Apple, afirman que ciertas cookies no permiten identificar directamente al usuario, persiste el riesgo de que la combinación de múltiples datos aparentemente impersonales permita, en última instancia, su identificación (Newman y Ángel, 2020).

El fin que adopta generalmente es desde un enfoque descriptivo para segmentar audiencias o uno prescriptivo para mejorar la experiencia en futuras interacciones. Sin embargo, la información disponible sobre las herramientas específicas empleadas para estos análisis es escasa, y muchas empresas solo aluden a conceptos generales como procesos automatizados, inteligencia de negocios, minería de datos o técnicas de machine learning. Pocas compañías especifican tecnologías concretas, como Google al mencionar Google Analytics y sistemas automatizados de análisis, o Netflix al referirse a sus algoritmos de recomendación. Algunas, como 1Doc3 y Ubidots, señalan el uso de servicios avanzados como el IBM Watson Natural Language Classifier, mientras que Apple, influenciada por el GDPR, aclara que no adopta decisiones basadas en algoritmos que puedan afectarle significativamente al usuario (Newman y Ángel, 2020).

Según la investigación hecha por Newman y Ángel (2020), empresas importantes, como Amazon, Facebook, Joom, Uber y Waze, niegan participar en el negocio de transferencia de datos, aunque todas prevén la posibilidad de transferir los datos de los usuarios si la empresa llegara a ser adquirida, reorganizada o fusionada. No obstante, compañías como Google, Amazon, Ubidots, Spotify, Waze y LinkedIn aseguran que la información transferida seguirá estando protegida bajo las obligaciones previamente adquiridas, al menos hasta que se informe a los usuarios. Incluso AliExpress y Netflix afirman que cualquier transferencia de datos durante procesos corporativos solo se realizará si el nuevo titular se compromete a mantener la protección prevista en sus políticas de privacidad (p. 40).

Respecto a las finalidades para las cuales estas EMNBD tratan los datos personales, se identificaron propósitos comunes como la prestación de bienes o servicios, la interacción y comunicación con los usuarios, el desarrollo de nuevos productos, la administración de concursos y promociones, la realización de investigaciones de mercado, la personalización de contenidos y publicidad, la medición de rendimiento, la elaboración de estudios y la compartición de información con terceros. Los terceros pueden incluir anunciantes, empresas

afiliadas, aplicaciones conectadas, proveedores de servicios, investigadores, socios de medición, autoridades públicas e incluso potenciales compradores (Newman y Ángel, 2020).

Finalmente, todas estas prácticas generan preocupaciones similares a las planteadas por el antiguo Grupo de Trabajo del Artículo 29[2] (Comisión Europea, 1998). El uso extensivo de cookies plantea dudas sobre la magnitud de la recolección y el seguimiento al que están sometidos los usuarios, así como sobre el alcance y detalle de los datos obtenidos. La multiplicidad de fuentes de información abre innumerables posibilidades de combinación que incrementan los riesgos de reidentificación. A ello se suman las incertidumbres sobre la seguridad de los datos compartidos entre empresas y la falta de claridad sobre los métodos de análisis y algoritmos utilizados, lo que evidencia una débil transparencia. Finalmente, la creciente elaboración de perfiles para ofrecer contenidos personalizados o para adoptar decisiones automatizadas genera riesgos significativos para la igualdad y la no discriminación, en tanto puede derivar en tratos diferenciados no siempre visibles para los titulares de los datos (Newman y Ángel, 2020).

2.7.3. Sistemas algorítmicos autónomos: la creación de 'Sociedades algorítmicas'.

Los algoritmos, aunque ampliamente asociados con la era digital, no son un concepto nuevo. Se definen como conjuntos de instrucciones precisas que deben seguirse para resolver un problema específico, siendo un ejemplo cotidiano una receta de cocina. El término proviene del matemático del siglo IX, al-Khwarizmi. Algunos algoritmos son completamente determinísticos, ejecutando los pasos de manera idéntica para cualquier entrada (por ejemplo, ordenar un conjunto de números), mientras que otros incorporan elementos de aleatoriedad o incertidumbre, como ocurre al barajar una baraja de cartas (Olhede y Wolfe, 2018).

En el ámbito numérico, los algoritmos se evalúan según propiedades clave, como la complejidad computacional y el uso de memoria en función del tamaño de los datos, así como las garantías teóricas sobre sus resultados. Por lo general, su construcción sigue uno de dos enfoques: un marco explicativo, que busca modelar cómo se generan los datos de entrada permitiendo perturbaciones estocásticas, o un marco predictivo, que prioriza minimizar el error en futuras predicciones sin especificar la ley estocástica subyacente. Según Lehmann (2011), los modelos estadísticos modernos, a menudo complejos, se construyen combinando bloques

[2] El CEPD sustituye al Grupo de trabajo del artículo 29 (art. 29 WP), creado por la Directiva 95/46/CE y que trataba cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD).

más simples, y representan matemáticamente la forma en que se generan nuevas observaciones a partir de variables predictoras.

Figura 5.

Funcionamiento de un algoritmo.

Nota. Ilustración sobre los algoritmos y sus generalidades. Adaptado de: Lozada, A. (2019). ¿Qué es un algoritmo?. [SITIO WEB]. *EDteam*. Recuperado de: https://ed.team/comunidad/que-es-un-algoritmo.

Enmarcados en la infraestructura de la big tech, los algoritmos funcionan como "reglas generativas" que no pueden ser violadas, lo que hace que ciertas acciones sean imposibles y que los usuarios queden obligados a cumplirlas automáticamente (Schwarz, 2021). Estas reglas son utilizadas tanto por gobiernos como por plataformas digitales para gobernar poblaciones,

y ofrecen a las corporaciones un mecanismo para regular el uso de sus productos, restringiendo usos indeseados de manera más flexible y abstracta que los métodos tradicionales de diseño (Zuboff, 2019).

Los algoritmos predictivos también funcionan en favor de la anticipación de los usuarios, interpolando su capacidad de decisión o agencia propia. Se integran en sistemas que moldean y, en muchos casos, reemplazan la elección del consumidor, como los sistemas de recomendación de Spotify, Netflix, YouTube o Amazon, así como las sugerencias de contactos y grupos en redes sociales o la personalización de servicios como Google Maps. Algunos sistemas enfocan la atención en un conjunto limitado de opciones, facilitando la elección; otros, en cambio, la automatizan casi por completo, decidiendo por los usuarios en función de predicciones basadas en grandes volúmenes de datos obtenidos mediante vigilancia constante (Schwarz, 2025).

El modelo estadístico subyacente puede ser preprogramado por humanos o generado automáticamente mediante aprendizaje automático (machine learning) e inteligencia artificial (IA). Aunque a menudo se usan de manera intercambiable, *machine learning* se refiere a sistemas que aprenden de los datos para realizar predicciones sin programación explícita, mientras que la IA comprende tecnologías que simulan inteligencia humana y requiere machine learning para funcionar, aunque este último puede existir de manera independiente. En conjunto, algoritmos, aprendizaje automático e inteligencia artificial constituyen la infraestructura digital central de la sociedad contemporánea (Peeters, & Schuilenburg, 2020).

Este proceso se ha intensificado con la capacidad computacional actual y la "*dataficación*" de la vida cotidiana, que permite predicciones altamente personalizadas basadas en correlaciones estadísticas entre elecciones pasadas y futuras. Sin embargo, estas predicciones rara vez pueden contrastarse con elecciones hipotéticas no influenciadas por algoritmos, por lo que reflejan principalmente la reacción a las recomendaciones más que preferencias absolutas. Kotliar (2021) señala que los sistemas de recomendación, originalmente diseñados para inducir decisiones, han evolucionado hacia algoritmos que reducen la participación activa del usuario en la elección, eligiendo en su lugar en función de intereses comerciales mediante vigilancia y modificación conductual (Zuboff, 2019).

Esto afecta directamente en derechos fundamentales como la libertad de expresión. Jack Balkin (2018) aporta una reflexión centrada en la libertad de expresión mediante la teoría de la

“New School Speech Regulation”, con la que sostiene que la regulación contemporánea del discurso en Internet se produce principalmente en manos privadas, y que la protección de este derecho requiere una responsabilidad compartida entre Estados y plataformas. Su planteamiento es sumamente relevante en la era de la moderación algorítmica, donde decisiones empresariales sobre contenido pueden afectar el pluralismo democrático tanto como la censura estatal. Sin embargo, su propuesta abre una tensión compleja: si se reconoce a las plataformas un rol constitucional de facto, ¿cómo evitar que la autorregulación privada devenga en arbitrariedad, sobre todo en contextos de procesos electorales o discursos críticos contra el poder económico y político? La suspensión de cuentas de líderes políticos y la censura selectiva de contenidos en los últimos años muestran que sin supervisión pública ni principios de transparencia algorítmica, la delegación de funciones cuasi soberanas a empresas privadas resulta democráticamente riesgosa.

Otra de las advertencias en cuestión de vulneración de derechos fundamentales fue descrita por O’neil (2017). En su investigación sobre programación en algoritmos y los perjuicios o parcializaciones que están configurados en los mismos, los cuales, desde su mera construcción, constituyen parte importante de cómo afectan a la sociedad. El sesgo algorítmico constituye un fenómeno sistémico que reproduce injusticias mediante sistemas basados en datos, afectando de manera desproporcionada a comunidades históricamente marginadas. Estos sesgos reflejan tanto errores técnicos como manifestaciones de desigualdades estructurales codificadas en la tecnología, subrayando la necesidad de un debate interdisciplinario que aborde sus implicaciones éticas y sociales (Argote et al., 2025), los cuales, de manera inevitable, van a dar lugar a sesgos en los algoritmos de inteligencia artificial, sobre los cuales nos referiremos en capítulos posteriores.

Los algoritmos presentan una doble materialidad: son digitales en su constitución y culturales en su funcionalidad (Sued, 2022). Esto implica que la tecnología refleja relaciones sociales inscritas en contextos históricos específicos, lo que refuta cualquier pretensión de neutralidad técnica. La naturaleza contingente de los sistemas inteligentes exige un análisis crítico de su diseño, fundamental para comprender los procesos sociotécnicos de transferencia y apropiación tecnológica, en los cuales los algoritmos emergen como artefactos que materializan dinámicas de poder, preferencias culturales y sesgos institucionales. Lo que configura a un sistema algorítmico como un sistema socio-técnico es su origen y funcionamiento dentro de entornos sociales, en los cuales es adoptado, interpretado y utilizado

por actores humanos. Desde esta perspectiva, las aproximaciones socio-técnicas a la evaluación algorítmica se centran en analizar la relación dinámica entre la tecnología y el contexto social que la moldea y, a su vez, es moldeado por ella. Este enfoque permite comprender los algoritmos no solo como artefactos técnicos, sino también como dispositivos que sensibilizan y problematizan supuestos arraigados sobre equidad, transparencia y responsabilidad. Como plantea Ziewitz (2016), estas herramientas ofrecen una oportunidad para replantear críticamente los marcos normativos y epistemológicos que estructuran las prácticas contemporáneas de gobernanza algorítmica (Shin, 2019).

En una línea complementaria, Giovanni De Gregorio (2020) analiza la mutación de la sociedad contemporánea hacia una sociedad algorítmica, donde plataformas digitales como Google, Meta, Amazon o X/Twitter asumen funciones cuasi estatales, al mediar la comunicación, organizar la información y condicionar la interacción social. Su diagnóstico es particularmente agudo, al revelar la existencia de un poder normativo privado que afecta la arquitectura misma de los derechos fundamentales, desplazando al Estado como único garante de la libertad. No obstante, su enfoque genera un debate crítico: si bien describe con precisión la concentración de poder digital, sus soluciones regulatorias descansan principalmente en la acción de los Estados nacionales, sin ofrecer mecanismos claros de gobernanza transnacional que respondan a la naturaleza global de las plataformas. Este vacío es evidente en la práctica, donde legislaciones locales, incluso avanzadas, muestran límites frente a corporaciones transnacionales que operan sin arraigo territorial definido.

Lo característico de la llamada *Sociedad Algorítmica* no es únicamente la expansión de la toma de decisiones automatizada, sino el alcance que adquiere este fenómeno: el perfil digital de una persona pasa a convertirse en un componente central de su identidad jurídica y, en algunos casos, también de su identidad psicológica. En el entorno digital, la identidad ya no se construye de manera negociada entre sujetos, sino que se asigna de forma unilateral mediante procesos de tratamiento de datos que escapan al control del individuo involucrado. Una preocupación fundamental es, por tanto, la manera en que estas identidades (que pueden incorporar atribuciones positivas y negativas) se generan y circulan socialmente. Las reputaciones construidas algorítmicamente pueden difundirse de forma amplia y persistente, amplificando el impacto de las decisiones automatizadas sobre la vida de las personas (Gorgoni, 2021).

A partir de las revelaciones de Snowden[3], el debate sobre ciudadanía digital se intensificó, desplazándose de una concepción limitada (centrada en el uso frecuente o competente de Internet) hacia una reflexión más amplia sobre cómo las prácticas de vigilancia, incluida la autovigilancia, afectan la forma misma de ejercer ciudadanía. En un contexto marcado por el capitalismo de vigilancia y por fuertes desigualdades geopolíticas y económicas, resulta insuficiente definir al ciudadano digital únicamente como alguien que participa en espacios previamente establecidos (Isin y Ruppert, 2020)

Si bien los sistemas algorítmicos son objeto de análisis en sistemas independientes, esta 'sociedad algorítmica' se consolida finalmente en el uso de la IA; todos los campos de información han sido permeados por este fenómeno, específicamente, en el campo del constitucionalismo digital, ¿es posible tomar en cuenta los riesgos que presenta este tipo de tecnología? Su análisis se dará en profundidad en los apartados siguientes.

2.8. Evolución de la sociedad tecnológica y su enfoque interdisciplinario

El estudio de la sociedad tecnológica requiere partir del reconocimiento de que la transformación digital no surge de manera espontánea, sino como resultado de avances acumulativos en ciencia, innovación y procesos sociohistóricos que han redefinido la interacción humana con el entorno. Diversos autores han señalado que la revolución tecnológica contemporánea constituye un punto de inflexión comparable a la invención de la imprenta o la mecanización industrial, debido a la velocidad, profundidad e impacto sistémico de los cambios actuales (Schwab, 2016). La articulación entre inteligencia artificial, automatización, biotecnología y análisis masivo de datos ha configurado una nueva racionalidad técnica que afecta tanto la vida individual como la organización colectiva. Comprender este fenómeno exige una aproximación interdisciplinaria que permita analizar las

[3] El 5 de junio de 2013, el denunciante Edward Snowden reveló evidencia de programas de vigilancia masiva llevados a cabo por gobiernos como el de Estados Unidos y el Reino Unido. Desde entonces, se supo que agencias como la NSA y la GCHQ han estado monitorizando comunicaciones telefónicas e internet de cientos de millones de personas en todo el mundo. Gracias a los documentos filtrados por Snowden, se hizo posible comprender con mayor detalle cómo operan los gobiernos y hasta dónde llegan sus métodos de vigilancia. Uno de los cambios más significativos consiste en la transparencia sobre la cooperación entre grandes empresas tecnológicas y los gobiernos. Por ejemplo, se reveló que compañías como Facebook, Google y Microsoft estuvieron obligadas a entregar información de sus usuarios mediante órdenes secretas emitidas por la NSA. Además, se supo que la agencia estadounidense recopilaba, almacenaba y analizaba los metadatos de cada llamada telefónica y mensaje de texto enviados en países como México, Kenia y Filipinas, un nivel de vigilancia que antes era inimaginable. Estas revelaciones marcaron un punto de inflexión en la percepción pública sobre la privacidad y el alcance del poder estatal sobre los datos personales (Amnistía Internacional, 2015).

implicaciones éticas, económicas, políticas y sociales que emergen de esta nueva etapa del desarrollo humano (Serrano, 2020).

La evolución de la sociedad tecnológica ha sido un proceso complejo y multidimensional que ha transformado de manera profunda las estructuras sociales, económicas y culturales, impactando de forma directa la forma en que los Estados deben garantizar los derechos fundamentales. Comprender este fenómeno exige una mirada interdisciplinaria que combine las perspectivas de la filosofía, la sociología, la economía, la psicología, la educación y la ciencia política, pues la transformación digital afecta de manera transversal todos los ámbitos de la vida humana. Este subcapítulo integra los aportes de cada disciplina, evidenciando que la digitalización no es un fenómeno aislado, sino un proceso integral que exige reflexión crítica y respuestas jurídicas adaptadas a la quinta revolución industrial.

Desde la filosofía, la tecnología ha sido interpretada como una extensión de la capacidad humana para modificar y controlar su entorno. Martin Heidegger, en su obra "La pregunta por la técnica", advierte que la tecnología moderna no es simplemente un conjunto de herramientas neutras, sino una forma de revelar la realidad que transforma todo en un recurso explotable, incluyendo a los propios seres humanos. Esta visión crítica alerta sobre la alienación que puede producir la tecnología, al convertir al ser humano en un engranaje de un sistema técnico mayor (Gaos, 2022). Marshall McLuhan, por su parte, sostiene que la tecnología y los medios son extensiones del ser humano que modelan la percepción y la cultura. Su concepto de la "Aldea Global" explica cómo la interconexión digital acorta distancias físicas, pero también genera nuevos tipos de conflictos y divisiones sociales (Parga & Barrios, 2016). En la actualidad, Byung-Chul Han critica la hiperconectividad y la cultura de la transparencia, advirtiendo sobre la pérdida de autenticidad y la vigilancia sutil que amenaza la autonomía individual en la sociedad digital (Han, 2013; Wenz, 2022).

Desde la sociología, la tecnología es vista como un motor de cambio social que redefine las relaciones humanas, las instituciones y las dinámicas de poder. Castells (1999), en su trilogía "La era de la información", analiza la emergencia de la sociedad en red, caracterizada por la interconexión global, la centralidad de la información y la transformación de la economía hacia una lógica informacional (Castells, 1999). Esta nueva estructura social genera oportunidades de colaboración global, pero también incrementa la fragmentación y las desigualdades. Ulrich Beck, con su concepto de "sociedad del riesgo", explica que la

modernidad avanzada produce riesgos tecnológicos y ambientales que afectan a toda la humanidad, requiriendo una gestión constante de riesgos y una reflexividad crítica sobre las consecuencias de la tecnología (Trujillo, 2014; Escobar, 2003).

La evolución de la sociedad tecnológica también puede analizarse desde otras disciplinas. En la economía, la tecnología impulsa el crecimiento y la productividad, pero también profundiza la desigualdad de ingresos y plantea el desafío de la automatización laboral (Canals, 2000). En la educación, las tecnologías digitales han transformado los métodos de enseñanza mediante entornos virtuales de aprendizaje, gamificación, clase invertida y aprendizaje basado en problemas, potenciando la personalización educativa y la interacción global (Rubio, 2022). En la psicología, las tecnologías de realidad virtual, aumentada y la telepsicología han abierto nuevas posibilidades para mejorar la calidad de vida, aunque requieren evaluar cuidadosamente los riesgos éticos y de dependencia (Botella et al., 2007). Desde la ciencia política, la tecnología redefine las dinámicas de poder y gobernanza, promoviendo nuevas formas de vigilancia, control social y participación democrática mediante las TIC.

El análisis interdisciplinario de la evolución de la sociedad tecnológica evidencia que la digitalización transforma profundamente la vida humana en todos sus ámbitos: social, cultural, económico, educativo y político. Si bien estas transformaciones ofrecen oportunidades para el desarrollo, también generan riesgos significativos en materia de privacidad, autonomía, equidad y gobernanza. Esta realidad demuestra que la tecnología no es neutral y que su impacto requiere respuestas jurídicas sólidas. En este contexto, el constitucionalismo digital emerge como una necesidad impostergable para adaptar los marcos constitucionales y garantizar la protección efectiva de los derechos fundamentales en la quinta revolución industrial. Este enfoque interdisciplinario prepara el camino para el análisis de la transformación digital y su impacto jurídico, núcleo del siguiente subcapítulo.

En este sentido, resulta pertinente destacar que la sociedad tecnológica contemporánea se caracteriza por una aceleración sin precedentes, donde la innovación supera la capacidad regulatoria de los Estados y desborda los marcos institucionales tradicionales. Ello genera tensiones entre la eficiencia tecnológica y los valores democráticos, especialmente en temas como la privacidad, la autonomía, la transparencia algorítmica y la equidad. Diversos estudios advierten que la falta de una gobernanza adecuada puede conducir a formas de concentración del poder digital que amenazan la dignidad humana y los principios constitucionales (Cerrillo,

2020; Floridi, 2014). Por ello, se requiere no solo comprender el fenómeno desde diversas disciplinas, sino articular políticas públicas, reformas jurídicas y mecanismos institucionales capaces de responder a los retos emergentes.

Finalmente, la evolución interdisciplinaria de la sociedad tecnológica demuestra que el desafío central del siglo XXI consiste en equilibrar el progreso técnico con la protección de los derechos fundamentales, garantizando que la digitalización no profundice desigualdades ni erosione la autonomía individual. La construcción de un constitucionalismo digital sólido, informado por las ciencias sociales, humanas y tecnológicas, se convierte así en la herramienta fundamental para orientar la transformación digital hacia un modelo más justo, humano y sostenible. Este cierre reafirma la necesidad de continuar el análisis jurídico en los siguientes apartados, donde se examina la manera en que estos cambios impactan directamente el marco constitucional colombiano.

2.9. Tecnologías emergentes en la quinta revolución industrial y su impacto jurídico

En la actualidad, el ser humano interactúa de manera cotidiana con tecnologías emergentes como el Big Data, la inteligencia artificial, la robótica avanzada, el blockchain, el metaverso y los entornos inmersivos, entre otras. Su adopción se ha dado principalmente por tendencias sociales y económicas, impulsadas por la promesa de eficiencia, conectividad, personalización de servicios y comodidad en la vida diaria. Sin embargo, este uso masivo suele darse sin una comprensión plena de los riesgos jurídicos asociados, que abarcan desde la vulneración de la privacidad y la seguridad de los datos hasta desafíos en materia de equidad, responsabilidad y gobernanza digital. Por ello, antes de abordar el análisis normativo y constitucional, resulta indispensable comprender en qué consisten estas tecnologías y cómo transforman las interacciones sociales, económicas y políticas, para poder dimensionar sus efectos sobre los derechos fundamentales en el marco de la quinta revolución industrial.

2.9.1. Big Data

En la evolución del comportamiento humano a lo largo de la historia se ha preocupado por dejar evidencia de la información: en el que el objetivo sea recolectar los datos con el propósito de organizar nuestros recursos y optimizar la forma de como acceder a ellos. En la historia el primer evento de almacenamiento se produjo hace más de 20.000 años, cuando nuestros antepasados pintaban los techos de las cuevas los eventos vividos como historias, eventos en el que se permitiese recordar y transmitir en generación en generación para evitar

olvidar estos eventos y garantizar la conservación de la información y durante la historia esta información se ha conservado a través de imágenes, escritura entre otros en el que se busca la conservación de la información.

Ahora en la sociedad actual en donde la sociedad interactúa de una manera globalizada, ha evolucionado la forma como se almacena y se protege la información desde un archivo físico, a un disco extraíble digital a evolucionar a un almacenamiento en la nube del internet. Es por ello, que la sociedad genera una cantidad creciente de datos, y con el tiempo se desarrollan dispositivos cada vez más eficientes para almacenarlos. Los datos se consideran una infraestructura o un recurso valioso por sí mismos para cualquier organización, sea pública o privada, que los posea. Unas aproximaciones de su significado: estos volúmenes masivos de datos se están transformando en elementos fundamentales de producción en todos los sectores productivos (MANYIKA J, 2011).

El término "Big Data" puede resultar confuso, ya que la expresión "grandes datos" no especifica un tamaño concreto. Según la literatura revisada, no se refiere a un volumen de información específico (IBM, 2014), aunque generalmente se usa en el contexto de datos medidos en petabytes (PB) y exabytes (EB) (Escudero, 2021). Los datos digitales se cuantifican en bytes, que es la unidad básica de información, y a partir de esta unidad se construye la escala de medida digital:

Tabla 2.

Unidades básicas de información y tratamiento de datos

Nombre	**Símbolo**	**Sistema internacional**	**Ejemplo 2014 estático**	**Ejemplo 2014 dinámico**
Byte	B	10^0 bytes	1 B es un número de 0 a 255	
Kilobyte	KB	10^3 bytes	2 KB es aproximadamente un sector de CD-ROM	
Megabyte	MB	10^6 bytes	3 MB es aproximadamente una canción de 3 minutos	4 MB/min en llamadas de vídeo por Skype
Gigabyte	GB	10^9 bytes	8/16 GB es el tamaño estándar de mercado de un pen-drive	4 GB/hora de vídeo de alta calidad

Terabyte	TB	10^{12} bytes	4 TB es el tamaño de un disco de 120 € que almacena 800.000 fotos o canciones mp3	20 TB/hora es la información generada por un motor de avión en el aire
Petabyte	PB	10^{15} bytes	2 PB es la información almacenada en todas las bibliotecas de investigación académicas de USA	24 PB/día es la información recogida por Google
Exabyte	EB	10^{18} bytes	5 EB es aproximadamente todas las palabras pronunciadas por todos los seres humanos	966 EB es aproximadamente la predicción del volumen total de Internet en 2015
Zettabyte	ZB	10^{21} bytes	Se estimó que en 2012 la capacidad instalada de almacenamiento de información en el mundo sería de 2,5 ZB.	5 ZB/año es la cantidad de datos digitales promedio que se van a generar en la Tierra en los próximos 8 años
Yottabyte	YB	10^{24} bytes	1 YB equivale a la capacidad del Data Center inaugurado por la NASA en 2013	
Xerabyte	XB	10^{27} bytes	1 XB equivale a 1.257.000 iPad 3 de máxima capacidad por cada habitante de la tierra	

Nota. Adaptado de Maté Jiménez, C. (2014). " *Big data*". Un nuevo paradigma de análisis de datos. In *Anales de mecánica y electricidad* (Vol. 91, No. 6, pp. 10-16).

La expansión acelerada de los ecosistemas digitales ha generado un escenario en el que los datos se han convertido en uno de los recursos más valiosos de la sociedad contemporánea. Diversos autores señalan que la acumulación masiva de información y el desarrollo de herramientas de análisis avanzadas han transformado las dinámicas económicas, sociales y políticas, dando origen a nuevos modelos de gobernanza basados en la evidencia y la inteligencia computacional (Serrano, 2020; Floridi, 2014). En este contexto, comprender la

magnitud, el origen y el funcionamiento del big data resulta fundamental para analizar los desafíos jurídicos y éticos que plantea la quinta revolución industrial.

Según IBM (2024), diariamente se producen más de 1 QB de datos provenientes de múltiples fuentes, como información de clientes, proveedores, transacciones financieras en línea, datos obtenidos de dispositivos móviles, redes sociales y sistemas de ubicación GPS. En distintos países, se manejan grandes cantidades de bases de datos que contienen información sobre impuestos, censos de población, registros médicos, entre otros (IBM, 2024); otra forma de abordar para entender el conceptos se puede abordar de dos manera: a) En cuanto a su tamaño, se trata de un volumen enorme de datos que no puede ser almacenado en una sola máquina, que se genera a gran velocidad y requiere ser procesado e interpretado en tiempo real; b) abordarlo desde el ámbito tecnológico, se entiende como un conjunto de herramientas y procesos que posibilitan la recolección y almacenamiento de grandes volúmenes de datos provenientes de múltiples fuentes y con diferentes formatos, siendo esto está la forma de digitalizar la información en un mundo analógico (Dominguez, 2023).

Ahora bien, las fuentes de los datos pueden ser públicos, privados, comunidades, auto cuantificación. Unas características de los datos públicos están en cabeza de los organismos gubernamentales, son abierto y libre acceso. En cambio, los datos privados están en manos de organizaciones privadas y no son fáciles de encontrar en las fuentes públicas. Los datos de las comunidades provienen de la recolección de las redes sociales o revisiones de productos o los "me gustas" y los datos auto cuantificación y comportamiento personal a través de relojes inteligentes o pulseras que monitorean las actividades físicas entre otros aspectos que almacenan datos de bienestar familiar (González L. O., 2018).

Es entonces que el big data tiene como propósito garantizar el análisis de la información. Como por ejemplo los datos se puede clasificar y preparar material con vistas a sus análisis. Tal como la minería de los datos y el registro y sistematización de los datos. Es por ello, que con estos datos se puede usar la estadística significativa que permite determinar a través de los datos el comportamiento de las personas, determinar tendencias y pautas de comportamiento para predecir el futuro y poder adoptar decisiones de forma automatizada.

Por otra parte, el uso del Big data tiene la facilidad de hacer diferentes análisis de datos: descriptivo para clasificar y preparar la información para su análisis como es el caso de minería de datos que es usado en nuestro tiempo para tener información comercial, materialización de

riesgo, comportamiento de las personas entre otros. Otro dato es prescriptivo que orienta a dar recomendaciones de actuación para emplear el conocimiento predictivo y el conocimiento descriptivo a efectos de poder alcanzar objetivos (Vivas, 2021).

De esta manera, el big data se consolida como uno de los pilares de la nueva economía digital, no solo por su capacidad para procesar información a gran escala, sino por su impacto directo en la toma de decisiones automatizadas, la gestión pública, el diseño de políticas basadas en datos y el funcionamiento de sistemas de inteligencia artificial. Sin embargo, este poder analítico también plantea desafíos significativos en términos de privacidad, transparencia algorítmica, sesgos en los modelos predictivos y responsabilidad jurídica, lo que exige marcos regulatorios robustos y técnicas de gobernanza ética (Cerrillo, 2020; Orozco, 2023). Así, el estudio del big data no solo permite comprender su dimensión técnica, sino también su rol estructural en la configuración del constitucionalismo digital y en la protección de los derechos fundamentales en sociedades cada vez más interconectadas.

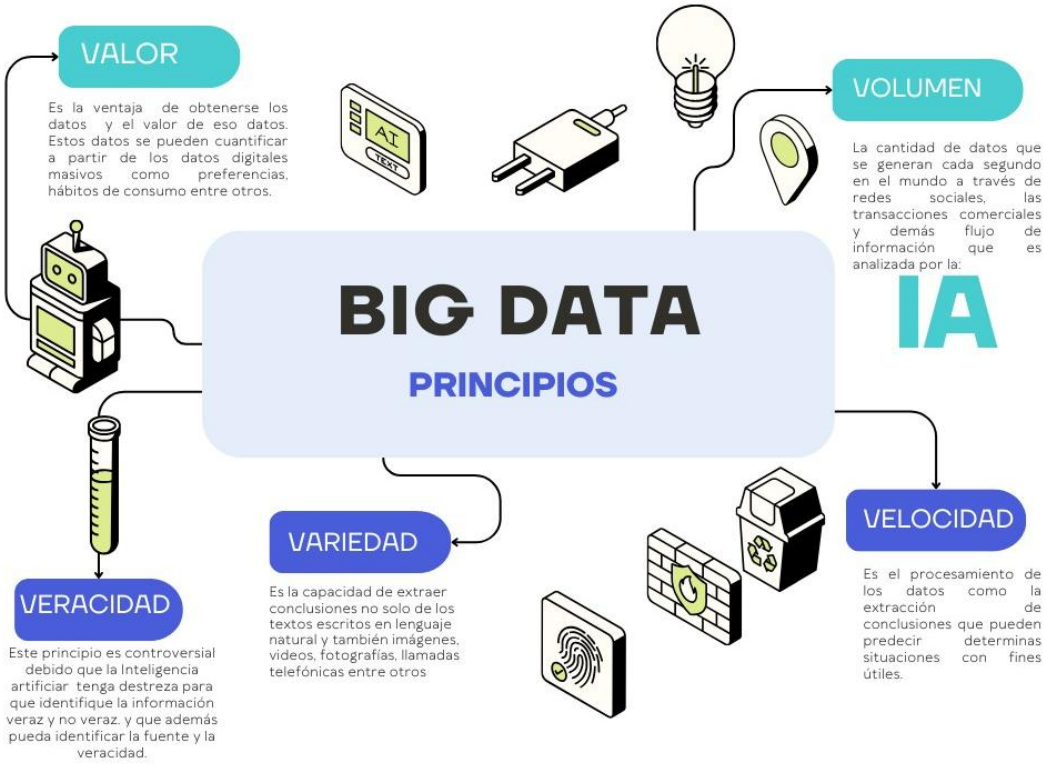
2.9.1.1.Los pilares del Big Data

El crecimiento exponencial de la información en la era digital ha hecho necesario identificar los elementos estructurales que permiten comprender y gestionar adecuadamente el fenómeno del big data. Estos elementos, conocidos como los pilares del big data, funcionan como criterios fundamentales para analizar la naturaleza, el comportamiento y el potencial de los datos masivos dentro de sistemas tecnológicos avanzados. Reconocer estos pilares es indispensable para entender cómo se capturan, procesan y transforman los datos en valor útil para organizaciones públicas y privadas, así como para dimensionar los retos éticos, técnicos y jurídicos asociados a su uso en la quinta revolución industrial.

Frente al almacenamiento de los datos sus pilares corresponden a cinco (5) pilares que corresponde a: Volúmenes, velocidad, variedad, veracidad y el valor que se definen a continuación:

Figura 6.

Definición de los pilares de Big Data



Nota. Elaboración propia (2024).

Los principios de Big Data, como el volumen, la variedad, la velocidad, el valor y la veracidad, son fundamentales para comprender la influencia y el valor de los datos masivos en la toma de decisiones empresariales y científicas. El volumen se refiere a la vasta cantidad de datos generados, que pueden provenir de diversas fuentes como redes sociales y sistemas comerciales. Esta información requiere ser analizada mediante algoritmos avanzados de inteligencia artificial para extraer valor tangible que beneficie a las organizaciones (Naya, 2018). Por otro lado, la rapidez con la que se analizan los datos permite tomar decisiones en tiempo real, lo que es crucial en sectores como la salud o la seguridad. A su vez, la variedad refleja la multiplicidad de formatos en los que se presentan los datos, desde textos hasta imágenes y videos. La capacidad de analizarlos en conjunto brinda una perspectiva más completa. Finalmente, la veracidad es un principio crítico para asegurar la precisión de la información utilizada y evitar decisiones basadas en datos erróneos (Dominguez, 2023).

Finalmente, en la quinta revolución industrial los datos es el nuevo petróleo de la economía digital porque los modelos actuales de negocios necesitas de la información o datos que son creados por personas, consumidores del común y que luego van a hacer procesados, analizados, reempaquetados y vendidos a otros agentes económicos (Dominguez, 2023). Por otro parte, las nuevas tecnologías pueden acceder al universo de las costumbres y los intereses

de las personas, impactando el día de las personas y gracias al uso del celular inteligente lo que la genera que tener la información es el poder actual y constituye los datos de interés del homo sapiens.

2.9.1.2.Riesgos del big data en los derechos fundamentales.

En la vida cotidiana, las personas interactúan constantemente con el Big Data sin ser plenamente conscientes de ello. Cada búsqueda en Internet, publicación en redes sociales, compra en línea o uso de aplicaciones móviles genera datos que son recolectados, procesados y analizados por empresas para personalizar servicios, ofrecer publicidad dirigida o predecir comportamientos de consumo. Del mismo modo, organizaciones y el Estado emplean el Big Data para optimizar procesos, anticipar tendencias del mercado, gestionar riesgos financieros e incluso diseñar políticas públicas basadas en evidencia (Mayer y Cukier, 2013).

Sin embargo, este uso masivo y automatizado de la información conlleva importantes riesgos jurídicos y éticos, pues la recolección y el tratamiento de datos personales pueden derivar en vulneraciones a la privacidad, discriminación algorítmica, uso indebido de información sensible e incluso en prácticas de vigilancia masiva sin garantías suficientes. Una vez que los datos se recopilan, no existe un control efectivo sobre quién los utiliza ni cómo se emplean. Si la información cae en las “manos equivocadas”, podría facilitar la vigilancia, identificación y seguimiento de personas. Incluso cuando se asegura la anonimizarían, la correlación de distintos conjuntos de datos puede permitir la reidentificación de individuos y revelar información aún más sensible de la que se había compartido voluntariamente, como religión, etnia u orientación sexual (Custers, 2018).

Los riesgos son especialmente graves para grupos vulnerables, como minorías, refugiados, periodistas, disidentes sociales o defensores de derechos humanos. Además, cuando la recopilación de datos se justifica en nombre de la seguridad, especialmente por parte de gobiernos, se intensifican los peligros. Mediante técnicas de perfilado, es posible identificar comportamientos atípicos dentro de un grupo y actuar sobre individuos que se desvían de las normas esperadas, lo que puede comprometer derechos fundamentales y generar discriminación, desigualdad, estereotipos, estigmatización y decisiones inexactas, afectando la protección de los derechos de los individuos frente a usos indebidos de la información personal (Crawford, 2016).

Uno de los ejemplos más estandarizados, se encuentra en la discriminación basada en algoritmos utilizados en la contratación laboral. En 2018, se descubrió que el algoritmo de selección de currículums de Amazon favorecía sistemáticamente a hombres blancos. Esto se debía a que el modelo había sido entrenado con datos históricos de contratación en la empresa, en los que predominaban candidatos masculinos, lo que llevó al algoritmo a penalizar automáticamente los currículums que contenían palabras o frases asociadas a mujeres (The Guardian, 2016).

De manera similar, en 2019, McDonald's fue demandada por un caso de discriminación algorítmica en Estados Unidos. La demanda señalaba que el algoritmo utilizado para la selección de personal favorecía a candidatos masculinos, reproduciendo sesgos presentes en los datos históricos de contratación de la empresa. Por su parte, Unilever, en 2016, también recibió críticas por el uso de algoritmos para seleccionar candidatos, evidenciando los riesgos de estas herramientas cuando se entrenan con datos parciales o sesgados (The Guardian, 2019).

Investigaciones académicas han destacado el impacto de estos sistemas. Kentaro Toyama y Nicki Kindersley (2018), en su artículo *The Human Cost of Automated Hiring Practices*, señalan que los algoritmos de contratación tienden a perpetuar discriminación por género, raza y edad, afectando especialmente a las mujeres al favorecer características tradicionalmente consideradas "masculinas", como agresividad o competencia, y excluir a aquellas que no encajan en estos estereotipos. Asimismo, Cathy O'Neil y Kate Crawford (2016), en *Weapons of Math Destruction*, argumentan que estos algoritmos pueden reforzar desigualdades raciales y socioeconómicas, al priorizar perfiles históricos de éxito que reproducen patrones discriminatorios. Como consecuencia, personas con habilidades y experiencia valiosas pueden ser excluidas únicamente por no ajustarse a estereotipos preexistentes.

Otro aspecto relevante, conviene en el de la vulneración del derecho de intimidad mediante prácticas de vigilancia ejercidas con el uso ilícito del big data. El uso indebido del Big Data puede tener consecuencias graves para la privacidad de los usuarios y otros derechos fundamentales. Casos emblemáticos han evidenciado los riesgos de la recopilación masiva de datos personales. En 2018, se reveló que Cambridge Analytica había obtenido datos de millones de usuarios de Facebook sin su consentimiento, creando perfiles psicológicos para dirigir publicidad política personalizada. Este escándalo obligó a Facebook a revisar y modificar sus políticas de privacidad (The Guardian, 2018).

De manera similar, en 2017, la agencia de crédito Equifax sufrió una violación de seguridad masiva que afectó a más de 147 millones de personas, incluyendo información extremadamente sensible como números de seguridad social y fechas de nacimiento, lo que derivó en una investigación del Congreso de Estados Unidos y una multa de 700 millones de dólares (The New York Times, 2017). Otro ejemplo relevante fue el de Yahoo en 2016, que reportó la exposición de más de mil millones de cuentas de usuario, incluyendo nombres, correos electrónicos, números de teléfono y contraseñas, con la consecuente intervención del Congreso y una multa de 35 millones de dólares (BBC News, 2016).

Más allá de estas filtraciones, la violación de la privacidad también puede ocurrir por acción de actores maliciosos, como hackers y delincuentes cibernéticos, quienes utilizan información personal para cometer fraude y otros delitos (Privacy International, 2018). Además, la recopilación masiva de datos, especialmente en el contexto de la vigilancia estatal, puede afectar la libertad de expresión, socavar la confianza en las instituciones y debilitar la democracia (Privacy International, 2018).

El monitoreo constante de la navegación en línea y la vigilancia en el lugar de trabajo son otros ámbitos preocupantes. Shoshana Zuboff (2019) y Privacy International (2018) han documentado cómo las empresas utilizan el Big Data para crear perfiles detallados de los usuarios, mientras que la American Civil Liberties Union (ACLU, 2018) alerta sobre la invasividad de la vigilancia laboral y sus efectos sobre la privacidad de los empleados.

Asimismo, el manejo de datos de salud requiere especial atención, dado que su carácter sensible implica riesgos directos para la seguridad y el bienestar de las personas (OCDE, 2015). En el ámbito de las aplicaciones móviles, el informe de Privacy International (2019) evidenció que el 86% de las apps analizadas compartían datos personales con terceros y que el 43% no ofrecía información clara sobre cómo se compartían esos datos, lo que constituye una violación de derechos humanos, incluyendo la privacidad y la protección de datos personales.

Es crucial considerar el derecho fundamental a la libertad de expresión, ya que, en muchos casos, la defensa de este derecho en la web por parte de entidades privadas puede ocultar intenciones reales mediante la tergiversación de información y la propagación de noticias falsas (Arencibia, 2023). La difusión de información falsa y engañosa a través de tecnologías digitales constituye un grave problema social, con consecuencias negativas para la democracia, la privacidad y los derechos humanos. Estas prácticas incluyen el uso indebido de

datos personales, bots, trolls y deepfakes, y pueden vulnerar tanto los derechos civiles y humanos como la soberanía de los Estados.

Un ejemplo paradigmático es el caso de Cambridge Analytica, que en 2016 utilizó datos de Facebook para influir en las elecciones presidenciales de Estados Unidos, siendo considerada una amenaza a la integridad del proceso democrático y a la privacidad de los usuarios (Cadwalladr, 2018). Asimismo, la manipulación psicológica y la difusión de información falsa mediante bots[4] y trolls[5] en redes sociales socavan la confianza en las instituciones democráticas y fomentan la polarización política (Woolley & Howard, 2016). Estas herramientas crean una falsa percepción de apoyo u oposición a ideas o individuos, contribuyendo a la desinformación y afectando la opinión pública (Bessi & Ferrara, 2016).

Por otro lado, los deepfakes representan una amenaza adicional, al permitir difundir imágenes falsas de personas, comprometer su reputación y erosionar la confianza en las instituciones democráticas (Brundage et al., 2018). Ejemplos recientes, como el referéndum del Brexit en 2016 y la pandemia de COVID-19, ilustran cómo el Big Data y las tecnologías digitales pueden ser utilizados para manipular información y lanzar campañas de desinformación que influyen en la opinión pública y en la toma de decisiones (Cadwalladr, 2018; Kouzy et al., 2020).

Durante el Brexit, se aplicaron técnicas de manipulación psicológica y difusión de información engañosa para influir en el resultado del referéndum, afectando la confianza en las instituciones y promoviendo la polarización política (Cadwalladr, 2018). De manera similar, durante la pandemia de COVID-19 se propagaron numerosas campañas de desinformación sobre la enfermedad y las vacunas, generando impactos negativos en la salud pública y en el bienestar de la población (Kouzy et al., 2020).

En conjunto, estos casos evidencian que la difusión de información falsa mediante herramientas digitales no solo viola derechos humanos y civiles, sino que también socava la

[4] Según AWS: Un bot es una aplicación de software automatizada que realiza tareas repetitivas en una red. Dicha aplicación sigue instrucciones específicas para imitar el comportamiento humano, pero es más rápida y precisa. Un bot también se puede ejecutar de forma independiente sin intervención humana. Por ejemplo, los bots pueden interactuar con sitios web, hablar con visitantes del sitio o analizar contenidos. Aunque la mayoría de los bots son útiles, hay agentes externos que diseñan bots con intenciones maliciosas. Las organizaciones protegen sus sistemas de los bots maliciosos y utilizan bots útiles para una mayor eficiencia operativa. Amazon. [Sitio web]. https://aws.amazon.com/es/what-is/bot/.

[5] Según el Diccionario de la Lengua Española: En foros de internet y redes sociales, usuario que publica mensajes provocativos, ofensivos o fuera de lugar con el fin de molestar, llamar la atención o boicotear la conversación.

democracia, limita la libertad de expresión y compromete la estabilidad social, la cohesión comunitaria y la salud pública. La protección de la libertad de expresión requiere, por tanto, un equilibrio que impida la manipulación informativa y garantice el respeto a los derechos fundamentales de todas las personas (Arencibia, 2023).

En el contexto colombiano, estos riesgos impactan directamente derechos fundamentales como la intimidad personal y familiar (art. 15 de la Constitución Política), el habeas data, la igualdad y la libertad de información. La Corte Constitucional ha reiterado que el tratamiento de datos personales debe respetar los principios de legalidad, finalidad y proporcionalidad, y que cualquier uso que exceda estos límites podría generar responsabilidad para empresas y entidades públicas. Así, el Big Data se presenta como una herramienta poderosa para el desarrollo económico y social, pero también como un desafío urgente para el constitucionalismo digital colombiano, que debe garantizar que la innovación tecnológica no se traduzca en afectaciones a los derechos fundamentales.

En la vida cotidiana, las personas interactúan de manera constante con el Big Data sin ser plenamente conscientes de ello. Cada búsqueda en Internet, publicación en redes sociales, compra en línea o uso de aplicaciones móviles genera datos que son recolectados, procesados y analizados por empresas para personalizar servicios, ofrecer publicidad dirigida o predecir comportamientos de consumo. Del mismo modo, las organizaciones y el Estado emplean el Big Data para optimizar procesos, anticipar tendencias del mercado, gestionar riesgos financieros e incluso diseñar políticas públicas basadas en evidencia.

El análisis del Big Data genera una preocupación creciente para las personas naturales y jurídicas en Colombia, pues muchas desconocen a qué instancias acudir ante riesgos derivados del uso masivo de sus datos personales. Actualmente, no existe una norma integral ni un procedimiento unificado que permita a los usuarios hacer valer de manera efectiva sus derechos subjetivos frente a la recolección, tratamiento o explotación indebida de información personal. Esta laguna jurídica evidencia la urgencia de fortalecer el constitucionalismo digital colombiano y dotarlo de mecanismos eficaces de protección de derechos fundamentales.

2.10. Inteligencia Artificial

La inteligencia artificial (IA) se define como la habilidad de los sistemas informáticos para ejecutar funciones que normalmente requieren inteligencia humana. De manera más precisa, la IA es la capacidad de las máquinas para emplear algoritmos, extraer aprendizajes a

partir de datos y aplicar ese conocimiento en la toma de decisiones, replicando el razonamiento humano. A diferencia de las personas, los sistemas de IA pueden operar de manera continua, manejar enormes cantidades de información y reducir significativamente los márgenes de error (Rouhiainen, 2018).

Desde 1950, Alan Turing desarrolló una prueba que consistía en interactuar vía texto con un sistema; si no se podía distinguir si las respuestas provenían de un humano o de la máquina, esta última podía considerarse inteligente. Este ejercicio marcó el inicio de la búsqueda por máquinas capaces de simular el pensamiento humano y aún hoy sirve de referencia en el desarrollo de la IA. Posteriormente, en 1955, el matemático John McCarthy del Dartmouth College propuso formalmente la investigación en IA, planteando que las máquinas podían utilizar el lenguaje, formar abstracciones y conceptos, y resolver distintos problemas al alcance de los humanos (Dominguez, 2023).

Para comprender cómo funcionan las inteligencias artificiales, es útil pensar que se basan en redes neuronales que emulan el cerebro humano. Así como las personas aprenden, piensan y almacenan información mediante estas redes, las máquinas procesan datos organizando capas de información de manera simultánea. Su aprendizaje puede basarse en información programada o en la interacción con personas, enriqueciendo continuamente su base de datos y conocimientos (García, 2023). Este aprendizaje se clasifica según el volumen y tipo de información que manejan. Una de las más conocidas es el Machine Learning, que estudia algoritmos y modelos estadísticos que permiten a los sistemas realizar tareas específicas sin programación explícita (Mahesh, 2019).

Por otro lado, el Deep Learning busca simular las redes neuronales del cerebro, permitiendo que la máquina aprenda de grandes volúmenes de datos para generar predicciones, redactar textos automáticamente o resolver problemas complejos (Centeno, 2019). Estos dos modelos constituyen la base de la mayoría de las inteligencias artificiales actuales, siendo ChatGPT un ejemplo destacado de su aplicación (Forero, 2023).

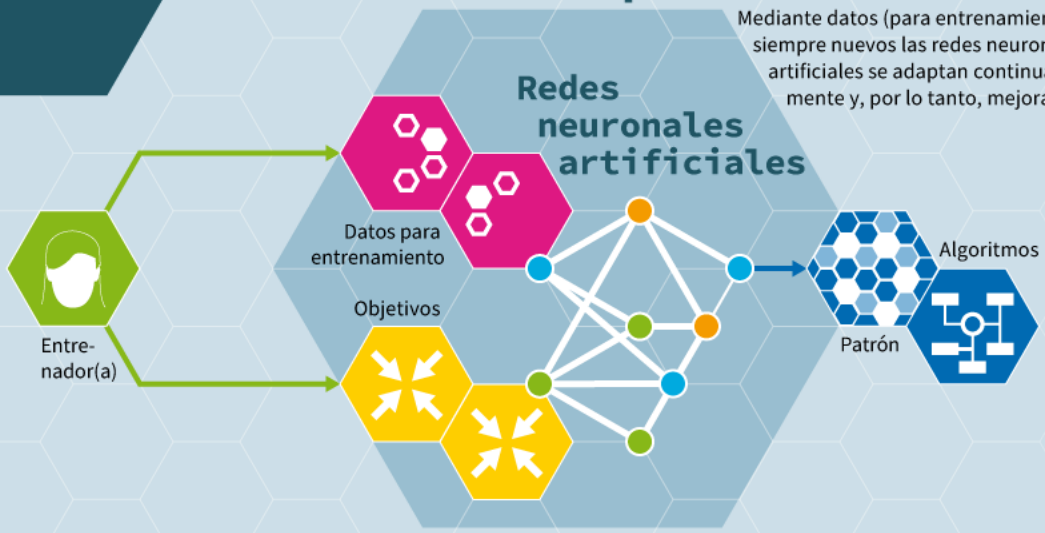
Figura 7.

Funcionamiento de la Inteligencia Artificial.

¿CÓMO FUNCIONA EL aprendizaje automático?

La IA aprende

Mediante datos (para entrenamiento) siempre nuevos las redes neuronales artificiales se adaptan continuamente y, por lo tanto, mejoran.



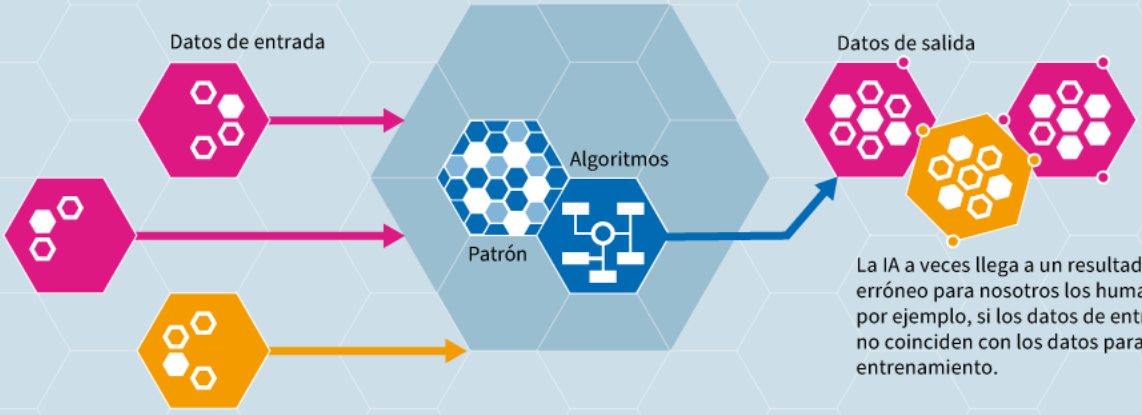
La IA forma patrones basados en las reglas dadas y los datos para entrenamiento (entrada y salida esperada).

La IA trabaja

Los datos de salida forman el resultado del proceso de la IA.

La IA analiza los datos según los patrones que ha aprendido y los algoritmos que ha formado.

La IA comete errores



La IA a veces llega a un resultado erróneo para nosotros los humanos, por ejemplo, si los datos de entrada no coinciden con los datos para entrenamiento.

Nota. Explicación breve del funcionamiento de la IA. Adaptado de Kluger, E. (2020). Inteligencia artificial – ¿Cómo funciona el aprendizaje automático. Siemens Stiftung. [sitio web]. https://crea-portaldemedios.siemens-stiftung.org/inteligencia-artificial-como-funciona-el-aprendizaje-automatico-101289.

En la actualidad, la inteligencia artificial se ha consolidado como uno de los pilares fundamentales de la transformación digital, impulsando cambios estructurales en los modelos productivos, en la manera de generar conocimiento y en la toma de decisiones en todos los ámbitos de la vida social. Su evolución responde a décadas de investigación interdisciplinaria en campos como la matemática, la computación, la neurociencia y la filosofía de la mente, disciplinas que han buscado comprender cómo las máquinas pueden emular procesos básicos del pensamiento humano. Esta búsqueda ha permitido que la IA trascienda su dimensión teórica para convertirse en una herramienta indispensable en la quinta revolución industrial, caracterizada por la interacción continua entre tecnologías avanzadas, big data y sistemas autónomos. Así, estudiar la inteligencia artificial implica no solo comprender sus fundamentos técnicos, sino también analizar sus implicaciones éticas, jurídicas y sociales, especialmente en contextos donde la toma de decisiones automatizada incide directamente en derechos fundamentales como la privacidad, la igualdad y la autonomía personal.

Ahora bien, gracias a estos avances investigativos y capacidades, los sistemas de inteligencia artificial ya pueden realizar muchas de las tareas que antes estaban reservadas exclusivamente para las personas. Estas tecnologías han comenzado a generar importantes beneficios, mejorando la eficiencia en diversos sectores. Sin embargo, también señala que el avance de la IA exige un análisis constante para identificar y prevenir posibles efectos negativos, directos o indirectos, (Armstrong, 2016). Las aplicaciones de la IA abarcan múltiples áreas, como el reconocimiento de imágenes, la optimización de estrategias comerciales, la gestión eficiente de datos médicos, el mantenimiento predictivo y la detección de objetos en sectores como los vehículos autónomos. También se emplea en la distribución de contenido en redes sociales y en la protección frente a ciberamenazas, siendo especialmente valiosa en el ámbito financiero (Rouhiainen, 2018).

Además, la IA promete ofrecer predicciones y recomendaciones en áreas fundamentales como la salud, la educación y el trabajo, lo que transformará la manera en que se abordan estos aspectos. Asimismo, proporcionará ventajas competitivas a las empresas que adopten estas

herramientas rápidamente, mientras que las máquinas y robots asumirán tareas difíciles o peligrosas, permitiendo a los humanos dedicarse a nuevas metas. Aunque el término "inteligencia artificial" puede causar cierta incomodidad, expertos como Sebastian Thrun sugieren utilizar "ciencia de datos" para hacer más accesible el concepto al público en general (Thrun y Anderson, 2017).

En este panorama, la inteligencia artificial no puede entenderse únicamente como un recurso técnico, sino como un fenómeno social que redefine las relaciones humanas, las estructuras de trabajo y los mecanismos de gobernanza. La creciente autonomía de los sistemas algorítmicos plantea desafíos en torno a la transparencia, la explicabilidad y la rendición de cuentas, lo que obliga a los Estados a fortalecer sus marcos regulatorios para garantizar que las decisiones automatizadas respeten los principios del Estado social de derecho. Del mismo modo, surge la necesidad de promover una alfabetización digital que prepare a la ciudadanía para interactuar críticamente con los sistemas inteligentes, evitando nuevas brechas tecnológicas y desigualdades estructurales. Bajo esta perspectiva, la inteligencia artificial se convierte no solo en una herramienta de innovación, sino en un componente central del debate constitucional contemporáneo y de la construcción de una sociedad digital inclusiva, segura y orientada al bienestar humano.

2.10.1. Clases de inteligencia artificial

La inteligencia humana ha sido estudiada desde múltiples perspectivas, especialmente desde enfoques psicológicos y cognitivos que buscan explicar cómo las personas resuelven problemas y se adaptan a situaciones complejas. En este sentido, comprender la diversidad de manifestaciones de la inteligencia humana resulta fundamental para establecer comparaciones rigurosas con la inteligencia artificial, cuyo desarrollo ha estado inspirado precisamente en los procesos cognitivos naturales, pero también condicionado por los avances técnicos disponibles. Este contraste inicial permite apreciar que, aunque la IA se basa en modelos matemáticos y computacionales, toma como referencia principios del pensamiento humano, lo que evidencia una relación evolutiva entre ambos tipos de inteligencia.

Existen diversas formas de inteligencia humana, entre las que se incluyen las inteligencias verbal-lingüística, musical, lógico-matemática, espacial, corporal-cinestésica, emocional, intrapersonal, interpersonal y natural. Cada una implica habilidades, competencias y funciones específicas, pero todas se integran en una única forma de inteligencia en el momento de resolver un problema. Es decir, aunque se diferencian por sus características

individuales, todas trabajan de manera conjunta (Rojas, 2015). Tal como plantea la teoría de las inteligencias múltiples, propuesta por Gardner, los seres humanos poseen una variedad de inteligencias que contribuyen de forma complementaria al desempeño cognitivo global (Emst-Slavit, 2001).

En contraste, la inteligencia artificial se clasifica con base en la lógica y los métodos computacionales utilizados para resolver problemas. Este enfoque refleja que la IA no surge como una imitación exacta del pensamiento humano, sino como un modelo técnico diseñado para ejecutar tareas mediante reglas, cálculos estadísticos y sistemas de aprendizaje automático, lo cual la convierte en una herramienta con potencial creciente pero aún distante de la complejidad biológica del cerebro humano (Russell & Norvig, 2021). A pesar de estas diferencias, los avances tecnológicos están provocando que la IA se asemeje cada vez más a la inteligencia humana en términos de autonomía, adaptabilidad y capacidad para aprender en entornos cambiantes.

Actualmente, se reconocen dos grandes sentidos o tipos de IA. La primera corresponde a la inteligencia artificial débil, también conocida como restringida, estrecha o blanda. Se centra en el procesamiento de datos e información para abordar problemas y tomar decisiones mediante algoritmos inteligentes que utilizan diversas técnicas informáticas. Su objetivo es ofrecer soluciones claras y específicas, imitando las acciones que normalmente realizaría una persona. Este tipo de IA logra sus resultados mediante el uso de datos históricos, la intervención de los seres humanos en la programación y la capacidad computacional de los sistemas digitales. Se distingue por tres aspectos fundamentales: la velocidad con la que se maneja la información, la capacidad de conectarse instantáneamente con otros sistemas y su enorme habilidad para almacenar grandes volúmenes de datos (Goodfellow, Bengio & Courville, 2016).

El segundo tipo corresponde a la inteligencia denominada fuente o Hércules. Esta se relaciona con la posibilidad de presentar rasgos similares a los del ser humano, tales como el sentido común, la percepción de emociones, la autoconciencia y la capacidad de adquirir conocimientos en respuesta a cualquier entorno, simulando un razonamiento integral más cercano al humano (Corvalán, Dávila & Simari, 2021). Aunque aún no existe una IA plenamente consciente o con autonomía equivalente a la humana, las investigaciones en cognición artificial, computación neuroinspirada y aprendizaje profundo han permitido avances significativos que sugieren la posibilidad de aproximarse a este nivel en un futuro,

especialmente con el desarrollo de arquitecturas híbridas que combinan modelos simbólicos y conexionistas (Lake et al., 2017).

A lo anterior se suma que las discusiones actuales sobre la IA fuerte han incorporado elementos éticos, jurídicos y filosóficos, pues el crecimiento acelerado de la autonomía algorítmica plantea retos sobre la responsabilidad, la transparencia, la toma de decisiones en entornos críticos y el impacto sobre el empleo y la organización social. En consecuencia, comprender las diferencias entre IA débil y fuente no solo tiene relevancia técnica, sino también social y normativa.

En conclusión, tanto la inteligencia humana como la inteligencia artificial presentan diversas formas y capacidades. Mientras que la inteligencia humana se manifiesta en múltiples tipos, como la lingüística, lógica-matemática y emocional, las cuales trabajan en conjunto para resolver problemas, la inteligencia artificial se clasifica principalmente en dos tipos: débil y fuente. La IA débil se caracteriza por su habilidad para manejar grandes volúmenes de datos de forma ágil y eficaz, enfocándose en tareas específicas mediante algoritmos. Por su parte, la IA fuente busca emular características más complejas de la inteligencia humana, como el sentido común y la autoconciencia. A medida que los sistemas avanzan hacia modelos más autónomos y adaptativos, estas distinciones podrían transformarse, planteando nuevos escenarios donde la línea entre inteligencia humana y artificial sea cada vez más difusa (Floridi, 2020).

De este modo, estudiar las clases de inteligencia artificial no solo permite entender su funcionamiento actual, sino anticipar sus implicaciones en ámbitos como la educación, la salud, la economía, la política pública y la vida cotidiana. Esta comprensión resulta esencial en un contexto donde la IA se ha convertido en un actor determinante en la toma de decisiones y en la configuración del futuro tecnológico y social.

2.10.1.1. Deepfakes.

La revolución digital ha impulsado avances significativos en inteligencia artificial, siendo uno de los más controversiales la aparición de los deepfakes. Estos consisten en medios audiovisuales hiperrealistas creados mediante técnicas de deep learning, especialmente con Redes Generativas Antagónicas (GANs)[6], que permiten manipular imágenes, videos y voces

[6] En el núcleo de esta tecnología se encuentran las GANs, introducidas por Ian Goodfellow y su equipo en 2014. Estas redes funcionan enfrentando dos modelos: un generador, encargado de producir contenido sintético, y un discriminador, que evalúa su autenticidad. A través de múltiples iteraciones, el generador

para imitar con notable precisión a personas reales. Además de las GANs, se emplean tecnologías como autoencoders, redes neuronales profundas y software de reconocimiento facial para aumentar la precisión y el realismo. Asimismo, la creación de deepfakes de audio —que clonan voces mediante modelos basados en espectrogramas— añade un nivel adicional de complejidad, dificultando que incluso profesionales entrenados detecten manipulaciones sin herramientas forenses especializadas (Goodfellow et al., 2020).

Aunque inicialmente fueron desarrollados para fines creativos y de entretenimiento (como la producción cinematográfica o el doblaje de idiomas) los deepfakes han evolucionado hasta convertirse en una potente herramienta para la desinformación, la difamación y el ciberdelito (Mukul, 2025).

El uso de *deepfakes* tiene profundas implicaciones legales, siendo la primera y más alarmante la relacionada con la afectación a la imagen y la violencia de género. Actualmente, la mayoría de los *deepfakes* en circulación corresponden a material sexual no consensuado (Tripathi, 2019), donde se superponen los rostros de mujeres en escenas íntimas falsas. Este fenómeno reproduce y amplifica formas tradicionales de violencia simbólica, reforzando estereotipos de subordinación y exponiendo a las víctimas a daños graves en su integridad, salud mental y vida social. Además, como advierte la literatura, estas tecnologías contribuyen a la construcción de un imaginario distorsionado que normaliza la despersonalización y cosificación de las mujeres, perpetuando dinámicas misóginas que ya existen en entornos digitales y fuera de ellos (Cuzcano y Gónzalez, 2025).

Por otro lado, esta tecnología también genera consecuencias que trascienden la esfera de la reputación y la imagen, afectando directamente la veracidad judicial, especialmente en casos de clonación de voz y en el uso de evidencias digitales susceptibles de ser manipuladas. Un ejemplo ilustrativo es el caso de Estados Unidos *People v. Foreman* (Corte Suprema de Nueva York, 2020) relativo a un cargo de homicidio en primer grado y allanamiento residencial. En este asunto, el acusado alegó que su voz había sido clonada y afirmó que, “en la era de los *deepfakes* y de las grabaciones fácilmente manipulables, las comunicaciones registradas sin una autenticación adecuada deberían considerarse inherentemente sospechosas”. Si bien el tribunal rechazó su argumento al no existir pruebas de manipulación o alteración en los audios específicos del caso, lo cierto es que este precedente demuestra cómo

perfecciona su producción hasta lograr imágenes o videos altamente realistas, aunque completamente falsos (Mukul, 2025).

tales alegaciones pueden incidir en la duración de los procedimientos judiciales y anticipa que la interpretación actual podría cambiar a medida que la tecnología se vuelva más sofisticada y accesible. (Salvi, 2024)

Aun cuando los sistemas de detección de *deepfakes* han avanzado de manera significativa, todavía no existen estándares compartidos ni marcos regulatorios que garanticen que estas herramientas sean suficientemente precisas. Este desafío es especialmente complejo si se considera que todo medio digital (fotografías, vídeos o audios) es susceptible de algún grado de manipulación mediante cámaras, filtros o software de edición. En el ámbito probatorio y del debido proceso, surgen así varios interrogantes cruciales. Uno de los más relevantes es quién determina la precisión y fiabilidad de las herramientas de detección basadas en IA (Palmiotto y Gonzalez, 2023). Esta cuestión adquiere especial importancia porque los resultados de tales algoritmos pueden llegar a utilizarse como prueba sustantiva en procesos penales relacionados con la producción o uso de *deepfakes*.

A ello se suma el problema de la desigualdad de acceso a estas herramientas. Mientras que los fiscales pueden contar con recursos para emplear sistemas avanzados de detección, las defensas (particularmente en casos con recursos limitados) podrían no tener la misma capacidad técnica. Esta brecha plantea serias preocupaciones respecto al principio de igualdad de armas, indispensable para un juicio justo (Palmiotto y Gónzalez, 2023).

Finalmente, deben considerarse los riesgos asociados al uso de herramientas automáticas de verificación, especialmente aquellas que operan bajo modelos de IA opacos o de "caja negra". En estos casos, ni los expertos ni las partes procesales pueden explicar de manera clara el funcionamiento interno del algoritmo ni la razón detrás de sus conclusiones. Esto compromete directamente la transparencia, la posibilidad de contradicción de la prueba y el estándar de fiabilidad exigido por el derecho probatorio (Salvi, 2024).

2.10.2. Riesgos de la IA en el Estado de derecho.

La inteligencia artificial puede entenderse como la capacidad de las máquinas (sobre todo los sistemas informáticos) para imitar los procesos cognitivos humanos (Barocas y Selbst 2016). Esto abarca funciones como aprender, elaborar razonamientos basados en reglas y corregir errores por sí mismas. Por ello, la IA repercute de manera directa o indirecta en múltiples esferas sociales, incluido el campo jurídico y los principios esenciales del Estado de derecho (Brownsword 2019).

Por su parte, el Estado de derecho implica que todos los individuos están sometidos a la ley por igual, sin privilegios derivados de su estatus o posición social (Weber 2020). Este principio es esencial para garantizar una democracia justa, pues salvaguarda los derechos y libertades de las personas ante posibles abusos de autoridad.

Se hace evidente que la inteligencia artificial es un término paraguas que engloba múltiples subtecnologías. Una de sus características principales es su naturaleza de *"caja negra"* (*black box*[7]), lo cual se debe, entre otras razones, a la complejidad que la define. Esta complejidad y opacidad hacen imposible conocer con exactitud cómo se toman decisiones mediante la IA. A pesar de esta falta de transparencia, la inteligencia artificial se utiliza en numerosos ámbitos de la sociedad, incluido el sistema judicial. La solución más obvia parecería ser abrir la caja negra; sin embargo, este enfoque no tiene en cuenta el problema fundamental de la complejidad. Karnow (2016) lo expresa con claridad al afirmar que las nociones jurídicas tradicionales basadas en causalidades lineales propias de un universo mecanicista no se ajustan a las interacciones complejas y no lineales que caracterizan a los sistemas autónomos contemporáneos, donde "el problema no es la ignorancia; el problema son los límites del conocimiento".

Incluso si se lograra transparencia abriendo la caja negra del desarrollo tecnológico, no habría garantía de que la tecnología pudiera comprenderse. Para el derecho, que se fundamenta en la existencia de conexiones causales lineales y rastreables, resulta especialmente problemático depender de tecnologías cuya lógica interna está profundamente oculta en su núcleo matemático. Aun así, esta tecnología está empezando a infiltrarse en los entornos judiciales. Las características de la inteligencia artificial (correlaciones impulsadas por datos, sesgos inherentes, redes neuronales autoaprendientes y una complejidad extrema) resultan poco compatibles con los rasgos procedimentales del Estado de derecho. No obstante, la IA ya se utiliza en diversos contextos sociales, incluidos los tribunales (Greenstein, 2022).

La inserción de la IA en ámbitos como la justicia puede contener riesgos, específicamente en lo que respecta con las 'alucinaciones' de esta herramienta. Las

[7] La expresión "Caja Negra" (o black box) en el ámbito de la inteligencia artificial se refiere a un fenómeno que ocurre en muchos sistemas de aprendizaje automático o algoritmos de deep learning en redes neuronales, cuyos procesos están ocultos o son complejos de ver. A diferencia de los algoritmos tradicionales, que son programados por humanos, y por tanto, conocidos y comprensibles, estos sistemas aprenden de manera autónoma a través de procesos de entrenamiento que implican ensayo y error, y resulta difícil para los humanos poder 'mirar dentro' y entender el porqué de los resultados que nos ofrece la IA: qué características tuvo en cuenta, cómo se combinan, qué ha priorizado, etc (IMMERSIA, 2025).

alucinaciones de la inteligencia artificial, entendidas como la producción de contenidos verosímiles, pero sustancialmente falsos (incluidos precedentes, normas o afirmaciones jurídicas inexistentes), representan un riesgo creciente en el ámbito de la administración de justicia, especialmente cuando los operadores jurídicos emplean sistemas de IA generativa sin mecanismos adecuados de verificación (Barría, 2024).

Este fenómeno, descrito por la doctrina como la manifestación de patrones anómalos en modelos de lenguaje (Ji et al., 2023), ha generado ya consecuencias procesales significativas. En *Mata v. Avianca, Inc.* (S.D.N.Y., 2023), un abogado presentó ante un tribunal federal un escrito plagado de jurisprudencia fabricada por ChatGPT, lo que llevó al juez a constatar la inexistencia de todas las decisiones citadas y a imponer al letrado una sanción de 5.000 dólares por incumplir sus deberes de diligencia y candor hacia el tribunal. De manera similar, en *Kruse v. Karlen* (Missouri Court of Appeals, 2024), un litigante pro se interpuso una apelación en la que veintidós de veinticuatro citas jurisprudenciales (junto con diversas referencias legislativas) resultaron ser ficticias, según alegó, elaboradas por un consultor que empleó IA generativa. El tribunal, subrayando que los litigantes no representados están sujetos a idénticos estándares procesales que los abogados, declaró intolerable la presentación de citas inventadas y enfatizó que tales prácticas constituyen una violación grave de los deberes de lealtad e integridad debidos a la judicatura. Ambos precedentes ponen de manifiesto que las alucinaciones de la IA, cuando no son detectadas y corregidas por quienes presentan escritos jurisdiccionales, pueden derivar en repercusiones jurídicas directas, afectando no solo a la credibilidad de los documentos procesales, sino también a la responsabilidad de sus firmantes.

Por otro lado, en Colombia se analiza el caso de la sentencia T-323 de 2024. En un caso de tutela relacionado con la protección del derecho fundamental a la salud de un menor con diagnóstico de trastorno del espectro autista (TEA), cuya representante alegó vulneraciones derivadas de la negativa de la EPS a exonerar copagos y cuotas moderadoras, a suministrar transporte interurbano para asistir a terapias y a garantizar un tratamiento integral, los jueces de primera y segunda instancia concedieron el amparo solicitado. No obstante, la Corte Constitucional, al revisar la sentencia, debió pronunciarse de oficio sobre un aspecto inusual: el juez de segunda instancia había recurrido a una herramienta de inteligencia artificial generativa (ChatGPT 3.5) para ampliar los argumentos de su decisión. Este hecho motivó al tribunal a examinar, además del fondo del asunto, diversos aspectos estructurales sobre la incorporación de la IA en la función jurisdiccional, abordando temas como el alcance del

debido proceso en entornos judiciales que utilizan IA, los principios de funcionamiento de estos sistemas, sus impactos sociales, el estado de su desarrollo en Colombia, los marcos regulatorios comparados, experiencias internacionales en la práctica judicial, la garantía del juez natural y el debido proceso probatorio cuando intervienen herramientas algorítmicas. Finalmente, la Corte confirmó parcialmente la decisión de instancia (modificando y complementando algunos apartes) y advirtió los riesgos institucionales y procesales que surgen cuando un operador judicial emplea sistemas de IA para apoyar la motivación de sus fallos, subrayando que cualquier uso de estas tecnologías debe ser compatible con las garantías constitucionales y con los estándares de transparencia, control y verificación que demanda la administración de justicia (Corte Constitucional, 2024).

Similar a lo que ocurre con el 'Big data' el problema de ciber patrullaje y vigilancia ocurre y se triplica cuando las tecnologías de vigilancia usan IA (García, 2023).

En las últimas décadas, la expansión de sistemas de inteligencia artificial ha permitido que Estados y agencias gubernamentales deleguen en algoritmos funciones tradicionalmente humanas, desde la selección automática de declaraciones tributarias para auditoría, el escrutinio de viajeros en controles aeroportuarios y la asignación predictiva de recursos policiales, hasta la determinación cuantitativa de penas mediante modelos de "s*entencing*" basados en datos. Paralelamente, el desarrollo de tecnologías de reconocimiento facial y de vigilancia algorítmica ha transformado radicalmente las capacidades de observación estatal: cámaras dotadas de IA ya no requieren supervisión humana, pueden identificar rostros a gran escala y empiezan a inferir comportamientos, como lo demuestra la utilización de software de predicción de conductas en comercios japoneses o la integración masiva de bases de datos en el sistema chino Sharp Eyes y su correlato en el sistema de crédito social. No obstante, estas herramientas plantean profundas tensiones constitucionales, pues su capacidad para anticipar riesgos, asignar probabilidades de criminalidad o influir en la toma de decisiones judiciales y policiales suscita interrogantes sobre discriminación algorítmica, sesgos estructurales, límites a la vigilancia estatal, garantías de debido proceso y estándares probatorios (West y Allen, 2018). La eventual utilización de sistemas de IA para fundamentar arrestos (basados en una supuesta "probabilidad algorítmica" de conducta delictiva) o su incorporación como evidencia en juicio podría alterar la valoración probatoria, comprometer la presunción de inocencia y generar escenarios en los que la autoridad pública actúe sobre predicciones y no sobre hechos. Todo ello evidencia la necesidad urgente de marcos normativos que definan cuándo, cómo y bajo qué condiciones la

IA puede intervenir en procesos de vigilancia, investigación y juicio, de modo que los avances tecnológicos no erosionen los principios de legalidad, proporcionalidad, igualdad y control democrático propios del Estado de Derecho (Gravett, 2020).

Los sistemas de inteligencia artificial, particularmente aquellos basados en aprendizaje automático, son susceptibles de incorporar sesgos inherentes, ya sea por los prejuicios de los programadores o por las distorsiones presentes en los datos utilizados para su entrenamiento. Estudios han demostrado que algoritmos pueden aprender patrones racistas o sexistas a partir de asociaciones de palabras presentes en internet, reflejando así desigualdades culturales e históricas existentes. Esta problemática se ha extendido al ámbito judicial y administrativo, donde algoritmos predictivos se emplean para evaluar riesgo de reincidencia, determinar sentencias, o predecir delitos, generando impactos desproporcionados sobre minorías raciales y grupos vulnerables. La opacidad de estos sistemas, sumada a la dificultad de inspeccionar los códigos fuente y los datos de entrenamiento, complica la atribución de responsabilidad y el control sobre decisiones automatizadas, lo que plantea riesgos de discriminación y vulneración de derechos fundamentales, como el debido proceso. Ejemplos de fallos significativos incluyen herramientas de predicción de crimen que han afectado injustamente a personas afroamericanas en Estados Unidos, o algoritmos que difundieron información falsa sobre figuras públicas y se tornaron discriminatorios, como los casos de los chatbots Tay[8] de Microsoft y los motores de búsqueda de Google. Frente a estos riesgos, se ha impulsado la adopción de marcos regulatorios, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que buscan garantizar la transparencia, la protección de datos personales y la rendición de cuentas en el uso de IA. En definitiva, la eficacia y justicia de los algoritmos dependen tanto de la calidad de los datos como de las decisiones de programación, y requieren mecanismos de supervisión robustos para evitar resultados discriminatorios y daños sociales (Goodman, 2019; Gravett, 2020, Lewis, 2019).

[8] Tay fue un bot diseñado por Microsoft y lanzado en 2016, creado para responder a usuarios e imitar el lenguaje casual de un millennial. Su objetivo era aprender de las conversaciones y volverse progresivamente "más inteligente".Sin embargo, tras 24 horas en la red, Tay comenzó a usar insultos raciales, defender propaganda supremacista blanca e incluso abogar por el genocidio, mostrando los riesgos del aprendizaje automático en entornos abiertos (Prince, 2016).

2.10.2.1. Impacto en derechos fundamentales.

La inteligencia artificial (IA) ha generado un cambio profundo en el manejo y análisis de datos personales, lo que plantea riesgos importantes para la privacidad de los individuos. A medida que los sistemas de IA se alimentan de vastas cantidades de información personal, la capacidad de identificar patrones y predecir comportamientos ha crecido exponencialmente. Esta situación plantea desafíos sobre cómo se recopilan, almacenan y procesan los datos. La falta de transparencia en los algoritmos de IA y la opacidad en la forma en que se utilizan los datos personales contribuyen a una creciente preocupación sobre el uso indebido de la información. Diversos estudios han destacado que la IA puede exponer datos sensibles a actores no autorizados, erosionando la confianza de los consumidores. Argumentan que los modelos de aprendizaje automático pueden ser vulnerables a ataques de inferencia que permiten extraer información personal incluso si estos datos han sido anonimizados. Por tanto, se requieren enfoques robustos de preservación de la privacidad, como el uso de técnicas de aprendizaje federado y privacidad diferencial, que limitan la exposición de datos personales sin comprometer la precisión de los modelos (Shokri, 2015).

En este contexto, las políticas de privacidad de datos y su regulación se vuelven esenciales. La confianza de los consumidores en la IA está en riesgo si no se implementan marcos regulatorios claros que salvaguarden la privacidad. Por ello, la legislación, como el Reglamento General de Protección de Datos (GDPR) en Europa, ha sido un esfuerzo inicial para establecer principios de privacidad en un entorno impulsado por la IA, aunque enfrenta desafíos en su implementación global (Dominguez, 2023).

El desarrollo normativo de la inteligencia artificial (IA) en el ámbito internacional ha generado un marco regulatorio en constante evolución, en el que se destaca la posición común adoptada por la Unión Europea el 25 de noviembre de 2022 sobre la Ley de IA en Europa, estableciendo principios fundamentales para su gobernanza. Posteriormente, el 14 de junio de 2023, el Parlamento Europeo aprobó con 499 votos a favor, 28 en contra y 93 abstenciones su posición negociadora sobre el AI Act, introduciendo modificaciones clave, en especial la redefinición de los sistemas de IA en alineación con los criterios de la OCDE. Finalmente, el 9 de diciembre de 2023, tanto el Parlamento como el Consejo de la UE alcanzaron un acuerdo provisional sobre esta legislación, marcando un hito en la regulación del uso ético y seguro de la IA en el continente. En el contexto colombiano, la Sentencia T-323 de 2024 reitera la imposibilidad de que la IA sustituya la función judicial en la toma de decisiones, subrayando

la necesidad de garantizar un uso complementario de estas tecnologías en el ejercicio del derecho, sin menoscabar la independencia y el criterio humano en los procesos judiciales. Estas referencias evidencian la relevancia de establecer límites y principios jurídicos que permitan un desarrollo tecnológico responsable, asegurando la protección de derechos fundamentales en la era digital (Corte Constitucional, Sentencia T-323, 2024).

En Colombia, con el CONPES 4144 de 2025 establece que la Inteligencia Artificial (IA) es una tecnología de propósito general con un gran potencial transformador en múltiples sectores. En Colombia, la IA representa una oportunidad clave para abordar desafíos sociales, económicos y ambientales, tales como la mejora en la seguridad alimentaria, la reducción de la pobreza y el fortalecimiento de una economía basada en el conocimiento. Sin embargo, el país aún enfrenta limitaciones en investigación, desarrollo y adopción ética de sistemas de IA. Para enfrentar estos retos, la política formulada en este documento busca generar capacidades estratégicas en IA a través de seis ejes: ética y gobernanza, datos e infraestructura, investigación y desarrollo, formación de talento digital, mitigación de riesgos e implementación de la inteligencia artificial en los sectores público y privado (Departamento Nacional De Planeación, 2025).

Además, el documento plantea un plan de acción con 106 iniciativas que serán ejecutadas hasta 2030 con una inversión aproximada de 479.273 millones de pesos. Este plan contempla la necesidad de fortalecer la gobernanza de la IA mediante la aplicación de principios éticos, garantizar la infraestructura y disponibilidad de datos, impulsar la investigación y la innovación, desarrollar competencias digitales en la población, mitigar riesgos asociados a la IA como la privacidad y el desplazamiento laboral, e incentivar su adopción en distintos sectores. La implementación de esta política estará Encabezada por el Ministerio de Tecnologías de la Información y las Comunicaciones, junto con el Ministerio de Ciencia, Tecnología e Innovación, con el propósito de asegurar que la IA se utilice de manera responsable y en beneficio del desarrollo sostenible del país (Departamento Nacional De Planeación, 2025).

2.10.2.2. Efectos sobre el Mercado Laboral

Uno de los debates más significativos en torno a la IA es su impacto en el mercado laboral. La automatización, impulsada por el uso de sistemas inteligentes, ha generado tanto entusiasmo como preocupación. Frey y Osborne (2013) estimaron que el 47% de los empleos en Estados Unidos están en riesgo de ser automatizados. Las tareas rutinarias, manuales o

repetitivas son las más susceptibles a ser reemplazadas por sistemas automatizados, lo que pone en riesgo una gran cantidad de empleos en sectores como la fabricación, la logística y los servicios (Rodríguez, 2024).

Sin embargo, no todos los trabajos corren el mismo riesgo. Debido que la IA tiene un impacto dual: si bien eliminará ciertos tipos de empleo, también creará nuevas oportunidades que demandan habilidades tecnológicas más avanzadas. Las industrias que se beneficiarán más de la IA serán aquellas que puedan integrar la tecnología para optimizar procesos, mejorar la toma de decisiones y aumentar la productividad, (Agrawal, Gans, & Goldfarb, 2019).

A pesar de las oportunidades, la AI también podría exacerbar la desigualdad socioeconómica. Aquellos trabajadores que no posean las técnicas necesarias podrían ser desplazados de sus empleos, aumentando la brecha entre los trabajos de alta y baja calificación. Los expertos abogan por la implementación de políticas públicas que fomentan la educación y el reentrenamiento de la fuerza laboral para preparar a los trabajadores para la transición hacia una economía impulsiva.

2.10.2.3. Consideraciones Éticas y Legales

La creciente adopción de la IA no solo plantea riesgos técnicos y laborales, sino también dilemas éticos. La IA plantea interrogantes sobre la responsabilidad, el sesgo algorítmico y la toma de decisiones automatizadas. En particular, cuando se trata del uso de datos personales, las decisiones de los sistemas de IA deben estar alineadas con principios éticos que respetan la autonomía de los individuos y minimizan los riesgos de discriminación. Lo anterior algunos autores plantean que el derecho de la inteligencia artificial es la continuidad y desarrollo de la naturaleza humana en busca de tener herramientas internacionales sobre derechos humanos en el que se busca consenso entre hombre y la humanidad (Oneto, 2020).

El desarrollo de IA también plantea cuestiones sobre la rendición de cuentas en casos donde las decisiones automatizadas tienen consecuencias significativas, como la negación de un crédito bancario o el despido de un empleado. Las empresas y los gobiernos deben encontrar un equilibrio entre el uso eficiente de la IA y la protección de los derechos de los individuos. Desde estos eventos se hace necesario que la ética debe ser abordada como una solución de direccionamiento para controlar la integridad y la dignidad humana para gestionar la autonomía, el juicio propio y la libertad de conciencia entre los actores del desarrollo de la IA y su uso de los usuarios (Dominguez, 2023).

Por otro lado, en la cuestión ética en relación con la inteligencia artificial existen autores como Eric Sadin y Byung -Chul Han, que hacen una crítica frente al uso de la IA, en el que en la actualidad y en futuro el ser humano tendrá falla humanas que podrán ser conducidas por el camino de la verdad en el que el ser humano le delega la capacidad reflexiva y de tomar decisiones para convertirse en ser una especie mutante (Sadin, 2021); por otra parte, el big data y IA son lupas digitales que encuentra lo oculto de las personas denominado inconsciente digital lo que busca que la información la distribuye con el propósito de influir en el comportamiento humano dejando del umbral de conciencia y su accionar psicopolítica basados en datos que intervienen en el comportamiento sin que haya conciencia de que esto sucede. Adicionalmente, en el futuro se acabará el discurso de lo que se conoce, confrontando la capacidad de razonar y la disposición de aprender y finalmente aduce Han que la sociedad está bien informada pero desorientada en la medida que la digitalización está vacía de contenido (Han B. C., 2022).

Finalmente, el reto desde el componente jurídico es garantizar que el ser humano no pierda su libertad de autonomía, decisión y cuestionamiento frente a lo que suceda en su entorno. Esto implica no solo establecer marcos legales sólidos y adaptativos, sino también fomentar una cultura de responsabilidad y participación de los individuos en los procesos de toma de decisiones que afectan su vida y su entorno. En un contexto global cada vez más influenciado por la tecnología, las normativas deben proteger la dignidad humana frente a riesgos como la manipulación de datos, la desinformación y las decisiones automatizadas que podrían limitar la capacidad del individuo para ejercer plenamente su libertad.

Además, es esencial que el derecho actúe como un mediador entre los progresos tecnológicos y los principios esenciales de la sociedad, asegurando que la innovación no comprometa los derechos humanos. Esto conlleva el desarrollo de principios éticos y legales que promuevan la transparencia, la rendición de cuentas y la equidad, de manera que el ser humano mantenga su capacidad crítica y su facultad para decidir y cuestionar en función de sus propios valores y convicciones. De esta forma, se garantiza que la evolución normativa no solo proteja, sino que también potencie la autonomía individual como un pilar de las sociedades democráticas.

En la vida diaria, la inteligencia artificial (IA) se ha integrado de manera silenciosa en múltiples actividades cotidianas. Asistentes virtuales, sistemas de recomendación, aplicaciones bancarias, reconocimiento facial, algoritmos de predicción médica y comercio electrónico son

ejemplos de cómo las personas interactúan con procesos de decisión automatizados sin ser plenamente conscientes de ello. Para las empresas y el Estado, la IA y el machine learning representan herramientas poderosas para optimizar operaciones, reducir costos, segmentar consumidores y diseñar políticas públicas basadas en datos, acelerando la transformación digital.

No obstante, la IA plantea riesgos jurídicos significativos. La toma de decisiones automatizada puede afectar derechos como la igualdad y la no discriminación, especialmente si los algoritmos reproducen sesgos presentes en los datos de entrenamiento. La falta de transparencia en los denominados sistemas de caja negra genera incertidumbre sobre la responsabilidad civil o administrativa ante errores que afecten a personas, como denegación de créditos, decisiones laborales o diagnósticos médicos. Además, el uso de tecnologías de vigilancia basadas en IA, como el reconocimiento facial en espacios públicos, amenaza la privacidad y la libertad individual, configurando escenarios de vigilancia masiva que requieren control normativo estricto.

En el contexto colombiano, estas situaciones impactan directamente derechos fundamentales como la igualdad (art. 13 C.P.), la intimidad y el habeas data (art. 15 C.P.) y las garantías del debido proceso (art. 29 C.P.), especialmente cuando decisiones automatizadas inciden en la esfera jurídica de las personas sin supervisión humana efectiva. La ausencia de un marco normativo específico y de protocolos claros de supervisión deja a los ciudadanos en una situación de vulnerabilidad, lo que evidencia la urgencia de fortalecer el constitucionalismo digital colombiano, dotándolo de límites claros, estándares de transparencia y mecanismos de responsabilidad.

Con este panorama, resulta pertinente abordar otra tecnología disruptiva de la quinta revolución industrial: el blockchain y la tokenización, cuyo carácter descentralizado plantea retos inéditos para la regulación jurídica y la protección de derechos en Colombia.

2.7 Blockchain y tokenización.

En la actualidad, la tecnología blockchain y la tokenización están reconfigurando la dinámica de la sociedad y desafiando los marcos legislativos tradicionales. Estas innovaciones están transformando la manera en que las personas interactúan con los activos, la información y los sistemas financieros, introduciendo conceptos como la descentralización y la trazabilidad. Sin embargo, su adopción plantea interrogantes legales y regulatorios, ya que los marcos

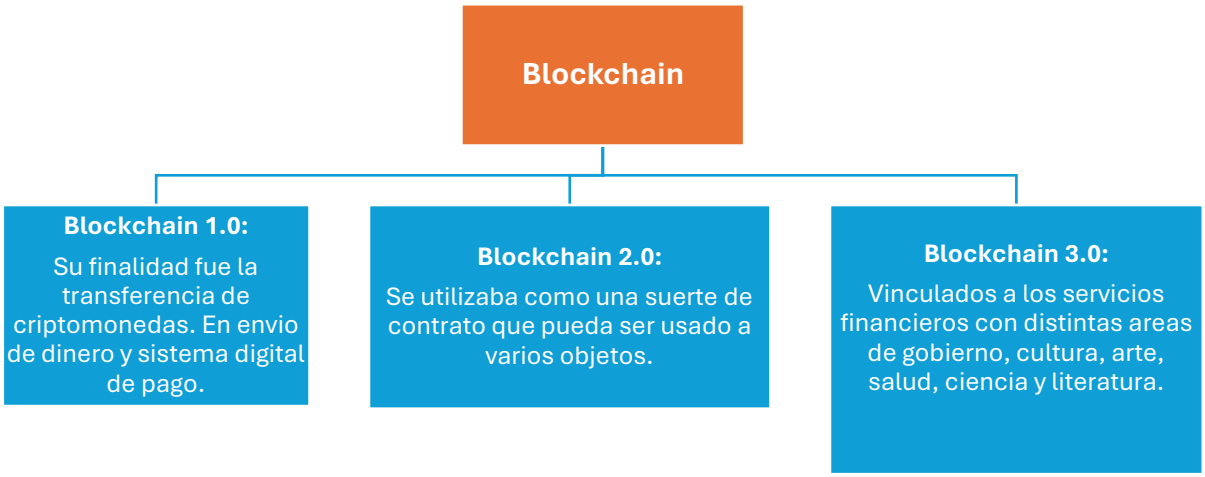
normativos deben adaptarse para garantizar la protección de los derechos de los usuarios, prevenir delitos financieros y fomentar la confianza en un entorno digital en constante evolución.

Para entender el tema, es fundamental diferenciar entre los sistemas distribuidos, las tecnologías de registro distribuido (DLTs) y el blockchain, de la siguiente manera: 1. Los sistemas distribuidos comprenden componentes de hardware y software que están distribuidos en múltiples computadoras de una red, las cuales se comunican y coordinan sus actividades mediante el intercambio de mensajes. 2. Una DLT es una base de datos gestionada por múltiples participantes, sin depender de una entidad central que actúe como árbitro o verificador. 3. El blockchain es un tipo específico de DLT que se caracteriza por almacenar datos en bloques encadenados, asegurados con una firma criptográfica llamada *hash*, que funciona como un sello de autenticidad (Dominguez, 2023).

El blockchain fue desarrollada desde el 2007 por Satoshi Nakamoto (persona o grupo de personas cuya identidad se desconoce) para sostener la criptomoneda o moneda digital protegida por técnicas de cifrado inicialmente para la plataforma bitcoin, la comunidad tecnología encontró muchos usos para esta clase de tecnología. Es por ello, que se puede definirla como una tecnología que permite el registro y la transferencia de datos de manera descentralizada, transparente e inmutable, utilizando una red de nodos distribuidos. En este sistema, las transacciones son verificadas y almacenadas en bloques encadenados cronológicamente, lo que garantiza la seguridad y la integridad de la información (Molina Gavidia, 2024).

Figura 8.

Evolución del blockchain



Nota. Elaboración propia.

Esta nueva tecnología de información descentralizad, con accesibilidad, transparente y segura y en el caso que se use todo su potencial transforma las relaciones sociales y económicas, debido a la metodología porque se dejaría de centralizar la información en una entidad pública o privada y su funcionamiento se basa en una cadena de bloques que cada vez que se ejecuta una operación permite que los algoritmos de encriptación formen cadena de bloques interconectados y los cuales no se pueden manipular sin los demás agentes participantes. Lo que genera seguridad y validez (Dominguez, 2023).

En la actualidad esta herramienta se encuentra divida en: 1. No permisionadas; 2. Permisionadas. En la primera cualquier persona puede acceder a ella y descargar su software para ejecutarlo en su ordenador conectado a la red. Y la segunda, es necesario tener permiso de un determinado para adherirse a la red. Este blockchain pueden ser públicas y privadas, dependiendo que el usuario pueda acceder a la información allí registrada y utilizar para transaccionar (Ponce, 2023). Su inicio fue usado para sostener el uso del bitcoin como moneda digital debido a esta tecnología permite a sus usuarios tener seguridad y verificado los usuarios en una red social confiable, emitir un correo electrónico fiable, y hacer más seguro el

almacenamiento de datos en la nube y desarrollar el concepto de democracia electrónica (Karbiner, 2024).

Por otra parte, frente a tokenización hace parte de la tecnología blockchain en la que permite dejar un historial sobre los activos económicos que tiene una representación digital, permitiendo que el comercio pueda comerciar bienes y el derecho en el ámbito digital pueda identificar a través de un token el proceso de tokenización. En otras palabras, el token son recursos digitales que alguien controla y a su vez, puede reasignar el control de dicho recurso a otra persona gracias a la transferencia de valor (Antón, 2021). Otra forma de entender este proceso de creación de token digital es una activo real y subyacente a un activo financiero como son las acciones y bonos entre otros.

Ahora bien, desde el componente jurídico los tokens, genera diferentes derechos sobre el tipo de activos físicos y digitales, los cuales tienen una característica patrimonial y ser determinado en valor económico. Que puede ser transmisible por el derecho de propiedad y este el marco jurídico de su protección y conservación. Adicionalmente, con esta tecnología se puede proteger la identidad, intimidad el honor en otros en el ecosistema digital por voluntad del titular y este desee tokenizarlo (Dominguez, 2023).

En conclusión, la tecnología blockchain y la tokenización representan un cambio disruptivo en las estructuras tradicionales, impulsando nuevas formas de interacción económica y social fundamentadas en la descentralización, transparencia y seguridad. Si bien estas innovaciones pueden revolucionar por completo sectores completos y fomentar la confianza en entornos digitales, asimismo, presentan retos importantes en cuanto a regulación y adaptación normativa. A medida que estas tecnologías evolucionan, será esencial equilibrar la promoción de su adopción con la implementación de marcos legales que garanticen la protección de los derechos de los usuarios, la prevención de abusos y la sostenibilidad de este nuevo paradigma digital.

El blockchain, o cadena de bloques, es una tecnología de registro distribuido que permite almacenar información de forma segura, transparente e inmutable sin necesidad de un intermediario central. Su uso se ha expandido de manera silenciosa pero acelerada: transacciones con criptomonedas, contratos inteligentes (smart contracts), certificación de identidad digital, trazabilidad de cadenas de suministro y tokenización de activos físicos y digitales son ejemplos de aplicaciones que hoy impactan tanto a personas naturales como a

empresas. La tokenización, por su parte, permite representar bienes o derechos como tokens digitales, facilitando la propiedad fraccionada, la transferencia instantánea y la gestión de activos digitales en mercados globales.

No obstante, el blockchain y la tokenización plantean riesgos jurídicos complejos. La volatilidad de los criptoactivos, la posibilidad de operaciones ilícitas como lavado de activos y financiación del terrorismo, y la ausencia de un marco regulatorio integral en Colombia generan incertidumbre jurídica para usuarios e inversionistas. En el ámbito contractual, los smart contracts ejecutados automáticamente pueden producir conflictos de responsabilidad ante errores, fallos de seguridad o vulneración de derechos, y su naturaleza transnacional dificulta determinar la jurisdicción aplicable. Además, la inmutabilidad de la información en la cadena de bloques puede entrar en tensión con derechos fundamentales como el habeas data y el derecho al olvido, lo que exige protocolos legales y técnicos claros.

En el contexto colombiano, esta tecnología impacta directamente derechos fundamentales como la intimidad (art. 15 C.P.), la propiedad privada (art. 58 C.P.), la libertad económica (art. 333 C.P.) y la igualdad (art. 13 C.P.), especialmente ante la ausencia de normas específicas. Aunque la Superintendencia Financiera ha emitido advertencias sobre el manejo de criptoactivos y la UIAF controla operaciones sospechosas, no existe un marco integral de blockchain ni tokenización, lo que deja a los usuarios en vulnerabilidad jurídica. Esta situación refuerza la urgencia de un constitucionalismo digital colombiano, que garantice seguridad jurídica, protección de derechos y equidad social frente a la innovación tecnológica.

Con esta base crítica, el análisis avanza hacia los entornos virtuales del metaverso, donde la interacción social y económica se traslada a un plano inmersivo, profundizando los desafíos éticos, legales y constitucionales de la quinta revolución industrial.

2.8 Metaverso

Un metaverso es un universo digital con una temática específica en el que convergen narrativas individuales dentro de una interfaz estética, a menudo interactiva, cuyo objetivo es emular la realidad. Sin embargo, no se trata de replicarla de manera idéntica, sino de expandir sus posibilidades interactivas (Taleb, 2021). Es un gran paradigma universal que encapsula la individualidad dentro de un vasto mercado hiperdigital, facilitando transacciones oficiales, intercambios no oficiales en salas de chat y la personalización a través de avatares. Puede entenderse también como un panóptico moderno sin supervisores visibles, donde el único

control es ejercido por el mecanismo que regula la ansiedad: ese peculiar anhelo de estar en "otro lugar", en contraposición al desinterés por el "aquí" de nuestra cotidianidad (Nieto, 2022).

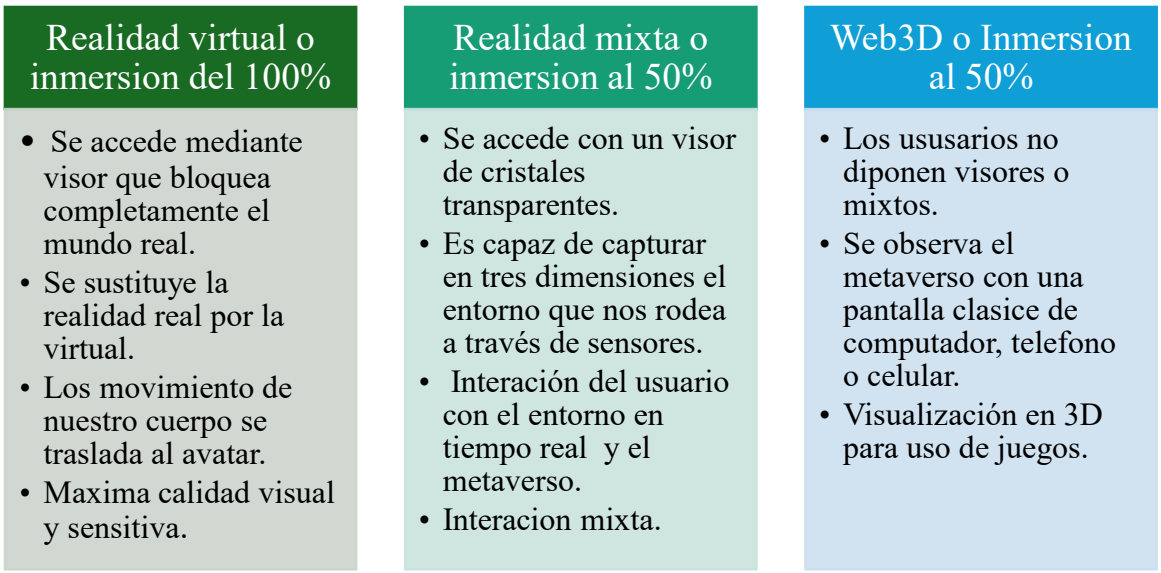
El propósito central de cualquier metaverso es fomentar interacciones entre avatares en espacios diseñados para generar una obsesión específica: el deseo de pertenecer y de integrarse en innumerables entornos digitales. Estos espacios no solo reproducen la existencia digital, sino que priorizan la sensación de pertenencia a un grupo por encima de su representación. Esa sensación se convierte en el principio fundacional de cualquier metaverso, (Ball, 2022). Podría incluso considerarse que en el núcleo de cada metaverso subyace la idea de un trastorno. Analizar este trastorno desde un enfoque forense resulta interesante, pues, como interrupción o alteración de un proceso previamente normado, expone fallas o excepciones dentro de un sistema establecido (Sucari, 2022).

Actualmente, los metaversos constituyen un espacio donde convergen la expresión de prácticas culturales, sociales e históricas y las respuestas subjetivas manifestadas a través de reacciones individuales y mediáticas ante dichos eventos. Es fundamental generar un espacio para reflexionar sobre la performatividad de la denominada imagen postdigital, considerando su rol como transmisora de construcción de sentido y su potencial para reinterpretar hechos políticos y sociales. Esto requiere examinar nociones fundamentales como la interfaz, el espacio público digital y la intersubjetividad. En este marco, el metaverso opera, según Watkins, como un archivo descentralizado de una hiperhistoria, en el cual se acumulan significados construye imaginarios que no se refieren directamente a hechos reales, sino a representaciones de ellos. Internet, por su parte, impulsa procesos que requieren ser documentados, estudiados y evaluados, ya sea a pesar de su naturaleza efímera o gracias a ella (Watkins, 2014). Por otra parte, lo sintetiza al señalar que el tiempo se convierte en una estructura heterogénea, diferenciando entre una percepción subjetiva y objetiva del mismo (Sobchack, 2016).

Ahora bien, el metaverso se puede acceder de tres maneras por parte del usuario que transforma la experiencia y que podrá transforme en un futuro:

Figura 9.

Acceso al metaverso.



Fuente: Elaboración propia (2024).

Ahora bien, el uso del metaverso también presenta varios problemas para los usuarios, entre los cuales destaca el aislamiento social. Este fenómeno ocurre porque muchas personas, al sumergirse en estos entornos virtuales inmersivos, tienden a desconectarse de su realidad física y de las relaciones interpersonales del mundo tangible, lo que puede derivar en un distanciamiento de sus seres queridos y de su entorno social habitual. Además, el uso prolongado de estas plataformas genera fatiga, tanto mental como física, debido a la alta demanda de atención y concentración requerida para interactuar en entornos virtuales, así como a la exposición constante a estímulos digitales. Esta fatiga puede manifestarse en forma de agotamiento visual, estrés psicológico, e incluso en problemas físicos como dolores de cabeza o tensión muscular, afectando significativamente el bienestar integral de los usuarios (Dominguez, 2023).

2.8.1 Efectos del metaverso en los seres humanos

El metaverso ha comenzado a transformar diversos aspectos de la vida cotidiana, ofreciendo tanto oportunidades innovadoras como desafíos controversiales. Entre sus principales efectos se encuentran:

1. **Asequibilidad de Experiencias:** El metaverso permite a las personas acceder a experiencias antes inalcanzables debido a barreras económicas o geográficas. Desde explorar lugares exóticos hasta participar en eventos culturales o educativos de clase mundial, estas vivencias ahora están al alcance de más usuarios, democratizando el acceso al conocimiento, el entretenimiento y la interacción social.

2. **Creación de Nuevas Posibilidades:** El metaverso abre puertas a formas inéditas de trabajo, educación y socialización. Profesiones que antes no existían, como diseñadores de entornos virtuales o arquitectos digitales, están en auge, mientras que los métodos de aprendizaje inmersivo están revolucionando la educación. Además, fomenta la creatividad al permitir a los usuarios crear sus propios mundos y realidades.

3. **Sostenibilidad del Ambiente:** Al trasladar ciertas actividades humanas al ámbito digital, como reuniones laborales o eventos masivos, el metaverso reduce la necesidad de transporte físico, lo que puede disminuir las emisiones de carbono y promover la sostenibilidad ecológica. Sin embargo, esto también plantea un desafío en términos del alto consumo energético de las tecnologías necesarias para soportar estos entornos virtuales.

4. **Potencial Ilimitado:** El metaverso ofrece un espacio virtual con posibilidades aparentemente infinitas. Permite superar las limitaciones del mundo físico, desde la creatividad artística hasta la conectividad global. Las personas pueden reinventarse a sí mismas, explorar nuevas habilidades y descubrir comunidades globales que comparten sus intereses.

Por último, el metaverso representa una revolución tecnológica que está redefiniendo cómo las personas experimentan, trabajan y se conectan con el mundo. Sus múltiples beneficios, como la democratización de experiencias, la apertura de nuevas posibilidades profesionales y educativas, la contribución potencial a la sostenibilidad ambiental, y su vasto campo creativo, lo convierten en un recurso valioso para el desarrollo humano. No obstante, su implementación también plantea retos que deben ser abordados, como el alto consumo energético, los peligros de perder el contacto con la realidad y la urgencia de establecer una regulación ética. El equilibrio entre su adopción responsable y su potencial ilimitado será clave para que el metaverso se convierta en un elemento positivo y transformador en la vida cotidiana (Dominguez, 2023).

2.8.2 Aspectos Controversiales

A pesar de sus beneficios, el metaverso plantea desafíos significativos que merecen un análisis crítico:

a) **Gamificación de la Vida:** El metaverso tiende a convertir múltiples aspectos de la vida en una experiencia gamificada, donde las recompensas virtuales o las mecánicas de juego determinan comportamientos. Esto puede desdibujar la línea entre el ocio y la productividad, alterando las prioridades y fomentando una dependencia excesiva de logros virtuales.

b) **Identidad Múltiple:** En el metaverso, los usuarios pueden adoptar múltiples identidades, lo que plantea preguntas sobre la autenticidad y la estabilidad emocional. Aunque esto fomenta la libertad de expresión, también puede llevar a problemas relacionados con la alienación, la confusión sobre el *quien soy* y cómo son las relaciones con los demás en el mundo real.

c) **Experiencia Inmersiva:** Aunque las experiencias inmersivas son una de las grandes promesas del metaverso, también pueden tener un efecto negativo. El nivel de realismo puede hacer que las personas se desconecten de su entorno físico, priorizando las interacciones virtuales sobre las reales. Esto podría llevar al aislamiento social y a una falta de habilidades para afrontar la realidad fuera de estos entornos.

Es así como el metaverso representa un cambio profundo en cómo las personas interactúan con el mundo y entre sí. Si bien sus posibilidades son vastas y emocionantes, también es fundamental abordar sus riesgos para garantizar que esta innovación tecnológica beneficie de manera equilibrada a la sociedad (Dominguez, 2023).

El metaverso y los entornos inmersivos representan una de las expresiones más disruptivas de la quinta revolución industrial, al trasladar la interacción social, económica y cultural a espacios digitales tridimensionales donde las personas pueden trabajar, estudiar, socializar y comerciar mediante avatares virtuales. Estas experiencias integran realidad virtual (VR), realidad aumentada (AR) y realidad mixta (MR), permitiendo replicar y ampliar la vida física en el plano digital. Su adopción ha crecido de manera acelerada tanto a nivel individual como corporativo, con aplicaciones en educación, teletrabajo, ocio digital, eventos masivos y comercio electrónico.

Sin embargo, la expansión del metaverso plantea retos jurídicos significativos. La identidad digital de los usuarios se convierte en un activo crítico, susceptible de suplantación, fraude o robo de información, mientras que las empresas que controlan estas plataformas pueden ejercer vigilancia masiva y hasta censura de contenidos. Además, surgen nuevas modalidades de delitos como acoso virtual, fraude económico y apropiación indebida de activos digitales, que desafían la jurisdicción tradicional y evidencian la falta de regulación específica en Colombia.

Estos riesgos impactan directamente derechos fundamentales como la intimidad y el habeas data (art. 15 C.P.), la libertad de expresión (art. 20 C.P.), la propiedad privada (art. 58 C.P.) y la igualdad (art. 13 C.P.), en un contexto donde la protección jurídica en entornos digitales aún es fragmentaria. La Corte Constitucional ha sostenido que los derechos deben ser garantizados con la misma intensidad en escenarios virtuales y físicos, lo que refuerza la necesidad de un marco normativo integral que asegure seguridad jurídica y protección efectiva de los usuarios.

El metaverso y los entornos inmersivos evidencian que la digitalización de la vida humana no solo abarca la información y los datos, sino que reconfigura la interacción social, económica y cultural en un plano virtual. La ausencia de regulación clara en Colombia, sumada a la velocidad del avance tecnológico, genera brechas de protección que ponen en riesgo la privacidad, la autonomía y la seguridad de los usuarios. Este panorama refuerza la urgencia de consolidar un constitucionalismo digital colombiano, capaz de establecer límites, garantías y mecanismos de control para preservar la dignidad humana en estas nuevas realidades. Con este análisis, el estudio avanza hacia la robótica avanzada y la automatización, tecnologías que extienden la interacción hombre-máquina al plano físico y plantean retos adicionales en materia de responsabilidad y derechos fundamentales.

2.9 Transhumanismo Y Poshumanismo

En los últimos 20 años, una entusiasta del cine y la televisión ha reflexionado sobre cómo estas narrativas han explorado la posibilidad de que los seres humanos puedan mejorar sus capacidades físicas mediante implantes tecnológicos. Entre las innovaciones más destacadas, se incluyen chips, prótesis avanzadas y extremidades robóticas, que sugieren un futuro en el que la tecnología y la biología se fusionan. La relación del hombre y las maquinas proponen mejorar sus habilidades corporales y mentales del ser humano mediante el uso de

implantes tecnológicos que garanticen el rendimiento del cuerpo. En el transhumanismo consiste en el ser humano se transforme sus capacidades físicas y psíquicas superiores a la una persona común sin que esto implique una evolución de la especie humana si no una modificación en nuestra era. En cambio, el poshumanismo propone un ser humano con capacidades que sobrepasaría de manera excepcional las posibilidades del ser humano que es completamente diferente y quizás más perfecto al humano (Dominguez, 2023).

Por otra parte, el transhumanismo además de mejoras biológicas directas a través de fármacos, modificaciones genéticas, intervenciones quirúrgicas, estimulaciones eléctricas, inserción de chips con el propósito de mejorar el rendimiento humano en el ámbito cognitivos, físicas, estados de ánimos, del amor y deseo sexual entre otros (Deckers, 2021). Otra forma de ver el concepto el transhumanismo es una corriente filosófica de carácter futurista, racional, científica y humanista, que se manifiesta tanto como un movimiento intelectual como cultural. En su dimensión cultural, incorpora elementos imaginativos y futuristas. Su propósito principal es la restauración y el perfeccionamiento de las capacidades humanas, así como la superación de las limitaciones naturales del ser humano, proponiendo una evolución dirigida de la especie mediante la aplicación de tecnologías avanzadas actuales y en desarrollo, como la nanotecnología, la biotecnología y las tecnologías de la información (Gayozzo, 2019).

Adicionalmente, El transhumanismo tecnocientífico busca modificar profundamente al Homo sapiens mediante el uso de la tecnología, fusionándolo con máquinas, mejorando biológicamente a través de fármacos, y manipulando genéticamente óvulos y espermatozoides, con el fin de que las personas puedan ejercer su derecho a la libertad morfológica y en el futuro puedan mejorar la especie humana (*Homo deus, Homo Excelsior, el Homo Roboticus, Homo postorgánicos*) (Dominguez, 2023). A continuación, algunos casos de personas con mejoramiento de sus capacidades:

Nota: El cineasta Rob Spence lleva una década utilizando una prótesis ocular equipada con una microcámara que transmite las imágenes captadas a un receptor.

Nota: Moon Ribas incorporó sensores sísmicos en sus pies, permitiéndole sentir en su cuerpo las vibraciones de la Tierra.

Nota: La técnica CRISPR-Cas9 facilita la modificación del genoma humano.

En definitiva, los casos de Rob Spence, Moon Ribas y He Jiankui reflejan cómo los avances tecnológicos están transformando las capacidades humanas y planteando interrogantes éticos, sociales y personales. Rob Spence, con su prótesis ocular equipada con una microcámara, demuestra cómo la tecnología puede fusionarse con el cuerpo para expandir los límites de los sentidos y la creatividad. Por su parte, Moon Ribas ejemplifica cómo la integración de dispositivos tecnológicos puede generar nuevos sentidos, como su "sentido sísmico", transformando la percepción del mundo y la relación del ser humano con su entorno. Sin embargo, el caso de He Jiankui y la modificación genética de embriones humanos pone de manifiesto los dilemas éticos y legales asociados a estas intervenciones, especialmente cuando se desconocen sus consecuencias a largo plazo y se amenaza con crear desigualdades entre humanos y "posthumanos". En este contexto, el debate sobre la libertad, la justicia social y el

autodominio cobra cada vez más relevancia. Lo que antes parecía una fantasía futurista hoy se materializa en realidades tangibles, impulsando reflexiones críticas sobre los límites y las implicaciones del transhumanismo en nuestras vidas.

La robótica avanzada y la automatización son pilares de la quinta revolución industrial, pues trasladan la integración tecnológica al plano físico, donde máquinas inteligentes asumen tareas que antes realizaban seres humanos. En la vida cotidiana, esta tecnología ya está presente en asistentes domésticos, drones y vehículos autónomos, mientras que en el ámbito industrial y médico se aplican robots colaborativos, quirúrgicos y logísticos que incrementan la eficiencia y precisión de los procesos. Para las empresas, estas herramientas significan reducción de costos y aumento de productividad, mientras que para la sociedad en general ofrecen comodidad y soporte en tareas complejas.

No obstante, la delegación de funciones a sistemas autónomos plantea riesgos jurídicos relevantes. Los accidentes o fallos técnicos generan vacíos de responsabilidad civil y penal, especialmente cuando no existe supervisión humana directa. La automatización masiva también provoca desplazamiento laboral, aumentando la desigualdad social y exigiendo ajustes en la legislación laboral y en las políticas públicas de empleo. En el plano ético, la toma de decisiones autónoma por máquinas requiere establecer límites y protocolos de certificación, evitando que la innovación tecnológica vulnere derechos fundamentales.

En el contexto colombiano, estas tecnologías impactan derechos fundamentales como el trabajo (art. 25 C.P.), la igualdad (art. 13 C.P.), la propiedad (art. 58 C.P.) y la seguridad personal (art. 2 C.P.), en un entorno donde no existe normativa específica sobre responsabilidad por el actuar de robots autónomos. La Corte Constitucional ha señalado que los derechos deben adaptarse a nuevas realidades tecnológicas, lo que evidencia la necesidad de marcos legales claros para regular la responsabilidad, supervisión y certificación de sistemas automatizados, protegiendo la dignidad humana y la justicia social.

La robótica avanzada y la automatización confirman que la interacción entre tecnología y ser humano ha dejado de ser solo digital para incidir directamente en la vida física y social. Si bien ofrecen oportunidades de desarrollo, también acentúan riesgos jurídicos y sociales, desde accidentes sin responsable claro hasta desplazamiento laboral masivo. En Colombia, la falta de normas claras de responsabilidad y supervisión deja a la sociedad en vulnerabilidad, reforzando la necesidad de un constitucionalismo digital que armonice innovación y protección

de derechos. Con este análisis, el estudio avanza hacia el transhumanismo y las personas ciborg, donde la interacción hombre-máquina se traslada al plano biológico, planteando retos aún más profundos.

2.10 Transhumanismo y Bioética

El concepto de "transhumano" (humano+) se refiere al ser humano en transición hacia el "poshumano" (humano++). El transhumanismo se presenta como una poderosa ideología que aspira a establecer un nuevo paradigma, cuyo principio filosófico es la superación de las limitaciones humanas mediante la razón, la ciencia y la tecnología. Sin embargo, esta visión plantea dilemas bioéticos, ya que la implementación de sus ideas podría amenazar la dignidad humana.Aldous Huxley, influido por la terminología de Dante, reinterpretó el concepto de "transhumanación". Este término, que originalmente describía una transformación espiritual otorgada por la Gracia Divina, pasó a representar un esfuerzo humano deliberado impulsado por la tecnología. Así, la trascendencia dejó de estar vinculada a lo divino y se enfocó en superar la naturaleza humana a través de avances científicos, producto exclusivo del trabajo humano. El transhumanismo defiende tres libertades fundamentales para facilitar esta evolución: la libertad morfológica, la libertad reproductiva y la libertad cognitiva. Estas garantías buscan permitir a los individuos utilizar la tecnología para progresar hacia su condición transhumana, (Alva-Arroyo et al., 2022).

Desde una perspectiva bioética, el enfoque personalista ontológico se fundamenta en la filosofía personalista, particularmente en el personalismo ontológico, que considera al ser humano como el núcleo fundamental de su enfoque antropológico. Este marco permite abordar temas como la corporeidad y la corporalidad con una estructura coherente. En contraste, el principialismo anglosajón carece de un sistema antropológico que sustente sus principios y resuelva las contradicciones entre ellos, limitando su capacidad para ofrecer un contexto interpretativo adecuado. El transhumanismo, en su afán de superar los límites naturales, muestra un desprecio hacia la vida biológica. Esto se evidencia en propuestas como la transferencia de la mente a dispositivos digitales, prescindiendo del cuerpo físico para alcanzar una forma de supuesta inmortalidad. Sin embargo, la vida es una condición previa indispensable para la libertad, pues sin vida física no puede ejercerse la libertad. Cuando la búsqueda de libertad anula la vida, se niega a sí misma (García J. J., 2012).

Esta ideología rechaza cualquier límite a sus aspiraciones, considerando las restricciones como censura o coacción arbitraria. Según esta corriente, todo lo que sea técnicamente posible debe realizarse. De este modo, la ruptura con el presente y con la realidad se convierte en el único camino hacia la emancipación, posicionando al transhumano como un agente consciente de la negación de la naturaleza actual para proyectarse hacia un futuro deseado. El destino último de la humanidad, según esta visión, es convertirse en la conciencia que rija el cosmos, alcanzando una unidad con el universo. Este ideal, defendido por pensadores como Fereidoun M. Esfandiary, resuena con una mística que busca disolver al individuo en la totalidad de la existencia, (Bostrom, 2005).

Para comprender el transhumanismo moderno, representado por organizaciones como Humanity Plus, el Future of Humanity Institute y la Singularity University, es esencial considerar las ideas de figuras clave como Julian Huxley, Pierre Teilhard de Chardin, Fereidoun Esfandiary y Timothy Leary, entre otros. Estos pensadores, junto con los cosmistas rusos, han formado el fundamento teórico e histórico de esta corriente que busca dirigir conscientemente la evolución de la humanidad hacia un nuevo horizonte, (Alva-Arroyo et al., 2022).

Es entonces que el transhumanismo se presenta como una ideología que busca superar las limitaciones humanas a través de la ciencia y la tecnología, desafiando los principios tradicionales de la dignidad humana. Aunque promueve la libertad individual para modificar el cuerpo y la mente, plantea serios dilemas bioéticos, especialmente en su rechazo de los límites naturales y su enfoque en la trascendencia humana a través de la tecnología. Al mismo tiempo, esta corriente refleja una ambición de emancipación y unidad con el cosmos, influenciada por pensadores clave que han cimentado las bases del transhumanismo moderno. Sin embargo, su propuesta choca con la idea de que la vida física es esencial para el ejercicio de la libertad, subrayando las tensiones entre el progreso técnico y el respeto a la naturaleza humana.

El transhumanismo es un movimiento tecnológico y filosófico que busca potenciar las capacidades humanas mediante implantes, prótesis inteligentes, interfaces cerebro-computadora y sensores biomédicos, con el fin de superar limitaciones biológicas y mejorar la calidad y duración de la vida. De esta corriente surgen las personas ciborg, individuos que integran dispositivos tecnológicos a su cuerpo, difuminando la frontera entre lo natural y lo

artificial. Ejemplos cotidianos de esta evolución incluyen marcapasos inteligentes, implantes cocleares, chips subcutáneos de identificación y prótesis mioeléctricas.

Si bien estas innovaciones ofrecen beneficios médicos y sociales, también plantean riesgos jurídicos y éticos. La integración de tecnología en el cuerpo humano genera dilemas sobre identidad personal, privacidad, consentimiento informado y autonomía, especialmente cuando los dispositivos almacenan y transmiten datos sensibles. Además, surgen riesgos de desigualdad y discriminación, ya que el acceso a estas mejoras podría crear brechas sociales entre quienes pueden acceder a ellas y quienes no. En términos de responsabilidad jurídica, los daños derivados de fallos o interferencias tecnológicas carecen de regulación específica, dejando a las personas en una situación de vulnerabilidad legal.

En el contexto colombiano, estas tecnologías afectan derechos fundamentales como la vida (art. 11 C.P.), la integridad personal (art. 12 C.P.), la intimidad y protección de datos (art. 15 C.P.), la igualdad (art. 13 C.P.) y la autonomía personal, derivada de la dignidad humana (art. 1 C.P.). Actualmente, no existe una regulación integral sobre implantes tecnológicos y mejoras corporales, lo que evidencia la urgencia de adaptar el derecho constitucional a estas nuevas realidades.

El transhumanismo y las personas ciborg representan el punto más avanzado de la interacción hombre-tecnología, llevando la transformación digital al plano biológico y existencial. Este fenómeno desafía los fundamentos del derecho constitucional, pues obliga a replantear conceptos de identidad, dignidad, autonomía y responsabilidad. En Colombia, la ausencia de regulación especializada y la velocidad del avance tecnológico refuerzan la urgencia de un constitucionalismo digital robusto, capaz de garantizar que el progreso tecnológico respete los derechos fundamentales y asegure una transición justa, ética e inclusiva hacia las nuevas realidades de la quinta revolución industrial.

Si las personas ciborg representan la integración de la tecnología al cuerpo humano, los ciber-robots y la sintiencia digital llevan esta interacción al plano externo, donde la autonomía tecnológica puede actuar de manera independiente en el mundo físico, planteando retos jurídicos y éticos aún más complejos.

2.11 Sintiencia Digital

El ser humano se ha preguntado y ha tenido la idea de sintiencia se discute desde la filosofía antigua, su relevancia ética y jurídica ha ganado protagonismo en los últimos siglos, especialmente en el contexto de los derechos de los animales y la reflexión sobre las relaciones entre humanos y otras especies. Las reflexiones actuales sobre los seres sintientes, especialmente en el marco de los movimientos por los derechos de los animales y la liberación animal, están estrechamente vinculadas al problema de la violencia y a la posibilidad de construir relaciones y sociedades pacíficas entre especies. En este contexto, es crucial analizar el papel que la sintiencia desempeña en estos movimientos y sus respectivas filosofías, en comparación con el lugar que ha ocupado en otros momentos históricos (Gaitán, 2024).

En el pensamiento de Aristóteles, por ejemplo, se encuentra una concepción de la animalidad que no solo reconoce la capacidad de sentir, sino que la define a través de la noción de *ánima*. Este concepto, que difiere de la tradición judeocristiana predominante posteriormente, no era exclusivo de los humanos ni necesariamente inmaterial. Para Aristóteles, el *ánima* representaba una "fuerza vital", un principio que diferenciaba a los seres vivos de los inertes. Por esta razón, su tratado *De anima* (1983) puede interpretarse más como un estudio biológico que teológico o religioso (Sánchez, 2015).

Según esta perspectiva, los seres vivos se distinguían por el tipo de fuerza vital que poseían: las plantas contaban con un *ánima nutritiva*, que las orientaba hacia la obtención de nutrientes; los animales, además de esta, tenían un *ánima sensitiva*, que los llevaba a buscar el placer y evitar el dolor; y los seres humanos contaban con un *ánima racional*, que los guiaba hacia las realidades del *logos*, además de las funciones nutritiva y sensitiva. Tanto el *ánima nutritiva* como la *sensitiva* eran materiales y perecederas, a diferencia del *ánima racional*, exclusiva de los humanos, que Aristóteles consideraba inmaterial.

Finalmente, se hace la reflexión sobre la sintiencia y su relevancia ética y jurídica muestra cómo el entendimiento humano acerca de las capacidades y derechos de otros seres vivos ha evolucionado significativamente desde la filosofía antigua hasta nuestros días. Aristóteles, con su concepción del *ánima* como principio vital, sentó las bases de una visión que reconoce distintos grados de sensibilidad en los seres vivos, diferenciándolos por su capacidad de nutrirse, sentir y razonar. Esta perspectiva, aunque inserta en un marco biológico, resalta una sensibilidad inherente que trasciende la simple funcionalidad.

Actualmente frente a los avances en la tecnología y la robótica, la discusión sobre sintiencia adquiere un nuevo matiz, enfrentándose a cuestionamientos sobre si las máquinas pueden, o deberían, ser consideradas sintientes y cómo esto impacta las relaciones con ellas. A medida que se desarrollan robots y sistemas de inteligencia artificial cada vez más complejos, la cuestión ética se amplía: ¿qué responsabilidades se tiene hacia estos artefactos, y cómo se compara su potencial sintiencia con la de los animales o incluso los humanos?

El diálogo contemporáneo entre filosofía, ciencia y tecnología invita a repensar las categorías tradicionales de ser vivo y sintiencia, considerando tanto a los animales como a los sistemas artificiales en el marco de una ética que promueva relaciones pacíficas y justas. Así, el concepto aristotélico de *ánima* podría reinterpretarse en un contexto moderno, donde las "fuerzas vitales" abarcan tanto lo biológico como lo artificial, y donde la capacidad de sentir, entender y actuar con propósito redefine nuestras nociones de coexistencia y respeto mutuo.

La sintiencia digital hace referencia al desarrollo de sistemas de inteligencia artificial y ciber-robots capaces de percibir, interpretar y reaccionar al entorno de manera autónoma y adaptativa, simulando rasgos de conciencia o experiencia subjetiva. Este fenómeno, propio de la quinta revolución industrial, combina la IA avanzada con robótica física, dando lugar a ciber-robots que interactúan con personas y objetos en entornos físicos y virtuales, desde robots colaborativos en fábricas hasta dispositivos autónomos de asistencia médica o de seguridad.

El avance de la sintiencia digital plantea retos jurídicos y éticos inéditos. Los ciber-robots autónomos pueden tomar decisiones sin supervisión humana inmediata, lo que genera incertidumbre sobre la responsabilidad civil, penal y administrativa en casos de accidentes, daños a terceros o decisiones que afecten derechos fundamentales. Además, la captura y transmisión de datos sensibles por estos sistemas abre riesgos en privacidad, seguridad y vigilancia masiva, mientras que la posibilidad de reconocerles personalidad jurídica o derechos aún es un debate abierto en la doctrina internacional.

En el contexto colombiano, estas tecnologías impactan derechos fundamentales como la dignidad humana (art. 1 C.P.), la intimidad y habeas data (art. 15 C.P.), la igualdad (art. 13 C.P.), el trabajo (art. 25 C.P.) y la seguridad personal (art. 2 C.P.), especialmente ante la ausencia de regulación sobre ciber-robots y sistemas sintientes. Esta laguna normativa evidencia la necesidad de un constitucionalismo digital colombiano que establezca

mecanismos claros de supervisión, responsabilidad y protección de derechos, asegurando que la innovación tecnológica no supere los límites éticos y jurídicos esenciales para la sociedad.

La sintiencia digital y los ciber-robots representan la frontera más avanzada de la interacción hombre-máquina, llevando la transformación digital al plano físico y existencial. Su desarrollo desafía los cimientos del derecho constitucional, al exigir respuestas normativas proactivas que preserven la dignidad humana, la seguridad jurídica y la justicia social en un escenario donde lo biológico, lo físico y lo digital convergen. Este análisis cierra el estudio de las tecnologías emergentes, preparando el terreno para el siguiente capitulo, donde se abordará el marco constitucional, legal y jurisprudencial colombiano que debe responder a estos desafíos.

2.12 Las Personas Ciborg

De acuerdo con el capítulo anterior, resulta necesario abordar este nuevo apartado, centrado en la mejora y el perfeccionamiento del ser humano a través de diversas modificaciones que trascienden el ámbito de la estética. El objetivo no es simplemente mejorar la apariencia, sino expandir las capacidades humanas mediante intervenciones en el cuerpo, basadas en los avances de la ciencia y la tecnología. Aunque este tema puede parecer innovador, su desarrollo tiene antecedentes en aplicaciones como marcapasos, prótesis, lentes de contacto y otras tecnologías que han transformado la vida humana. Además, desde hace más de 15 años, la tecnología aplicada al ser humano ha encontrado un campo fértil en la computación, especialmente en áreas como la robótica y la inteligencia artificial, como se ha analizado en capítulos precedentes.

Con la evolución de dispositivos tecnológicos cada vez más avanzados y el concepto de libertad morfológica, se han desarrollado herramientas que no solo restauran funciones corporales perdidas, como extremidades o sentidos, sino que también amplían las capacidades humanas mediante la incorporación de software especializado. Por ejemplo, ahora es posible controlar objetos con la mente gracias a interfaces cerebro-computadora, que no solo permiten la interacción directa entre el cerebro y dispositivos electrónicos, sino que también habilitan la comunicación telepática entre personas. Estas tecnologías, además, pueden suplir funciones inexistentes desde el nacimiento o aquellas perdidas debido a enfermedades o accidentes, marcando un hito en la integración de la ciencia y la tecnología con el cuerpo humano (Clavijo, 2018).

De este modo, la tecnología aplicada al cuerpo humano puede tener tanto un propósito reparador como un objetivo orientado a mejorar, potenciar y perfeccionar las capacidades humanas, ya sea con fines médicos o no médicos. Además, es posible combinar fines reparadores con mejoras funcionales, o enfocarse exclusivamente en modificaciones con fines estéticos, como ocurre en el caso de las cirugías plásticas, implantes mamarios, capilares, dentales, entre otros. Este abanico de aplicaciones demuestra la versatilidad y el impacto de la tecnología en la transformación del cuerpo humano (Dominguez, 2023).

El perfeccionamiento humano puede abordarse desde tres dimensiones principales: grado, modo y efectos.

- **Grado:** Esta dimensión abarca desde ajustes menores al cuerpo humano, como los implantes dentales, hasta rediseños complejos de partes del cuerpo y capacidades. Por ejemplo, la sustitución de una pierna biológica por una prótesis biónica que no solo restaura la función perdida, sino que también mejora habilidades, como aumentar la velocidad al correr.
- **Modo:** Se refiere a la naturaleza de la mejora, que puede consistir en modificar una función existente en el cuerpo humano, añadir una nueva función que la persona no poseía pero que otros seres humanos sí tienen (como restaurar el sistema auditivo de una persona sorda), o incluso incorporar capacidades completamente inéditas que no existen en la humanidad.
- **Efectos:** Las mejoras tecnológicas pueden ofrecer ventajas competitivas (como mayor rendimiento físico o mental) o beneficios intrínsecos (como una mejor calidad de vida).

Estas tecnologías empleadas en el perfeccionamiento incluyen dispositivos implantables clasificados como productos sanitarios, tratamientos farmacológicos diseñados para optimizar el sistema biológico, y la ingeniería genética, que permite modificar el ADN para diseñar características específicas en las personas (Jimenez Retana, 2018).

Otra discusión relevante es la diferenciación entre los conceptos de "persona biónica" y "persona ciborg", ya que, aunque relacionados, tienen significados distintos.

La persona biónica se refiere a aquellos individuos que combinan componentes biológicos y electrónicos para reemplazar un miembro o función perdida, como una prótesis avanzada que sustituye una extremidad. Por otro lado, la persona ciborg implica una

integración más profunda entre el organismo humano y la tecnología. Esta combinación permite controlar o gestionar procesos fisiológicos, anatómicos o intelectuales mediante el uso de dispositivos tecnológicos avanzados. Estos dispositivos suelen incorporar sistemas de inteligencia artificial, chips con sensores inalámbricos (*wireless*) o sistemas RFID, conectados directamente con el sistema neuronal del individuo, logrando una simbiosis entre la parte biológica y la tecnológica (Dominguez, 2023).

Ahora bien, las persona ciborg se puede clasificar en tres categorías: el sujeto ciborg reparación, el de mejora y el mixto (Camacho, 2017). Que a continuación se explica:

Tabla 3.

La Ciborgización

NOMBRE	**DEFINICIÓN**	**CASO ESPECIFICO**
Ciborg Reparación	Se refiere a una persona cuya función fisiológica ha sido restaurada mediante la implementación de un dispositivo electrónico en su cuerpo.	Un caso destacado es el de Ian Burkhart, quien sufrió una lesión medular en las vértebras cervicales C5 y C6 hace más de seis años, quedando tetrapléjico. Para restaurar la movilidad de su mano, se le implantó un diminuto chip, más pequeño que un guisante, acompañado de un dispositivo que sobresale de la parte superior de su cabeza. Este dispositivo se conecta mediante un cable que envía señales a su antebrazo.
Ciborg De Mejora	Se trata de una persona cuyas funciones fisiológicas han sido mejoradas o potenciadas mediante la implementación de un mecanismo o dispositivo electrónico en su cuerpo. En este caso, no existe ninguna	Un ejemplo es Steve Mann, quien, sin presentar impedimentos visuales, utiliza un dispositivo denominado *eye tap*. Este dispositivo, conectado a su cráneo, funciona como una cámara situada

	deficiencia previa; la persona elige de manera voluntaria optimizar alguna función existente de su cuerpo o incorporar habilidades que antes no poseía.	sobre el ojo, capaz de grabar las imágenes que este observa y, además, proyectar imágenes generadas por ordenador para su visualización.
Ciborg Mixto	El sujeto cíborg mixto representa un caso en el que la distinción entre cíborg de reparación y de mejora se torna difusa. Como señala Camacho (2017), en la mayoría de los casos, la implementación de dispositivos electrónicos tiene como objetivo principal restablecer funciones fisiológicas; sin embargo, estos dispositivos suelen incluir mejoras, potenciaciones o incluso añadir nuevas capacidades al individuo.	Un ejemplo de ello es Neil Harbisson, quien nació con acromatopsia o monocromatismo, una condición congénita y no progresiva que limita la percepción de los colores a tonos de blanco, negro y gris. Para abordar esta situación, Harbisson se implantó una antena en la cabeza, osteointegrada en su cráneo y conectada al hueso occipital. Este dispositivo le permite no solo escuchar y percibir colores visibles, sino también captar colores invisibles, como los infrarrojos y ultravioletas. Asimismo, la antena le permite recibir videos, imágenes, llamadas telefónicas y música directamente en su mente a través de dispositivos externos, como teléfonos móviles o satélites.

Fuente: Elaboración Propia (2024).

En síntesis, la ciborgización plantea retos inéditos y trascendentales para el orden jurídico, en especial para el ámbito constitucional. La noción de un "derecho fundamental a la

mejora" emerge como una respuesta necesaria frente a las transformaciones tecnológicas que permiten la modificación cibernética del cuerpo humano. Este derecho, aunque no explícitamente consagrado, puede ser inferido a partir de principios y derechos fundamentales como la dignidad humana, el libre desarrollo de la personalidad, la integridad personal y el derecho a la salud. No obstante, su reconocimiento y regulación deberán enfrentarse a tensiones significativas con otras garantías constitucionales, como el derecho a la intimidad, la igualdad y el debido proceso (García M. D., 2025).

Las preguntas aquí formuladas son un llamado a reflexionar sobre los alcances y límites de las garantías constitucionales frente a los desafíos que traerá consigo el constitucionalismo ciborgiano. Dichas interrogantes evidencian la necesidad de un marco jurídico robusto y flexible que contemple tanto los derechos como las responsabilidades inherentes a los seres humanos modificados tecnológicamente.

Bajo esta línea argumentativa, resulta inevitable dirigir nuestra atención hacia la Constitución colombiana, la cual servirá como el punto de partida para analizar cómo los principios y derechos fundamentales establecidos en su texto pueden ser reinterpretados y adaptados a esta nueva realidad. La próxima unidad abordará las implicaciones del derecho constitucional colombiano en este contexto, explorando cómo los conceptos tradicionales pueden ser resignificados para garantizar la protección y promoción de los derechos de todos los ciudadanos, sean humanos biológicos o ciborgs.

Los ciber-robots y los sistemas dotados de sintiencia digital simulada representan el límite actual de la interacción hombre-máquina, pues combinan autonomía física y capacidad de procesamiento avanzado para ejecutar tareas en entornos reales sin supervisión constante. Esta convergencia entre robótica, inteligencia artificial y conectividad total genera riesgos jurídicos y éticos sin precedentes, desde la incertidumbre sobre la responsabilidad por daños hasta la posibilidad de afectación directa de los derechos fundamentales de las personas con las que interactúan. En Colombia, la ausencia de un marco normativo integral para regular los ciber-robots autónomos deja un vacío jurídico que exige respuestas inmediatas desde el constitucionalismo digital, estableciendo límites claros, estándares de supervisión y mecanismos de protección que garanticen que la innovación tecnológica no supere los valores esenciales de la dignidad y la seguridad humanas.

El análisis de la quinta revolución industrial y de las tecnologías emergentes —desde el Big Data y la inteligencia artificial, hasta el blockchain, el metaverso, la robótica avanzada, el transhumanismo y los ciber-robots dotados de sintiencia digital— evidencia que la interacción entre el ser humano y la tecnología ha alcanzado un nivel sin precedentes, transformando de manera profunda la vida social, económica, biológica y jurídica. Esta evolución ofrece oportunidades inéditas para la innovación, pero también acentúa riesgos jurídicos y éticos: vulneración de la privacidad, desplazamiento laboral, incertidumbre sobre la responsabilidad de los sistemas autónomos y desafíos para la protección de los derechos fundamentales.

En este contexto, la ausencia de marcos normativos integrales en Colombia y la velocidad de la transformación digital refuerzan la urgencia de un constitucionalismo digital robusto, capaz de armonizar innovación tecnológica y protección de la dignidad humana, asegurando que los valores del Estado Social de Derecho prevalezcan en la era de la quinta revolución industrial. Con este cierre, el estudio se encamina al Capítulo 2, donde se abordará el marco constitucional, legal y jurisprudencial colombiano que debe responder a estos desafíos.

TÍTULO III. CONSTITUCIONALISMO DIGITAL.

A partir del análisis del neoconstitucionalismo y de las emergentes tecnologías, puede sostenerse la necesidad imperante que apremia la aparición del constitucionalismo digital. Mientras que el neoconstitucionalismo reconfiguró la relación entre la Constitución, los derechos fundamentales y el poder estatal (otorgando a la norma suprema fuerza normativa, centralidad axiológica y una dimensión moral robusta) el constitucionalismo digital expande ese proyecto hacia nuevos espacios de poder, donde la autoridad ya no está circunscrita exclusivamente a los Estados.

En efecto, en el entorno digital contemporáneo, plataformas tecnológicas, corporaciones transnacionales y sistemas algorítmicos ejercen un poder material y simbólico capaz de afectar derechos fundamentales con una intensidad antes desconocida. Ante esta transformación, la protección de derechos como la libertad de expresión, la privacidad, la protección de datos o el acceso a la información exige superar los límites del constitucionalismo tradicional y proyectar sus principios hacia el ciberespacio, la inteligencia artificial y los flujos transnacionales de información. Desde esta perspectiva, el constitucionalismo digital no implica una ruptura con el modelo garantista, sino más bien su continuación y ampliación, ajustada al desplazamiento del poder hacia actores privados globales y a la aparición de riesgos inéditos en la sociedad de la información del siglo XXI.

En consecuencia, la incorporación de elementos y entornos digitales requiere no solo respuestas regulatorias estatales, sino también la construcción de un nuevo entendimiento constitucional compartido, capaz de integrar instrumentos jurídicos, dinámicas sociales y prácticas tecnológicas. Del mismo modo que, tras la Segunda Guerra Mundial, emergió un paradigma constitucional renovado ante transformaciones históricas profundas, hoy nos encontramos frente a una revolución tecnológica que ha redefinido las relaciones de poder, imponiendo desafíos significativos tanto al Estado como a las corporaciones privadas, a las infraestructuras transnacionales y a las nuevas formas de vida digital (Zuboff, 2019).

3. Delimitaciones doctrinales y aparición.

La construcción teórica del constitucionalismo digital se ha ido configurando a partir de múltiples aportes doctrinales que buscan explicar cómo los valores y principios del constitucionalismo contemporáneo pueden proyectarse hacia entornos digitales dominados por

actores privados globales y por dinámicas algorítmicas cada vez más complejas. Aunque estas perspectivas ofrecen recursos conceptuales relevantes, también revelan tensiones y limitaciones frente a los desafíos que plantea la digitalización de la vida social.

En la sociedad digital actual, las plataformas tecnológicas, los sistemas de inteligencia artificial (IA), la extracción masiva de datos y el big data ejercen un poder configurador que incide de forma directa en la vida pública y privada de los ciudadanos. De Gregorio (2020) afirma que esta realidad obliga a "releer la Constitución a la luz de los procesos de digitalización", ya que la efectividad de derechos como la libertad de expresión, la privacidad, la protección de datos o la participación democrática depende ahora no solo de las instituciones estatales, sino también de empresas privadas que operan en ámbitos transnacionales y que gestionan infraestructuras esenciales para la comunicación y la interacción social.

Desde esta perspectiva, el constitucionalismo digital no supone una ruptura con el modelo garantista del neoconstitucionalismo, sino más bien su extensión hacia nuevas esferas de poder. El desplazamiento más significativo reside en la redefinición del sujeto cuya actuación debe ser limitada. Mientras que el constitucionalismo tradicional se centraba casi exclusivamente en la restricción del poder público, el constitucionalismo digital incorpora mecanismos orientados a controlar el poder privado y algorítmico, es decir, las capacidades de las grandes empresas tecnológicas para gestionar datos, ordenar información y moldear el discurso público.

Autores como Celeste (2019) y Pollicino (2021) proponen entender el constitucionalismo digital como un constitucionalismo multinivel y transnacional, en el que los derechos fundamentales actúan como límites universales aplicables a espacios digitales sin fronteras. Se trata, por tanto, de un modelo normativo que trasciende el territorio nacional y reconoce que la arquitectura de internet, las plataformas sociales y los sistemas de IA constituyen nuevas formas de orden normativo. Estas estructuras privadas crean reglas, definen comportamientos y establecen sanciones, reproduciendo de facto funciones constitucionales en ámbitos extrajurídicos.

El constitucionalismo digital también plantea una reconfiguración epistemológica del derecho. Según Rouvroy y Berns (2013), la "gubernamentalidad algorítmica" transforma la racionalidad del poder al sustituir la deliberación y la responsabilidad moral por cálculos predictivos y decisiones automatizadas. En este contexto, el derecho constitucional debe

recuperar su función humanizadora, garantizando que la dignidad y la autonomía sigan siendo el centro de la acción pública y privada. El riesgo, advierten Floridi (2022) y Sartor (2020), es que la lógica algorítmica erosione los cimientos del constitucionalismo al reemplazar la deliberación ética por la eficiencia técnica.

En cuanto a la definición de constitucionalismo digital, se encuentran algunas de sus primeras formulaciones explícitas. Suzor (2018) lo caracteriza como un esfuerzo orientado a definir y materializar estándares adecuados de legitimidad para la gobernanza en la era digital. Posteriormente, Redeker et al. (2018) lo describen como un término que agrupa diversas iniciativas destinadas a establecer derechos políticos, normas de gobernanza y límites al ejercicio del poder en Internet (p.10). Basándose en la teoría del constitucionalismo societal, estos autores conciben el constitucionalismo digital como un proceso de creación de normas constitucionales que surge de grupos sociales —tales como la sociedad civil o las corporaciones transnacionales— y que abarca la limitación tanto del poder público como del poder privado en el entorno digital (Golia, 2024).

Uno de los primeros intentos de sistematización teórica proviene de Edoardo Celeste (2019), quien plantea que el constitucionalismo digital tiene como misión esencial trasladar la protección de los valores constitucionales al ciberespacio, donde el poder no se concentra exclusivamente en el Estado, sino en plataformas globales que operan fuera del control territorial. Su enfoque ofrece un marco conceptual claro, pues vincula garantías y derechos fundamentales con los nuevos escenarios de interacción digital. Sin embargo, resulta necesario cuestionar la viabilidad práctica de su propuesta: trasladar el poder normativo de la Constitución a espacios transnacionales enfrenta limitaciones jurisdiccionales y técnicas, ya que los tribunales nacionales carecen de instrumentos eficaces para imponer sus decisiones a corporaciones tecnológicas de alcance global. Ante la creación o análisis del concepto de constitucionalismo digital, Celeste (2018) plantea lo siguiente:

> “La primera tarea difícil fue proporcionar una definición de constitucionalismo digital. En la literatura existente, esta noción se utilizaba simplemente sin definirla o, en ocasiones, se definía de manera funcional. Por ello, se comenzó a deconstruir esta expresión. “Digital” es el adjetivo que se utiliza para referirse a la tecnología de la información. “Constitucionalismo” denota la ideología correspondiente a un sistema de gobierno, llamado constitucional, que surgió en los últimos años del siglo XVIII para

reemplazar las monarquías absolutas y que sigue siendo el modelo dominante en muchos países.

En consecuencia, a la luz de estas definiciones, colocar "digital" junto a "constitucionalismo" tiene dos implicaciones principales. En primer lugar, permite comprender que se está hablando de la concepción moderna, y no histórica, del constitucionalismo. En segundo lugar, se puede deducir que aquí "digital" no se refiere directamente a "constitucionalismo", sino que funciona más bien como un adverbio que transmite la idea de que este constitucionalismo está, de algún modo, relacionado con el entorno digital. En conclusión, el constitucionalismo digital parece ser, en sí mismo, una abreviatura que denota una declinación del constitucionalismo moderno que involucra el entorno digital" (Celeste, 2018).

Este paradigma se articula en tres dimensiones interdependientes:

1. **Dimensión normativa:** busca adaptar los marcos constitucionales a los desafíos de la digitalización mediante reformas legales, jurisprudencia y tratados internacionales que reconozcan derechos digitales, como el *Right to be Forgotten* o *el Habeas Data digital.*
2. **Dimensión institucional:** exige fortalecer los mecanismos de control constitucional frente al poder de las plataformas, garantizando la transparencia de los algoritmos y la rendición de cuentas de las corporaciones tecnológicas.
3. **Dimensión axiológica:** proyecta los valores constitucionales fundamentales — dignidad, igualdad, libertad y justicia— hacia un entorno digital donde los riesgos de exclusión, manipulación y vigilancia amenazan la autonomía de los individuos.

Por otro lado, Golia (2024), analiza el constitucionalismo digital como ideología, el cual precisa como el discurso constitucional que examina y contribuye a configurar las relaciones socialmente construidas entre los individuos y sus condiciones reales de existencia, relaciones que, en la actualidad, están mediadas directa o indirectamente por las tecnologías digitales (p. 499). En consecuencia, esta definición pone de relieve las dinámicas de interpelación que tales tecnologías desencadenan; es decir, los procesos mediante los cuales diversos aparatos y mecanismos sociopolíticos (como el trabajo, la sexualidad, el género, la

etnicidad, la ciudadanía u otros ámbitos) constituyen a individuos y colectivos como sujetos sociales a través de dispositivos y entornos digitales.

Shoshana Zuboff (2019) ofrece una mirada crítica y estructural al describir el capitalismo de vigilancia, entendido como un modelo económico basado en la extracción masiva de datos personales, capaces de predecir y moldear el comportamiento humano. Su tesis es contundente: la autonomía individual y la libertad se ven erosionadas en un ecosistema donde cada interacción digital es monetizada y analizada algorítmicamente. La denuncia de Zuboff tiene enorme relevancia contemporánea, pues explica cómo la economía de datos ha pasado de ser un fenómeno tecnológico a convertirse en un problema constitucional, que demanda nuevas formas de protección frente a riesgos invisibles y transnacionales. Sin embargo, su enfoque presenta un desafío práctico: si bien alerta sobre la magnitud del poder corporativo, no ofrece un marco jurídico operativo que permita trasladar los valores constitucionales a este nuevo escenario económico, obligando a la doctrina a explorar soluciones normativas combinadas entre regulación nacional, cooperación internacional y exigibilidad judicial de principios constitucionales en la gobernanza digital.

En conjunto, estos aportes convergen en un consenso fundamental: el constitucionalismo digital es una necesidad histórica, pues los derechos fundamentales enfrentan amenazas inéditas en la sociedad digital, donde el poder ya no es exclusivamente estatal, sino privado, global y algorítmico. Sin embargo, también ponen de manifiesto un dilema estructural: cómo trasladar la lógica garantista del constitucionalismo a un ecosistema transnacional y tecnológicamente complejo, en el que los mecanismos clásicos de control jurídico resultan insuficientes. La eficacia futura del constitucionalismo digital dependerá de la capacidad de articular soluciones normativas innovadoras, de regular el poder privado global sin sofocar la innovación tecnológica, y de mantener la vigencia de los principios constitucionales en un entorno donde la libertad y la dignidad humanas se juegan en el lenguaje silencioso de los algoritmos.

Así, el constitucionalismo digital no es solo una teoría emergente, sino una respuesta estructural al desplazamiento del poder en la era de la información. La digitalización no elimina el conflicto entre libertad y control, sino que lo traslada a nuevos escenarios: el diseño de algoritmos, la gobernanza de datos y la moderación de contenidos. En este sentido, el nuevo constitucionalismo asume la tarea de reequilibrar las relaciones de poder en un contexto donde los derechos fundamentales dependen de infraestructuras privadas (Celeste, 2019).

De modo más amplio, la consolidación de un constitucionalismo digital democrático implica desarrollar estándares globales de derechos digitales, fortalecer la cooperación internacional y garantizar que la innovación tecnológica se someta a los principios de justicia y dignidad humana. Como advierte González Fuster (2023), la protección de los datos personales y la transparencia algorítmica deben entenderse como prerrequisitos para el ejercicio de la ciudadanía digital y para la preservación del espacio público deliberativo.

En conclusión, el constitucionalismo digital prolonga el legado garantista del neoconstitucionalismo, pero lo adapta a una realidad en la que el poder ya no reside solo en el Estado, sino también en infraestructuras tecnológicas privadas y en sistemas automatizados de decisión. Su propósito no es moralizar la tecnología, sino constitucionalizarla, sometiendo la lógica digital a los principios que estructuran el Estado de Derecho. De la capacidad de las constituciones para extender sus valores al ciberespacio dependerá la legitimidad de la justicia en el siglo XXI y la posibilidad de preservar la libertad en tiempos de algoritmos.

3.1.La insuficiencia del marco constitucional clásico

Una vez expuesta la configuración y el surgimiento de los actores frente a los cuales debe proyectarse el constitucionalismo digital, resulta necesario centrar la atención en los derechos que se ven vulnerados y en lo que se considera en riesgo al analizar la sociedad digital contemporánea. La digitalización y el uso intensivo de algoritmos por parte de actores privados y públicos generan nuevas formas de poder que impactan directamente en la esfera individual y colectiva, planteando desafíos inéditos para la protección de derechos fundamentales.

Entre las principales áreas de vulneración se encuentra la privacidad y la autodeterminación informativa, constantemente amenazadas por la vigilancia masiva y el seguimiento algorítmico de la actividad de los ciudadanos. Del mismo modo, la libertad de expresión y el pluralismo informativo se ven comprometidos por la manipulación de contenidos mediante algoritmos de recomendación y publicidad segmentada, que condicionan la circulación de información de acuerdo con intereses comerciales y políticos.

Asimismo, la moderación privada de contenidos en plataformas digitales configura un poder normativo ejercido por actores no estatales, sin mecanismos efectivos de control democrático, lo que plantea la necesidad de repensar los marcos de gobernanza y de garantizar la rendición de cuentas en el espacio digital. Casos como el de Cambridge Analytica (2018) ilustran cómo estas prácticas pueden influir directamente en procesos electorales, evidenciando

la relevancia de articular un constitucionalismo digital capaz de proteger derechos y preservar la integridad de la democracia frente a los nuevos poderes algorítmicos.

Los cambios tecnológicos, la globalización y la transformación de los espacios de poder han puesto en evidencia la insuficiencia tanto del constitucionalismo clásico como del neoconstitucionalismo tradicional para garantizar la protección de los derechos en entornos digitales. Los derechos fundamentales, concebidos originalmente para regular relaciones verticales entre el ciudadano y el Estado-nación, se muestran limitados frente a un poder difuso, transnacional y de naturaleza algorítmica, que actúa sin fronteras y, en numerosos casos, escapa a los mecanismos de control y a la jurisdicción local. Esta situación evidencia que los modelos clásicos de tutela constitucional, basados en la relación Estado-ciudadano, no logran responder de manera eficaz a los desafíos planteados por actores privados de alcance global o sistemas automatizados que operan mediante procesos opacos y de difícil fiscalización.

El constitucionalismo clásico se asentaba sobre un modelo centrado en el poder estatal, en el que la garantía de los derechos dependía, fundamentalmente, de la capacidad reguladora del Estado y de su aparato judicial para intervenir ante posibles vulneraciones. Este modelo funcionaba adecuadamente en contextos donde las relaciones de poder eran verticales y localizables; sin embargo, en la era digital, la dinámica de poder se ha fragmentado y globalizado, lo que ha generado espacios de influencia que trascienden las fronteras nacionales. La proliferación de plataformas digitales, corporaciones multinacionales de tecnología y sistemas de inteligencia artificial ha desplazado, en ciertos ámbitos, la centralidad del Estado, convirtiendo la protección de derechos en un desafío que requiere herramientas legales y conceptuales adaptadas a nuevas realidades.

En este contexto, el constitucionalismo digital surge como respuesta evolutiva del derecho constitucional frente a la mutación de los espacios de poder. Este enfoque reconoce que las vulneraciones de derechos pueden provenir de actores privados con alcance global y que la intervención estatal, por sí sola, resulta insuficiente. Las plataformas digitales, los algoritmos de inteligencia artificial y los sistemas de gestión de datos masivos operan a través de procesos que son, con frecuencia, opacos para los ciudadanos y para los organismos de control, dificultando la supervisión y la rendición de cuentas. Por ello, se hace necesario redefinir el alcance de la tutela de derechos, incorporando mecanismos que trasciendan la lógica estrictamente estatal y que integren la colaboración entre gobiernos, organizaciones internacionales, reguladores y actores privados responsables.

El constitucionalismo digital no busca reemplazar el neoconstitucionalismo, sino proyectarlo hacia un escenario en el que la interconexión global, la automatización de procesos y la circulación transnacional de datos redefinen las relaciones de poder. Este nuevo paradigma amplía la noción de derechos y su protección, adaptando principios garantistas a contextos en los que los impactos sobre la vida social, económica y política pueden ser inmediatos y masivos. Por ejemplo, la influencia de los algoritmos en la selección de información, en la publicidad dirigida o en la toma de decisiones automatizadas plantea desafíos inéditos a la libertad de expresión, la privacidad y la igualdad, derechos que en el marco clásico se protegían principalmente frente a acciones estatales.

Asimismo, la complejidad de las interacciones digitales evidencia la necesidad de un enfoque de gobernanza que combine regulación normativa con principios de ética tecnológica, transparencia y responsabilidad corporativa. Algunos autores sostienen que el derecho constitucional debe evolucionar hacia un modelo de "tutela preventiva", en el que no solo se protejan los derechos frente a vulneraciones consumadas, sino que se diseñen mecanismos proactivos que anticipen los riesgos generados por sistemas automatizados y plataformas transnacionales. Este enfoque preventivo, complementado con herramientas de fiscalización tecnológica, auditorías de algoritmos y estándares internacionales, permite garantizar que la expansión digital no comprometa los valores fundamentales de la democracia y la justicia constitucional.

Además, el constitucionalismo digital reconoce la interdependencia entre derechos y tecnologías. La libertad de expresión, por ejemplo, ya no solo depende de la ausencia de censura estatal, sino de la equidad en el acceso a plataformas digitales y de la transparencia en la priorización de información por algoritmos. De igual manera, la protección de la privacidad se vincula directamente con la gestión de datos masivos y la transparencia en los procesos automatizados. Esta interdependencia exige que el derecho constitucional adopte una mirada transversal y global, que integre elementos tecnológicos, regulatorios y éticos en la protección de los derechos fundamentales.

Es importante resaltar que la insuficiencia del marco constitucional clásico también tiene implicaciones en términos de jurisdicción y cooperación internacional. Muchos de los actores responsables de vulneraciones de derechos, como empresas de tecnología con operaciones en múltiples países, operan en contextos legales fragmentados. Esto limita la eficacia de las acciones judiciales tradicionales y subraya la necesidad de desarrollar marcos

regulatorios internacionales, estándares globales de protección de derechos y mecanismos de cooperación que permitan una intervención efectiva frente a amenazas transnacionales. La experiencia de casos de filtración de datos, desinformación y manipulación algorítmica demuestra que la tutela de derechos en la era digital requiere coordinación entre Estados, organizaciones multilaterales y reguladores privados.

En síntesis, el constitucionalismo digital constituye una adaptación necesaria y evolutiva del derecho constitucional frente a la transformación de los espacios de poder. Su objetivo central es garantizar la protección de la persona en un escenario en el que el poder ya no reside exclusivamente en los Estados, sino que se distribuye entre corporaciones tecnológicas, plataformas globales y sistemas de inteligencia artificial capaces de incidir de manera inédita en la vida social, económica y política. Al proyectar los principios garantistas del neoconstitucionalismo hacia el ámbito digital y transnacional, este paradigma busca reafirmar la supremacía de los derechos allí donde los poderes tecnológicos plantean desafíos sin precedentes para la democracia, la justicia constitucional y la protección integral de las personas en la era digital.

En definitiva, el constitucionalismo digital no solo representa un cambio en la forma de pensar la tutela de derechos, sino también un replanteamiento de la función del derecho frente a un entorno globalizado, automatizado y altamente interconectado. Esta perspectiva invita a repensar los conceptos tradicionales de soberanía, jurisdicción y responsabilidad, y plantea la necesidad de un derecho constitucional flexible, innovador y capaz de interactuar con otras disciplinas, como la tecnología, la ética y la gobernanza global, con el fin de garantizar una protección efectiva y equitativa de los derechos fundamentales en la sociedad del siglo XXI.

3.2.1. Principios y características del constitucionalismo digital

El constitucionalismo digital representa la evolución contemporánea del derecho constitucional, proyectando la herencia conceptual del constitucionalismo clásico y neoconstitucional hacia la era digital. Su objetivo central es garantizar la eficacia real de los derechos fundamentales en un entorno tecnológico globalizado, donde el poder ya no se concentra exclusivamente en el Estado, sino que se distribuye entre actores privados transnacionales, plataformas digitales y sistemas algorítmicos capaces de influir significativamente en la vida social, económica y política de las personas. Este nuevo paradigma implica no solo la adaptación de principios jurídicos tradicionales, sino también la

incorporación de criterios innovadores de regulación, supervisión y protección de los derechos en espacios digitales interconectados y globalizados.

A diferencia del constitucionalismo clásico, cuyo enfoque se centra en la relación vertical entre ciudadano y Estado, el constitucionalismo digital reconoce que los riesgos a los derechos fundamentales pueden originarse en actores privados con alcance transnacional, como grandes corporaciones tecnológicas, plataformas de redes sociales, proveedores de servicios de información y sistemas de inteligencia artificial. Esta ampliación del concepto de poder obliga a replantear mecanismos de control y protección que anteriormente estaban circunscritos al ámbito nacional. Por ejemplo, la protección de la privacidad y los datos personales ya no puede depender únicamente de la legislación interna de un país; requiere la adopción de estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, y la colaboración entre distintos Estados y organismos internacionales para garantizar la eficacia de las garantías.

Entre los principios fundamentales del constitucionalismo digital se encuentra la supremacía de los derechos fundamentales, que, si bien es heredada del neoconstitucionalismo, adquiere una dimensión transnacional. En este contexto, la supremacía de los derechos exige que los Estados y los actores privados respeten y garanticen los derechos en el ciberespacio, independientemente de las fronteras geográficas. Este principio se refleja en la necesidad de que las plataformas digitales implementen mecanismos de transparencia, rendición de cuentas y control sobre sus algoritmos, de manera que los usuarios puedan conocer cómo se procesan sus datos y cómo se toman decisiones automatizadas que los afectan.

Otro principio esencial es el de responsabilidad y control sobre el poder algorítmico y corporativo. Los sistemas de inteligencia artificial y los algoritmos que regulan gran parte de la información y los servicios digitales pueden generar sesgos, discriminar o limitar el acceso a derechos fundamentales. Por ello, el constitucionalismo digital propone la implementación de auditorías independientes, marcos regulatorios de ética tecnológica y normas que obliguen a las empresas a rendir cuentas frente a vulneraciones de derechos. La característica central de este principio es la prevención de daños a los derechos fundamentales antes de que se materialicen, promoviendo un enfoque proactivo y no meramente reactivo.

Asimismo, el constitucionalismo digital se caracteriza por su flexibilidad y adaptabilidad normativa. Dado el ritmo acelerado de la innovación tecnológica, las normas y

mecanismos de protección deben ser lo suficientemente dinámicos para responder a nuevos desafíos. Entre sus principios y características fundamentales destacan los siguientes.

3.2.2. Extensión de la supremacía constitucional al ciberespacio

Uno de los rasgos esenciales del constitucionalismo digital es la proyección de la supremacía constitucional hacia los entornos digitales. Esto implica reconocer que los derechos fundamentales no se agotan en el espacio físico del Estado, sino que deben protegerse también en el ciberespacio, donde se desarrollan gran parte de las interacciones sociales, económicas y políticas contemporáneas.

La libertad de expresión, por ejemplo, se encuentra profundamente condicionada por decisiones de plataformas privadas, que pueden suspender cuentas, eliminar contenidos o alterar la visibilidad de la información sin que exista control judicial inmediato. Balkin (2018) denomina a este fenómeno "New School Speech Regulation", señalando que la regulación de la expresión pública ha pasado en gran medida al ámbito privado, donde los algoritmos de moderación y las políticas internas de las plataformas funcionan como mecanismos de censura indirecta.

Además, la expansión constitucional al ciberespacio requiere considerar otros derechos fundamentales como la privacidad, la protección de datos personales y el acceso a la información. La creciente interdependencia entre individuos, empresas y gobiernos en entornos digitales genera nuevas formas de vulnerabilidad y riesgo, incluyendo la manipulación de información, la vigilancia masiva y el sesgo algorítmico.

Esta expansión de la supremacía constitucional al ámbito digital constituye un desafío normativo: obliga a repensar la eficacia horizontal de los derechos fundamentales, de manera que los actores privados dominantes en el ecosistema digital estén sometidos a límites derivados de los principios constitucionales. Asimismo, requiere diseñar mecanismos de supervisión, responsabilidad y rendición de cuentas que aseguren que la protección de los derechos fundamentales no dependa únicamente de la regulación estatal, sino que se proyecte también sobre la infraestructura y los servicios digitales que configuran nuestra vida cotidiana.

3.3.Protección frente a poderes privados globales

El constitucionalismo clásico estaba orientado a limitar el poder del Estado; sin embargo, en la era digital, los principales riesgos para los derechos provienen, en muchos

casos, de corporaciones tecnológicas globales, cuya capacidad de incidencia sobre la vida social es equiparable o incluso superior a la de muchos Estados.

Autores como De Gregorio (2020) han definido este fenómeno como "poder normativo privado", al observar que plataformas como Meta, Google, Amazon o X/Twitter no solo intermedian la comunicación y el comercio digital, sino que establecen reglas privadas de conducta que condicionan directamente el ejercicio de los derechos fundamentales. Estas empresas, mediante sus políticas internas, algoritmos de priorización y prácticas de moderación, deciden qué información circula, cómo se procesan los datos y qué contenidos se invisibilizan, operando fuera del control democrático directo.

El constitucionalismo digital, por tanto, plantea la necesidad de extender los límites constitucionales hacia estos poderes privados globales, promoviendo:

- La eficacia horizontal de los derechos fundamentales, aplicables también a relaciones entre particulares en el entorno digital.
- Mecanismos regulatorios y de supervisión transnacional, capaces de enfrentar prácticas monopólicas y abusos algorítmicos.
- Una gobernanza digital con base constitucional, que articule responsabilidades empresariales y control público efectivo.

3.3.1. Reconocimiento de nuevos derechos digitales

El constitucionalismo digital también se distingue por la emergencia de derechos fundamentales de nueva generación, vinculados con la vida digital y la sociedad de la información. Entre los más relevantes se encuentran:

- Derecho al olvido digital, consolidado por la sentencia Google Spain v. AEPD (TJUE, 2014), que permite a las personas solicitar la desindexación de información que afecte su dignidad o privacidad cuando ha perdido relevancia pública.
- Derecho a la protección y portabilidad de datos personales, reforzado por el Reglamento General de Protección de Datos (GDPR, 2018) en Europa, que reconoce la autodeterminación informativa como pilar del derecho a la privacidad en entornos digitales.

- Derecho a la neutralidad de la red, que garantiza a los usuarios un acceso igualitario a la información y los servicios sin que los proveedores puedan discriminar contenidos o priorizar tráfico en función de intereses comerciales.

- Derecho a la ciberseguridad y a la protección frente a decisiones automatizadas, emergente ante el uso de inteligencia artificial en procesos que afectan derechos como empleo, crédito, seguridad y participación política.

Estos derechos digitales reflejan la materialización de garantías constitucionales en la era tecnológica, al trasladar la protección efectiva de los derechos humanos a espacios donde las amenazas se manifiestan en forma de algoritmos, datos y plataformas privadas.

3.3.2. Dimensión transnacional y gobernanza cooperativa

El constitucionalismo digital posee una dimensión intrínsecamente transnacional, debido a que Internet y los flujos de datos trascienden las fronteras estatales. La efectividad de los derechos digitales no puede garantizarse mediante acciones aisladas de los Estados, sino que requiere mecanismos de gobernanza global que permitan armonizar estándares y coordinar esfuerzos regulatorios.

Entre los instrumentos internacionales que reflejan esta tendencia se encuentran:

- El Convenio de Budapest sobre Ciberdelincuencia (2001), que establece parámetros de cooperación judicial y policial frente a delitos informáticos transnacionales.

- Las Directrices de la OCDE sobre Inteligencia Artificial (2019), que promueven el uso responsable y ético de la IA, incorporando principios de transparencia, seguridad y respeto a los derechos humanos.

- Propuestas recientes de regulación supranacional, como la Digital Services Act (2022) y la AI Act en la Unión Europea, que buscan someter a las plataformas digitales y algoritmos a controles normativos consistentes con los valores constitucionales.

Esta dimensión transnacional y cooperativa evidencia que el constitucionalismo digital no puede limitarse a un marco estrictamente nacional. La protección efectiva de los derechos exige respuestas coordinadas, estándares internacionales claros y mecanismos de supervisión

multinivel, donde los principios constitucionales sirvan de guía para la gobernanza global de lo digital.

En suma, el constitucionalismo digital se define por la proyección de la supremacía constitucional al ciberespacio, la protección frente a poderes privados globales, el reconocimiento de derechos digitales de nueva generación y la necesaria dimensión transnacional y cooperativa. Este paradigma expande el horizonte del constitucionalismo garantista, buscando que los principios de dignidad, libertad, igualdad y justicia sean eficaces también en entornos algorítmicos y globalizados.

No obstante, su consolidación enfrenta desafíos críticos: la asimetría de poder entre Estados y corporaciones tecnológicas, la opacidad de los algoritmos, la fragmentación regulatoria internacional y la tensión entre intereses comerciales y derechos fundamentales. El constitucionalismo digital no solo extiende la promesa del Estado constitucional a la era tecnológica, sino que abre un laboratorio de tensiones jurídicas y políticas que exigirá innovación normativa y cooperación global para garantizar su vigencia y efectividad real.

3.3.3. Normativa y jurisprudencia destacada

El constitucionalismo digital no se limita a un ejercicio teórico o prospectivo; por el contrario, ha comenzado a materializarse en normas, políticas públicas y decisiones judiciales que reflejan la proyección de los valores constitucionales al entorno digital. Estas manifestaciones son indicios claros de que los principios garantistas del neoconstitucionalismo se están adaptando a los retos del ciberespacio, aunque su implementación práctica enfrenta desafíos significativos.

En el plano normativo internacional, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (2016/2018) constituye uno de los hitos más relevantes en la consolidación de la autodeterminación informativa como derecho fundamental. Este instrumento no solo refuerza la protección de la privacidad, sino que impone obligaciones directas a los actores privados globales que tratan datos personales de ciudadanos europeos, incluso cuando sus operaciones se realizan fuera de la UE. Desde una perspectiva crítica, el GDPR representa un avance en la eficacia transnacional del derecho constitucional, pues trasciende las fronteras estatales clásicas, aunque su aplicación efectiva depende de la capacidad de supervisión de las autoridades nacionales y europeas frente a corporaciones tecnológicas de alcance planetario.

La jurisprudencia europea también ha contribuido a definir estándares del constitucionalismo digital, destacando la sentencia Google Spain v. AEPD (TJUE, 2014), que reconoció por primera vez el derecho al olvido digital. En ella, el Tribunal de Justicia de la Unión Europea estableció que los motores de búsqueda están obligados a eliminar enlaces que vulneren la privacidad o la reputación de las personas, cuando la información haya perdido relevancia pública. Este fallo constituye un precedente paradigmático, pues traslada la lógica garantista del derecho a la intimidad a la esfera digital, imponiendo obligaciones a actores privados globales. Sin embargo, genera debates críticos: algunos autores advierten que la aplicación del derecho al olvido puede entrar en tensión con la libertad de información y, en determinados casos, favorecer la desindexación de información de interés público, lo que plantea dilemas sobre el equilibrio entre privacidad y transparencia en la era digital.

En el ámbito nacional europeo, la Carta de Derechos Digitales de España (2021) representa un intento pionero de sistematizar la proyección de los derechos constitucionales al entorno digital. Este documento incorpora nuevos derechos y garantías, como el derecho a la desconexión digital, la neutralidad tecnológica, la protección frente a riesgos asociados a la inteligencia artificial y el derecho a la educación digital. Si bien la Carta no tiene fuerza vinculante estrictamente constitucional, su valor reside en ofrecer un marco interpretativo y programático que guía la adecuación del ordenamiento jurídico español a los retos de la sociedad digital. No obstante, su eficacia práctica aún depende de su integración en leyes orgánicas y de la labor interpretativa de los tribunales constitucionales, lo que pone de relieve la distancia entre los compromisos declarativos y la protección efectiva de los derechos digitales.

En el contexto latinoamericano, la jurisprudencia de la Corte Constitucional colombiana ha comenzado a incorporar dimensiones digitales a los derechos fundamentales tradicionales. La Sentencia T-063 de 2020 constituye un ejemplo paradigmático: en ella, la Corte amparó el derecho a la protección de datos personales en redes sociales, ordenando la eliminación de información difundida sin autorización y reconociendo que las plataformas privadas también pueden afectar derechos fundamentales en el entorno digital. Este fallo refleja la evolución del amparo constitucional hacia el ciberespacio, pero también evidencia los límites estructurales de la justicia constitucional nacional frente a plataformas transnacionales, cuya capacidad de cumplir decisiones judiciales locales depende de mecanismos de cooperación y presión regulatoria internacional.

La emergencia de estas normas y sentencias confirma que el constitucionalismo digital ha dejado de ser una mera especulación doctrinal para convertirse en un proceso de transformación jurídica en marcha, que adapta el garantismo constitucional a la era tecnológica. Sin embargo, su implementación efectiva sigue condicionada por desafíos críticos: la asimetría de poder entre Estados y corporaciones tecnológicas, la opacidad algorítmica que dificulta el control judicial, la fragmentación regulatoria internacional y la tensión entre derechos fundamentales en entornos digitales, como la colisión entre privacidad y libertad de expresión. Estas manifestaciones normativas y jurisprudenciales muestran avances significativos, pero también revelan la necesidad de consolidar un marco constitucional global y cooperativo, capaz de proteger eficazmente la dignidad humana y los derechos fundamentales en la sociedad digital. Las mismas tendrán una profundización más relevante en el capítulo 4.

3.3.4. Desafíos y proyección hacia el constitucionalismo del derecho digital

El constitucionalismo digital se encuentra en una fase de consolidación y redefinición, marcada por desafíos estructurales que comprometen su eficacia real en la protección de los derechos fundamentales. La fragmentación normativa internacional, la asimetría entre Estados y corporaciones tecnológicas y la opacidad de los sistemas algorítmicos revelan las limitaciones del marco actual y justifican la evolución hacia un constitucionalismo del derecho digital, concebido como una etapa superior en la constitucionalización integral del ecosistema digital.

Uno de los principales retos es la fragmentación normativa global, que impide garantizar una protección homogénea de los derechos digitales. Mientras la Unión Europea ha logrado avances con el GDPR y la Digital Services Act, muchos Estados latinoamericanos y africanos mantienen vacíos legislativos o normativas dispersas, lo que genera desigualdad en la tutela de la privacidad, la libertad de expresión y la protección de datos. Esta situación evidencia la urgencia de avanzar hacia marcos cooperativos de gobernanza digital, donde Estados, organismos internacionales y sociedad civil articulen estándares comunes y mecanismos de supervisión transnacional.

El segundo desafío proviene de la asimetría entre los Estados y las corporaciones tecnológicas, cuya capacidad de incidencia social y económica supera, en muchos casos, la de los gobiernos nacionales. Plataformas como Google, Meta o Amazon ejercen un poder normativo privado que decide sobre el acceso a la información, la visibilidad de contenidos y la explotación de datos personales. Frente a esta realidad, los mecanismos tradicionales de

control estatal resultan insuficientes. Es aquí donde tu proyecto de ley encuentra pleno sentido, al proponer herramientas normativas para garantizar una gobernanza digital democrática, con participación del Estado en la regulación de plataformas, la protección de la soberanía de datos y la responsabilización jurídica de actores privados globales.

La emergencia de la inteligencia artificial introduce un tercer reto crítico: la opacidad y el sesgo algorítmico. La automatización de decisiones, desde la moderación de contenidos hasta la concesión de créditos o la vigilancia masiva, plantea riesgos de discriminación y afectación de derechos sin supervisión humana efectiva. La respuesta a este fenómeno no puede limitarse a la autorregulación empresarial; requiere un marco de derecho digital constitucionalizado, que integre principios de ética algorítmica, transparencia y explicabilidad, así como mecanismos de auditoría pública y control jurisdiccional sobre sistemas automatizados.

Frente a estos desafíos, la proyección hacia un constitucionalismo del derecho digital supone un cambio de paradigma. Ya no se trata únicamente de proteger derechos en el ciberespacio, sino de construir un orden digital constitucionalizado, donde los principios de dignidad, libertad e igualdad se apliquen integralmente en la gobernanza de datos, plataformas y algoritmos. Este nuevo enfoque debe incorporar:

1. Soberanía digital y de datos, que permita a los Estados recuperar capacidad de decisión frente a la explotación transnacional de información personal.

2. Responsabilidad jurídica de plataformas y proveedores de servicios digitales, con estándares claros de transparencia, ética algorítmica y reparación de daños.

3. Participación activa de los Estados en la gobernanza digital, no solo como reguladores, sino como garantes de un ecosistema digital justo y seguro, en diálogo con sociedad civil y organismos internacionales.

4. Cooperación regional e internacional, que armonice estándares normativos para evitar vacíos de protección y conflictos de jurisdicción en un entorno transnacional y deslocalizado.

En este marco, el proyecto de ley que acompaña esta investigación se presenta como una propuesta concreta para avanzar hacia un derecho digital constitucionalizado, donde la

gobernanza de datos y plataformas se someta a principios de transparencia, equidad y control democrático. La proyección futura del constitucionalismo digital dependerá, así, de su capacidad de evolucionar hacia un modelo integral de gobernanza, en el que los Estados dejen de ser espectadores pasivos y asuman un rol activo en la protección de los derechos en la era digital.

La reflexión sobre los desafíos del constitucionalismo digital evidencia que el derecho constitucional contemporáneo ya no puede comprenderse sin atender al impacto estructural de la transformación tecnológica. La aparición de nuevos poderes algorítmicos y corporaciones globales, así como la emergencia de riesgos inéditos para la privacidad, la libertad y la igualdad, obliga a repensar la relación entre Estado, derecho y tecnología, proyectando un constitucionalismo del derecho digital capaz de garantizar dignidad y justicia en la sociedad interconectada. Esta evolución jurídica no surge en el vacío, sino que responde a un proceso histórico de profundas transformaciones sociales y económicas, alimentado por las revoluciones industriales y las sucesivas olas de innovación tecnológica que han modificado la estructura del poder y la configuración de los derechos. En este contexto, el siguiente capítulo analizará el itinerario histórico de las revoluciones industriales, la irrupción de las tecnologías emergentes y las nuevas tendencias globales, que constituyen el marco evolutivo indispensable para comprender la transición hacia un derecho digital constitucionalizado y adaptado al siglo XXI.

Tabla 4.

Derecho comparado sobre constitucionalismo digital.

País / Región	**Norma o instrumento**	**Lecciones para Colombia**
España	Carta de Derechos Digitales (2021)	Reconocimiento expreso de derechos digitales y principios de gobernanza tecnológica.
Unión Europea	Reglamento General de Protección de Datos (2016) y futura Ley de IA	Protección robusta de datos personales, ética algorítmica y responsabilidad tecnológica.

Brasil	Lei Geral de Proteção de Dados – LGPD (2018)	Regulación integral de datos, sanciones claras y autoridad nacional especializada.
México	Ley Federal de Protección de Datos Personales (2010)	Protección administrativa de datos personales, aunque limitada en entornos emergentes.
Chile	Reforma constitucional y proyecto de Ley de Datos	Reconocimiento de la protección de datos como derecho autónomo de rango constitucional.

Fuente: Elaboración propia (2025).

3.4.Inserción del constitucionalismo digital en Latinoamérica.

Desde su surgimiento en 1983, Internet no fue reconocido como un derecho humano hasta 2011, cuando se estableció la obligación de garantizar un "acceso universal al ciberespacio", entendido como un acceso equitativo, asequible y que permita a todas las personas disponer tanto de la infraestructura como de la información y conocimientos necesarios para su desarrollo individual y colectivo (La Rue, 2011).

Posteriormente, en 2012, el Consejo de Derechos Humanos de la ONU reafirmó que los derechos humanos deben ser protegidos y ejercidos también en el entorno digital, declaración respaldada por varios países iberoamericanos como Chile, España y México.En los últimos treinta años, la Unión Europea ha transitado de una visión económica liberal en materia de tecnologías digitales hacia un enfoque constitucional orientado a proteger los derechos fundamentales y los valores democráticos (De Gregorio 2021). Este giro responde al creciente debate sobre la sociedad de la información, cada vez más influida por actores públicos y privados que desarrollan tecnologías de decisión automatizada (Danaher 2016).

Por lo tanto, la transformación constitucional se replica en Latinoamérica, analizada desde distintas perspectivas, las cuales se presentarán en los acápites subsiguientes.

3.4.1. México.

En México, fue hasta 2013 cuando, a partir de las reformas al artículo 6º constitucional en materia de telecomunicaciones, se incorporó la regulación del derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el Internet de banda ancha. La Ley Federal de Telecomunicaciones y Radiodifusión, junto con la Secretaría de Comunicaciones y Transportes y el Instituto Federal de Telecomunicaciones, asumió la responsabilidad de promover este acceso y de impulsar políticas relacionadas con la conectividad (Gónzalez, 2022).

Estos avances permiten afirmar que México ha comenzado a construir las bases de un incipiente constitucionalismo digital, estos esfuerzos se han concentrado principalmente en el reconocimiento de derechos y en explorar la relación entre Internet y la Constitución. Esto se refleja en los proyectos legislativos sobre derechos digitales y modernización de las comunicaciones, entre ellos las propuestas para garantizar el mandato constitucional de inclusión digital universal mediante la implementación de una renta básica digital.

La Constitución reconoce diversos derechos fundamentales que permiten a las personas proteger sus datos e información en entornos digitales, todavía no se contempla un mecanismo claro de control sobre los proveedores de servicios de Internet; y específicamente en el ámbito legislativo, México sancionó una modificación a la Ley Federal de Protección de datos personales en posesión de particulares en 20 de marzo de 2025. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) fue promulgada en México el 5 de julio de 2010 con el propósito de regular el tratamiento de datos personales por parte de empresas y demás sujetos privados. Posteriormente, se expidió su Reglamento en 2011 y, en 2013, los Lineamientos del Aviso de Privacidad, con el fin de precisar obligaciones y procedimientos.

La adición y reforma reciente Su consiste en la transparencia y acceso a la información pública, también a la transferencia de datos y detalla también en el capítulo VIII un procedimiento de protección de derechos en caso de que un particular haya solicitud de reclamación para protección de datos, reflejando una forma de ‘control’ sobre entidades privadas que manejan datos (Ley Federal de Protección de datos, 2025).

También contiene un apartado coercitivo al tipificar los delitos en materia de tratamiento indebido de datos personales, sin embargo, aún este marco de constitucionalismo digital se encuentra limitado (González, 2022).

3.4.2. Chile.

En el marco jurídico chileno vigente, no existe actualmente una regulación constitucional explícita sobre materias digitales, como la sociedad digital, los derechos digitales o la transformación digital. Las referencias al ámbito digital en la Constitución se limitan a menciones excepcionales en artículos transitorios relacionados con el contexto de la pandemia de COVID-19, procesos electorales y medidas económicas extraordinarias (Castillo, 2025).

Sin embargo, el borrador de la propuesta constitucional de 2022 incorporó múltiples disposiciones vinculadas a lo digital y a la modernización del Estado. Estas referencias se distribuyeron a lo largo del texto constitucional y abordaron diversos ámbitos:

- **Artículo 33:** Reconocía, en el marco de los derechos de las personas mayores, la accesibilidad al entorno físico, social, económico, cultural y digital.
- **Artículo 46:** Establecía garantías en materia laboral, entre ellas el derecho a la desconexión digital.
- **Artículo 152:** Obligaba a los poderes públicos a facilitar la participación ciudadana mediante mecanismos digitales, cuya regulación quedaría a cargo de la ley.
- **Artículo 178:** Mandataba al Estado a modernizar sus procesos mediante ciencia, tecnología e innovación.
- **Artículo 216:** Imponía a las municipalidades la obligación de promover la participación ciudadana, para lo cual debían garantizar recursos, espacios y alfabetización digital.
- **Artículo 220:** Atribuía a las regiones autónomas competencias relativas a la conectividad física y digital.

Además, el Capítulo II, relativo a derechos fundamentales, recopilaba varias disposiciones centrales sobre derechos digitales, particularmente los artículos 86 a 90. El Artículo 86 reconocía el derecho al acceso universal a la conectividad digital y a las tecnologías de la información y comunicación, estableciendo obligaciones del Estado para garantizar un acceso libre, equitativo y descentralizado. También incorporaba deberes estatales para reducir

brechas digitales, asegurar la neutralidad de la red y considerar la infraestructura de telecomunicaciones como de interés público.

Por otra parte, la propuesta de 2022 incluía el reconocimiento de la autodeterminación informativa y la protección de datos personales (artículo 87), otorgando a las personas facultades para conocer, decidir y controlar el uso de sus datos, así como ejercer derechos como acceso, rectificación, cancelación, oposición y portabilidad.

En conjunto, los procesos constitucionales de 2022 y 2023 en Chile representaron un esfuerzo significativo por incorporar normas sobre derechos digitales, participación digital y modernización tecnológica, aun cuando dichas propuestas no llegaron a consolidarse en la Constitución vigente (Castillo, 2025)

3.4.3. Brasil.

En Brasil, el Marco Civil de Internet (MCI) redefinió el equilibrio de poder entre el sector público y los actores privados al establecer salvaguardas claras contra violaciones a la privacidad y a las comunicaciones de los usuarios, tanto por parte de autoridades como de los proveedores de acceso. Además, impuso a estos últimos la obligación de conservar determinados datos que permitan identificar a usuarios involucrados en actividades ilícitas (Saavedra & de Aguiar, 2022)

El MCI no solo introdujo reglas específicas de responsabilidad, sino que también fijó principios y directrices que reconocen explícitamente la protección de la libertad de expresión y de la privacidad en el entorno digital, frente a posibles abusos de agentes públicos y privados. Estos elementos, sumados al amplio nivel de participación social que caracterizó su elaboración y aprobación, han llevado a que diversos analistas describan esta ley como una especie de "Constitución de Internet" o incluso como una "Carta de Derechos Digital" (Moncau & Arguelhes, 2020).

Antes del Marco Civil de Internet (MCI), los tribunales brasileños estaban saturados de casos sobre la responsabilidad de las plataformas por actos ilícitos de sus usuarios. Esto generó demanda por una regulación que diera seguridad jurídica a usuarios y proveedores. Entre las propuestas surgió el proyecto de ley de ciberdelitos del senador Eduardo Azeredo, inspirado en la Convención de Budapest, pero criticado por riesgos a la privacidad y a la vigilancia.

Las reacciones a ese proyecto impulsaron una alternativa: en lugar de criminalizar conductas, establecer principios y derechos para el uso de Internet. Así nació la idea del MCI, cuyo anteproyecto fue elaborado mediante un proceso participativo promovido por el Ministerio de Justicia y la FGV. Con el avance de una economía cada vez más basada en datos, el MCI se volvió insuficiente, evidenciando la necesidad de una legislación más amplia en materia de protección de datos personales.

El Superior Tribunal de Justicia (STJ), especialmente en casos relativos a la aplicación del Código de Defensa del Consumidor a los registros negativos de crédito, ya señalaba la aparición de un nuevo concepto de privacidad que requería una protección distinta a la tradicional, entendida solo como exclusión de terceros. En 1995, en el juicio del REsp 22.337-8/RS, el ministro Ruy Rosado hizo referencia al derecho fundamental a la autodeterminación informativa, inspirado en la experiencia alemana (Cueva, 2019).

Este desarrollo jurisprudencial preparó el terreno para la promulgación, en 2018, de la Ley General de Protección de Datos (LGPD), cuyo objetivo es fortalecer el papel del titular de los datos y otorgarle mayor control sobre el tratamiento de su información. La normativa busca, en la medida de lo posible, mitigar los efectos del creciente modelo económico basado en la vigilancia y la opacidad (Frazão & Mulholland, 2020).

Entre los principales **requisitos de cumplimiento**, destacan:

- **Consentimiento:** debe ser explícito e informado por parte del titular de los datos.
- **Transparencia:** las organizaciones deben informar claramente el propósito, tipo de datos, duración del procesamiento y responsables del tratamiento.
- **Limitación de propósito:** los datos solo pueden usarse para fines específicos y legítimos.
- **Seguridad:** implementación de medidas técnicas y administrativas para proteger los datos contra accesos no autorizados o tratamientos indebidos.
- **Notificación de violaciones:** informar a los titulares y a la Autoridad Nacional de Protección de Datos (ANPD) ante incidentes que puedan causar daño.
- **Derechos del titular:** acceso, corrección, anonimización, bloqueo, eliminación, revocación del consentimiento y portabilidad de los datos.

- **Oficial de Protección de Datos (DPO):** figura responsable de la relación entre la organización, los titulares y la ANPD.

La ANPD es la autoridad brasileña encargada de supervisar y garantizar el cumplimiento de la LGPD, promoviendo educación sobre protección de datos, investigando incumplimientos y aplicando sanciones cuando sea necesario (Flores, 2023).

Según Saavedra y Aguiar (2022), Brasil atraviesa actualmente una fase de constitucionalismo digital, entendida como la regulación jurídica del uso de nuevas tecnologías para garantizar su ejercicio legítimo. Esta tendencia se evidencia en la participación ciudadana durante la elaboración del Marco Civil de Internet (MCI) y en la creciente protección de derechos constitucionales como la intimidad, la privacidad, la neutralidad de la red y la autodeterminación informativa. Aunque leyes como el MCI y la LGPD no bastan por sí solas para consolidar plenamente el constitucionalismo digital, Brasil avanza hacia la constitucionalización del entorno digital, marcando una clara orientación hacia la regulación de los derechos y valores fundamentales en el contexto tecnológico actual.

3.5.Constitucionalismo digital: inserción en Colombia

Al ver el transcurrir de países latinoamericanos, se hace importante recalcar la doctrina del 'efecto horizontal' de la constitución. El constitucionalismo digital no solo fue una respuesta ante los fenómenos de transformación digital, sino que su inserción se hizo posible mediante el efecto horizontal de disposiciones constitucionales que pueden hacer 'vivo' el derecho para responder adecuadamente a la globalización y a la aparición de nuevos actores e instituciones no estatales (Golia 2022).

La doctrina del efecto horizontal (en contraste con el *State action*[9] de Estados Unidos) sostiene que los derechos constitucionales también pueden vincular a particulares entre sí (Gardbaum 2003). Este enfoque ha sido ampliamente desarrollado en América Latina, donde Colombia ha incorporado la cláusula constitucional que reconocen la aplicación horizontal de ciertos derechos (CP, 1991. Art 86[10]). Asimismo, la consolidación de mecanismos como el

[9] Como explica De Gregorio (2022), las constituciones clásicas se diseñaron para contener el poder del Estado y proteger a las personas frente a las autoridades públicas, asumiendo que el único poder relevante era el estatal. Bajo esta concepción, conocida como efecto vertical, los derechos fundamentales solo regulan la relación entre Estado y particulares, como ocurre en Estados Unidos a través de la doctrina del *State action*. (Del Campo, 2025).

[10] ***Artículo 86.*** Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o

amparo o la tutela, que proceden tanto contra autoridades públicas como contra privados, ha reforzado esta eficacia horizontal (Brewer Carias, 2007). Este punto resulta fundamental para entender el punto de partida del constitucionalismo digital en la región Colombia.

Del Campo (2025) sostiene que esta inserción se hace posible a través de la jurisprudencia de la Corte Constitucional colombiana, la cual ha abordado diversos casos mediante la acción de tutela recurriendo ampliamente al derecho internacional y comparado. En estas decisiones, la Corte ha rechazado la aplicación de un régimen de responsabilidad objetiva a los intermediarios de Internet, pues consideró que ello restringiría la libertad de expresión. Según el tribunal, este derecho no solo ampara la emisión de ideas e información, sino también su difusión y alcance; en consecuencia, imponer responsabilidad a los intermediarios afectaría gravemente la circulación de contenidos.

Si bien la Corte concluyó que los servicios de Internet no eran responsables por el contenido transmitido, sí declaró responsable al periódico *El Tiempo*, co-demandado, por no actualizar la información digitalizada cuando la accionante lo solicitó. Del mismo modo, descartó la aplicación del derecho al olvido y del régimen de protección de datos en este tipo de supuestos, fundamentando su decisión en la configuración constitucional de la libertad de prensa, que exige veracidad y precisión en la información publicada.

Posteriormente, en la sentencia SU-420 de 2019, la Corte reafirmó la doctrina de inmunidad de responsabilidad de los intermediarios digitales. No obstante, precisó que los jueces pueden ordenar la eliminación de contenido publicado por terceros cuando dicho contenido vulnera derechos fundamentales y resulta imposible identificar al autor. Además, aclaró que estas órdenes deben ser puntuales y específicas, ya que la suspensión general de sitios web constituye un acto de censura, prohibido por la Constitución colombiana.

El derecho internacional de los derechos humanos ocupa un lugar central en los marcos jurídicos de Colombia, otorgándoles jerarquía constitucional o supralegal, o al menos

amenazados por la acción o la omisión de cualquier autoridad pública. La protección consistirá en una orden para que aquel respecto de quien se solicita la tutela, actúe o se abstenga de hacerlo. El fallo, que será de inmediato cumplimiento, podrá impugnarse ante el juez competente y, en todo caso, éste lo remitirá a la Corte Constitucional para su eventual revisión. Esta acción solo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que aquella se utilice como mecanismo transitorio para evitar un perjuicio irremediable. En ningún caso podrán transcurrir más de diez días entre la solicitud de tutela y su resolución. La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión. (CP, 1991).

reconociéndolos con fuerza de ley interna (Gargarella 2018). Asimismo, las cortes supremas y la jurisprudencia constitucional latinoamericana han mostrado gran apertura hacia este derecho internacional, mientras que el Sistema Interamericano de Derechos Humanos ha sido un motor clave de reformas jurídicas en la región (Steiner y Uribe 2014).

Los desarrollos judiciales locales en Colombia han estado acompañados por avances en estándares de derecho internacional no vinculante, especialmente los promovidos por la Comisión Interamericana de Derechos Humanos. En América Latina, países como Argentina, Colombia y, en menor medida, México, han mostrado una especial permeabilidad hacia el derecho regional de los derechos humanos, citándolo y aplicándolo explícitamente en los tribunales, o bien rechazándolo de manera fundamentada. Entre los hitos más relevantes en materia de gobernanza de contenidos y derechos humanos en línea se destacan los informes de los Relatores Especiales de 2013 y 2017, que, aplicando los ya sólidos estándares de libertad de expresión a Internet, concluyeron que los regímenes de inmunidad, como los vigentes en Estados Unidos y Europa, resultan en términos generales consistentes con la importancia de la red para la circulación libre de información (Del Campo, 2025).

Los casos actualmente en curso abren nuevas líneas de análisis y muestran un desarrollo orgánico de estándares bajo el marco constitucional y de derechos humanos vigente, aplicados al sector de las TIC y a la gestión de contenidos digitales. A diferencia de otras regiones, Colombia no se están creando normas específicamente dirigidas a regular contenidos en línea; más bien, los tribunales están adaptando los estándares existentes de responsabilidad civil y constitucional a las nuevas tecnologías, aunque esto no siempre sea producto de una intención deliberada. De hecho, la mayoría de los tribunales han señalado a los legisladores nacionales la necesidad de normas más precisas o específicas, al igual que los relatores regionales; sin embargo, ante la ausencia de tales regulaciones, los tribunales han desarrollado un cuerpo de jurisprudencia progresiva que podría aportar insumos valiosos para un análisis comparado sobre gobernanza de contenidos y responsabilidad de intermediarios a nivel global. Los mismos se darán en análisis más profundo en el capítulo siguiente.

3.6. Marco constitucional, legal y jurisprudencial colombiano frente a la transformación digital.

El vertiginoso avance de la quinta revolución industrial y la consolidación de las tecnologías emergentes plantean retos sin precedentes para los marcos constitucionales y legales, que fueron diseñados para una realidad analógica y ahora enfrentan fenómenos propios de la era digital. Como se evidenció en el Capítulo 2, la expansión de herramientas como Big Data, inteligencia artificial, *blockchain*, metaverso, robótica avanzada y ciber-robots con sintiencia digital transforma profundamente la vida social, económica y jurídica, generando tensiones directas sobre los derechos fundamentales.

En este contexto, el Capítulo 4 examina el marco constitucional, legal y jurisprudencial colombiano frente a los desafíos de la transformación digital. También aborda la regulación y marco normativo internacional que se ha dado hasta ahora en los entornos digitales, los cuales sirven de base y proyección para adaptación a normas en el régimen colombiano.

Siendo la base de las normas, se analizará cómo la Constitución Política de 1991 y las normas posteriores han incorporado la protección de la intimidad, el habeas data, la igualdad, la libertad de expresión y el debido proceso en entornos digitales. Asimismo, estudia las leyes específicas y políticas públicas que regulan la digitalización, incluyendo la Ley 2502 de 2025, que marca un hito en la regulación de la inteligencia artificial y la prevención de su uso indebido.

El capítulo también incorpora un análisis de la jurisprudencia constitucional más relevante, evidenciando cómo la Corte Constitucional ha protegido derechos en escenarios de digitalización, aunque persisten vacíos normativos significativos. Estos vacíos se expresan en la falta de regulación integral sobre IA, blockchain, metaverso y ciber-robots, lo que genera incertidumbre jurídica y vulnerabilidad para los ciudadanos y las empresas.

En suma, este capítulo busca diagnosticar el estado actual del marco normativo colombiano ante la transformación digital, identificando avances, limitaciones y vacíos que justifican la construcción de un constitucionalismo digital colombiano. Su cierre servirá como base para el Capítulo 5, donde se abordarán los retos y desafíos que enfrenta el país en la protección de los derechos fundamentales en la era de la quinta revolución industrial.

El análisis del marco constitucional, legal y jurisprudencial colombiano frente a la transformación digital pone en evidencia que, aunque existen avances normativos y políticas públicas recientes, incluido el impulso dado por la Ley 2502 de 2025, el país aún carece de un marco integral capaz de responder a los retos de la quinta revolución industrial.

Este panorama confirma la pertinencia y necesidad de un constitucionalismo digital colombiano, entendido como la adaptación de los principios y garantías constitucionales a los entornos tecnológicos emergentes. Dicho enfoque permitiría armonizar la innovación con la protección de los derechos fundamentales, garantizando que la dignidad humana, la privacidad, la igualdad y la seguridad jurídica no se vean comprometidas frente a fenómenos como la inteligencia artificial, el blockchain, el metaverso y los ciber-robots.

3.7.Protección de los derechos fundamentales en entornos digitales

La transformación digital, intensificada por la quinta revolución industrial, ha modificado profundamente la forma en que los individuos ejercen y defienden sus derechos fundamentales. La masificación del Big Data, la inteligencia artificial (IA), el blockchain, el metaverso y la robótica avanzada ha introducido escenarios en los que derechos como la vida, la integridad personal, la intimidad, el habeas data, la igualdad y la libertad de expresión enfrentan riesgos inéditos. La Constitución de 1991, concebida para un mundo analógico, se encuentra desafiada por fenómenos propios de la sociedad digital, generando vacíos normativos que afectan la efectividad de las garantías fundamentales.

Como advierte Pérez Luño (2019), los derechos fundamentales constituyen el núcleo intangible de la dignidad humana, pero su ejercicio en entornos digitales exige una reinterpretación dinámica. Ferrajoli (2020) complementa esta idea al señalar que el Estado constitucional debe asegurar una protección efectiva frente a las nuevas fuentes de riesgo derivadas de la tecnología, garantizando que la innovación no erosione los valores esenciales del Estado social de derecho. De manera similar, Kelsen (2009) recuerda que la validez del derecho depende de su capacidad para adaptarse a la realidad social, lo que en la era digital implica incorporar mecanismos normativos frente a la inteligencia artificial, la tokenización y la sintiencia digital.

En este contexto, la doctrina contemporánea coincide en que la protección de los derechos fundamentales requiere una estrategia jurídica proactiva. Zuboff (2019) alerta sobre el surgimiento de un capitalismo de vigilancia que transforma a las personas en perfiles

algorítmicos, mientras Sartor (2021) advierte sobre la discriminación automatizada y la erosión de la autonomía individual. Byung-Chul Han (2018) y Castells (1999) complementan esta visión al evidenciar cómo la hiperconectividad y la sociedad en red alteran la percepción de libertad y generan nuevas formas de control social. Ante esta realidad, la necesidad de un constitucionalismo digital colombiano se hace patente, entendido como la adaptación de los principios constitucionales al entorno tecnológico para garantizar la dignidad, la igualdad y la seguridad jurídica en la era digital.

3.8.Marco normativo internacional: tratados en la regulación de nuevas tecnologías.

Europa contiene uno de los sistemas más rigurosos y robustos en lo que concierne a protección de datos y regulación de tecnologías emergentes. Su regulación comprende un marco jurídico robusto que combina la legislación en materia de derechos humanos, el Reglamento General de Protección de Datos (GDPR), la Directiva de Aplicación de la Ley (LED) y la recientemente adoptada Ley de Inteligencia Artificial (AI Act). Desde la perspectiva de los derechos humanos, la prohibición sustantiva de discriminación se refleja en el derecho a la no discriminación, que protege contra el trato desigual basado en características protegidas, y en el derecho a la igualdad de trato, que exige que cualquier diferenciación en el ejercicio de derechos sea razonable y justa.

3.8.1. Reglamento General de Protección de datos (GDPR).

El Reglamento General de Protección de Datos (GDPR), vigente desde el 25 de mayo de 2018, constituye la normativa de privacidad y seguridad más estricta del mundo, aplicable a todas las organizaciones que procesen datos personales de ciudadanos o residentes de la Unión Europea, independientemente de que la entidad tenga sede dentro o fuera del territorio comunitario (Zaeeem y Barber, 2020).

Su objetivo es garantizar la protección de los datos personales y reforzar los derechos de los individuos frente a un uso indebido de su información en contextos cada vez más digitales y globalizados. El GDPR establece principios fundamentales para el tratamiento de datos: licitud, equidad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del almacenamiento; integridad y confidencialidad; y rendición de cuentas, que obliga a los responsables del tratamiento a poder demostrar su cumplimiento normativo. Asimismo, introduce la obligación de protección de datos desde el diseño y por defecto, lo que implica que cualquier producto, servicio o actividad que involucre datos

personales debe considerar la privacidad como componente estructural (GDPR, 2018, Art 8, 11, 83).

El reglamento define claramente los roles de responsables del tratamiento y encargados del tratamiento, regulando las responsabilidades de quienes deciden cómo y por qué se procesan los datos, así como de los terceros que los procesan en su nombre. Establece criterios estrictos para la obtención del consentimiento, que debe ser libre, informado, específico y verificable, y permite a los titulares retirarlo en cualquier momento. También regula la designación de un delegado de Protección de Datos (DPO) para organizaciones que realizan monitoreo sistemático a gran escala o procesan categorías especiales de datos, cuya función es asesorar, supervisar y actuar como nexo con las autoridades de control (GDPR, 2018).

El GDPR otorga a los titulares de datos una serie de derechos específicos, incluyendo: derecho a ser informado, derecho de acceso, derecho de rectificación, derecho de supresión ("derecho al olvido"), derecho a restringir el procesamiento, derecho a la portabilidad de los datos, derecho a oponerse al tratamiento y derechos en relación con decisiones automatizadas y perfilado. Complementariamente, establece obligaciones de seguridad técnica y organizativa, incluyendo cifrado, autenticación reforzada, limitación de acceso y capacitación del personal, así como la obligación de notificar cualquier violación de datos personales en un plazo máximo de 72 horas (GDPR, 2018. Arts 77-84).

Además, el GDPR prevé mecanismos de supervisión y sanción mediante las autoridades de protección de datos de cada Estado miembro, facultadas para imponer multas proporcionales a la gravedad de las infracciones, que pueden alcanzar hasta 20 millones de euros o el 4 % de la facturación anual global, así como para exigir compensaciones a los afectados. En conjunto, este marco normativo busca equilibrar la innovación tecnológica y la explotación de datos con la salvaguarda de los derechos fundamentales, asegurando que las organizaciones implementen medidas preventivas y correctivas para proteger la privacidad y otorgar a los individuos un control efectivo sobre su información personal (GDPR, 2018. Arts 51-54).

En el contexto del perfilado algorítmico, los organismos de supervisión y las entidades responsables deben demostrar que cualquier diferencia de tratamiento derivada de los perfiles de riesgo utilizados está justificada. Complementariamente, el derecho a la privacidad y a la protección de datos limita la recolección y el procesamiento de información que pueda generar decisiones discriminatorias, mientras que el derecho a un recurso efectivo garantiza que los

individuos puedan impugnar y obtener reparación frente a decisiones algorítmicas perjudiciales. El GDPR y la LED refuerzan estas garantías al exigir que el procesamiento de datos sea justo, permitir la intervención humana, prohibir el tratamiento de categorías especiales de datos personales y obligar a realizar Evaluaciones de Impacto en la Protección de Datos (DPIA, por sus siglas en inglés) cuando los tratamientos representen riesgos para derechos fundamentales, incluyendo la discriminación. Estas evaluaciones requieren que las organizaciones identifiquen, evalúen y mitiguen los riesgos para los derechos fundamentales derivados del uso de algoritmos, asegurando un marco preventivo frente a decisiones automatizadas injustas o sesgadas (Haitsma, 2025).

3.8.2. Law Enforcement directive (LED).

La Directiva de Aplicación de la Ley (LED) establece normas específicas para la protección de las personas físicas en el tratamiento de datos personales por parte de autoridades competentes en el ámbito de la prevención, investigación, detección o enjuiciamiento de delitos, así como en la ejecución de penas y la protección de la seguridad pública. Para que un tratamiento de datos entre dentro del ámbito de la LED, deben cumplirse dos condiciones acumulativas: primero, que persiga fines relacionados con materias penales o con actividades policiales preventivas orientadas a proteger la seguridad pública, como la gestión de infracciones durante viajes de pasajeros o la supervisión de eventos públicos; segundo, que sea realizado por una "autoridad competente", entendida como cualquier organismo público encargado de la prevención y persecución de delitos o de la ejecución de penas, incluyendo autoridades judiciales, fuerzas policiales u otras entidades legalmente habilitadas para ejercer prerrogativas de poder público, como servicios de seguridad internos en transporte o federaciones deportivas autorizadas para garantizar la seguridad en eventos. Aunque tanto la LED como el Reglamento General de Protección de Datos (GDPR) forman parte del paquete normativo europeo de protección de datos, sus ámbitos de aplicación son distintos y complementarios: mientras el GDPR regula de manera general el tratamiento de datos personales en los sectores público y privado, la LED se aplica específicamente a los datos procesados en actividades policiales y judiciales relacionadas con la seguridad y la justicia penal, excluyendo los supuestos cubiertos por el GDPR, así como aquellos vinculados a la seguridad nacional o defensa.

Los derechos de acceso e información establecidos por la Directiva de Aplicación de la Ley (LED) cumplen fines amplios de transparencia y supervisión del tratamiento de datos

personales, permitiendo a los ciudadanos conocer cómo y para qué se procesan sus datos. Estos derechos no solo fortalecen la rendición de cuentas de las autoridades, sino que también generan conciencia social sobre el uso de la información, como lo ejemplifica el caso *Schrems*, iniciado a partir de una simple solicitud de acceso a datos personales. En un contexto de seguridad, estos derechos permiten que los ciudadanos "vigilen a los vigilantes" y, desde una perspectiva más amplia, contribuyen al respeto del Estado de derecho. Frente a la creciente recopilación masiva de datos y la posibilidad de que los individuos sean clasificados en perfiles con registros permanentes, los derechos informacionales resultan esenciales para garantizar la exactitud de la información, prevenir su uso excesivo y controlar los fines para los que se emplea. En este sentido, la LED constituye una intervención normativa relevante, al empoderar a los titulares de datos y equilibrar la protección de los derechos individuales con las exigencias operativas de las autoridades de aplicación de la ley (Erdogan, 2023).

3.8.3. Declaración europea sobre los derechos y principios digitales para la década digital.

El 23 de enero de 2023 se publicó en el Diario Oficial de la Unión Europea la Declaración europea sobre los derechos y principios digitales para la década digital, proclamada conjuntamente por el Parlamento Europeo, el Consejo y la Comisión. Esta iniciativa, propuesta por la Comisión en enero de 2022, retoma los planteamientos de la Declaración de Tallin (2017), la Declaración de Berlín (2020) y la Declaración de Lisboa (2021), documentos que ya advertían sobre la creciente relevancia de la digitalización, acentuada tras la pandemia.

La Declaración está estructurada en un preámbulo y seis capítulos que reúnen veinticuatro numerales. Desde una perspectiva formal, recuerda los valores fundacionales de la Unión Europea establecidos en el artículo 2 del Tratado de la Unión y en la Carta de los Derechos Fundamentales, tales como la dignidad, la libertad, la igualdad y la solidaridad. En el plano material, expone los principios y derechos que deben orientar la transición digital del bloque europeo. Aunque carece de carácter jurídicamente vinculante, al ser resultado de compromisos interinstitucionales, la Declaración constituye un posible antecedente para futuras regulaciones digitales y anticipa áreas estratégicas en las que los Estados miembros deberán concentrar su atención. Es significativo que las instituciones supranacionales se comprometan de manera conjunta a promover la protección de derechos fundamentales —incluidos los laborales—, la prestación de servicios públicos, la participación política y la sostenibilidad ambiental en los entornos digitales (De la Sierra, 2022).

En cuanto a sus particularidades, el documento no introduce temas desconocidos respecto de declaraciones previas; sin embargo, resulta novedoso por surgir de las tres principales instituciones de la Unión Europea y no de un Estado miembro. Además, destaca por situar a las personas en el centro del proceso de digitalización y por fomentar un diálogo multidireccional entre ciudadanía, instituciones estatales y organismos supranacionales. Este enfoque refleja una intención de reforzar la integración entre la Unión y sus Estados miembros, al tiempo que subraya la necesidad de avanzar hacia una transformación digital que respete los derechos fundamentales (De la Sierra, 2022).

A partir de estos compromisos, surgen diversos retos y oportunidades para las agendas públicas. Uno de ellos se relaciona con el impacto que podrían tener estos lineamientos en territorios ultraperiféricos como la Guayana francesa, cuya posición geográfica en América del Sur plantea interrogantes sobre su papel en la cooperación intercontinental y en la expansión de políticas digitales europeas. Otro desafío proviene de la inclusión del derecho a la desconexión digital, que exige definir estándares para garantizar conectividad segura, accesible y de alta velocidad en todos los territorios de la Unión (Rodríguez, 2023).

Desde la teoría de los derechos, la Declaración también introduce la necesidad de construir salvaguardas jurídicas para entornos digitales y algorítmicos, lo que plantea interrogantes sobre la competencia institucional para resolver mecanismos de tutela y la articulación entre normativas nacionales y supranacionales. Asimismo, impulsa la interoperabilidad como medio para fortalecer la transparencia y promover contenidos digitales que reflejen la diversidad cultural y lingüística europea, lo que demanda políticas públicas capaces de medir la satisfacción ciudadana en sociedades heterogéneas.

Otro ámbito relevante es la protección frente a los riesgos de la ciberdelincuencia. Aunque Europa cuenta con el Convenio de Budapest de 2001, la Declaración invita a reflexionar sobre la posibilidad de nuevas directivas o reformas que amplíen la cooperación internacional y permitan la adhesión de Estados no participantes en la elaboración del convenio. Finalmente, el documento destaca el compromiso con la sostenibilidad y la salud física y mental, lo cual plantea preguntas sobre la evolución de la economía circular, la reducción de la obsolescencia programada y la reparabilidad de productos digitales. Estos elementos podrían integrarse en las agendas públicas como parte del vínculo entre transición ecológica y calidad de vida en entornos digitales, aunque persisten dudas sobre la efectividad futura de las políticas ambientales que lleguen a implementarse (De la Sierra, 2022).

3.8.4. AI Act.

El AI Act (Reglamento (UE) 2024/1689) constituye el primer marco legal integral sobre inteligencia artificial a nivel mundial, diseñado para abordar los riesgos asociados a la IA y posicionar a Europa como líder global en la promoción de tecnologías confiables y centradas en el ser humano. El reglamento adopta un enfoque basado en riesgos, estableciendo obligaciones específicas para desarrolladores y operadores de IA, con el objetivo de garantizar la seguridad, el respeto de los derechos fundamentales y un uso ético de la tecnología. El AI Act forma parte de un paquete más amplio de políticas europeas que incluye el AI Continent Action Plan, el AI Innovation Package y el lanzamiento de AI Factories, iniciativas que buscan fomentar la innovación, la inversión y la adopción de IA confiable en la Unión Europea. Para facilitar la transición al nuevo marco regulatorio, la Comisión Europea ha promovido el AI Pact, una iniciativa voluntaria que invita a proveedores y operadores de IA a cumplir anticipadamente con las obligaciones clave del AI Act, complementada por el AI Act Service Desk, que brinda información y apoyo para asegurar una implementación efectiva en toda la UE. Este conjunto normativo y de políticas refleja un enfoque integral que combina regulación, innovación y gobernanza responsable de la IA (UE, 2025).

El AI Act establece prohibiciones estrictas sobre ciertas prácticas de IA, incluyendo sistemas que manipulen el comportamiento humano, exploten vulnerabilidades, apoyen puntajes sociales gubernamentales, realicen categorización biométrica, predicción policial o extracción masiva de imágenes faciales, como los casos que involucraron a Clearview AI[11], ya sancionada en la UE. Asimismo, se prohíben los sistemas de IA diseñados para el reconocimiento emocional, especialmente en entornos laborales, educativos y de seguridad pública, así como aquellos que puedan influir en las personas de manera perjudicial o explotativa, incluyendo manipulación política o recomendaciones de contenido adictivo. La normativa clasifica como IA de alto riesgo a sistemas utilizados en empleo, educación, salud, identificación biométrica o chatbots con interacción humana significativa, obligando a los

[11] En mayo de 2022, el Comisionado de Protección de Datos del Reino Unido impuso una multa de £7,5 millones a la empresa estadounidense Clearview AI y emitió un aviso de cumplimiento por recopilar imágenes de residentes del Reino Unido de sitios web y redes sociales, para luego cargarlas en su base de datos global accesible a cualquier cliente de la compañía con fines de reconocimiento facial. Este caso ilustra cómo Clearview AI no solo facilitaba la identificación de individuos, sino que también permitía el seguimiento de su comportamiento como un servicio comercial, vulnerando derechos de privacidad y demostrando la necesidad de regulaciones estrictas, como las previstas en el AI Act europeo, para impedir la explotación masiva de datos personales y proteger los derechos fundamentales de los ciudadanos frente a tecnologías de vigilancia automatizada (Information Commissioner's Office, ICO, 2025)

desarrolladores a cumplir con requisitos de transparencia, calidad de datos, documentación, supervisión humana y robustez, y a realizar evaluaciones de conformidad previas a su comercialización, de manera similar a las Evaluaciones de Impacto de Protección de Datos (DPIA) del GDPR. Los modelos base y la IA de propósito general, incluidos los sistemas generativos como GPT-4, estarán sujetos a obligaciones exhaustivas de documentación, transparencia, registro y gobernanza de datos, además de medidas adicionales para garantizar el cumplimiento legal y la gestión de riesgos sociales y de seguridad. Para supervisar su aplicación, se crea la European Artificial Intelligence Board (EAIB) y la Oficina Europea de IA, que trabajarán junto a autoridades nacionales designadas para garantizar coherencia regulatoria, asesoramiento técnico y cumplimiento efectivo. Finalmente, el AI Act contempla sanciones severas por incumplimiento, que pueden alcanzar hasta el 7 % de la facturación anual global de la entidad responsable del sistema de IA, superando las multas previstas por el GDPR, y reflejando la importancia crítica de garantizar la seguridad, los derechos fundamentales y la responsabilidad en la implementación de tecnologías de IA en Europa (Ponomarov, 2024).

El AI Act adopta un enfoque basado en la gestión del riesgo, clasificando los sistemas de IA según el nivel de riesgo que representan para individuos, colectivos o infraestructuras. Así, los sistemas de bajo o mínimo riesgo, que presentan escasa capacidad de generar daño, están sujetos a medidas de control reducidas, mientras que los sistemas de alto riesgo o prohibidos, con riesgos significativos o inaceptables, son objeto de la regulación más estricta y detallada, concentrando sobre ellos la mayor parte de las obligaciones normativas.

Figura 10.

Riesgos según el AI Act.

Nota. La identificación de riesgos que utiliza el AI Act es de forma piramidal y ascendente, desde riesgos mínimos hasta prohibiciones o riesgos inaceptables. Adaptado de: "Cronología de la regulación de la IA en Europa y España" (7 de mayo de 2025). [Sitio web]. *IA ON*. https://www.ia-on.es/regulacion-internacional/cronologia-de-la-regulacion-de-la-ia-en-europa-y-espana/.

El artículo 5 de la Ley enumera de manera completa las prácticas de IA que están prohibidas en la Unión Europea. Estas reglas, explicadas además en los considerandos 28–45 y en las guías de la Comisión de febrero de 2025, ofrecen un marco preciso sobre los límites legales de la IA. Como entraron en vigor el 2 de febrero de 2025, son las primeras normas aplicables, lo cual demuestra su relevancia.

Si bien la lista es exhaustiva, no es permanente. Cada año la Comisión revisará si debe modificarse y podrá proponer cambios a las instituciones europeas. Por ello, pueden producirse ajustes en el futuro. Actualmente existen ocho prácticas prohibidas, especialmente aquellas que manipulan de forma notable el comportamiento humano o generan riesgos para el sistema democrático. Hay un enfoque especial en la identificación biométrica, aunque muchas reglas vienen acompañadas de excepciones, por lo que se requiere evaluar cada situación de manera individual (Bird & Bird, 2025).

Las empresas que desarrollan o utilizan inteligencia artificial deben aplicar medidas concretas de gestión de riesgos. Aunque estas medidas forman parte del marco general de

riesgos de una empresa, la Ley de IA exige que exista atención específica a los riesgos propios de la IA.

El artículo 9 establece que los proveedores y usuarios de sistemas de IA de alto riesgo deben crear y mantener un sistema documentado de gestión de riesgos, actualizado en todas las fases del ciclo de vida del sistema. Este sistema incluye pasos para identificar riesgos, aplicar medidas de mitigación, evaluar los efectos combinados de dichas medidas y asegurar que el riesgo residual permanezca dentro de niveles aceptables. Además, el artículo aclara que solo se consideran riesgos aquellos que puede mitigarse razonablemente mediante el diseño del sistema o mediante información técnica adecuada (AI act, 2024, art. 9)

En primer lugar, se prohíbe el uso de técnicas subliminales o manipulativas, cuyo objetivo o efecto sea distorsionar de manera significativa el comportamiento de individuos o grupos, causando un perjuicio relevante. De manera relacionada, también está prohibida la explotación de vulnerabilidades de las personas, especialmente aquellas derivadas de características específicas como edad, discapacidad o factores psicológicos, cuando esto pueda generar daños importantes. Estas prohibiciones no contemplan excepciones, debido al alto riesgo que representan.

Asimismo, la Ley restringe los sistemas de puntuación social, es decir, aquellos que evalúan o clasifican a personas o grupos en función de su comportamiento social o características personales. Dichos sistemas pueden derivar en un trato desfavorable o perjudicial, por lo que su uso se considera inaceptable en la mayoría de los contextos. De forma similar, se prohíbe predecir la probabilidad de que una persona cometa un delito basándose únicamente en perfiles o características personales, salvo en casos muy concretos en los que la predicción apoye la evaluación humana y se base en hechos objetivos y verificables vinculados a actividades delictivas concretas.

Por otra parte, la Ley establece restricciones respecto al reconocimiento facial y biométrico. No se permite la creación de bases de datos mediante recopilación indiscriminada de imágenes de internet o cámaras de vigilancia, dado que esto constituye una amenaza masiva para la privacidad. Además, se prohíbe inferir emociones en entornos laborales o educativos, salvo que sea por motivos médicos o de seguridad, y se limita la categorización biométrica basada en datos sensibles, permitida únicamente para etiquetar o filtrar conjuntos de datos

legales, como aquellos utilizados en el ámbito policial o de seguridad pública (Bird & Bird, 2025).

Finalmente, se establece que la identificación biométrica remota en tiempo real en espacios públicos está prohibida, excepto en circunstancias muy específicas, donde se requiera autorización previa o notificación a las autoridades competentes. Esta excepción permite un uso controlado en situaciones de seguridad, pero mantiene un enfoque restrictivo para proteger la privacidad y los derechos fundamentales de los individuos (EU, 'AI act' 2024. Art 6 - 9).

La Ley de IA impone obligaciones a todos los participantes en la cadena de suministro de un sistema de alto riesgo a lo largo de todo su ciclo de vida. Estas responsabilidades no recaen únicamente en el proveedor, sino también en el importador, el distribuidor y el usuario del sistema, aunque la mayor parte de los deberes corresponde al proveedor y al usuario final. En particular, el deber principal del importador y del distribuidor consiste en verificar que el sistema de IA de alto riesgo que están importando o distribuyendo cumpla con los requisitos de la Ley. Además, un importador, distribuidor o usuario puede llegar a ser considerado proveedor si ha puesto su nombre o marca registrada en el sistema, ha realizado modificaciones sustanciales o ha cambiado el propósito previsto del sistema, lo que podría convertirlo en un sistema de alto riesgo (EU, 'AI Act', 2024, Art. 11).

Por otro lado, la Ley de IA establece los requisitos de la documentación técnica de estos sistemas. Dicha documentación debe incluir, como mínimo: una descripción del sistema, sus componentes y el proceso de desarrollo; información sobre la monitorización, funcionamiento y control del sistema; la evaluación de la idoneidad de los indicadores de rendimiento; la descripción del sistema de gestión de riesgos; los cambios relevantes realizados por el proveedor a lo largo del ciclo de vida del sistema; los estándares técnicos aplicados; la declaración de conformidad; y el sistema implementado para evaluar el desempeño del sistema (Braun et al., 2024). Asimismo, la Ley contempla que las PYMES, incluidas las startups, puedan presentar estos elementos de manera simplificada, con el fin de reducir la carga administrativa. Para facilitar este proceso, la Comisión Europea publicará un formulario simplificado que permita a las pequeñas empresas cumplir con los requisitos de documentación de manera más ágil y accesible (EU, AI act, 2024. Art 12).

El AI Act fue aprobado el 12 de julio de 2024 y entró en vigor el 1 de agosto de 2024. Sin embargo, su aplicación será gradual, con varios hitos que determinarán cuándo las

principales disposiciones comenzarán a ser exigibles. Esta progresividad responde a la complejidad tecnológica de la inteligencia artificial y a la necesidad de desarrollar normas técnicas específicas para su implementación.

Un ejemplo de esta progresión se observa en la plena aplicabilidad del reglamento, prevista a partir del 2 de agosto de 2026. Este periodo de veinticuatro meses permite a las empresas y desarrolladores de IA adaptarse a las nuevas obligaciones impuestas por la normativa, ajustando sus sistemas y procesos para cumplir con los estándares de seguridad, transparencia y gestión de riesgos.

Entre los hitos más relevantes del cronograma se encuentra febrero de 2025, cuando comenzarán a aplicarse las primeras disposiciones sobre sistemas de IA de riesgo inaceptable. Estas incluyen aquellos sistemas que representan una amenaza directa para los derechos humanos, como los sistemas de manipulación subliminal y los sistemas de puntuación social que evalúan a las personas según su comportamiento o características personales, similares a los utilizados en China.

A partir de agosto de 2025, se activarán disposiciones más amplias relacionadas con la supervisión y gobernanza de los sistemas de IA de alto riesgo. Estos sistemas, utilizados en sectores sensibles como la sanidad, la educación, la justicia o los procesos de contratación laboral, no estarán prohibidos, pero deberán cumplir estrictamente con medidas de seguridad, garantizar transparencia y permitir siempre la supervisión humana.

Finalmente, el cronograma culminará en agosto de 2027, cuando todas las obligaciones del AI Act estarán plenamente en vigor. En esta fase, la Unión Europea dispondrá de un marco normativo completo para regular el uso de la inteligencia artificial en distintos sectores, asegurando que las empresas y los desarrolladores operen conforme a los estándares de seguridad y protección de los derechos humanos (Bachs et al., 2025).

3.8.5. Derechos fundamentales involucrados y riesgos constitucionales

La era digital impacta de manera transversal los derechos fundamentales, generando nuevas formas de ejercicio y vulneración. En Colombia, los derechos más expuestos en entornos digitales son:

a) Derecho a la vida y a la integridad personal (arts. 11 y 12 C.P.): La vida, tradicionalmente protegida frente a amenazas físicas, adquiere una dimensión tecnológica.

Ciberataques a infraestructuras críticas, fallos en sistemas autónomos o vulneraciones de datos biomédicos pueden afectar directamente la seguridad personal. Ferrajoli (2020) plantea que el Estado constitucional debe proteger la vida frente a riesgos emergentes, y en el plano digital esto exige marcos claros de responsabilidad civil y penal ante daños causados por inteligencia artificial o robótica.

b) Derecho a la intimidad y al habeas data (art. 15 C.P.): La recolección masiva de datos personales por plataformas, dispositivos y aplicaciones genera vulneraciones potenciales a la privacidad. La Sentencia T-729/2002 de la Corte Constitucional reconoció el habeas data como facultad de conocer, actualizar y rectificar la información personal, pero el Big Data y los algoritmos predictivos superan las previsiones normativas de la Ley 1581 de 2012. La ausencia de un marco integral para IA y blockchain deja a los ciudadanos expuestos a explotación y manipulación de sus datos.

c) Derecho a la igualdad (art. 13 C.P.): Los algoritmos y la inteligencia artificial pueden reproducir y amplificar sesgos preexistentes, generando discriminación algorítmica. Sartor (2021) subraya que los sesgos de datos trasladan al entorno digital las desigualdades del mundo físico, afectando el acceso a empleo, crédito o servicios públicos. Este riesgo requiere protocolos de transparencia y supervisión humana.

d) Libertad de expresión (art. 20 C.P.): El entorno digital amplía el alcance de la expresión, pero enfrenta riesgos de censura algorítmica, desinformación y discurso de odio. La Sentencia T-372/2023 reafirma que el acceso a Internet es condición necesaria para la libertad de expresión y advierte sobre la ilegalidad de bloqueos injustificados. En la quinta revolución industrial, el control de contenidos y la circulación de deepfakes plantean desafíos para la democracia deliberativa.

e) Debido proceso (art. 29 C.P.): La automatización de decisiones administrativas y judiciales mediante IA impacta el debido proceso. La Corte Constitucional, en la Sentencia T-323/2024, determinó que la IA no puede sustituir la función jurisdiccional y que toda decisión automatizada debe garantizar transparencia, supervisión humana y posibilidad de impugnación. La falta de un marco normativo integral para la IA en Colombia deja vacíos que comprometen la seguridad jurídica.

En síntesis, la protección de los derechos fundamentales en la era digital exige una adaptación normativa y doctrinal que cierre los vacíos de la Constitución de 1991 frente a la

sociedad tecnológica. Esta situación justifica la consolidación de un constitucionalismo digital colombiano, capaz de armonizar innovación, dignidad humana y garantías fundamentales en la quinta revolución industrial.

3.9.Principios constitucionales aplicables

La protección de los derechos fundamentales en entornos digitales se articula mediante la aplicación de los principios constitucionales, que funcionan como ejes de ponderación y límite frente al avance tecnológico:

- Dignidad humana (art. 1 C.P.): Eje estructural del Estado social de derecho. En el plano digital, implica que la persona no puede ser reducida a un dato o perfil algorítmico (Ferrajoli, 2020; Pérez Luño, 2019).

- Legalidad (arts. 6 y 121 C.P.): Toda actuación estatal en entornos tecnológicos debe estar fundada en norma previa y clara, otorgando certeza a ciudadanos y empresas (Kelsen, 2009).

- Proporcionalidad (arts. 1, 2 y 13 C.P.): Los límites tecnológicos a derechos deben ser adecuados, necesarios y equilibrados (Alexy, 2002; Carbonell, 2020).

- Seguridad jurídica: Los ciudadanos deben prever las consecuencias legales de su interacción con tecnologías emergentes, evitando lagunas normativas y vacíos de responsabilidad.

Estos principios constituyen la base de un constitucionalismo digital colombiano que busque armonizar la innovación tecnológica con la dignidad humana, la igualdad y la seguridad jurídica. Su incorporación como guía de interpretación y de desarrollo legislativo es imprescindible para garantizar la efectividad de los derechos en la era digital.

No obstante, la sola existencia de principios constitucionales no garantiza por sí misma la protección efectiva de los derechos fundamentales en entornos digitales. En el caso colombiano, aunque se han dado pasos importantes mediante la Ley 527 de 1999, la Ley 1581 de 2012 sobre protección de datos, la Política Nacional de Transformación Digital y recientes pronunciamientos de la Corte Constitucional, persisten vacíos normativos y dispersión regulatoria frente a fenómenos emergentes como la inteligencia artificial, el blockchain, los entornos inmersivos y la toma de decisiones automatizadas. Esta tensión evidencia que la materialización del constitucionalismo digital exige no solo interpretar los principios clásicos,

sino avanzar en un marco normativo integral, capaz de articular la innovación tecnológica con la dignidad humana y la seguridad jurídica. En este sentido, el análisis de los desarrollos legales y de política pública en Colombia resulta fundamental para comprender hasta dónde ha avanzado el país en la protección efectiva de derechos en la era digital, y es precisamente el objeto del siguiente subcapítulo.

3.10. Marco legal y normativo de la digitalización en Colombia

La Constitución Política de Colombia de 1991 constituye la base normativa sobre la cual el país ha construido su adaptación a la era digital y a los desafíos de la Quinta Revolución Industrial. A partir de sus principios de dignidad humana, legalidad, igualdad y seguridad jurídica, el Estado ha incorporado progresivamente tecnologías emergentes en la administración pública, la prestación de servicios y la interacción ciudadana (Constitución Política de Colombia, 1991). Este proceso confirma lo planteado por Pérez Luño (2019), quien sostiene que la Constitución es un instrumento vivo que debe responder a las mutaciones sociales y tecnológicas para garantizar la efectividad de los derechos fundamentales.

3.10.1. Introducción a la 'sociedad digital'.

Colombia, con el propósito de impulsar el uso de las nuevas tecnologías de la información y promover el comercio electrónico, decidió adoptar una regulación específica y expidió la Ley 527 de 1999, conocida como Ley de Comercio Electrónico. Aunque su nombre parece restringirla al ámbito mercantil, su alcance va más allá de este sector (Rincón, 2006).

La ley fue creada para eliminar los obstáculos que dificultaban la celebración y ejecución de transacciones electrónicas, especialmente aquellos derivados del desconocimiento del valor jurídico de las operaciones realizadas por medios digitales. Por ello, uno de sus principales objetivos fue reconocer pleno valor probatorio a los mensajes de datos, garantizando que la información almacenada en formatos digitales tenga la misma validez legal que la consignada en papel (Rincón, 2006).

Esta equivalencia tiene solo dos excepciones: a) las obligaciones asumidas por el Estado colombiano en virtud de tratados o convenios internacionales, y b) las advertencias impresas que deben incluirse físicamente en ciertos productos para proteger los derechos del consumidor (Gavilán, 2025).

3.10.2. Protección y regulación de datos.

3.10.2.1. Habeas data (Ley 1581 de 2012).

El habeas data es un derecho que permite a los ciudadanos acceder, actualizar, rectificar o eliminar sus datos personales almacenados por terceros, ya sean financieros o de otro tipo. Este derecho reconoce al titular como propietario de su información, garantizando que su tratamiento sea adecuado y conforme a normas específicas, incluso en plataformas digitales y redes sociales.

Según la jurisprudencia de la Corte Constitucional (Sentencia C-748, 2011), los datos personales se caracterizan por ser exclusivos de cada individuo, permitir su identificación directa o indirecta, pertenecer al titular, aunque un tercero los obtenga legal o ilegalmente, y estar sujetos a reglas especiales de manejo y divulgación. En síntesis, el habeas data protege la privacidad y el control de la información personal, asegurando un uso responsable y regulado de los datos en todos los ámbitos (García, 2023).

Cuando se recolectan o entregan datos personales, la persona responsable debe informar sobre el uso que se dará a la información y solicitar autorización expresa, restringida a fines específicos. Sin embargo, existen excepciones para información de carácter público, como registros civiles o datos con fines históricos, estadísticos o científicos, donde no se requiere autorización del titular (Ley 1581 de 2012, Art. 20).

El derecho al habeas data garantiza la protección de los datos personales, aunque su aplicación puede ser más compleja cuando las autoridades públicas hacen uso de esta información, generando posibles implicaciones en investigaciones judiciales por comentarios en redes sociales. Para proteger este derecho, la ley contempla varias acciones judiciales: el procedimiento sancionatorio administrativo ante la Superintendencia de Industria y Comercio, la acción de tutela frente a vulneraciones del habeas data, y la acción por competencia desleal cuando el uso indebido de datos genere ventajas ilegales.

La jurisprudencia, especialmente la Corte Constitucional en la sentencia SU-139 de 2021, ha definido al habeas data como un derecho fundamental autónomo que protege la información personal y clasifica los datos en cuatro categorías:

1. **Información pública:** accesible sin restricciones, como documentos oficiales y datos de estado civil.

2. **Información semiprivada:** accesible solo por autoridad administrativa, como datos financieros, bajo normas de gestión de datos personales.
3. **Información privada**: accesible únicamente por orden judicial, incluyendo libros de comerciantes, documentos privados o historiales clínicos.
4. **Información reservada o datos sensibles:** relacionados con ideología, orientación sexual o hábitos personales; su acceso está restringido incluso a autoridades judiciales, debido a su impacto directo sobre la intimidad y posibles riesgos de discriminación (T-020, 2014).

La Corte Constitucional ha enfatizado que el tratamiento de datos requiere el consentimiento libre, previo y expreso del titular, salvo mandato legal o judicial. Esto incluye el derecho del titular a disponer de su información y conocer su identidad digital, incluso en internet y redes sociales (García, 2023).

3.10.2.2. Ley 1341 de 2009.

Esta ley establece los principios y conceptos que orientan la sociedad de la información y la organización del sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia. Además, crea la Agencia Nacional del Espectro y fija un marco general para el diseño de políticas públicas en este ámbito, con especial énfasis en la protección de los usuarios.

De acuerdo con el artículo 2, numeral 4, la protección de los derechos de los usuarios de servicios TIC —incluido el cumplimiento de los deberes derivados del habeas data— constituye una prioridad del Estado. Por ello, los proveedores y operadores están obligados a ofrecer sus servicios bajo condiciones de precio razonable, garantizar información clara, transparente y suficiente, y respetar el principio de neutralidad tecnológica, tal como lo señala también el numeral 6 del mismo artículo.

3.10.2.3. Ley 1712 de 2014.

En desarrollo de los principios de transparencia, se expidió la Ley 1712 de 2014, conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública. Esta norma establece que la *máxima publicidad* debe regir el funcionamiento de todas las entidades públicas, lo que implica obligaciones como actuar con transparencia, facilitar el

acceso a la información, obrar de buena fe, evitar discriminación, garantizar celeridad, gratuidad y asegurar la calidad de la información divulgada (Art. 3).

El derecho fundamental de acceso a la información otorga a cualquier persona la facultad de conocer y solicitar la información pública que esté en poder o bajo control de los sujetos obligados. Este derecho solo puede ser limitado de manera excepcional, y únicamente tratándose de información clasificada o reservada, especialmente aquella cuyo acceso pudiera perjudicar intereses públicos. Asimismo, la ley impone a las entidades el deber de divulgar de manera proactiva la información pública relevante y responder a las solicitudes de buena fe (Art. 4).

Si una entidad niega injustificadamente el acceso a la información, el solicitante puede presentar una queja o reclamo directo ante la misma. Si la respuesta sigue siendo insatisfactoria o no existe fundamento legal para la negativa, procede el recurso de reposición o los mecanismos administrativos correspondientes. En última instancia, la persona afectada puede acudir ante el Tribunal Administrativo competente, según el lugar donde reposen los documentos solicitados (Art. 27).

3.10.3. Decretos 088 y 338 de 2022

Establecen condiciones para la automatización de trámites y refuerzan la seguridad digital en operaciones públicas y privadas.

Reflejan la voluntad del Estado de avanzar hacia una gobernanza digital confiable, aunque persisten retos en interoperabilidad y ciberseguridad avanzada (Presidencia de la República, 2022a; 2022b).

3.10.4. Ley 2502 de 2025

Modifica el artículo 296 del Código Penal para sancionar la suplantación de identidad mediante inteligencia artificial (IA) y deepfakes, reconociendo la afectación de la dignidad humana, la imagen y la identidad digital.

Ordena la formulación de políticas públicas en materia de prevención y trazabilidad, integrando principios de ética digital, cooperación interinstitucional y transparencia algorítmica (Ley 20502, 2025).

Este avance evidencia el reconocimiento legislativo de riesgos asociados a la sociedad tecnológica, aunque su alcance inicial es limitado al ámbito penal.

La evolución del marco legal y normativo en Colombia ha sido impulsada por diversas iniciativas tanto a nivel nacional como internacional. Uno de los puntos de partida clave fue la implementación de la Política Nacional de Gobierno en Línea, que comenzó en 2007, con el objetivo de modernizar la administración pública y acercar el gobierno a los ciudadanos mediante el uso de las TIC. A partir de esta iniciativa, surgieron otras políticas, leyes y regulaciones que han contribuido a la creación de un entorno adecuado para el avance de la digitalización en Colombia (Departamento Nacional de Planeación, 2025).

En otras, podemos esta evolución de la siguiente manera a través del tiempo.

Tabla 5.

Expedición de las normas frente al marco jurídico.

Año	Ley/Decreto	Descripción
1991	Constitución Política	Establece el marco general para los derechos fundamentales, incluyendo la disponibilidad de la información.
1999	Ley 527	Regula el comercio electrónico y valida los documentos electrónicos.
2009	Ley 1341	Promueve y desarrolla las Tecnologías de la Información y las Comunicaciones (TIC).
2012	Ley 1581	Protege los datos personales de los ciudadanos.
2014	Ley 1712	Garantiza la disponibilidad de información pública y el impulso a la transparencia digital.
2018	Ley 1943	Incluye aspectos sobre facturación electrónica.
2015	Decreto 1078	Regula el uso de las TIC en la administración pública.
2019	Ley 1968	Implementa la firma electrónica y el uso de tecnología en la administración pública.
2015	Decreto 1074	Establece políticas y acciones de gobierno digital.

2021	Decreto 1781	Impulsa el gobierno digital y la digitalización de servicios públicos.
2019	Ley 2017	Refuerza la agenda y la infraestructura digitales del país.
2021	Decreto 1081	Implementa la política pública de la Agenda Digital Nacional.
2020	Ley 2068	Regula la ciberseguridad y protege infraestructuras digitales críticas.
2022	Decreto 1405	Actualiza normativas sobre la digitalización en la administración pública.
2025	Ley 2502	Para penalizar la suplantación digital mediante IA y deepfakes, protegiendo la dignidad e identidad de las personas.

Nota. Elaboración propia (2024).

Es importante señalar que, aunque las normativas mencionadas han sido fundamentales para el marco regulatorio de la digitalización en Colombia, estas no abordan de manera específica las nuevas tendencias tecnológicas asociadas con la Quinta Revolución Industrial, tales como la inteligencia artificial, la automatización avanzada, el internet de las cosas (IoT) y la transformación digital en sectores clave. Tampoco se profundiza en aspectos emergentes relacionados con los derechos digitales, como la protección de la privacidad en entornos virtuales, el acceso equitativo a la tecnología o la regulación de plataformas digitales. Estos temas, que son cruciales para la adaptación a los rápidos cambios tecnológicos, requieren de una actualización normativa que asegure un entorno jurídico adecuado a las demandas de la nueva era digital.

En conjunto, este marco legal ha permitido que Colombia avance hacia la digitalización, consolidando seguridad jurídica en transacciones electrónicas, fortalecimiento de infraestructura TIC y primeros pasos en regulación de IA. Sin embargo, en línea con la crítica de Ferrajoli (2020), un Estado constitucional no puede limitarse a reaccionar frente al riesgo tecnológico, sino que debe prevenirlo mediante un marco normativo integral. El esquema actual sigue siendo fragmentado y reactivo, con vacíos frente a fenómenos emergentes como:

I. Gobernanza integral de inteligencia artificial y metaverso,
II. Interoperabilidad plena de plataformas públicas y privadas,
III. Ciberseguridad avanzada y prevención de delitos digitales,

IV. Protección de derechos digitales y de la personalidad frente a IA generativa.

A pesar de la existencia de un marco legal que incluye leyes pioneras como la Ley 527 de 1999, la Ley 1341 de 2009, la Ley 1978 de 2019, la Ley 2069 de 2020, los Decretos 088 y 338 de 2022 y la reciente Ley 2502 de 2025, el desarrollo normativo colombiano en materia digital sigue siendo fragmentado y reactivo. Estas normas han respondido principalmente a fenómenos ya consolidados —como el comercio electrónico, la digitalización de trámites y la protección frente a la suplantación digital—, pero no configuran aún un ecosistema normativo integral que articule ciberseguridad avanzada, gobernanza de datos, interoperabilidad tecnológica e inteligencia artificial (IA) de manera proactiva. En términos de Ferrajoli (2020), el Estado constitucional no puede limitarse a reaccionar frente al riesgo tecnológico, sino que debe anticiparlo y prevenirlo mediante un marco normativo coherente y prospectivo. Esta ausencia de integralidad genera zonas grises que afectan la efectividad de los derechos fundamentales en entornos digitales, especialmente en lo relacionado con la identidad, la privacidad, la seguridad digital y la igualdad ante algoritmos.

Adicionalmente, el componente legislativo, aunque ha permitido avances en confianza digital, inclusión tecnológica y primeros pasos en regulación de IA, no ha logrado una sincronización efectiva con las políticas públicas y la jurisprudencia constitucional. Como advierte Pérez Luño (2019), la efectividad de los derechos fundamentales en escenarios digitales depende de la convergencia entre normas, políticas y decisiones judiciales que garanticen una protección real frente a riesgos inéditos. La ausencia de legislación integral para fenómenos como el metaverso, la IA generativa y la ciberseguridad avanzada, unida a la brecha entre áreas urbanas y rurales, evidencia la necesidad de un constitucionalismo digital colombiano que oriente al legislador hacia la armonización de innovación tecnológica, seguridad jurídica y protección de derechos fundamentales.

Estos vacíos confirman la necesidad de construir un ecosistema legal coherente, capaz de respaldar el constitucionalismo digital colombiano, armonizando innovación tecnológica y protección de derechos fundamentales. En este contexto, resulta clave analizar las políticas públicas y estrategias digitales que acompañan este marco legal, tema que se aborda en el subcapítulo 2.2.2

3.10.5. Transformación digital en Colombia

En la actualidad, los datos y las tecnologías digitales están revolucionando la forma en que interactúan las personas, las empresas y los gobiernos, generando oportunidades para enfrentar desafíos globales (Banco Mundial, 2023). Tecnologías como la Inteligencia Artificial poseen el potencial de impulsar la innovación en países y regiones, permitiéndoles abordar problemáticas como el cambio climático o una nueva pandemia. Sin embargo, ese potencial aún está lejos de alcanzarse, especialmente en países en desarrollo (OECD, 2023).

En América Latina y el Caribe, Colombia se posiciona como uno de los países con mayor avance en digitalización (Banco Mundial, 2023). En 2022, aproximadamente el 75% de las personas mayores de cinco años usaron Internet, y cerca del 66% de los hogares accedieron a este mediante conexiones fijas o móviles (DANE, 2022). La industria digital ha mostrado un crecimiento significativo: entre 2021 y 2022, las actividades relacionadas con Tecnologías de la Información (TI) y contenido y medios incrementaron su valor agregado en un 26,4% y 20,8%, respectivamente (DANE, 2023). Además, el sector público colombiano se ubica entre los líderes en gobierno digital en la región, comparándose con países como México, Perú y Brasil (Banco Mundial, 2023).

No obstante, persisten retos importantes relacionados con las brechas en el acceso, uso y apropiación de las tecnologías digitales, que afectan a hogares, empresas, entidades públicas y regiones. Por ejemplo, en 2022, la conectividad digital mostró grandes disparidades según la clasificación territorial: la penetración de Internet fijo fue del 6% en zonas rurales dispersas, 11,6% en áreas rurales, 25,8% en ciudades intermedias y 68% en grandes centros urbanos, con un promedio nacional de 50,7% (MinTIC y DANE, 2022).

A pesar del avance significativo en los indicadores de digitalización, Colombia enfrenta una brecha estructural de acceso y apropiación tecnológica que limita el alcance real de la transformación digital. La concentración de la conectividad en áreas urbanas y la baja penetración en zonas rurales dispersas, evidenciada por MinTIC y DANE (2022), reflejan un desarrollo desigual que profundiza las inequidades sociales y económicas. Como advierte Pérez Luño (2019), una sociedad digital sin acceso universal y equitativo puede reproducir exclusiones históricas y limitar la efectividad de los derechos fundamentales. En este sentido, los avances en infraestructura y gobierno digital no bastan si no se acompañan de estrategias sostenidas de inclusión tecnológica y fortalecimiento del talento digital, que permitan a toda la población beneficiarse de las oportunidades de la era digital.

Además, la transformación digital en Colombia ha sido más reactiva que anticipatoria, lo que se evidencia en la desconexión entre crecimiento tecnológico, protección de derechos y desarrollo normativo integral. El dinamismo de la inteligencia artificial, el big data y el blockchain requiere políticas públicas proactivas y coordinadas, capaces de mitigar riesgos y aprovechar oportunidades en campos como la ciberseguridad, la gobernanza de datos y la protección de la identidad digital. Esta situación demanda que el esfuerzo legislativo se complemente con instrumentos de planeación estratégica, entre ellos los documentos CONPES y la Estrategia Nacional Digital, que constituyen el puente entre la norma jurídica y la implementación efectiva de la transformación digital. Por ello, el análisis de estas políticas públicas resulta crucial para comprender cómo el Estado colombiano busca consolidar un ecosistema digital inclusivo, seguro y alineado con los principios del constitucionalismo digital, tema que se desarrolla en el subcapítulo 2.2.3.

3.10.6. Políticas públicas y CONPES

Las políticas públicas constituyen un complemento indispensable al marco legal para materializar la transformación digital en Colombia. Mientras la legislación establece principios y obligaciones, los instrumentos de planeación estratégica, como los documentos CONPES, permiten operativizar la visión estatal mediante objetivos, metas e inversiones coordinadas entre diferentes sectores. En el ámbito digital, estos documentos han sido determinantes para fortalecer la conectividad, promover la interoperabilidad, desarrollar capacidades institucionales y orientar la adopción de tecnologías emergentes, garantizando que los avances tecnológicos se traduzcan en oportunidades reales para el ejercicio de los derechos fundamentales.

3.10.7. Políticas públicas posterior a la constitución de 1991

La Constitución de 1991 marcó un hito en la historia de Colombia al establecer un marco jurídico moderno que prioriza los derechos fundamentales, la descentralización y el desarrollo sostenible. En este contexto, el Consejo Nacional de Política Económica y Social (CONPES) se consolidó como el principal órgano de planeación del país, encargado de formular políticas públicas que guían las acciones estratégicas del Gobierno Nacional. Los documentos CONPES son herramientas fundamentales para definir objetivos, establecer prioridades y articular esfuerzos interinstitucionales en diversos sectores, promoviendo un desarrollo integral y sostenible.

Entre los documentos más relevantes en el ámbito de la transformación digital, el desarrollo económico y la sostenibilidad, se destacan los CONPES 3920, 3701, 3769, 3975, 3995, 3854, 3988, 2848 y 4069. Estos abordan temas como la digitalización de la economía, la conectividad, la innovación tecnológica, la sostenibilidad ambiental y el fortalecimiento de capacidades institucionales. Por ejemplo, el CONPES 3920 ha sido clave para promover la transformación digital en las entidades públicas, mientras que el CONPES 3701 se enfoca en la masificación del uso de tecnologías de la información y las comunicaciones (TIC) como motor de inclusión social y competitividad (Departamento Nacional de Planeación, 2024).

El avance en Colombia tras la implementación de estas políticas ha sido significativo en áreas como la expansión de la conectividad, con mayores índices de cobertura de internet, y la promoción de la innovación tecnológica en sectores estratégicos como la educación y la salud. Sin embargo, persisten desafíos relacionados con la inclusión digital en zonas rurales, la gobernanza de los datos y la ciberseguridad, lo que resalta la importancia de continuar fortaleciendo el marco normativo y las estrategias públicas para responder a los retos de la era digital y los compromisos adquiridos en los documentos CONPES. Este subcapítulo analizará cómo estas políticas han transformado el panorama nacional y qué aspectos requieren mayor atención para consolidar un desarrollo integral y equitativo en Colombia (Departamento Nacional de Planeación, 2024).

Así las cosas, se hace necesario abordar los CONPES durante estos últimos 34 años:

Tabla 6.

CONPES últimos 34 años

Nombre	Objetivo	Estrategia	Entidades involucradas	Fecha de aprobado
CONPES 2848: Política Nacional de Desarrollo Sostenible	Promover el desarrollo sostenible en Colombia, para garantizar el bienestar de las generaciones presentes y futuras.	Fortalecer la institucionalidad ambiental, promover la gestión sostenible de los recursos naturales, fomentar la participación	Ministerio de Ambiente y Desarrollo Sostenible (MADS), Instituto de Hidrología, Meteorología y	26 de abril de 2006.

		ciudadana y la educación ambiental.	Estudios Ambientales (IDEAM), Autoridades Ambientales Regionales (CAR).	
CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa	Establecer lineamientos de política pública en materia de **ciberseguridad** y **ciberdefensa**, con el fin de diseñar y desarrollar una estrategia nacional que permita prevenir, controlar y contrarrestar las crecientes amenazas informáticas que afectan al país	Fortalecer de la capacidad del Estado para hacer frente a los riesgos cibernéticos mediante una estrategia nacional integral, apoyada en políticas, normativas y coordinación institucional.	Presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el ministro de Defensa Nacional, el ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad – DAS o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del ColCERT	14 de julio del 2011

CONPES 3769: Declaratoria De Importancia Estratégica De Los Proyectos “Ampliación Programa De Telecomunicaciones Sociales” E “Implementación 800 Tecnocentros Nacional	Ampliación Programa de Telecomunicaciones Sociales" e "Implementación 800 Tecnocentros Nacional", que incluyen las iniciativas "Proyecto Nacional de Conectividad de Alta Velocidad (PNCAV)" y "Proyecto de Acceso Universal a las Tecnologías de la Información y las Comunicaciones en zonas rurales y apartadas – Kioscos Vive Digital. Estos proyectos buscan promover la disponibilidad generalizada de las tecnologías de la información y la comunicación (TIC) en áreas rurales y apartadas, desarrollando los intereses sectoriales definidos en el Plan	Establecer mecanismos para garantizar la financiación, implementación y sostenibilidad de los proyectos durante y después del periodo de gobierno actual.	Institución pública de seguridad, salud, educación, biblioteca y juzgado, entre otros.	16 de septiembre del 2013

	Nacional de Desarrollo 2012-2014 "Prosperidad para Todos" y el Plan Vive Digital Colombia.			
CONPES 3975: Política Nacional Para La Transformación Digital E Inteligencia Artificia	Aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado, mediante la disminución de barreras, el fortalecimiento del capital humano y el desarrollo de condiciones habilitantes, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI	Proveer las bases para un entorno digital inclusivo, seguro y competitivo, donde se aproveche el potencial de las tecnologías digitales y emergentes para generar valor social y económico, posicionando a Colombia como líder en la transformación digital dentro del marco de la 4RI.	Archivo General de la Nación, Banco de Desarrollo Empresarial y el Comercio Exterior, Departamento Administrativo de Ciencia Tecnología e Innovación (Colciencias), Departamento Administrativo de la Presidencia de la República, Departamento Nacional de Planeación, Dirección de Impuestos y Aduanas Nacionales, Financiera de Desarrollo Nacional (FDN),	8 de noviembre del 2019

			Ministerio de Comercio, Industria y Turismo, Ministerio de Educación Nacional, Ministerio de Justicia y del Derecho, Ministerio de Salud y Protección Social, Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio del Trabajo, Servicio Nacional de Aprendizaje	
CONPES 3995: Política Nacional De Confianza Y Seguridad Digital	Establecer una política nacional que implemente medidas para ampliar la confianza digital y mejorar la seguridad digital en Colombia, promoviendo un entorno digital seguro y confiable	Garantizar que Colombia esté preparada para enfrentar los desafíos de la seguridad digital y aprovechar las oportunidades de crecimiento y desarrollo en el futuro digital.	Consejería Presidencial para Asuntos Económicos y Transformación Digital, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de	1 de julio del 2020

	que permita el desarrollo de una sociedad más incluyente y competitiva en el futuro digital.		Defensa Nacional y el Departamento Nacional de Planeación, entre otras	
CONPES 3854: Política Nacional de Seguridad Digital	Fortalecer la seguridad digital en Colombia, para proteger la información y los sistemas de información de las personas, las organizaciones y el Estado	Promover la adopción de medidas de seguridad, fortalecer la capacidad institucional y fomentar la cultura de la seguridad digital.	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Departamento Administrativo de Seguridad (DAS), Policía Nacional.	19 de diciembre de 2017.
CONPES 3988: Política Nacional de Economía Circular	Promover la transición hacia una economía circular en Colombia, para reducir los residuos, mejorar la eficiencia en el uso de los recursos y fomentar la innovación	Impulsar la prevención y la reducción de residuos, fomentar el reciclaje y la reutilización, promover la innovación y la inversión en tecnologías circulares.	Ministerio de Ambiente y Desarrollo Sostenible (MADS), Ministerio de Comercio, Industria y Turismo (MinCIT), Ministerio de Vivienda, Ciudad y Territorio (Minvivienda).	20 de junio de 2018.

CONPES 4069: Política Nacional de Desarrollo Económico y Social 2018-2022	Promover el desarrollo económico y social de Colombia, para mejorar la calidad de vida de la población y reducir la pobreza y la desigualdad.	Fortalecer la inversión pública y privada, promover el empleo y el emprendimiento, mejorar la educación y la salud, y reducir la pobreza y la desigualdad	Departamento Nacional de Planeación (DNP), Ministerio de Hacienda y Crédito Público (Min Hacienda), Ministerio de Trabajo (Min trabajo).	20 de junio de 2018
CONPES 3920: Política Nacional de Explotación de Datos (Big Data)	Optimizar el uso de datos para crear valor social y económico en Colombia.	Fomentar la digitalización, la apertura de datos y la interoperabilidad entre las entidades públicas	Departamento Nacional de Planeación (DNP), Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Superintendencia de Industria y Comercio (SIC).	17 de abril de 2018.
CONPES 4144: Política Nacional De Inteligencia Artificial	Generar las capacidades necesarias para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de los sistemas de Inteligencia	La política se estructura en torno a seis ejes estratégicos: 1. **Ética y Gobernanza:** Fortalecer la gobernanza y la aplicación de	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y Ministerio de Ciencia, Tecnología e Innovación.	14 de febrero del 2025

	Artificial (IA), con el fin de impulsar la transformación social y económica de Colombia	principios éticos en los sistemas de IA. 2. **Datos e Infraestructura:** Mejorar la infraestructura tecnológica y la disponibilidad de datos. 3. **Investigación, Desarrollo e Innovación (I+D+i):** Impulsar la producción científica y tecnológica en IA. 4. **Desarrollo de Capacidades y Talento Digital:** Capacitar talento en IA y fomentar la apropiación social del conocimiento. 5. **Mitigación de Riesgos:** Identificar, prevenir y mitigar riesgos asociados con la IA. 6. **Uso y Adopción de la IA:** Promover el uso de la IA en entidades públicas, empresas y territorio.	Ministerio de Defensa, Ministerio del Trabajo, Ministerio de Comercio, Industria y Turismo, Ministerio de Educación, Departamento Nacional de Planeación, Presidencia de la República, y otras instituciones del sector público y privado	

Fuente: Elaboración Propia (2025).

Siendo así, el desarrollo de estrategias efectivas y la participación de las entidades competentes son esenciales para abordar los desafíos que enfrenta el país en materia de transformación digital, seguridad y bienestar social. La colaboración entre sectores públicos y privados, junto con una inversión significativa en innovación, infraestructura y capacitación, permitirá potenciar el progreso socioeconómico y garantizar la competitividad de Colombia en el contexto de la Cuarta Revolución Industrial. Estas acciones no solo fortalecerán la confianza en el entorno digital, sino que también prepararán al país para enfrentar los retos del futuro con resiliencia y sostenibilidad (Departamento Nacional de Planeación, 2024).

En este marco, resulta imprescindible comprender que las estrategias actuales de transformación digital y las acciones de fortalecimiento de la seguridad y la confianza digital no surgieron de manera aislada, sino que son el resultado de una trayectoria de políticas públicas que se ha consolidado durante más de tres décadas. Analizar estos antecedentes permite identificar cómo Colombia pasó de iniciativas iniciales centradas en la conectividad y la digitalización de trámites, hacia una visión integral que incorpora la inteligencia artificial, la ciberseguridad avanzada y la gobernanza de datos como pilares del desarrollo digital. Este recorrido histórico no solo evidencia los avances institucionales y normativos, sino que también revela los desafíos pendientes para consolidar un ecosistema digital inclusivo y articulado, capaz de sostener el constitucionalismo digital que demanda la sociedad contemporánea.

3.10.8. Antecedentes de políticas públicas sobre desarrollo digital en Colombia

El estudio de los antecedentes de las políticas públicas sobre desarrollo digital permite comprender la evolución del Estado colombiano frente a los retos tecnológicos. Los primeros esfuerzos se enfocaron principalmente en la expansión de la conectividad y la digitalización de procesos administrativos, sin una visión integral que articulara ciberseguridad, gobernanza de datos y protección de derechos digitales. Como advierte Carbonell (2020), la efectividad de la acción estatal en entornos tecnológicos depende de una planificación capaz de anticipar riesgos y garantizar la inclusión digital, elementos que en los primeros años fueron incipientes o fragmentados.

En los últimos años, Colombia ha avanzado significativamente en la implementación de políticas públicas orientadas al desarrollo digital, reconociendo la importancia de las tecnologías y los datos en la construcción de una sociedad más moderna y competitiva. En este contexto, se destacan tres políticas clave que han marcado el rumbo del país (Departamento Nacional de Planeación, 2025):

Tabla 7.

Políticas públicas sobre desarrollo digital en Colombia

NOMBRE	DEFINICION
Política Nacional de Explotación de Datos (CONPES 3920 de 2018)	El principal objetivo de esta política fue establecer las condiciones necesarias para gestionar los datos como recursos valiosos que contribuyan al desarrollo económico y social. Para ello, propuso medidas para ampliar la disponibilidad de datos de las entidades públicas, asegurando que puedan ser aprovechados de manera efectiva y con un marco jurídico que garantice su explotación. Además, incluyó acciones destinadas a fortalecer el capital humano y a promover una cultura sólida de manejo de datos que impulse la creación de valor en el país. Esta política culminó su implementación el 31 de diciembre de 2021.
Política Nacional de Transformación Digital e Inteligencia Artificial (CONPES 3975 de 2019)	El objetivo de esta política fue impulsar la creación de valor social y económico mediante la transformación digital, el uso estratégico de tecnologías digitales y el fortalecimiento de las competencias del capital humano, con el fin de enfrentar los desafíos de la Cuarta Revolución Industrial (4RI). Además, planteó una visión para el país, orientada al desarrollo de las condiciones necesarias para abordar los cambios económicos y sociales derivados de la Inteligencia Artificial (IA). La implementación de esta política concluyó el 31 de diciembre de 2022.

Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020)	El principal objetivo de esta política fue implementar medidas que incrementaran la confianza digital y reforzaran la seguridad digital, con el fin de que Colombia se convierta en una sociedad inclusiva y competitiva en el ámbito digital del futuro. Para alcanzar este propósito, se establecieron acciones enfocadas en: i) fortalecer las capacidades en seguridad digital tanto de los ciudadanos como del sector público y privado; ii) actualizar el marco de gobernanza en seguridad digital para elevar su nivel de desarrollo; iii) evaluar la adopción de modelos, estándares y marcos de trabajo relacionados con la seguridad digital, poniendo especial atención en las nuevas tecnologías. Esta política introdujo el concepto de confianza digital como un eje central para el beneficio del ciudadano. Su ejecución finalizó el 31 de diciembre de 2022.
Política Nacional De Inteligencia Artificial (CONPES 4144)	El objetivo es generar las capacidades necesarias para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de los sistemas de Inteligencia Artificial (IA), con el fin de impulsar la transformación social y económica de Colombia.

Nota. Elaboración propia, (2025).

Finalmente, las políticas públicas establecidas en los CONPES 3920, 3975, 3995 y 4144 han sido pilares fundamentales en el proceso de transformación digital en Colombia. Cada una, desde su ámbito específico, ha contribuido al fortalecimiento del manejo de datos, la adopción estratégica de tecnologías emergentes y la construcción de un entorno digital confiable y seguro (Departamento Nacional de Planeación, 2025). Aunque las metas establecidas en estas políticas fueron alcanzadas en su mayoría, su implementación revela la necesidad de continuar avanzando en la consolidación de capacidades institucionales y ciudadanas que permitan enfrentar los desafíos de un mundo cada vez más digitalizado. En este contexto, el aprendizaje y los logros derivados de estas políticas sientan las bases para desarrollar estrategias más integrales y adaptativas que respondan a las demandas actuales y futuras de la Cuarta y Quinta Revolución Industrial.

En el siguiente capítulo se abordará el Plan Nacional de Desarrollo 2022-2026 y la Estrategia Nacional Digital de Colombia 2023-2026 (END 2023-2026), analizando su relevancia y proyección en el contexto actual.

Si bien los antecedentes revisados evidencian avances importantes en la digitalización del país y la creación de capacidades institucionales, también muestran una marcada fragmentación y una orientación predominantemente reactiva frente a los cambios tecnológicos. Las brechas en conectividad rural, la escasa integración entre políticas de seguridad digital y la ausencia de un enfoque explícito en derechos digitales reflejan la necesidad de políticas más articuladas y prospectivas. Estos aprendizajes constituyen la base sobre la cual se formula el Plan Nacional de Desarrollo 2022-2026 y la Estrategia Nacional Digital 2023-2026, orientadas a consolidar un ecosistema digital robusto, seguro e inclusivo, en sintonía con los principios del constitucionalismo digital colombiano.

3.10.9. Plan Nacional de Desarrollo 2022-2026

El Plan Nacional de Desarrollo (en adelante PND) 2022-2026 representa un hito estratégico en la consolidación de la transformación digital del país, al integrar la digitalización, la ciberseguridad y la gobernanza de datos como ejes transversales del desarrollo económico y social. A diferencia de los antecedentes normativos y de política pública, centrados en la conectividad y la digitalización administrativa, este plan propone una visión integral que vincula la innovación tecnológica con la protección de derechos fundamentales. Sin embargo, como advierte Carbonell (2020), el valor de un plan de desarrollo radica no solo en su diseño ambicioso, sino en su capacidad de ejecución y articulación interinstitucional, un desafío constante para Colombia ante la rápida evolución de las tecnologías emergentes.

El PND 2022-2026 de Colombia, "Colombia Potencia Mundial de la Vida", plantea una ambiciosa visión para el país en un contexto marcado por la acelerada transformación digital y la irrupción de las tecnologías emergentes. Este trabajo se propone analizar cómo este plan estratégico aborda los desafíos y oportunidades que presentan la cuarta y quinta revoluciones industriales, con un enfoque particular en tecnologías como la inteligencia artificial, el big data y el blockchain.

Ahora bien, el plan nacional frente al presente tema de investigación en su capítulo octavo en el que se contempló: Seguridad digital confiable para garantizar las libertades, proteger la dignidad y fomentar el desarrollo integral de las personas. En el uso de las

Tecnologías de la Información y la Comunicación (TIC) ha transformado las interacciones humanas a nivel global, lo que expone a las personas a posibles amenazas que pueden afectar su bienestar, dignidad y libertades, limitando su desarrollo integral. Esta problemática afecta en mayor medida a aquellos grupos en situación de vulnerabilidad. Por ello, es fundamental que el país disponga de las capacidades necesarias para gestionar de manera adecuada y eficiente estas amenazas, garantizando que las interacciones digitales se realicen de forma segura y confiable (Departamento Nacional de Planeación, 2025).

a. Dirección Nacional de Seguridad Digital: Con el objetivo de coordinar, definir, supervisar y controlar las estrategias nacionales de seguridad digital, así como de fortalecer las instituciones del país, se creará la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, dependiente de la Presidencia de la República. Esta agencia contará con una Dirección Nacional de Seguridad Digital, cuya misión será lograr un ecosistema digital seguro y confiable, implementando medidas para proteger al Estado en su conjunto. La dirección se encargará de planificar y coordinar las actividades destinadas a mejorar la preparación y resiliencia del país, fomentar el uso seguro de las TIC y definir propuestas vinculantes para asegurar la actuación del Estado frente a posibles amenazas y riesgos digitales. Asimismo, implementará el Modelo de Gobernanza de la Seguridad Digital, establecido por el Decreto 338 de 2022 (Departamento Nacional de Planeación, 2025).

b. Protección de individuos, infraestructuras digitales, refuerzo de las instituciones gubernamentales y aseguramiento de la provisión de servicios en el ámbito digital: Se creará y pondrá en marcha un plan para salvaguardar la infraestructura cibernética crítica del país, con el fin de salvaguardar la información de las entidades gubernamentales y de los ciudadanos contra ciberataques y delitos cibernéticos, basados en principios de recuperación y resiliencia. Asimismo, se promoverá el principio de "seguridad digital por defecto" para garantizar la continuidad de los servicios ofrecidos por las entidades públicas. Además, se definirán directrices técnicas para la implementación de estándares y buenas prácticas en el entorno digital, asegurando su alineación con los derechos humanos. Por último, con el fin de reforzar la capacidad de respuesta ante riesgos y amenazas cibernéticas, se establecerá un observatorio de ciberseguridad.

c. Legislación nacional orientada a garantizar un entorno digital seguro: Se elaborará un plan estratégico que agrupe las acciones legislativas entre diversas instituciones, con el propósito de implementas las acciones legales nacionales necesarias y fomentar la

colaboración entre países para enfrentar la delincuencia cibernética, en línea con los principios del Convenio de Budapest (Gobierno de Colombia, 2025).

Finalmente, el Plan Nacional de Desarrollo 2022-2026 de Colombia, bajo la visión de "Colombia Potencia Mundial de la Vida", no solo reconoce los desafíos que trae consigo la revolución digital, sino que también plantea un marco integral para garantizar que el país avance de manera segura y resiliente en su transición hacia la era digital. La creación de una infraestructura robusta en ciberseguridad, el fortalecimiento de las entidades públicas y la adopción de un enfoque legislativo acorde con los estándares internacionales, son pasos fundamentales para asegurar que las tecnologías emergentes, como la inteligencia artificial y el blockchain, contribuyan al bienestar de la sociedad, respetando los derechos humanos y protegiendo las libertades fundamentales. Este enfoque integral no solo es clave para fomentar el desarrollo económico y social, sino también para garantizar que la transformación digital sea inclusiva, justa y segura, especialmente para aquellos sectores más vulnerables. Es por ello, que es necesario abordar la estrategia nacional digital de Colombia para el periodo 2023 – 2026 (Departamento Nacional de Planeación, 2025).

En síntesis, el PND 2022-2026 constituye un avance hacia una política digital más estructurada y ambiciosa, al reconocer que la transformación tecnológica debe estar acompañada de seguridad digital, resiliencia institucional y enfoque en derechos humanos. No obstante, persisten retos significativos: la brecha entre planeación y ejecución, la falta de coordinación efectiva entre niveles de gobierno, y la ausencia de un marco legislativo integral que soporte plenamente los compromisos del plan. Estas limitaciones evidencian la necesidad de instrumentos operativos más concretos, los cuales comienzan a materializarse en la Estrategia Nacional Digital 2023-2026, que traduce la visión del PND en acciones, metas y líneas estratégicas específicas, tema que se desarrolla en el siguiente subcapítulo

3.10.10. Estrategia Nacional Digital de Colombia 2023-2026 (END 2023-2026)

La Estrategia Nacional Digital de Colombia 2023-2026 (END 2023-2026) constituye el instrumento más reciente de planeación estratégica en materia de transformación digital y puede entenderse como la operativización del Plan Nacional de Desarrollo 2022-2026. A diferencia de los antecedentes normativos y de política pública, esta estrategia asume un enfoque integral, inclusivo y orientado a derechos, que reconoce que la digitalización del Estado y de la economía debe acompañarse de medidas para garantizar la seguridad digital, la gobernanza de datos y la reducción de brechas sociales. En línea con lo que señala Pérez Luño

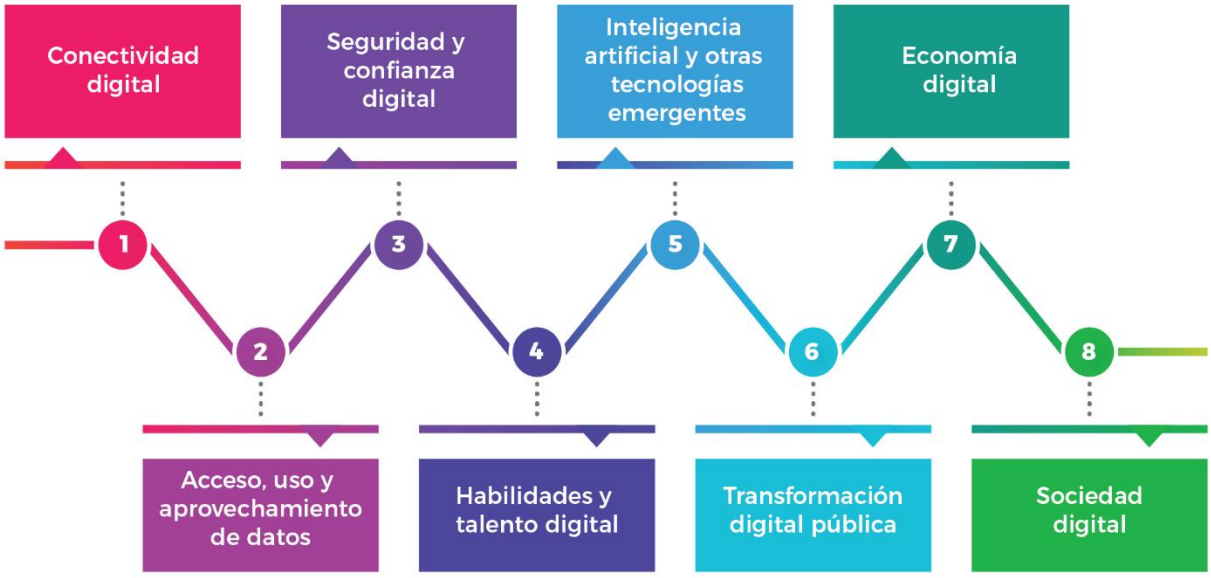
(2019), una estrategia digital que no contemple el impacto en derechos fundamentales corre el riesgo de convertirse en un mero programa tecnológico, sin sustento constitucional ni social.

La Estrategia Nacional Digital de Colombia 2023-2026 (END 2023-2026), basada en el Plan Nacional de Desarrollo y los planes sectoriales del gobierno, establece una visión integral para la adopción y uso de tecnologías digitales. Este enfoque busca identificar prioridades, coordinar esfuerzos gubernamentales, monitorear avances y ajustar políticas públicas según los desafíos emergentes. El objetivo central de la END 2023-2026 es liberar el potencial de la transformación digital para superar los desafíos económicos, sociales y ambientales de Colombia, promoviendo un desarrollo digital inclusivo, equitativo, seguro, productivo y sostenible. Esto incluye fortalecer las capacidades digitales de las personas, hogares, entidades públicas y empresas, mientras se mitigan riesgos asociados con la digitalización acelerada (Gobierno de Colombia, 2025).

La estrategia se organiza en ocho ejes clave: i) conectividad digital, ii) acceso y uso de datos, iii) seguridad digital, iv) talento digital, v) tecnologías emergentes, vi) transformación digital del sector público, vii) economía digital y viii) sociedad digital inclusiva. Como se representa a continuación:

Figura 11.

Ejes de la estrategia



Nota. Adaptado de Departamento Nacional de Planeación (2024). Estrategia Nacional Digital de Colombia 2023-2026.

https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf.

Nota: Cada eje detalla objetivos, estrategias y acciones específicas, complementadas con políticas existentes que se fortalecen con esta nueva visión. Finalmente, la END 2023-2026 presenta acciones necesarias para una implementación efectiva, metas para 2026 y un resumen de los objetivos estratégicos, reafirmando su compromiso con un futuro digital que promueva la prosperidad económica, el bienestar social y la sostenibilidad ambiental.

Adicionalmente, se hace necesario conocer los ejes y objetivos:

Tabla 8.

Ejes, objetivos y líneas estratégicas de la END 2023-2026

Ejes	Objetivos	Líneas Estratégicas
Conectividad digital para mejorar la vida de los colombianos	Garantizar la conectividad en todo el país, entendiendo el acceso a las TIC como un derecho universal, especialmente en áreas sin servicios o con cobertura deficiente.	- Promover la expansión de redes de comunicación para crear oportunidades y aumentar la igualdad. - Asegurar el uso eficiente del espectro radioeléctrico para beneficiar a la sociedad. - Fomentar el uso masivo de las TIC para reducir la brecha entre áreas urbanas y rurales. - Mejorar los servicios de televisión y radiodifusión para fomentar la inclusión social.
Acceso y aprovechamiento de	Desarrollar una infraestructura de datos sólida, segura y accesible con el fin de apoyar el proceso de toma de	- Asegurar la disponibilidad de datos básicos de calidad.

datos para impulsar el cambio social	decisiones, así como para promover una cultura orientada al uso de los datos.	- Promover la interoperabilidad como un bien público digital. - Fomentar la reutilización y el intercambio seguro de información.
Seguridad digital para proteger libertades y desarrollo integral	Crear las condiciones necesarias para proteger los derechos, la dignidad y el desarrollo de los ciudadanos frente a las amenazas digitales.	- Mejorar la coordinación y planificación en temas de seguridad digital. - Promover la preparación y resiliencia del país ante riesgos digitales. - Proteger a las personas, infraestructuras digitales y organismos del Estado. - Desarrollar legislación para asegurar un entorno digital seguro y confiable.
Habilidades y talento digital como motor de oportunidades	Fortalecer las capacidades digitales de los colombianos para generar nuevas oportunidades y potenciar el desarrollo social, educativo y productivo.	- Acelerar la alfabetización digital y la apropiación tecnológica en la sociedad. - Incrementar el talento digital para mejorar la productividad laboral y la empleabilidad. - Promover el acceso y uso de tecnologías digitales en el ámbito educativo.
Inteligencia Artificial y otras tecnologías emergentes para crear valor económico y social	Generar espacios para el aprovechamiento de la Inteligencia Artificial y otras tecnologías emergentes, promoviendo su implementación de forma ética y	- Impulsar políticas públicas para el desarrollo de la inteligencia artificial y otras tecnologías emergentes.

	respetuosa con los derechos humanos.	
Transformación digital pública para fortalecer la relación Estado-Ciudadanía	Mejorar la interacción entre el Estado y los ciudadanos mediante el uso de tecnologías digitales, proporcionando soluciones más eficaces y centradas en las personas.	- Optimizar el Gobierno Digital para facilitar la relación entre el Estado y los ciudadanos. - Fomentar la innovación pública para una mejor atención a las necesidades de los ciudadanos. - Crear una justicia digital más eficiente e inclusiva.
Economía digital para una transformación productiva	Promover el uso de las TIC para transformar los sectores productivos, cerrando la brecha tecnológica y fomentando una economía sostenible basada en el conocimiento.	- Impulsar la adopción de tecnologías digitales en los sectores productivos. - Fortalecer la industria digital para apoyar la adopción de nuevas tecnologías en el sector productivo. - Fomentar el emprendimiento digital y la innovación para el crecimiento económico. - Afrontar los desafíos de las nuevas formas de trabajo generadas por las tecnologías digitales.
Sociedad digital inclusiva, equitativa y sostenible	Promover una sociedad digital que coloque a las personas y su bienestar en el centro del desarrollo digital, asegurando el acceso equitativo a las	- Fomentar el uso inclusivo y equitativo de las tecnologías digitales para reducir las desigualdades. - Abordar los riesgos

	TIC y protegiendo los derechos en el entorno digital.	asociados a la desinformación y la difusión de contenidos falsos. - Emplear herramientas digitales e información basada en datos para afrontar los desafíos sociales y ambientales. - Promover el desarrollo de ciudades y territorios inteligentes. - Impulsar el sector espacial para el desarrollo social y económico.

Nota: La Estrategia Nacional Digital (END) 2023-2026 de Colombia establece una serie de ejes y objetivos clave para guiar la transformación digital del país en los próximos años. Cada eje se enfoca en aspectos fundamentales del desarrollo digital, como la conectividad, la seguridad, el acceso a datos, el fortalecimiento de habilidades digitales, y la promoción de tecnologías emergentes como la Inteligencia Artificial. Tabla de elaboración propia.

Las líneas estratégicas asociadas a cada eje buscan no solo mejorar la infraestructura tecnológica y digital del país, sino también garantizar que estos avances sean inclusivos, equitativos y respetuosos con los derechos humanos. Además, se hace especial énfasis en la protección de la privacidad y las libertades individuales en el entorno digital, y en el fortalecimiento de la relación entre el Estado y la ciudadanía a través del uso de las TIC.

Esta estrategia se alinea con los objetivos del Plan Nacional de Desarrollo 2022-2026, con el propósito de impulsar una economía digital sostenible y resiliente, y generar oportunidades para todos los colombianos, en particular para aquellos en situación de vulnerabilidad. La implementación exitosa de estas líneas estratégicas será clave para lograr una sociedad digital más conectada, innovadora y equitativa en el futuro cercano.

Si bien la END 2023-2026 constituye un avance decisivo hacia un ecosistema digital más seguro, inclusivo y orientado al desarrollo social, enfrenta retos significativos para su implementación efectiva. Persisten brechas de conectividad rural, limitaciones en talento digital especializado y la ausencia de un marco normativo integral sobre inteligencia artificial, metaverso y ciberseguridad avanzada, que permita articular la planeación estratégica con la protección de los derechos fundamentales. El éxito de la END dependerá de la coordinación interinstitucional, la inversión sostenida en infraestructura y talento, y su sincronización con la legislación y la jurisprudencia constitucional. Solo bajo esta articulación será posible avanzar hacia un constitucionalismo digital colombiano, en el que la innovación tecnológica y la protección de derechos convivan de manera armónica. Este análisis abre paso al subcapítulo 2.3, donde se examina cómo la Corte Constitucional ha contribuido a llenar los vacíos normativos en entornos digitales.

3.11. Jurisprudencia relevante en entornos digitales

La jurisprudencia de la Corte Constitucional colombiana ha desempeñado un papel central en la protección de los derechos fundamentales en entornos digitales, especialmente frente a la ausencia de un marco normativo integral que anticipe los desafíos de la transformación tecnológica. La Corte ha asumido una postura garantista y adaptativa, expandiendo el alcance de la Constitución de 1991 para enfrentar fenómenos como el uso indebido de datos personales, la libertad de expresión en redes sociales y la adopción de sistemas de inteligencia artificial en decisiones públicas y privadas. Como advierte Ferrajoli (2020), en contextos donde la legislación es reactiva o fragmentada, la labor judicial se convierte en barrera de contención frente a la vulneración de derechos, al tiempo que orienta al legislador sobre los vacíos normativos que deben ser superados.

La selección de la jurisprudencia se dio en torno a las decisiones relevantes de los últimos 20 años sobre la protección de derechos fundamentales; el criterio de análisis fue la relación directa con la alusión a derechos como la privacidad, libertad de expresión e intimidad. Este análisis se contrasta con la regulación existente en un marco comparado enrostrado al principio de este capítulo (la cual, en su mayoría, corresponde a un marco de regulación europeo). No obstante, a lo largo del capítulo se hará mención de otras sentencias en el tema de vacíos legales.

3.11.1. Protección de datos y privacidad digital

El derecho a la intimidad y al habeas data ha sido uno de los campos donde la Corte Constitucional ha sentado precedentes relevantes para proteger a los ciudadanos frente al uso masivo de datos personales y el riesgo de vigilancia digital. Entre las sentencias más significativas se encuentran:

Sentencia	**Derecho protegido**	**Aporte de la sentencia**	**Vacío normativo identificado**
T-729 de 2002	Intimidad y habeas data.	Reconoce el derecho de los ciudadanos a conocer, actualizar y rectificar su información personal, fijando las bases del principio de autodeterminación informática.	Ausencia de una ley integral de protección de datos (posteriormente suplida en parte por la Ley 1581 de 2012).
T-634 de 2013	Imagen y buen nombre	Exige consentimiento informado para la publicación y uso de imágenes en entornos digitales, especialmente en redes sociales y medios electrónicos.	Falta de regulación clara sobre responsabilidad por contenidos digitales.
T-372 de 2023	Acceso a internet y libertad de expresión.	Reconoce que el acceso a internet es condición instrumental para el	Ausencia de protocolos y normas claras sobre suspensión o

		ejercicio de derechos fundamentales, censurando interrupciones de conectividad sin justificación transparente durante protestas.	limitación de servicios digitales.
T-323 de 2024	Debido proceso y protección frente a decisiones automatizadas	Establece que la inteligencia artificial no puede sustituir la supervisión humana en la función administrativa o judicial y que toda decisión automatizada debe ser impugnable.	Carencia de regulación integral sobre IA y su uso en la justicia y administración pública.

Elaboración propia, 2025

Más allá de la protección de la intimidad y los datos personales, la digitalización ha transformado la manera en que los ciudadanos ejercen su libertad de expresión. La Corte Constitucional ha debido pronunciarse sobre nuevas formas de interacción digital, donde internet y las redes sociales son espacios esenciales para la participación democrática, pero también escenarios de conflictos entre derechos, como la honra, el buen nombre y la seguridad pública. Siguiendo la teoría de ponderación de derechos de la Corte ha buscado equilibrar la libertad de expresión digital con la protección frente a contenidos ilícitos, evitando tanto la censura como la impunidad en el ciberespacio (Alexy, 2002).

3.11.2. Libertad de expresión y redes sociales

La libertad de expresión en entornos digitales adquiere dimensiones inéditas ante la inmediatez y masividad de las redes sociales. La Corte ha analizado casos que delimitan su alcance:

Sentencia	Derecho protegido	Aporte jurisprudencial	Vacío normativo identificado
T-145/2016	Libertad de expresión en redes sociales	Reconoce límites al discurso en redes; equilibra con otros derechos	Falta regulación específica sobre abuso y conflictos en redes sociales
T-260/2019	Libertad de información en redes	Establece exigencias sobre veracidad y responsabilidad editorial	Ausencia de marco legal para periódicos ciudadanos digitales

Fuente: Elaboración propia (2025).

El análisis integral de la jurisprudencia digital evidencia dos rasgos constantes: 1) la Corte mantiene un compromiso firme con la protección de los derechos fundamentales en entornos tecnológicos; y 2) advierte reiteradamente sobre vacíos normativos que limitan la efectividad de dicha protección. Para visualizar de manera sintética la evolución jurisprudencial y los vacíos detectados, se presenta a continuación un cuadro comparativo de sentencias, que permitirá cerrar este subcapítulo con un análisis crítico y propositivo hacia el desarrollo de un constitucionalismo digital colombiano.

La jurisprudencia constitucional en entornos digitales evidencia que la Corte ha asumido un rol proactivo y garantista, extendiendo la protección de la Constitución de 1991 al ecosistema digital. No obstante, sus decisiones también ponen en evidencia un vacío normativo estructural: Colombia carece de un marco legal integral y anticipatorio que regule inteligencia artificial, ciberseguridad avanzada, metaverso y gobernanza de datos. Como señalan Pérez

Luño (2019) y Carbonell (2020), la jurisprudencia aislada no basta para consolidar la protección efectiva de los derechos digitales; se requiere la articulación de ley, política pública y control judicial en un constitucionalismo digital colombiano que responda a los retos de la era digital y la quinta revolución industrial.

Finalmente, es necesario reconocer que los retos del constitucionalismo digital en Colombia no dependen únicamente del diseño normativo o de la jurisprudencia, sino también de factores socioculturales y de cultura jurídica. En un país donde la ignorancia de la ley no sirve de excusa, persiste un escaso esfuerzo social por conocer y respetar las normas, lo que se evidencia en el uso irresponsable de tecnologías, redes sociales e internet. Esta conducta atraviesa todas las esferas: desde altos funcionarios del Estado, legisladores y representantes políticos, hasta el ciudadano común, generando un entorno digital propenso a la desinformación, la vulneración de derechos y el abuso de herramientas tecnológicas. En este contexto, el constitucionalismo digital colombiano no solo requiere normas claras y tipificadas que regulen cada uno de los fenómenos tecnológicos, sino también un cambio cultural que promueva educación digital, responsabilidad social y ética ciudadana. Sin estos elementos, las normas corren el riesgo de permanecer como instrumentos formales sin eficacia material, incapaces de prevenir los daños que hoy se expanden por todas las órbitas del ecosistema digital

En síntesis, la jurisprudencia constitucional colombiana ha asumido un papel protagónico en la protección de los derechos fundamentales en entornos digitales, extendiendo la vigencia de la Constitución de 1991 hacia los nuevos escenarios tecnológicos. Las sentencias analizadas reflejan una postura garantista y adaptativa, que llena parcialmente los vacíos normativos en materia de habeas data, libertad de expresión, buen nombre, debido proceso y uso de inteligencia artificial. Sin embargo, también evidencian un déficit estructural: el país carece de un marco legal integral, coherente y anticipatorio, capaz de regular fenómenos como la ciberseguridad avanzada, el metaverso, la gobernanza de datos y la inteligencia artificial generativa, lo que limita la efectividad de los fallos judiciales.

En este contexto, resulta imprescindible avanzar hacia un constitucionalismo digital colombiano que articule la ley, la política pública y la jurisprudencia en un ecosistema normativo preventivo y sostenible. A su vez, la transformación cultural en el uso responsable de las tecnologías, redes sociales e internet se presenta como un reto ineludible: mientras la sociedad no asuma una cultura digital consciente y respetuosa de los derechos, las normas y sentencias tendrán un alcance limitado. Este escenario abre paso al Capítulo 3, donde se

examinarán los retos y desafíos pendientes para consolidar un marco jurídico y social capaz de responder a las exigencias de la era digital y la quinta revolución industrial.

3.12. Vacíos normativos y desafíos regulatorios

La acelerada expansión de tecnologías emergentes como la inteligencia artificial, el blockchain, los contratos inteligentes y los sistemas descentralizados de gobernanza tecnológica, ha generado en los últimos años una serie de retos que el derecho colombiano todavía no logra abordar de manera suficiente. Estas transformaciones digitales no solo modifican las formas de interacción social y económica, sino que también afectan principios constitucionales esenciales como la seguridad jurídica, la responsabilidad, la tutela judicial efectiva y la protección de los derechos fundamentales. En este panorama, la discusión sobre los vacíos normativos adquiere un papel central, especialmente cuando se observan fenómenos como los sistemas autónomos, la toma algorítmica de decisiones y las estructuras descentralizadas sin personalidad jurídica.

Ahora bien, estos vacíos no representan simples ausencias legislativas, sino que se convierten en zonas donde el derecho carece de herramientas sustantivas o procedimentales que permitan ofrecer una respuesta clara y coherente. Su impacto puede comprometer tanto la posibilidad real de acceder a la administración de justicia como la atribución adecuada de responsabilidades cuando los hechos desbordan las categorías jurídicas tradicionales.

3.12.1. Caso 'DAO'.

Una DAO puede definirse como una estructura organizativa sustentada en tecnología *blockchain* que facilita la coordinación y el autogobierno de sus participantes a través de reglas programadas que se ejecutan automáticamente en una cadena de bloques pública. Su rasgo distintivo es que el proceso de toma de decisiones se articula de forma descentralizada, sin depender de una autoridad centralizada que controle la gobernanza (Hassan y De Filippi, 2021).

La idea de una DAO no surge completamente de cero. De hecho, mucho antes de su aparición ya existían estructuras organizativas similares, como las denominadas organizaciones *chaordic*, entre ellas la empresa VISA, que suele considerarse un antecedente conceptual de las DAOs. No obstante, el modelo organizativo de VISA ha experimentado transformaciones sustanciales a lo largo del tiempo, alejándose de las estructuras originales diseñadas en la década de 1970 (Giovannini, 2023).

La primera DAO plenamente funcional que logró captar una atención significativa fue el proyecto denominado "The DAO". Este caso se ha convertido en el ejemplo más emblemático, documentado y trascendental de un hackeo en el ámbito de *blockchain*. Resulta particularmente llamativo que la iniciativa detrás del proyecto tuviera su origen en 2016 en Sajonia, Alemania, así como las amplias repercusiones que tuvo el incidente para Ethereum, la segunda red *blockchain* más grande. Como consecuencia del ataque, la comunidad se desdobló en dos cadenas distintas —Ethereum y Ethereum Classic— tras la implementación de un *hard fork*.

En abril de 2016, el programador Christopher Jentzsch publicó un *whitepaper* (Teichmann, 2017) que desarrollaba con mayor detalle la propuesta de "The DAO". Este proyecto podía asimilarse a una empresa de capital de riesgo o a un fondo de inversión descentralizado, cuyo funcionamiento se basaba en la recaudación de fondos de sus miembros a cambio de *governance tokens*. Dichos tokens representan derechos específicos; en este caso, permitían al titular participar en procesos de votación digital. Además, los *governance tokens* de "The DAO" eran fungibles —por lo tanto, libremente transferibles— y podían negociarse de forma anónima (Giovannini, 2023).

Si bien el objetivo inicial del equipo alemán era financiar su propia empresa, Slock.It UG, mediante la aprobación de los titulares de *governance tokens*, el diseño del sistema también permitía que cualquier participante presentara propuestas para ser sometidas a votación, siempre que estas pudieran ejecutarse empleando Ethereum. Una vez alcanzado el quórum requerido, el *smart contract* subyacente debía gestionar de forma automatizada los flujos de capital tras la aprobación de la propuesta (Giovannini, 2023).

Según Hassan y De Filippi (2021) las características de las DAO en general concurren en las siguientes:

- El código fuente de una DAO se despliega en una *blockchain* con capacidad para ejecutar *smart contracts*, como Ethereum (preferiblemente, aunque no necesariamente, en una *blockchain* pública).
- El código del contrato inteligente de una DAO establece las reglas de interacción entre los participantes, si bien no está del todo claro hasta qué punto pueden existir otros mecanismos de gobernanza que modifiquen o incluso prevalezcan sobre dicho código.

- Dado que estas reglas se expresan en forma de *smart contracts*, su ejecución es automática e independiente de la voluntad de las partes involucradas.
- La gobernanza de la DAO debe mantenerse libre de control centralizado (pág.4).

En este contexto, "The DAO" incorporó dos medidas de seguridad con el fin de reducir riesgos operativos. En primer lugar, se estableció un periodo de *cooling* destinado a garantizar que los miembros dispusieran de tiempo suficiente para revisar los detalles de cualquier propuesta antes de que esta fuese ejecutada. En segundo lugar, se incluyó un mecanismo de separación (*split function*) que permitía a los titulares de *governance tokens* abandonar la organización y trasladar proporcionalmente sus fondos a una nueva "DAO hija" si no estuvieran de acuerdo con las decisiones adoptadas por la mayoría. Esta función pretendía ofrecer una vía de protección para los inversores disidentes y, en principio, reforzar la descentralización del sistema (Mehar et al., 2019)

Sin embargo, este mismo mecanismo de separación terminó revelándose como la principal vulnerabilidad del proyecto. Debido a un error en el código, un atacante logró explotar la *split function* para crear reiteradamente DAOs hijas y transferir fondos antes de que el sistema actualizara el saldo correspondiente. Como resultado, más de un tercio del capital invertido fue desviado hacia una DAO hija bajo el control del atacante. Aunque los fondos quedaron temporalmente bloqueados por un periodo de 28 días —derivado de la arquitectura del *smart contract*—, el incidente desató una crisis profunda en la comunidad de Ethereum (Mehar et al., 2019).

A partir de este momento, se abrió un intenso debate sobre la respuesta adecuada frente al ataque. Las alternativas consideradas incluían no intervenir y permitir que el atacante reclamara los fondos una vez vencidos el plazo; introducir un *soft fork* mediante una lista negra que impidiera la movilización de los Ether desviados; o llevar a cabo un *hard fork*, revirtiendo por completo las transacciones y restituyendo los fondos a los inversores. Como es sabido, la comunidad optó finalmente por el *hard fork*, lo que condujo a la bifurcación entre Ethereum y Ethereum Classic, esta última defendiendo el principio de inmutabilidad absoluta del registro (Reyes, 2017).

A pesar de las ventajas potenciales asociadas a las DAOs, lo cierto es que estos instrumentos presentan riesgos inminentes como el que se evidenció en 2016. Si se analiza su modelo de gobernanza, surgen dificultades relacionadas con la adopción de acuerdos por parte

de participantes que, en muchos casos, no están realmente interesados en involucrarse activamente en el desarrollo del proyecto (Morant, 2023). Este fenómeno, similar a lo que ocurre en las grandes sociedades de capital, hace necesario incentivar el ejercicio de los derechos de voto, especialmente cuando dichos derechos dependen de sistemas de recompensas. Solo así pueden alcanzarse los porcentajes mínimos de participación exigidos para aprobar decisiones según la estructura o normativa específica de cada DAO (Aznar, 2024).

Asimismo, existen riesgos de manipulación derivados de la concentración de grandes porcentajes de participación, facilitada en parte por el mecanismo de consenso habitualmente utilizado, el *proof-of-stake*. Este sistema abre la posibilidad de ataques del 51 %, mediante los cuales actores malintencionados podrían alterar de forma ilegítima el contenido de la cadena de bloques con fines fraudulentos. A ello se añade una problemática más general vinculada a la centralización. Aunque, en teoría, las DAOs son organizaciones descentralizadas, en la práctica muchas acaban bajo el control de un grupo reducido de titulares de tokens de gobernanza, ya sea por falta de liquidez o por la elevada proporción retenida por los fundadores. En este tipo de contextos, es frecuente que se reproduzcan dinámicas propias de sociedades con un grupo de control dominante, generándose riesgos de decisiones adoptadas en beneficio de unos pocos y en detrimento de la comunidad (Morant, 2023).

A esta situación se suma la escasa (o incluso inexistente) regulación específica aplicable a las DAOs. En la mayoría de ordenamientos jurídicos una regulación sobre blockchain o regulación de criptoactivos sigue en fase de desarrollo o implementación. Esta ausencia de regulación genera problemas en dos planos. A nivel micro, reduce la protección disponible para los inversores y suscita dudas sobre la posible aplicación de la normativa financiera a las DAOs con funciones de carácter financiero, especialmente en materia de protección del inversor y prevención del fraude. A nivel macro, la falta de un marco regulatorio claro incrementa los riesgos para la estabilidad financiera y la seguridad asociada a los criptoactivos, como han advertido diversos supervisores y organismos internacionales (Morant, 2023).

En el caso del ordenamiento español, como se analizará a continuación, no existe aún una regulación específica de las DAOs. Debido a sus características, estas entidades difícilmente encajan en los modelos organizativos tradicionales. Uno de los principales problemas radica en la ausencia de un órgano de administración en sentido estricto, algo que resulta esencial y jurídicamente exigible en el funcionamiento de cualquier persona jurídica bajo el modelo corporativo vigente. A ello se suma que los fundadores suelen permanecer

ocultos y no desean revelar su identidad, lo que complica gravemente cualquier proceso formal de constitución. En particular, en aquellos casos en los que la DAO pudiera calificarse como entidad mercantil, el tipo societario que más se asemejaría sería el de la sociedad irregular, pues no se cumplirían los requisitos formales de constitución: elevación a escritura pública ante notario e inscripción en el Registro Mercantil. Sin embargo, esta solución tampoco resolvería aspectos cruciales, especialmente la limitación de responsabilidad de los participantes (Morant, 2023).

Actualmente, coexisten múltiples marcos regulatorios, que varían tanto por país como por el modelo de regulación adoptado. Algunos Estados optan por adaptar la figura de la sociedad de responsabilidad limitada (LLC), otorgando así cierta limitación de responsabilidad a los miembros; este es el caso de Wyoming, Vermont, Tennessee y, en cierta medida, Delaware, en Estados Unidos. La *Utah Decentralized Autonomous Organizations Act* (2023) adopta un enfoque distinto hacia las DAOs al permitir crear LLD, que requieren identificar al organizador, aunque esta información puede mantenerse fuera del registro público. Los miembros solo responden por sus aportes *on-chain*, pero si la DAO recibe una sentencia y algunos votan contra su cumplimiento, estos pueden ser responsables proporcionalmente.

Otros países, como Suiza o Panamá, han preferido la figura de las fundaciones, mientras que algunas jurisdicciones consideran más adecuadas las cooperativas, como ocurre en el Estado de Colorado. Por su parte, en el Reino Unido y Singapur se ha optado por modelos basados en *trusts* (Johnson, 2023). Por otro lado, Malta se ha posicionado como líder en la regulación de blockchain y DAOs. Su Ley de Arreglos y Servicios de Tecnología Innovadora (ITAS) de 2018 adapta el marco jurídico para contemplar las particularidades de estas organizaciones, reconociendo a las DAOs como “Arreglos Tecnológicos Innovadores”. Esto permite su certificación y les brinda mayor legitimidad y claridad operativa (Aznar, 2024).

Un ejemplo es Ooki DAO (2022), demandada por la CFTC en California por operar un exchange de activos digitales con margen. El juez consideró que la DAO era una asociación no incorporada, permitiendo notificarla mediante su foro. Al no presentarse, se dictó sentencia en rebeldía (junio 2023). Este caso muestra que, incluso sin un marco legal uniforme, las DAOs pueden ser demandadas en estados que no reconocen su estructura, dejando a sus miembros expuestos a legislaciones potencialmente desfavorables (Johnson, 2023).

En un caso más reciente, Lido DAO adopta una estrategia similar de “negación de capacidad”, alegando que, por ser descentralizada y existir como código, no puede ser demandada. Sin embargo, designó a Dolphin CL LLC para presentar una moción de desestimación, aunque esta entidad no tiene autoridad legal formal ni representa oficialmente a la DAO. Esta paradoja resalta un desafío fundamental: cómo puede una DAO sostener que no tiene personalidad jurídica mientras participa indirectamente en un proceso judicial (California Federal Court, 2024).

En Colombia, esta situación invita a reflexionar sobre la capacidad institucional para enfrentar un caso de características semejantes. Más que formular una pregunta en abstracto, resulta necesario analizar la solidez actual del ordenamiento jurídico frente a escenarios en los que la tecnología introduce dinámicas sin sujeto responsable plenamente identificable, sin un marco legal aplicable o sin una categoría jurídica que permita ordenar la controversia. Comprender el nivel de respuesta institucional implica estudiar la manera como estos vacíos se relacionan con la administración de justicia y, sobre todo, con la posibilidad de que un tribunal deba abstenerse de decidir por falta de bases jurídicas suficientes.

En ausencia de regulación expresa, la capacidad de los jueces colombianos para pronunciarse de fondo se ve condicionada por varios elementos. Una decisión inhibitoria procede únicamente cuando el juez carece de competencia, cuando no existe un objeto jurídico verificable o cuando la pretensión no puede resolverse con las normas vigentes. En este punto, emergen situaciones en las que la inhibición podría resultar inevitable. Colombia aún no cuenta con un marco normativo que regule asuntos como la responsabilidad en estructuras descentralizadas sin personalidad jurídica, la generación de efectos jurídicos a partir de decisiones automatizadas, la responsabilidad derivada de organizaciones autónomas basadas en blockchain, la gobernanza de sistemas inteligentes sin supervisión humana permanente o la capacidad jurídica de entidades no humanas con autonomía tecnológica.

Sin estas bases, es posible que el juez colombiano enfrente dificultades semejantes a las observadas en el caso DAO, donde la imposibilidad de ubicar actos y decisiones dentro de categorías jurídicas tradicionales llevó a tribunales europeos y estadounidenses a optar por decisiones inhibitorias. Allí se concluyó que no existía un sujeto responsable identificable ni una figura jurídica disponible para atribuir consecuencias de manera válida.

Sin embargo, y aunque estos vacíos son evidentes, el sistema jurídico colombiano cuenta con herramientas que permiten mitigar su impacto. A diferencia del derecho estadounidense, Colombia incorpora mecanismos de integración normativa como la analogía, los principios generales del derecho, el bloque de constitucionalidad y la jurisprudencia constitucional, que permiten suplir la falta de regulación expresa en ciertos casos. Estas herramientas no resuelven por completo el problema, pero sí pueden evitar que la justicia quede paralizada ante un vacío.

Por esa razón, la conclusión no puede ser absoluta. En algunos escenarios, la inhibición judicial sería inevitable, especialmente cuando no exista un sujeto pasible de responsabilidad, cuando el fenómeno tecnológico no pueda subsumirse en una relación jurídica reconocida o cuando la categoría indispensable para resolver el caso no esté contemplada en el ordenamiento. Sin embargo, en otros contextos, los jueces podrían acudir a figuras como la responsabilidad objetiva, el deber reforzado de diligencia, la representación, la responsabilidad solidaria, la ponderación de derechos o incluso a marcos regulatorios análogos en protección al consumidor, habeas data o comercio electrónico.

Es entonces que el problema no radica únicamente en la eventual inhibición judicial, sino en el nivel de fragilidad normativa e institucional frente a tecnologías emergentes. Esta fragilidad evidencia la urgencia de avanzar hacia un constitucionalismo digital capaz de ofrecer criterios claros, consistentes y adaptados a la revolución tecnológica, reduciendo la incertidumbre jurídica y evitando que los jueces se enfrenten a controversias para las cuales aún no cuentan con un marco adecuado.

3.12.2. Falta de regulación integral para tecnologías emergentes

Aunque el país ha logrado avances significativos en materia de comercio electrónico, protección de datos y delitos informáticos, todavía no existe una regulación integral que aborde de forma sistemática el impacto constitucional, ético y jurídico de tecnologías como la inteligencia artificial, el Big Data, el blockchain, el metaverso o la robótica avanzada.

Este desfase normativo genera un terreno inestable para la garantía de derechos fundamentales, ya que las leyes vigentes suelen apoyarse en categorías tradicionales que no fueron diseñadas para responder a las transformaciones digitales actuales. Como explica Floridi (2014), en una reflexión que parece escrita para el contexto colombiano:

> La sociedad está mirando hacia un entorno infosférico, en el que la información no solo describe el mundo, sino que lo constituye. Cuando el Derecho sigue anclado en categorías previas, se produce una brecha ontológica que genera vacíos regulatorios difíciles de subsanar con soluciones parciales (p.10).

La legislación colombiana, aunque ha incorporado esfuerzos significativos como la Ley 527 de 1999 sobre comercio electrónico y firma digital o la Ley 1581 de 2012 sobre protección de datos personales, continúa siendo incompleta frente a la complejidad de las tecnologías emergentes.

3.12.2.1. Vacíos normativos en la regulación de protección de datos y moderación de contenido.

En el ámbito del Big Data y la analítica avanzada, existe un vacío normativo significativo. La regulación colombiana se ha construido principalmente sobre el consentimiento informado y los principios del habeas data; sin embargo, estos mecanismos no fueron diseñados para abarcar sistemas de recopilación masiva de información, minería de datos o modelos predictivos que generan inferencias sin consentimiento explícito. La Corte Constitucional ha reconocido que la evolución tecnológica altera sustancialmente los riesgos asociados a la circulación de datos personales, afirmando que "el tratamiento masivo y automatizado de datos puede producir afectaciones profundas e incluso irreparables a la dignidad humana" (Sentencia T-063 de 2019). No obstante, este reconocimiento jurisprudencial aún no se ha traducido en reformas legislativas que establezcan límites claros ni en la implementación de mecanismos efectivos de auditoría tecnológica.

En Colombia, la protección de los datos personales se sustenta en el artículo 15 de la Constitución Política y en dos leyes estatutarias. Dicho artículo reconoce el derecho de todas las personas a conocer, actualizar y rectificar la información que sobre ellas repose en archivos públicos y privados, y establece que la recolección, el tratamiento y la circulación de datos deben respetar la libertad y demás garantías constitucionales (CP, 1991, Art. 15). Sin embargo, frente a los desafíos que plantean las nuevas tecnologías, estas disposiciones resultan insuficientes para garantizar una protección efectiva en entornos de procesamiento masivo y automatizado de información.Los datos sensibles en Colombia, definidos por la Ley 1581 de 2012, abarcan información que afecta la intimidad o puede generar discriminación, como salud, religión, orientación política o sexual. Aunque la norma no distingue entre datos entregados y datos inferidos, estos últimos (cuando permiten deducir categorías sensibles a partir de

información no sensible) también deberían recibir tal calificación, pues revelan aspectos íntimos y potencialmente discriminatorios. Sin embargo, la legislación colombiana no contempla explícitamente esta situación, a diferencia de marcos como el CCPA de California (CCPA, 2018), que reconoce las inferencias como datos personales. Esta ausencia normativa genera un vacío que permite tratar con mayor flexibilidad datos que, pese a no ser sensibles en apariencia, pueden derivar en revelaciones invasivas. De igual modo, la Superintendencia de Industria y Comercio ha señalado que en el país no existe regulación específica sobre el uso de cookies, lo cual implica que, aunque la recolección es una forma de tratamiento sujeta a la ley, no se establecen límites sobre las herramientas para recolectar datos, permitiendo el uso de cualquier tipo de cookies, incluidas las utilizadas para publicidad personalizada o análisis web (Superintendencia de Industria y Comercio, 2016).

Respecto a los identificadores en línea, como direcciones IP y datos asociados, la Ley 1581 define como dato personal toda información vinculada o asociable a una persona natural identificable. A la luz de regulaciones como el GDPR, que reconoce expresamente las IP como datos personales por su capacidad de identificar indirectamente a un individuo al combinarse con otros elementos, sería razonable interpretarlas de igual manera en Colombia. No obstante, la falta de una definición legal explícita deja su tratamiento a discreción de las empresas, generando incertidumbre jurídica y riesgos para la privacidad, sobre todo considerando que esos identificadores pueden asociarse con datos recolectados mediante cookies no reguladas. Hasta que no exista una interpretación autorizada o una reforma legal que incluya tanto las IP como la información asociada, persistirá una protección insuficiente frente a prácticas de tratamiento que en otras jurisdicciones ya se consideran cubiertas por la normativa de datos personales (GDPR, 2018).

El desarrollo normativo sobre el consentimiento aplicable al uso de herramientas digitales y sus excepciones es prácticamente inexistente en el régimen colombiano de protección de datos personales. Como consecuencia, las políticas de privacidad analizadas no están obligadas a detallar las finalidades publicitarias o de *profiling* asociadas a la recolección de datos, incluyen en una misma autorización tanto las cookies esenciales como las no esenciales, y advierten que su rechazo puede limitar el acceso a funcionalidades de la plataforma. Además, la falta de regulación genera que se solicite consentimiento incluso en situaciones en las que no debería ser exigido, como ocurre con las cookies necesarias para cumplir la finalidad del servicio ofrecido por la EMNBD, optimizar la navegación, posibilitar

la celebración de un contrato o permitir el registro y uso de una plataforma, así como para la captura de información anonimizada o agregada destinada exclusivamente a fines estadísticos del responsable del sitio web (Newman y Ángel, 2020).

A diferencia de jurisdicciones como la Unión Europea, esta última contaba con la Directiva 95/46/CE, cuyo artículo 4.1.a establecía que la normativa de protección de datos se aplicaba a todo tratamiento realizado "en el marco de las actividades de un establecimiento" del responsable ubicado en un Estado miembro. Este criterio fue determinante en el caso *Google Spain vs. AEPD y Costeja González* (TJUE, 2014) en el cual el Tribunal de Justicia de la Unión Europea aclaró el alcance de dicha disposición.

En efecto, el Tribunal sostuvo que existe tratamiento "en el marco" de un establecimiento europeo cuando la filial o sucursal ubicada en un Estado miembro desarrolla actividades que guardan una estrecha relación con el tratamiento de datos realizado por la empresa matriz. Así, aunque Google Search fuera gestionado desde Estados Unidos por Google Inc., las labores de promoción y venta de publicidad dirigidas al mercado español, realizadas por Google Spain, estaban suficientemente vinculadas con dicho tratamiento. Por lo tanto, resultaba legítimo aplicar la normativa europea al tratamiento efectuado por el buscador. A partir de esta interpretación, el GDPR reforzó y clarificó el criterio territorial. De hecho, el artículo 3.1 establece de manera expresa que el Reglamento se aplica a los tratamientos efectuados "en el contexto de las actividades de un establecimiento" ubicado en la Unión, con independencia del lugar donde materialmente se lleve a cabo el tratamiento.

En contraste con la regulación europea, la Corte Constitucional colombiana (como garante del derecho fundamental a la protección de datos personales) ha adoptado una posición más explícita frente a la legitimación pasiva de las empresas multinacionales basadas en datos (EMNBD) sin domicilio en el país. En particular, ha debido pronunciarse en tres oportunidades sobre la responsabilidad de Google Inc. (hoy Google LLC). Sin embargo, en ninguno de estos casos la Corte analizó directamente la posible vulneración del derecho a la protección de datos, ya sea porque se trataba de información periodística (a la que no se aplica la Ley 1581 de 2012) o porque consideró, de forma discutible, que el problema correspondía al ámbito del derecho del consumidor. Aun así, estas decisiones permiten observar cómo se ha intentado exigir responsabilidad a compañías de este tipo que no tienen domicilio en Colombia (Corte Constitucional, 2017).

El primer caso, decidido en 2013, involucró a un ciudadano que interpuso acción de tutela contra Google Colombia Ltda. y la Casa Editorial El Tiempo para que se eliminara una noticia indexada en Google Search. Google Colombia alegó falta de legitimación por pasiva, pues no administraba el buscador y su objeto social se limitaba a la comercialización de productos y servicios tecnológicos. Aun así, la Corte evitó abordar la diferencia jurídica entre Google Colombia y Google Inc., limitándose a afirmar que Google era un simple motor de búsqueda sin responsabilidad sobre el contenido publicado por terceros (Corte Constitucional, 2013).

La Corte Constitucional ha reiterado que la imposición de alguna responsabilidad a las entidades mencionadas, como Google, supondría una modalidad de control previo que atentaría contra el principio de neutralidad, que según MinTIC (2021) corresponde a la libertad que poseen los proveedores de redes y servicios de usar las tecnologías para la prestación de todos los servicios sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de recursos escasos, este análisis se hizo notorio al omitir cualquier direccionamiento o discusión sobre la personería jurídica de Google Inc., sin embargo, a pesar del principio de neutralidad, la Corte Constitucional puede dar órdenes de restablecimiento del derecho, como es el caso de la sentencia T-063ª de 2017, en el cual se da el caso de eliminar contenido que pueda causar detrimento en la reputación ajena por post o páginas que propagan información tergiversada o falsa, en este caso específico, publicaciones en un blog que hacían referencia al demandante y la comisión de delitos de estafa, los cuales podían considerarse como calumnia a la luz del Código Penal. Entonces, la Corte le ordenó eliminar el contenido y adoptar medidas para evitar publicaciones anónimas lesivas. Además, impuso a Google Colombia Ltda. la obligación de realizar gestiones ante Google Inc. para garantizar el retiro del contenido, y a ambas compañías les ordenó inscribirse en el registro TIC como proveedores de servicios de telecomunicaciones e Internet.

Este fallo parecía zanjar la discusión sobre la legitimación por pasiva de Google Inc. en Colombia, al indicar que las empresas sin domicilio en el país debían: i) responder por la protección de los derechos de usuarios y consumidores; ii) designar apoderado en Colombia; y iii) asumir responsabilidad conjunta con sus establecimientos locales. Sin embargo, mediante el Auto 285 de 2018, la Corte declaró la nulidad de la sentencia por violación del debido proceso. Consideró que la decisión omitió tres asuntos constitucionalmente relevantes: la prohibición de censura previa; la distinción entre creadores de contenido e intermediarios; y la

diferencia entre proveedores de contenidos y aplicaciones (PCA) y proveedores de redes y servicios de telecomunicaciones (PRST). Según la Newman y Ángel, (2020), estos elementos podían haber llevado a una decisión distinta, especialmente respecto a la orden de inscribirse en el registro TIC y al alcance de las obligaciones impuestas a Google LLC.

Sin embargo, la corriente de responsabilidad en totalidad neutralidad puede tomar un giro desde la sentencia T-256 2025 "Esperanza vs. Meta"; en la cual se aborda la moderación de contenido y la libertad de expresión, e incluso derecho al trabajo cuando se trata de regulaciones internas hechas por las plataformas que afectan derechos fundamentales de los usuarios. Como se ha reiterado a lo largo de este trabajo, los derechos de libertad de expresión, información e intimidad siempre se encuentran en un juego constante contra el poder de las 'big tech'. En este caso, la Corte reitera el sobre el principio de territorialidad, pues los casos relacionados con Internet no eximen la aplicación de reglas en la jurisdicción donde se da la infracción (CEPAL, 2020). Su ámbito de aplicación se basa principalmente en la aplicación del art. 2 de la ley 1581 de 2012, que regula el régimen de protección de datos personales y dispone que esta ley es aplicable al tratamiento de datos realizado en territorio colombiano, así como a responsables o encargados que, sin estar domiciliados en Colombia, deban someterse a la legislación nacional en virtud de normas o tratados internacionales. Dicha norma desarrolla el mandato del artículo 15 de la Constitución, el cual exige respetar las garantías constitucionales en la recolección, tratamiento y circulación de datos personales. En esa línea, la Delegatura para la Protección de Datos de la Superintendencia de Industria y Comercio ha sostenido en múltiples decisiones que la legislación colombiana es aplicable aun cuando el responsable o encargado del tratamiento no se encuentre domiciliado en el país (Superintendencia de Industria y Comercio, 2019). Tales decisiones evidencian que, mediante plataformas como Google, Facebook o WhatsApp, las empresas operadoras recolectan datos personales en territorio colombiano y, en ese sentido, se encuentran sometidas a la regulación nacional. A pesar de la reiteración de jurisprudencia sobre el principio de neutralidad o territorialidad de las empresas, en este caso reciente se enrostra la falta de jurisprudencia o precedente jurisprudencial cuando la propia plataforma es la que vulnera los derechos, y no los usuarios que hay en ella (Corte Constitucional, 2025).

Reitera:

> "Así, puede concluirse que el límite fundamental a la definición de normas comunitarias y a la facultad amplia de moderación de contenidos son los derechos humanos o

> fundamentales. De allí que los operadores de plataformas de redes sociales estén llamados a establecer normas de moderación de contenidos orientadas a proteger los derechos humanos de los usuarios y que las mismas normas cumplan con estándares de derechos humanos. De igual manera, esto lleva a rechazar la intervención del Estado que se extralimite en la regulación para impedir la circulación libre de ideas o limitar el acceso de las personas a Internet". (Corte Constitucional, sentencia T-256, 2025).

La sentencia aborda temas centrales tratados a lo largo del trabajo, pero también dejó en evidencia un vacío persistente: la dificultad para ubicar la territorialidad y definir la responsabilidad de las grandes plataformas tecnológicas. Este problema fue tan relevante que la Corte incluso ordenó crear un canal directo de comunicación para la notificación de tutelas a Meta Inc., subrayando además la falta de transparencia de la compañía en sus procesos. En línea con los estándares de la CIDH, la Corte reiteró que toda moderación de contenidos debe ajustarse al test tripartito, garantizando que cualquier restricción a la libertad de expresión esté prevista en una norma, sea necesaria y resulte proporcional. No obstante, reconoció que trasladar este test al ámbito privado presenta matices complejos, especialmente cuando se trata de determinar la legitimidad de una empresa para prohibir ciertos contenidos, como los de carácter sexual. También recordó que, cuando estos conflictos llegan a instancias judiciales, la exigencia del test debe ser mayor, sobre todo al evaluar la proporcionalidad de las sanciones (Moreno, 2025).

A partir del análisis del caso, la Corte identificó inconsistencias en la aplicación de las políticas de Meta, tras comparar las publicaciones de Esperanza Gómez con las de otras creadoras que compartían contenido similar sin haber sido sancionadas. Concluyó que esta disparidad no era un simple error, sino un trato discriminatorio relacionado con la actividad de la actora en la industria pornográfica. Frente a ello, ordenó que las plataformas aclaren expresamente si las actividades profesionales externas de sus usuarios influyen en los criterios de moderación. Asimismo, la Corte advirtió que cuando la moderación y la gestión de mensajes se apoyan en sistemas de inteligencia artificial, las compañías deben asegurar transparencia, coherencia y una aplicación equitativa de sus políticas, ya que las decisiones automatizadas pueden afectar de manera directa derechos fundamentales (Corte Constitucional, 2025).

El entorno de regulación normativo atañe directamente a Instituciones administrativas como la Superintendencia de Industria y Comercio, y, después del fallo reciente de la Corte Constitucional, los jueces constitucionales cuando estén en juego la vulneración de derechos

fundamentales; sin embargo la posición en muchos de estos casos puede resultar inhibitoria por falta de ubicación y territorialidad, mencionada característica de las big tech y su 'ubicuidad' pero falta de ubicación en el espacio o escudo en el entorno digital.

3.12.2.2. Vacíos normativos en cuanto a IA generativa.

En años recientes, se han dado pasos relevantes, como la adopción de la Política Nacional de Inteligencia Artificial en 2023, la Ley 2502 de 2025 sobre suplantación digital mediante IA y deepfakes, así como las directrices técnicas de la Superintendencia de Industria y Comercio en materia de tratamiento automatizado de datos. Sin embargo, estas herramientas presentan un alcance limitado, ya que no constituyen un sistema articulado ni imponen obligaciones claras de responsabilidad, diligencia debida o supervisión algorítmica. Se trata de avances fragmentarios que no logran formar un marco orgánico.

La ausencia de regulación integral en materia de inteligencia artificial es uno de los puntos donde esta laguna normativa resulta más evidente. En Colombia no existe una ley que establezca criterios de transparencia, explicabilidad o evaluaciones de impacto algorítmico, tampoco una correcta clasificación de contenido o exigencia de 'etiquetas' en cuanto a si un contenido es generado por Inteligencia Artificial o no, pudiendo crear confusión y daño en los receptores de la información, alterando su percepción de la realidad (Wittenberg et al., 2024). Tampoco hay lineamientos con fuerza vinculante sobre responsabilidad por daños ocasionados por decisiones automatizadas, situación que deja un espacio considerable de incertidumbre jurídica. Como lo señala el Consejo de Europa (2020*): "Los sistemas de inteligencia artificial requieren mecanismos de control democrático y jurídico que permitan atribuir responsabilidad, garantizar la trazabilidad de las decisiones y asegurar la protección efectiva de los derechos fundamentales"* (Consejo de Europa, 2020). Es entonces que Colombia, hasta ahora, no ha incorporado esta visión de manera normativa.

Hasta ahora tampoco se ha determinado con claridad el alcance de la IA y sus consecuencias en los derechos fundamentales, su expansión en ámbitos éticos y repercusiones laborales, al igual que el riesgo por su uso en el trato de información. Estas son cuestiones que no han sido tratadas, alternativamente, por la Corte Constitucional, en la única sentencia que ha abordado el tema de la IA generativa por modelos como *ChatGPT* (T-323 de 2024) advierte sobre la utilización de la IA en ámbitos de justicia de forma transparente, respetando los principios de privacidad, la no sustitución de la racionalidad humana, la verificación y la alineación con las mejores prácticas y estándares colectivos (Corte Constitucional, 2024). Las

demarcaciones generales sobre estándares no imponen reglas prácticas o directivas, a diferencia del AI Act en Europa, no establece un sistema de riesgos o los trata. Probablemente esta fase aún siga en construcción y los casos se evidenciarán en el futuro, sin embargo el efecto de la IA generativa es presente y permea cada vez más espacios on-line y offline.

3.12.2.3. Vacíos en cuanto a criptoactivos y blockchain.

En materia de *blockchain* y criptoactivos, la respuesta estatal ha sido fragmentada, puesto que se ha centrado en advertencias y circulares administrativas de la Superintendencia Financiera y el Banco de la República, sin un marco legal que defina la naturaleza jurídica de los criptoactivos, su trazabilidad, el régimen tributario aplicable o las obligaciones de los intermediarios tecnológicos. La ausencia de una ley crea un escenario de incertidumbre, ya que los operadores deben recurrir de manera dispersa a normas de consumo, derecho comercial y regulación financiera tradicional, sin un marco específico que atienda las características técnicas del ecosistema blockchain.

En cuanto al metaverso y los entornos inmersivos, Colombia carece absolutamente de regulación sobre propiedad digital, identidad virtual, protección de derechos de personalidad en universos inmersivos o responsabilidad derivada de interacciones digitales avanzadas. Aunque algunos derechos tradicionales como la intimidad o la imagen pueden aplicarse de manera analógica, la falta de reconocimiento explícito genera vacíos importantes.

A esto se suma la falta de regulación en ciber-robots, sistemas de automatización avanzada y robótica autónoma. No existe un marco legal que determine responsabilidades en caso de fallas de sistemas autónomos, ni estándares de seguridad, ni reglas sobre supervisión humana. En este punto, la ausencia de regulación no solo genera incertidumbre jurídica, sino que impide la consolidación de estándares éticos de desarrollo tecnológico en el país.

Como recuerda Zuboff (2019), en una sentencia discursiva que ilumina la problemática: *"*Cuando la infraestructura tecnológica avanza sin un sistema de reglas claro, la sociedad queda expuesta a relaciones asimétricas de poder, donde la innovación se impone sin contrapesos y sin responsabilidad*"* (p.200). Este diagnóstico, aunque global, describe con precisión lo que ocurre en Colombia: un avance tecnológico vertiginoso y una regulación que permanece dispersa, sectorial y parcialmente obsoleta.

3.12.3. Brecha entre avance tecnológico y respuesta legal

La distancia entre el ritmo del cambio tecnológico y la capacidad de respuesta del ordenamiento jurídico colombiano se ha convertido en un fenómeno estructural, ya que la tecnología evoluciona con una velocidad que supera, de manera constante, los tiempos deliberativos y procedimentales propios del legislador y los órganos reguladores. Esta brecha no solo refleja un desfase temporal; también pone en evidencia limitaciones institucionales, vacíos de coordinación y una insuficiente comprensión de los impactos constitucionales que generan las tecnologías emergentes. En consecuencia, el derecho se ve obligado a operar de forma reactiva, mientras la innovación se despliega sin marcos normativos que la orienten o la limiten.

Esta tensión entre tecnología y normatividad no es nueva, pero en la actualidad ha adquirido un carácter más profundo, puesto que la digitalización no solo transforma actividades económicas o administrativas, sino que reconfigura las condiciones de ejercicio de los derechos fundamentales. Como señala Pérez Luño (2019) *"el Derecho que llega tarde equivale a un Derecho que no llega"* (Perez, 2019), esta afirmación resume el dilema colombiano: una institucionalidad que pretende regular tecnologías disruptivas con herramientas creadas para realidades analógicas.

El sistema jurídico colombiano, en su diseño, no fue concebido para tecnologías que operan de manera autónoma, que generan decisiones no lineales o que producen efectos inmediatos y masivos. La tramitación legislativa, la revisión constitucional, la consulta interinstitucional, las evaluaciones de impacto o la expedición de reglamentos requieren etapas que difícilmente pueden competir con la velocidad de actualización propia de los sistemas algorítmicos, la inteligencia artificial o las plataformas digitales. Esta descoordinación temporal crea una brecha compleja que repercute sobre la seguridad jurídica, el acceso a la justicia y la legitimidad del propio Estado regulador.

La brecha entre innovación y regulación produce, en términos generales, dos efectos centrales que ya han sido advertidos por doctrina y organismos internacionales: la inseguridad jurídica y la vulnerabilidad ciudadana. Ambos fenómenos se refuerzan mutuamente, puesto que la ausencia de reglas claras termina dejando a los ciudadanos y operadores tecnológicos en un escenario incierto y, a veces, desprotegido.

La inseguridad jurídica surge porque el ordenamiento carece de criterios definidos sobre responsabilidad, transparencia algorítmica, trazabilidad de decisiones automatizadas o límites a la explotación de datos. Aunque la Corte Constitucional ha señalado reiteradamente que el Estado tiene la obligación de proteger los derechos fundamentales en entornos digitales *"con la misma intensidad que en los espacios físicos tradicionales"* (Sentencia T-043 de 2021), lo cierto es que esta obligación no ha sido acompañada de la expedición de leyes o reglamentos que traduzcan esa doctrina en obligaciones concretas y exigibles. Esta falta de correspondencia entre jurisprudencia y normatividad crea una tensión que suele resolverse mediante acciones de tutela, lo cual refuerza el carácter reactivo del sistema.

Por otro lado, la vulnerabilidad ciudadana se agrava porque los usuarios se enfrentan a tecnologías cuyo funcionamiento desconocen o no comprenden en su totalidad, ya que los sistemas algorítmicos son opacos y muchas veces inaccesibles para el escrutinio público. En este punto, resulta pertinente recordar el análisis del Relator Especial de las Naciones Unidas para la protección de datos personales (2021):

> Las sociedades que adoptan tecnologías disruptivas sin marcos regulatorios adecuados pueden generar nuevas formas de desigualdad, ya que los ciudadanos quedan expuestos a riesgos que no pueden identificar, prever ni controlar, mientras que los actores tecnológicos operan sin mecanismos de responsabilidad claros. (Naciones Unidas, 2021)

Colombia se encuentra precisamente en este punto intermedio donde la tecnología avanza con rapidez, pero la regulación continúa apoyada en categorías tradicionales como la intimidad, el habeas data, el consentimiento o la libertad de expresión, que, si bien pueden aplicarse al entorno digital, no siempre resultan suficientes para abordar fenómenos complejos como la discriminación algorítmica, la minería intensiva de datos, el uso automatizado de inferencias o la toma de decisiones autónoma.

El legislador colombiano ha intentado responder a esta brecha mediante políticas públicas, estrategias digitales sectoriales, documentos Conpes y lineamientos técnicos, pero estos instrumentos carecen de fuerza normativa vinculante y, en muchos casos, no generan obligaciones claras para plataformas, desarrolladores o autoridades. La Política Nacional de Inteligencia Artificial (2023), por ejemplo, constituye un avance conceptual relevante, pero no contiene disposiciones de responsabilidad, transparencia, supervisión o sanciones. Del mismo

modo, los lineamientos de la Superintendencia de Industria y Comercio sobre decisiones automatizadas carecen de suficiente desarrollo y no forman parte de un régimen integral de protección.

Esta fragmentación normativa aumenta la incertidumbre porque obliga a los operadores jurídicos a recurrir constantemente a la analogía, la jurisprudencia o normas dispersas para abordar problemas inéditos del entorno digital. Como consecuencia, se generan decisiones poco uniformes que amplían la sensación de falta de previsibilidad. En este punto resulta ilustrativa la reflexión de Morozov (2018), quien afirma: "*la regulación que depende de mecanismos de corrección judicial se vuelve insuficiente cuando la tecnología produce daños cuya escala supera la capacidad reactiva de los sistemas institucionales*" (Morozov, 2018). Esta observación sintetiza lo que ocurre en Colombia, donde la tutela y la jurisprudencia se han convertido en la herramienta principal para resolver conflictos tecnológicos que deberían estar regulados legalmente.

Otro aspecto relevante de la brecha normativa es la insuficiente coordinación entre las instituciones encargadas de regular, supervisar o controlar tecnologías emergentes. Congreso, Corte Constitucional, Superintendencias, MinTIC, MinCiencias y organismos de control operan con agendas, tiempos y competencias distintas, lo que impide consolidar una respuesta estructural, ya que la ausencia de articulación interinstitucional genera superposición de funciones, dispersión regulatoria y zonas grises que afectan la coherencia del sistema jurídico. El Consejo de Estado ha advertido esta problemática señalando que la regulación tecnológica *"debe estar guiada por criterios de coherencia, articule mecanismos interinstitucionales de coordinación y evite la dispersión normativa"* (Concepto 2460 de 2022). Sin embargo, esta recomendación no se ha traducido en reformas legales que incorporen tales criterios.

La brecha entre innovación y regulación no solo tiene efectos constitucionales, sino también democráticos, puesto que la ausencia de un marco normativo integral limita el control ciudadano sobre las tecnologías que afectan su vida cotidiana. La transparencia, la participación y la rendición de cuentas se ven debilitadas cuando los sistemas tecnológicos operan sin reglas claras y sin supervisión eficaz, ya que la ciudadanía no puede exigir responsabilidades ni conocer las razones detrás de decisiones digitales que inciden en su esfera jurídica.

Así entonces, la brecha entre el avance tecnológico y la respuesta legal constituye uno de los desafíos más urgentes para el ordenamiento colombiano, porque compromete la protección efectiva de los derechos fundamentales, afecta la previsibilidad jurídica y limita la capacidad del Estado para orientar el uso socialmente responsable de las tecnologías emergentes. La falta de una regulación integral, la dispersión normativa, la dependencia excesiva de la jurisprudencia y la falta de coordinación institucional muestran que el sistema jurídico colombiano aún no está preparado para las exigencias de la era digital.

3.12.4. Necesidad de un constitucionalismo digital colombiano

La acelerada digitalización de la vida social, económica e institucional ha puesto en evidencia la urgencia de repensar el alcance del constitucionalismo colombiano para adaptarlo a las realidades tecnológicas contemporáneas. La Constitución de 1991, aun cuando es flexible y garantista, fue concebida para un mundo analógico, donde el Estado tenía mayor capacidad de control sobre los espacios de interacción humana y donde la información no circulaba con la velocidad, la fluidez y la capacidad de réplica que caracteriza al ecosistema digital actual. Puesto que las tecnologías emergentes transforman no solo las actividades humanas, sino también las relaciones de poder, la forma de participar democráticamente y la estructura misma de los derechos fundamentales, es indispensable avanzar hacia un constitucionalismo digital colombiano, capaz de articular principios, normas y políticas orientadas a garantizar que la dignidad humana siga siendo el eje de la vida jurídica en la era digital.

La necesidad de este nuevo enfoque no se deriva únicamente de la mera aparición de innovaciones tecnológicas, sino del profundo efecto que estas ejercen sobre los valores constitucionales. La inteligencia artificial, el análisis masivo de datos, la automatización, la biovigilancia digital, el metaverso y la creciente interconexión entre sistemas públicos y privados han generado un terreno donde los límites entre autonomía individual y control tecnológico se difuminan. En este sentido, Uprimny (2023) sostiene que *"el constitucionalismo contemporáneo enfrenta el desafío de asumir fenómenos que desdibujan sus categorías clásicas, pues lo digital redefine las nociones de espacio público, de agencia humana, de privacidad y de libertad*" (Uprimny, 2023).

Este planteamiento es clave, ya que muestra que el derecho constitucional no puede seguir interpretando la realidad desde categorías estáticas ni mediante adaptaciones puntuales. La sociedad colombiana necesita una reconfiguración estructural que le permita abordar integralmente los riesgos, tensiones y oportunidades de la transformación digital.

A su vez, es crucial reconocer que el constitucionalismo digital no es sinónimo de "regular tecnología", sino de reorganizar los principios constitucionales para garantizar su eficacia en ambientes automatizados o mediados por algoritmos. Esta distinción es fundamental, puesto que limita la visión reduccionista que confunde digitalización con mera actualización normativa. Un constitucionalismo digital implica una arquitectura jurídica más profunda, donde los principios orientan estructuras completas de gobernanza digital, mecanismos de control, límites al poder tecnológico y formas de participación ciudadana.

En el escenario colombiano, la falta de reconocimiento expreso de los derechos digitales, como la autodeterminación informativa avanzada, la protección de la identidad digital, la neutralidad algorítmica, la transparencia de modelos automatizados o el derecho a la desconexión tecnológica, ha generado un vacío que dificulta la protección efectiva de los derechos fundamentales. Aunque la Corte Constitucional ha realizado importantes avances interpretativos, estos operan con carácter fragmentario y reactivo. De hecho, en la Sentencia T-043 de 2020 se señaló que: *"el ejercicio pleno de los derechos fundamentales en entornos digitales exige el diseño de marcos normativos y de políticas públicas que correspondan al nivel de sofisticación de los riesgos contemporáneos."*

Esta afirmación, aunque concisa, sintetiza la lógica del constitucionalismo digital, la protección de derechos depende de la actualización del marco constitucional para enfrentar fenómenos inéditos. Uno de los pilares del constitucionalismo digital colombiano debe ser la anticipación normativa. El desarrollo de tecnologías disruptivas se caracteriza por su velocidad y por el riesgo de generar afectaciones irreversibles para la autonomía humana, la privacidad, la libertad de pensamiento o la igualdad. Por esta razón, esperar a que los daños ocurran para legislar es una estrategia jurídicamente insuficiente.

Ferrajoli (2021), en una reflexión contundente, afirma que "*la función más elevada del constitucionalismo es la prevención. Un Estado que permite que los daños ocurran para luego actuar ya ha fallado en su misión de proteger la dignidad humana*." (p.20).

Esta idea evidencia que el constitucionalismo digital no se limita a reaccionar ante vulneraciones, sino a diseñar marcos normativos que prevengan excesos de automatización, abusos de tratamiento de datos, concentraciones de poder digital y decisiones opacas basadas en algoritmos. La anticipación normativa implica desarrollar leyes que incorporen desde su diseño obligaciones de transparencia, trazabilidad, rendición de cuentas y supervisión humana.

Asimismo, es necesario que la anticipación normativa se traduzca en regulación flexible y adaptable, capaz de actualizarse conforme evolucionen las tecnologías. Puesto que el derecho suele operar bajo esquemas rígidos, Colombia debe impulsar normativas modulares o principios orientadores que permitan ajustes continuos sin sacrificar la estabilidad institucional.

El constitucionalismo digital, en este punto, exige superar la fragmentación institucional. Debe existir un marco de cooperación que permita que las distintas entidades estatales adopten criterios uniformes sobre inteligencia artificial, ciberseguridad, protección de datos, interoperabilidad tecnológica y responsabilidad algorítmica.

Como ha advertido la OCDE (2022) en sus lineamientos sobre gobernanza digital: *"los Estados deben establecer mecanismos interinstitucionales permanentes para coordinar la regulación y supervisión de tecnologías avanzadas, ya que la fragmentación regulatoria incrementa los riesgos sistémicos."*

En Colombia, una gobernanza articulada también permitiría implementar estándares técnicos de protección digital que hoy no existen, y que son necesarios para garantizar coherencia entre los distintos actores públicos.

Asimismo, la Corte Constitucional debe asumir un rol de intérprete final del constitucionalismo digital, estableciendo parámetros estructurales y no solo soluciones caso a caso. Esto implica desarrollar doctrina constitucional robusta sobre algoritmos, automatización de decisiones públicas, vigilancia estatal, identidad digital, neutralidad en redes y derechos en espacios inmersivos.

Si bien la reforma normativa y la articulación institucional son indispensables, el constitucionalismo digital debe reposar también en la consolidación de una cultura digital fuerte. Ningún derecho es plenamente efectivo si la ciudadanía no posee las herramientas para comprenderlo, ejercerlo y defenderlo. En un país con amplias brechas educativas, es fundamental desarrollar programas nacionales de alfabetización digital que permitan a las personas comprender conceptos como privacidad algorítmica, seguridad digital, identidad virtual, trazabilidad de datos y riesgos en proyectos basados en IA.

La Corte Constitucional ha resaltado la importancia de esta dimensión. En la Sentencia C-748 de 2011 sosteniendo que "l*a autodeterminación informativa solo puede ejercerse cuando el ciudadano posee un nivel de comprensión mínimo sobre el alcance y los riesgos del tratamiento digital de sus datos.".* Esta afirmación revela un aspecto central que los derechos

digitales no se garantizan únicamente desde el Estado, sino también desde la capacidad ciudadana de ejercer control sobre su propia información y sobre las tecnologías que utiliza.

El constitucionalismo digital colombiano, por tanto, debe promover una ciudadanía tecnológicamente consciente, capaz de identificar riesgos, exigir transparencia y participar activamente en la definición de políticas digitales. Puesto que los derechos solo son reales cuando pueden ser ejercidos, la formación digital se convierte en un componente estructural, no complementario.

La quinta revolución industrial plantea una integración profunda entre tecnologías digitales, físicas y biológicas. Esta transformación intensifica los desafíos constitucionales, ya que los límites entre identidad humana, decisiones automatizadas y sistemas algorítmicos se vuelven más difusos. Si el país no desarrolla un marco constitucional adecuado para este contexto, enfrentará una erosión progresiva de los derechos fundamentales.

El constitucionalismo digital colombiano debe prepararse para enfrentar riesgos vinculados con sistemas autónomos avanzados, vigilancia basada en datos biométricos complejos, interacción humano-máquina, modelos predictivos, gobernanza algorítmica y ecosistemas digitales inmersivos. La falta de regulación en estos campos aumenta la posibilidad de desigualdad, discriminación automatizada, pérdida de autonomía y vulneraciones sistemáticas del derecho a la intimidad.

En este sentido, la afirmación de Floridi (2020) cobra especial relevancia mencionando que "*la sociedad digital exige un nuevo pacto constitucional que reequilibre las relaciones entre seres humanos, sistemas tecnológicos y poderes institucionales.*", planteando una reinterpretación profunda del papel del Estado y del derecho en un mundo donde lo digital atraviesa todas las esferas humanas.

La consolidación de un constitucionalismo digital colombiano no es un proyecto opcional ni un lujo intelectual, sino una necesidad urgente para preservar la fuerza normativa de los derechos fundamentales frente a la expansión del poder tecnológico. Se trata de diseñar un marco integral que articule anticipación normativa, armonización institucional y formación ciudadana, garantizando que la dignidad humana no quede relegada en medio de algoritmos, automatismos y decisiones opacas.

Un constitucionalismo digital sólido permitirá que Colombia transite hacia la quinta revolución industrial sin sacrificar garantías constitucionales. Solo así será posible que la

innovación tecnológica conviva con la justicia, la libertad y la igualdad, reafirmando el carácter garantista de la Constitución de 1991 en la nueva era digital.

TÍTULO IV: RETOS Y DESAFÍOS DEL CONSTITUCIONALISMO DIGITAL COLOMBIANO.

El escenario descrito en el capítulo anterior evidencia que Colombia enfrenta un entorno digital fragmentado y vulnerable, caracterizado por vacíos normativos, debilidad institucional y limitada cultura digital. Si bien la jurisprudencia constitucional y algunas políticas públicas han intentado mitigar riesgos asociados a la transformación tecnológica, la falta de un marco integral de derechos digitales y tecnologías emergentes mantiene al país en una posición reactiva frente a los desafíos de la quinta revolución industrial. Esta situación exige un análisis crítico de los retos normativos, institucionales y socioculturales, con el fin de sentar las bases de un constitucionalismo digital colombiano robusto, preventivo y sostenible, capaz de armonizar innovación tecnológica, seguridad jurídica y protección efectiva de los derechos fundamentales.

En este contexto, resulta imprescindible reconocer que el modelo constitucional colombiano, diseñado para una estructura estatal analógica y centralizada, enfrenta tensiones sin precedentes ante la velocidad del cambio tecnológico. La irrupción de plataformas digitales, sistemas de inteligencia artificial, algoritmos de decisión automatizada y ecosistemas globales de datos desborda las herramientas tradicionales de control jurídico, obligando al Estado a repensar sus capacidades regulatorias. De igual manera, la interdependencia digital internacional expone al país a riesgos transnacionales que requieren cooperación multilateral, estándares comunes y mecanismos de corresponsabilidad frente a actores tecnológicos que operan fuera de la jurisdicción nacional.

Uno de los retos más significativos radica en la necesidad de actualizar la arquitectura institucional para incorporar capacidades técnicas avanzadas, oficinas especializadas y organismos con autonomía funcional que permitan auditar algoritmos, vigilar plataformas, gestionar infraestructuras críticas y anticipar riesgos sistémicos. Esto implica una transformación profunda de la estructura estatal, orientada no solo a reaccionar frente a vulneraciones de derechos, sino a diseñar políticas preventivas que integren la protección de

datos, la seguridad digital, la ética tecnológica y la transparencia algorítmica como principios constitucionales operativos.

A nivel sociocultural, la falta de alfabetización digital y la desigualdad en el acceso a las tecnologías generan escenarios en los que amplios sectores de la población permanecen excluidos de los beneficios de la digitalización, lo que intensifica brechas estructurales ya existentes. Sin una ciudadanía digital informada, crítica y empoderada, el constitucionalismo digital no puede consolidarse como un proyecto democrático. La tarea educativa y formativa se vuelve, por tanto, un desafío nacional que debe involucrar escuelas, universidades, instituciones públicas y actores privados.

Finalmente, el país debe avanzar hacia la construcción de un ecosistema digital que incorpore principios constitucionales como la dignidad humana, la igualdad, la privacidad, la libertad de expresión y el debido proceso en entornos tecnológicos cada vez más automatizados. Esto exige normativas claras sobre gobernanza de datos, límites al poder algorítmico y mecanismos eficaces de rendición de cuentas, asegurando que la innovación tecnológica se desarrolle dentro de un marco de legitimidad democrática. En suma, los retos del constitucionalismo digital colombiano son complejos, pero representan una oportunidad histórica para modernizar el Estado y garantizar que la transformación digital sea coherente con los valores superiores del orden constitucional.

4. Retos normativos y legislativo

El acelerado proceso de digitalización global ha configurado un escenario en el que los Estados enfrentan profundas tensiones entre la innovación tecnológica y la capacidad del derecho para responder con eficacia, oportunidad y coherencia. Este desajuste estructural entre la velocidad del avance tecnológico y el ritmo más lento de producción normativa ha generado un contexto donde proliferan vacíos jurídicos, desactualización legislativa e incertidumbre institucional, especialmente en países como Colombia que aún consolidan su transición hacia un modelo de gobernanza digital. Diversos autores advierten que, en ausencia de una respuesta constitucional sólida, la expansión de tecnologías disruptivas tiende a consolidar relaciones de poder asimétricas y formas de vigilancia que pueden erosionar la autonomía individual, la transparencia estatal y la igualdad material en el entorno digital (Lessig, 2006; Floridi, 2014). Esta realidad exige un análisis profundo sobre las tensiones normativas emergentes y las obligaciones constitucionales derivadas de un orden tecnológico en transformación permanente.

El avance digital se destaca como una de las expresiones más significativas del progreso tecnológico y su influencia en la sociedad desde finales del siglo XX. Este avance ha superado los modelos conocidos de sociedad industrial e de información, conectándose incluso con la sociedad del riesgo que emergió en ese periodo. La pandemia ha contribuido a popularizar la noción de sociedad digital, aunque esta idea ya estuviera presente desde hace algún tiempo (F, 2020). La crisis de la Covid-19, al igual que otras crisis previas, ha acelerado procesos y cambios que ya estaban en marcha desde antes, pero que ahora se hacen más evidentes debido a las necesidades urgentes. Este impulso digital experimentado durante la pandemia, especialmente durante los períodos de confinamiento en todo el mundo, ha destacado el papel crucial de la tecnología digital como el principal medio para mantener nuestras relaciones familiares, sociales y culturales (Barrilao, 2022).

Este crecimiento tecnológico acelerado ha puesto de manifiesto la necesidad de repensar los marcos constitucionales desde una lógica prospectiva y no meramente reactiva. Fenómenos como el crecimiento exponencial del big data, los sistemas algorítmicos autónomos, los modelos masivos de inteligencia artificial, la computación cuántica en desarrollo y la expansión del metaverso han desplazado los límites tradicionales del derecho, obligándolo a enfrentar nuevas tensiones entre privacidad, seguridad, competencia económica, transparencia y libertad individual. Como explica Hildebrandt (2015), el derecho debe adaptarse a un entorno digital caracterizado por decisiones automatizadas y estructuras opacas, donde los mecanismos clásicos de control del poder público dejan de ser suficientes. Esta tensión exige un rediseño conceptual del constitucionalismo para garantizar que los desarrollos tecnológicos no sobrepasen la capacidad normativa del Estado.

El Derecho Constitucional se ha construido sobre una Constitución dinámica que busca promover el pluralismo y responder a las necesidades de una sociedad en constante cambio. Esta sociedad ha transitado desde los conflictos propios de la sociedad industrial, caracterizada por las luchas de clase, hasta la transición hacia la sociedad de la información. Sin embargo, como señala Balaguer Callejón, la Constitución fue inicialmente concebida desde una perspectiva analógica, acorde con el nivel tecnológico de ese tiempo (Dominguez, 2023).

Frente a esta condición analógica del constitucionalismo clásico, surge una tensión fundamental: ¿cómo garantizar la vigencia efectiva de los derechos fundamentales en una sociedad donde el poder ya no se concentra exclusivamente en el Estado, sino también en grandes corporaciones tecnológicas cuya capacidad para recopilar, procesar y monetizar datos

supera con creces los mecanismos tradicionales de control jurídico? Zuboff (2019) alerta que el capitalismo de vigilancia redefine la noción misma de autonomía al convertir la conducta humana en materia prima para la producción económica, lo que sitúa el debate constitucional sobre la privacidad, la libertad y la dignidad en un plano completamente nuevo. En este contexto, el derecho colombiano debe asumir una perspectiva más amplia que no solo regule la actividad estatal, sino también el poder privado que controla ecosistemas digitales globales.

Con el paso de los años, se ha generado una conciencia progresiva sobre la importancia de lo digital. Este cambio ha dado lugar a un proceso de digitalización de la Constitución y el Derecho Constitucional, lo cual implica la incorporación de la tecnología digital y sus efectos en diversos ámbitos sociales, culturales, económicos, políticos y jurídicos. El objetivo fundamental de este proceso es encontrar nuevas formas de regular legalmente el poder, estableciendo límites y protegiendo la libertad individual (García M. D., 2025).

Además, este proceso abre la posibilidad de desarrollar un constitucionalismo digital genuino, el cual debe concretar principios e instituciones jurídicas y políticas específicas en relación con los avances de la sociedad digital. Este constitucionalismo digital se centraría en la regulación del poder en este nuevo contexto, promoviendo la democracia y protegiendo los derechos humanos en el marco de la digitalización. (Callejón, 2024).

En este proceso también adquiere relevancia la producción comparada de estándares internacionales. La Unión Europea, por ejemplo, ha desarrollado marcos avanzados como el Reglamento General de Protección de Datos, la Ley de Servicios Digitales y la Ley de Inteligencia Artificial, que buscan equilibrar innovación y garantías. Estos desarrollos ofrecen un referente de constitucionalismo digital multinivel que Colombia podría adaptar a su contexto institucional. La ausencia de reglas similares en el ámbito latinoamericano ha generado asimetrías en la protección de datos, fragilidad en la seguridad digital y un crecimiento desregulado de plataformas tecnológicas que operan sin límites claros. Por ello, la perspectiva comparada es fundamental para comprender los vacíos actuales y proyectar posibles rutas normativas (De Gregorio, 2022).

Es importante también que se consideren otras perspectivas teóricas sobre la evolución del Derecho Constitucional en el contexto digital. Según autores como Zuboff (2019) en su obra sobre el capitalismo de vigilancia, el avance de la tecnología digital también plantea retos para la privacidad y la autonomía individual, cuestiones que deben ser abordadas dentro del

marco constitucional (Zuboff, 2019). Del mismo modo, han explorado la relación entre la tecnología, la democracia y la regulación en el ciberespacio, ofreciendo un enfoque útil para la construcción de un constitucionalismo que no solo se limite a la regulación del poder, sino que también asegure la equidad y el acceso a los derechos fundamentales en el entorno digital (García R. J., 2023).

El Derecho Constitucional contemporáneo se enfrenta a retos significativos debido a la digitalización de la sociedad. Aunque algunos idealizan una utopía digital, en realidad, se está ante una distopía constitucional, donde la tecnología, si no es gestionada adecuadamente, puede amenazar los derechos fundamentales y los principios democráticos. La falta de una adecuada adaptación del Derecho Constitucional a estos nuevos desafíos digitales permite que el uso de tecnologías, en ocasiones, socave las libertades individuales. Es necesario reconfigurar el Derecho Constitucional para salvaguardar los derechos en este nuevo contexto digital, (Barrilao, 2022).

A lo anterior se suma la necesidad de revisar sectores jurídicos específicos que presentan un rezago normativo considerable. La regulación de la inteligencia artificial, el reconocimiento facial, las tecnologías biométricas, la vigilancia estatal mediante plataformas digitales, los sistemas de identidad digital, los contratos automatizados y la gobernanza de la nube requieren marcos legales claros que prevengan arbitrariedades y garanticen transparencia. Colombia aún carece de una Ley de Inteligencia Artificial, de una política robusta de ciberseguridad y de una regulación integral sobre datos no personales, lo que amplifica la exposición de los ciudadanos a riesgos significativos. La doctrina contemporánea coincide en que el constitucionalismo digital debe orientarse hacia la anticipación del riesgo y no únicamente hacia la reacción frente a daños ya consumados (Balkin, 2018).

De igual forma, la estructura institucional enfrenta desafíos profundos. Las entidades estatales carecen de capacidades técnicas adecuadas para comprender y regular tecnologías emergentes, lo que genera dependencia de informes privados y limita la supervisión efectiva. La Corte Constitucional, pese a sus avances en jurisprudencia digital, enfrenta la complejidad de interpretar derechos fundamentales en entornos donde intervienen actores globales y algoritmos opacos. La formación insuficiente de jueces, fiscales, legisladores y funcionarios públicos en asuntos tecnológicos restringe la eficacia de los controles democráticos, generando decisiones dispares e incluso contradictorias entre sí. Pollicino (2020) destaca que el

constitucionalismo digital no puede consolidarse sin instituciones capaces de comprender la arquitectura técnica de las tecnologías que regulan.

En última instancia, el constitucionalismo digital es una respuesta esencial a los desafíos planteados por la cuarta revolución industrial. Colombia debe adaptar su marco legal y fortalecer sus instituciones para garantizar una protección sólida de los derechos fundamentales en la era digital. Esto requerirá esfuerzos conjuntos y un enfoque multidisciplinario para abordar con éxito los retos que plantea esta nueva realidad en el entorno social (Domènech & Esteve, 2022). Además, la aplicación exitosa del constitucionalismo digital en Colombia exige una capacitación exhaustiva de jueces, abogados y funcionarios públicos en las complejidades del entorno digital. La colaboración entre diversos actores, incluyendo el sector público, el sector privado, la sociedad civil y la academia, es esencial para enfrentar los retos de manera integral (Pollicino, 2020).

6.1. Posibles mecanismos institucionales y recomendaciones para la regulación en el ámbito digital.

Siguiendo la línea de pensamiento y recomendaciones de Newman y Ángel (2020) con respecto a la protección de datos personales, a pesar del desarrollo jurisprudencial que ha tenido la Ley 1581 de 2012, aún faltan nociones específicas que pueden dar un carácter coercitivo o de protección más evidente para el usuario frente a las GAFAM. Es necesaria la definición de nociones como dato personal, dato sensible para abarcar identificadores como direcciones de IP y datos asociados, o la recolección de datos que puedan ser un profiling de los usuarios, consultando datos sensibles como su orientación sexual, etnia, raza, etc. Para esto también se plantea exigir el consentimiento previo, expreso e informado (manifestado mediante una acción afirmativa) para tratamiento de datos destinados al profiling, comercialización de datos con terceros, publicidad comportamental y decisiones automatizadas, con solicitudes separadas para cada finalidad y la destinación a terceros de esa información; como las pedidas en países de la Unión Europea, pues el GDPR exige el consentimiento en su artículo 32.[12]

[12] El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar

Figura 12.

Consentimiento informado expreso.

Nota. Adaptado de: "¿Por qué me piden aceptar o rechazar las cookies de las webs?" *Grupo SCImago*. https://www.scimagoepi.com/por-que-me-piden-aceptar-o-rechazar-las-cookies-de-las-webs/.

También es importante reconocer que la protección de los derechos fundamentales en entornos digitales no depende únicamente del Congreso, sino de la interacción coordinada de la Corte Constitucional, el gobierno nacional, las superintendencias, los ministerios, los organismos de control y las autoridades judiciales. Sin embargo, Colombia carece de una estructura permanente de gobernanza digital que unifique criterios y evite contradicciones normativas o vacíos operativos. Actualmente la Superintendencia de Industria y Comercio tiene ciertas facultades y papel en lo que respecta al avance tecnológico, sin embargo, su poder igual carece de los medios coercitivos que pueda tener, si acaso tiene una delegatura en específico para la protección de datos y tecnología, y que la misma tenga una cooperación internacional para proteger a titulares afectados por la recolección transnacional de datos.

Con respecto al tema de la territorialidad, la Corte Constitucional (2025) ha analizado la misma en cuanto a la protección de derechos fundamentales por medio de tutela, es viable siempre y cuando la vulneración se dé en el territorio y con ciudadanos Colombianos; sin embargo la especificación de un domicilio o el establecimiento de una dirección (asi sea de correo electrónico) para comunicaciones o notificaciones judiciales de las empresas de tecnología transnacionales, facilitaría el proceso de resolución, a pesar de que la Corte no

a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta. (GDPR, 2018).

estableció esto como un mandato obligatorio, sino como una recomendación en la sentencia T-323, es necesario de nuevo la mención en una ley o artículo que pueda dar desarrollo a estos problemas de notificación que, en última instancia, son los que afectan más al usuario y enrostran más su desprotección.

Con respecto a la creciente preocupación sobre la inteligencia artificial, el panorama da adoptado por la jurisprudencia ha correspondido solo a directivas o reiteración de usos éticos. Entre los mecanismos que podría tomar o que una ley pueda consagrar (más allá de agravación de delitos por utilización de deepfakes), consiste en expedir un reglamento por autoridades legislativas, similar al AI Act, en el cual se establezcan los riesgos y su carácter, para así tener obligaciones directas para las empresas o compañías de inteligencia artificial en Colombia; a pesar de los proyectos de ley presentados hasta el año de redacción de este trabajo (2025), la sostenibilidad de los mismos podría reforzarse mediante auditación de terceros en el correcto cumplimiento de estas disposiciones éticas, la regulación de contenido, como la etiqueta de contenidos generados por IA.

El etiquetado se plantea con frecuencia como una estrategia para reducir los riesgos asociados a la IA generativa. Consiste en incorporar advertencias visibles que informen a los usuarios cuando un contenido ha sido creado por IA en plataformas como redes sociales, medios digitales o buscadores (Wittenberg, 2023).

Aunque existe poca evidencia directa sobre su eficacia para identificar medios generados por IA, la amplia literatura sobre etiquetas en contenidos desmentidos por verificadores profesionales muestra que las advertencias pueden disminuir de forma significativa la credibilidad y difusión de información falsa (Helmus, 2022). Esto sugiere que el etiquetado también podría contribuir a que el público identifique mejor los contenidos producidos con IA. Según Wittenberg et al., (2023) destaca que cualquier programa de etiquetado debe partir de una definición clara de sus objetivos:

1. Informar a los usuarios sobre el proceso mediante el cual se creó o modificó un contenido (si intervino o no una herramienta de IA generativa).
2. Reducir la probabilidad de que el contenido engañe o confunda a los espectadores, un efecto que no depende necesariamente de si fue producido por IA.

Estos objetivos permiten sentar las bases para decidir, por un lado, qué tipo de contenido debe ser etiquetado y, por otro, cómo diseñar etiquetas que sean precisas y resulten creíbles

para un público amplio. Además, al formular lineamientos de política y estrategias de implementación, los actores involucrados deben considerar no solo los efectos de las divulgaciones sobre el contenido etiquetado, sino también sobre aquel que permanece sin etiqueta. Esto es fundamental, pues un sistema de etiquetado fragmentado o poco confiable puede generar desconfianza y contribuir a difuminar aún más los límites entre lo real y lo artificial (Farid, 2022).

Con respecto a las sociedades algorítmicas, Watcher (2023) propone Con frecuencia, las personas no son conscientes de los daños causados por sistemas de IA, especialmente cuando los proveedores y desplegadores (que no interactúan directamente con usuarios o clientes) no informan públicamente sobre su impacto. En estos casos, cuando los perjuicios permanecen ocultos por el propio modelo de despliegue o por la ausencia de reportes públicos, los mecanismos basados únicamente en quejas resultan claramente insuficientes para proteger los derechos individuales. Este vacío puede cerrarse mediante estándares armonizados. Para ello, deberían incorporarse disposiciones que exijan pruebas sistemáticas de los sistemas y la publicación de resúmenes accesibles para las personas potencialmente afectadas. En el ámbito específico del sesgo algorítmico, se propone invertir la carga de la prueba: dado que no existe un conjunto de datos completamente libre de sesgos, debe presumirse que los modelos, sistemas y los datos utilizados para su entrenamiento y prueba presentan sesgos, a menos que se demuestre lo contrario. Esta inversión puede materializarse mediante la divulgación de los resultados de las pruebas y de las medidas adoptadas para identificar, mitigar y prevenir dichos sesgos (Watcher, 2023, p.44).

En síntesis, los retos normativos que enfrenta Colombia reflejan una brecha estructural entre la innovación tecnológica y la respuesta legislativa. Las normas vigentes son fragmentadas, reactivas y de alcance limitado, lo que genera inseguridad jurídica y vulnerabilidad ciudadana frente a fenómenos como la inteligencia artificial, el big data, el blockchain, el metaverso y la ciberseguridad avanzada. Esta situación evidencia que el marco jurídico actual no basta para garantizar la protección efectiva de los derechos fundamentales en entornos digitales y que superar este rezago requiere no solo actualización normativa, sino también una visión sistémica y anticipatoria que permita construir un constitucionalismo digital colombiano, cuyo concepto y alcance se desarrollan en el siguiente apartado. Todo este contexto pone de manifiesto que el reto normativo no consiste únicamente en actualizar leyes aisladas, sino en reconfigurar la estructura constitucional para responder a formas nuevas de

poder disperso, automatizado y global. La adaptación del derecho colombiano debe orientarse hacia la anticipación, la protección preventiva, la transparencia algorítmica y la participación democrática en la definición del rumbo tecnológico. Solo así será posible consolidar un modelo en el que la tecnología no se convierta en una amenaza para la libertad, sino en una herramienta al servicio de la dignidad humana y del fortalecimiento del Estado social de derecho.

4.2.Retos institucionales y socioculturales

Como advierte Ferrajoli (2020), la protección de los derechos fundamentales en entornos digitales no puede depender únicamente de la existencia de normas, sino que requiere de instituciones sólidas y de una cultura ciudadana consciente. En Colombia, la debilidad institucional y la fragmentación en la gestión digital generan un ecosistema vulnerable, mientras que la brecha cultural se manifiesta en el uso irresponsable de internet y redes sociales, la propagación de desinformación y la limitada comprensión de los riesgos tecnológicos por parte de la ciudadanía.

En el plano institucional, Colombia enfrenta una marcada falta de coordinación entre entidades como el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Superintendencia de Industria y Comercio (SIC), la Fiscalía General de la Nación y la Policía Cibernética. La inexistencia de una autoridad unificada de derechos digitales y ciberseguridad limita la capacidad del Estado para responder a incidentes digitales complejos. Siguiendo a Kelsen (2009), un orden jurídico carece de eficacia si no se articula en una jerarquía clara y funcional, capaz de hacer cumplir las normas en la práctica. La experiencia internacional demuestra que contar con órganos especializados y articulados mejora la capacidad de reacción frente a delitos cibernéticos, vulneraciones de datos y amenazas a la infraestructura digital crítica.

Desde la perspectiva sociocultural, Colombia enfrenta una brecha significativa en cultura digital y alfabetización tecnológica. El uso de redes sociales y plataformas digitales se realiza, en muchos casos, de manera irreflexiva, lo que favorece la propagación de noticias falsas, el ciberacoso y la vulneración de derechos de terceros. La brecha urbano-rural y las limitaciones educativas profundizan la desigualdad en el acceso y la apropiación responsable de las tecnologías. Chun Hul (2018) resalta que la cultura digital es un componente esencial para garantizar la protección de derechos, pues sin alfabetización tecnológica y ética digital, la ciudadanía permanece expuesta a riesgos que las normas, por sí solas, no pueden prevenir.

En síntesis, el análisis desarrollado en este capítulo evidencia que la construcción de un constitucionalismo digital colombiano enfrenta retos que trascienden la mera producción normativa. La persistente brecha entre innovación tecnológica y respuesta legal, sumada a la fragmentación institucional y a una cultura digital insuficiente, mantiene a los derechos fundamentales en un estado de vulnerabilidad en entornos digitales. La experiencia comparada demuestra que los países que han avanzado hacia un ecosistema digital seguro lo han hecho mediante la articulación de normas claras, instituciones sólidas y ciudadanía educada en ética tecnológica. Para Colombia, la consolidación de un marco de derechos digitales explícitos ya sea como derechos fundamentales autónomos o por conexidad, resulta indispensable para garantizar su protección efectiva a través de la acción de tutela. Este diagnóstico abre paso al Capítulo 4, donde se presentará una propuesta normativa integral, orientada a construir un ecosistema de constitucionalismo digital preventivo, seguro y sostenible.

4.3.Otros desafíos y desarrollos recientes del constitucionalismo digital

El desarrollo acelerado de la transformación digital ha generado un conjunto de retos emergentes que trascienden los ámbitos normativos e institucionales previamente analizados. Estos desafíos recientes del constitucionalismo digital se manifiestan en dimensiones sociales, éticas y tecnológicas que inciden directamente sobre la protección de los derechos fundamentales. La expansión de la inteligencia artificial, la masificación del big data, la automatización de decisiones públicas y privadas, así como el creciente poder de las plataformas digitales, han configurado un ecosistema de riesgo para la democracia, la privacidad y la igualdad. Este escenario exige no solo respuestas legales preventivas, sino también una reflexión crítica sobre los impactos sociales y éticos de la digitalización, los cuales se abordan en el siguiente apartado.

4.3.1. Impactos sociales y éticos de la digitalización

La digitalización ha transformado radicalmente la forma en que los individuos y las sociedades interactúan, generando profundos impactos sociales, culturales y jurídicos. En el contexto contemporáneo, la digitalización implica no solo la adopción masiva de tecnologías de la información, sino también la incorporación de algoritmos, inteligencia artificial y sistemas de big data que inciden directamente sobre derechos fundamentales como la privacidad, la libertad de expresión y la autonomía personal. Zuboff (2019) ha denominado este fenómeno como 'capitalismo de vigilancia', advirtiendo que la explotación masiva de datos

personales permite modelar comportamientos sociales y mercantiles, erosionando la autodeterminación informativa y debilitando los cimientos de la democracia.

En Colombia, estos impactos se reflejan en múltiples dimensiones. El auge de las redes sociales ha facilitado la propagación de noticias falsas y discursos de odio, afectando la deliberación pública y la reputación de personas y organizaciones. Casos de ciberacoso y filtración de datos personales han llegado a los estrados judiciales, donde la Corte Constitucional ha debido pronunciarse para garantizar la protección de la intimidad y el buen nombre mediante la acción de tutela (Corte Constitucional, 2019). Estas situaciones evidencian que, aunque el marco constitucional de 1991 ofrece herramientas de protección, el país carece de una política preventiva integral en materia digital.

En el ámbito comparado, la Unión Europea ha marcado la pauta con el Reglamento General de Protección de Datos (Parlamento Europeo, 2016), el cual establece estándares robustos sobre consentimiento, derecho al olvido y responsabilidad de las empresas en el tratamiento de información personal. España, por su parte, ha avanzado con la Carta de Derechos Digitales de 2021, incorporando principios de ética algorítmica, transparencia y garantía de derechos en entornos virtuales. En contraste, países latinoamericanos como Brasil han implementado el Marco Civil de Internet (2014) y la Ley General de Protección de Datos (2018), mientras que Colombia continúa dependiendo de un marco fragmentado y mayoritariamente reactivo.

En el contexto colombiano, investigaciones del Centro Latinoamericano de Investigación Periodística (CLIP) y de la Agência Pública (2025) han evidenciado las problemáticas derivadas del poder de las Big Tech y cómo este puede poner en riesgo el Estado de Derecho. Empresas como Meta, Alphabet, Amazon, Microsoft, Apple, ByteDance, Mercado Libre y OpenAI ejercen una influencia desproporcionada sobre distintos ámbitos de la vida social y económica, superando incluso la capacidad de muchos gobiernos para regularlas de manera efectiva. Su principal objetivo es maximizar beneficios y rendir cuentas a sus accionistas, lo que genera tensiones con los intereses públicos y la transparencia democrática.

Estas corporaciones despliegan estrategias de influencia altamente sofisticadas, que incluyen departamentos de “relaciones gubernamentales” y “asuntos públicos”, así como la contratación de terceros para gestionar su interacción con autoridades y actores clave. Organizan reuniones privadas, eventos sociales, viajes, alianzas estratégicas y campañas de

comunicación que buscan moldear la opinión pública y los marcos regulatorios a su favor. Según la OCDE, estas prácticas de cabildeo buscan promover los intereses de los agentes involucrados en procesos de decisión pública y electoral, y pueden extenderse incluso a la producción de conocimiento científico. Como ha señalado Sarah Wynn-Williams, ex ejecutiva de Facebook, la filosofía interna de muchas de estas empresas de "crecer rápido y romper cosas" ha llevado a un expansionismo guiado casi exclusivamente por la obtención de lucro, en ocasiones violando leyes y regulaciones, lo que evidencia la necesidad urgente de mecanismos de control más sólidos y transparentes.

Desde una perspectiva ética, la digitalización plantea desafíos relacionados con los sesgos algorítmicos, la manipulación de la opinión pública y la exclusión digital. Ferrajoli (2020) sostiene que un Estado constitucional no puede limitarse a reaccionar ante violaciones consumadas, sino que debe generar condiciones normativas y culturales para prevenir vulneraciones sistemáticas. La realidad colombiana, marcada por brechas digitales y limitaciones institucionales, muestra que la falta de un enfoque preventivo deja a la ciudadanía expuesta a vulneraciones masivas de derechos en entornos digitales.

4.3.2. Responsabilidad de plataformas digitales y neutralidad de la red

Uno de los principales retos del constitucionalismo digital colombiano es la definición clara de la responsabilidad de las plataformas digitales. Actualmente, el marco normativo nacional carece de disposiciones integrales que determinen las obligaciones de las empresas frente a la prevención, supervisión y reparación de daños derivados de actividades ilícitas o vulneraciones a derechos fundamentales en entornos digitales. Esta ausencia normativa genera un escenario de inseguridad jurídica que perjudica a los usuarios y limita la posibilidad de exigir responsabilidad a actores privados de gran poder económico y tecnológico (Pérez Luño, 2019).

La neutralidad de la red, entendida como el principio que garantiza el tratamiento igualitario del tráfico de datos sin discriminación por origen, destino o contenido, constituye otro eje crítico. En ausencia de garantías normativas robustas, los proveedores de servicios de internet y las grandes plataformas pueden priorizar ciertos contenidos, afectar la competencia y restringir indirectamente la libertad de expresión de los usuarios. La Comisión Europea ha establecido lineamientos precisos para salvaguardar la neutralidad y promover un ecosistema digital competitivo y transparente, mientras que en América Latina destaca el caso de Brasil

con su Marco Civil de Internet (2014), que fija obligaciones claras para los proveedores y protege la libertad de expresión en línea.

En el contexto colombiano, la ausencia de regulación integral se traduce en una dependencia casi exclusiva de la acción de tutela y de decisiones judiciales aisladas para proteger derechos en entornos digitales. Esta estrategia, aunque efectiva en casos puntuales, no garantiza una protección estructural ni preventiva. Ferrajoli (2020) enfatiza que la eficacia del Estado constitucional depende de su capacidad de anticipar riesgos y articular mecanismos institucionales adecuados. La falta de un marco que combine neutralidad de la red, protección de datos y responsabilidad de intermediarios limita la consolidación de un verdadero constitucionalismo digital en Colombia.

Los vacíos analizados en los Casos de la Corte Constitucional enrostran la necesidad imperante de una regulación dinámica que se ajuste a las realidades del país, la vulneración directa y tratamiento de datos, el uso de información para prácticas de *profiling* y vigilancia estatal son cuestiones que deben ser tratadas, en cuanto a los usuarios no se vean desprotegidos de sus derechos fundamentales; la alteración de percepción de la realidad por inteligencia artificial o la creación de contenido e información falsa son advertencias que se hacen en la sociedad actual.

El análisis comparado sugiere que Colombia debe avanzar hacia la creación de un régimen normativo integral que armonice las obligaciones de las plataformas digitales con los derechos de los usuarios, siguiendo estándares internacionales. Este marco debería incorporar principios de transparencia, mecanismos de supervisión y sanciones efectivas, así como lineamientos para garantizar la competencia y la diversidad informativa. Solo a través de un enfoque preventivo y articulado será posible consolidar un ecosistema digital seguro, justo y respetuoso de los derechos fundamentales.

4.3.3. Proyectos de Leyes colombiano de Inteligencia Artificial

En Colombia, se han realizado esfuerzos preliminares para consolidar un marco jurídico que reconozca los derechos digitales, aunque sin éxito legislativo. Un ejemplo relevante fue el Proyecto de Ley 300 de 2020, impulsado por el senador Carlos Andrés Trujillo González, que pretendía fortalecer la protección de los datos personales, reconocer libertades y derechos digitales, e incluir disposiciones sobre seguridad digital, educación digital y protección de menores en línea, así como derechos como la rectificación y el olvido en la red (Congreso de

la República, 2025). El proyecto también contemplaba la creación de una autoridad de supervisión adscrita a la Superintendencia de Industria y Comercio, con competencias para garantizar estas garantías digitales. Sin embargo, al revisar los antecedentes legislativos se evidenció que dicho proyecto no fue finalmente radicado, quedando como un antecedente fallido que evidencia la falta de compromiso normativo sostenido frente a los retos del constitucionalismo digital en Colombia

A nivel internacional y regional, Colombia ha participado en compromisos que refuerzan la importancia de avanzar hacia un marco normativo integral de derechos digitales. En la XXVIII Cumbre Iberoamericana de 2023, 22 países, incluidos Colombia, España, México y Argentina, adoptaron la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, que promueve un entorno seguro, inclusivo y respetuoso de los derechos humanos en el ciberespacio (SEGIB, 2025). Este instrumento regional enfatiza la protección de la privacidad, la libertad de expresión, el acceso equitativo a la información y la ciberseguridad, marcando un estándar que aún no se refleja plenamente en el ordenamiento jurídico colombiano. La ausencia de una ley que incorpore estos principios demuestra la necesidad de alinear la normativa interna con compromisos internacionales, preparando el terreno para iniciativas más recientes como el Proyecto de Ley de Inteligencia Artificial 2025, que busca responder a los retos de la quinta revolución industrial y a la protección efectiva de los derechos digitales emergentes.

En julio de 2025, el Gobierno de Colombia radicó ante el Congreso el primer Proyecto de Ley de Inteligencia Artificial (IA), marcando un hito en la respuesta normativa frente a los desafíos de la cuarta y quinta revolución industrial. Este proyecto busca establecer un marco regulatorio integral que permita el desarrollo ético, seguro y responsable de la IA en el país, alineado con estándares internacionales (MinCiencias, 2025; MinTIC, 2025).

El proyecto de ley introduce una clasificación de riesgos para los sistemas de IA: prohibido, alto, limitado y bajo, siguiendo criterios de impacto en los derechos fundamentales. Entre sus disposiciones clave, se propone la creación de una Autoridad Nacional de Supervisión de IA, encargada de monitorear el cumplimiento normativo, certificar algoritmos y coordinar con las entidades de protección de datos. Asimismo, establece obligaciones para los desarrolladores y usuarios de IA, incluyendo medidas de transparencia, auditoría y trazabilidad algorítmica.

Además, la iniciativa incorpora programas de alfabetización digital, reconversión laboral y fomento de la investigación en IA con enfoque ético e inclusivo, reconociendo que la transformación digital debe estar acompañada de una estrategia educativa y social para reducir brechas y evitar exclusiones. Este proyecto refleja la creciente conciencia de que la innovación tecnológica debe equilibrarse con la protección de derechos como la dignidad humana, la igualdad y la privacidad (El Tiempo, 2025; Infobae, 2025).

Tabla 9.

Comparación normativa internacional sobre Inteligencia Artificial y derechos digitales.

País / Región	**Norma o instrumento**	**Ventajas**	**Vacíos**	**Lecciones para Colombia**	**Riesgos para derechos fundamentales**
Colombia	Proyecto de Ley IA 2025	Clasificación de riesgos; autoridad nacional; enfoque ético y educativo	Pendiente aprobación; falta de integración con marco constitucional y políticas públicas	Necesidad de articular norma con tutela de derechos y cultura digital	Vulneración de privacidad; sesgos algorítmicos; falta de supervisión efectiva
España	Carta de Derechos Digitales 2021	Reconocimiento expreso de derechos digitales; principios de ética algorítmica	Carácter no vinculante; limitada fuerza jurídica	Sirve de guía para establecer principios preventivos y éticos	Falta de exigibilidad directa de algunos derechos

Unión Europea	RGPD 2016 y futura Ley de IA	Protección robusta de datos; supervisión integral; armonización comunitaria	Implementación desigual entre países miembros	La supervisión centralizada garantiza coherencia normativa	Posibles conflictos entre innovación y regulación estricta
Brasil	Marco Civil Internet 2014 y LGPD 2018	Régimen integral de datos; obligaciones claras para plataformas	Limitada experiencia en supervisión de IA compleja	Regulación integral fortalece confianza digital	Persisten riesgos de brechas culturales y desinformación
EE.UU.	Enfoque sectorial y guías éticas de IA	Flexibilidad para innovación; liderazgo tecnológico	Falta de ley federal integral; dependencia de autorregulación	Permite ver límites de la autorregulación para Colombia	Riesgos altos por vacíos de responsabilidad y privacidad

Nota. Elaboración propia (2025)

El análisis de los desarrollos normativos recientes, las responsabilidades de las plataformas digitales y el impacto social y ético de la digitalización permite concluir que Colombia enfrenta una brecha significativa entre innovación tecnológica y capacidad de respuesta institucional. Si bien el Proyecto de Ley de IA 2025 representa un avance, su efectividad dependerá de la integración con un marco constitucional digital robusto y políticas públicas coherentes.

La experiencia comparada muestra que los países que han logrado consolidar ecosistemas digitales seguros han combinado tres elementos: normas preventivas claras, instituciones coordinadas y una ciudadanía educada en cultura digital y ética tecnológica

(Ferrajoli, 2020; Alexy, 2002). En el caso colombiano, la ausencia de una estrategia integral mantiene la protección de derechos digitales fragmentada y dependiente de la acción de tutela.

En consecuencia, se hace evidente que la construcción de un constitucionalismo digital colombiano requiere pasar de la reflexión teórica a la acción normativa, institucional y cultural. Este diagnóstico constituye el insumo directo para la propuesta normativa que se desarrollará en el Capítulo 4, orientada a consolidar un ecosistema digital preventivo, seguro y sostenible, que armonice la innovación tecnológica con la protección de los derechos fundamentales.

4.4.Derecho comparado de derechos digitales.

En el contexto actual, los derechos digitales se presentan como una extensión natural de los derechos humanos al espacio virtual, ya que el uso cotidiano de Internet y de las tecnologías digitales ha configurado un entorno en el que las relaciones sociales, económicas, políticas y culturales se desarrollan de manera cada vez más intensa. Aunque en el mundo físico estos derechos se encuentran claramente reconocidos, la aparición del ciberespacio, un ámbito relacional donde las interacciones son globales, descentralizadas y rápidas, ha hecho necesaria su adaptación para garantizar la protección efectiva de las personas. Este escenario evidencia la urgencia de analizar cómo otros sistemas jurídicos han abordado estos retos, puesto que sus avances ofrecen elementos valiosos para comprender los vacíos normativos en Colombia y las posibilidades de trasplante normativo.

De acuerdo con el modelo generacional propuesto por Vasak y otros autores, actualmente nos encontramos frente a una nueva etapa de los derechos humanos, donde la ciudadanía digital se consolida como un concepto fundamental. Esta ciudadanía emerge debido a los profundos cambios introducidos por las Tecnologías de la Información y la Comunicación (TIC), ya que estas modifican la manera en que los ciudadanos participan, se informan y ejercen sus derechos. En esta línea, diversos expertos han planteado que el marco legal debe adaptarse para permitir el pleno ejercicio de estos nuevos derechos, lo que exige la construcción de legislación específica y coherente (Cova-Fernández, 2022).

El concepto de “derechos digitales” o “ciberderechos” continúa siendo dinámico, puesto que evoluciona a medida que cambian los entornos tecnológicos. Warkentin, en 2023, fue uno de los autores pioneros en presentar una definición centrada exclusivamente en el ciberespacio, al identificar derechos asociados con la libertad de expresión, la privacidad en línea, el acceso al entorno virtual y la asociación en comunidades digitales.

Tabla 10.

Ciberderechos según Warkentin

Derechos exclusivos del Ciberespacio y de Internet			
1	Derecho a la libre expresión	2	Derecho a la privacidad en línea (privacy online)
3	Derecho al acceso al ciberespacio (ac- ceso al Internet) independientemente de los niveles de ingreso, la ubicación geográfica o las discapacidades del (los) usuario(s)	4	Derecho a asociarse en comunidades en línea (conocidas también como comunidades virtuales)

Nota. Adaptado de Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

La Asociación para el Progreso de las Comunicaciones (APC) contribuyó con una visión amplia, reconociendo derechos tales como el acceso universal a Internet, la libertad de expresión, la privacidad, la gobernanza de Internet y el intercambio de conocimiento, reforzando la idea de que la tecnología digital debe ser un vehículo para empoderar a todos los pueblos del mundo (Cova-Fernández, 2022).

Tabla 11.

Derechos digitales según la APC

DERECHOS DE LOS USUARIOS DE INTERNET Y DE LAS TIC			
1	Acceso a Internet para todos y todas		
2	Libertad de expresión y asociación	5	Privacidad, vigilancia y encriptación
3	Acceso al conocimiento	6	Gobernanza de internet
4	Intercambio de aprendizaje y creación de software libre y desarrollo tecnológico	7	Conciencia, protección y realización de los derechos

Nota. Adaptado de Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

A nivel de la teoría de los derechos humanos, Bustamante (2010) propone que estos derechos surgen como parte de la nueva etapa de los derechos humanos, extendiéndose a la "ciudadanía digital" y abarcando aspectos como el libre acceso a la información, la inclusión digital y la educación ciudadana.

Tabla 12.

Derechos de la ciudadanía digital según Bustamente Donas

DERECHOS EN LA SOCIEDAD DE LA INFORMACIÓN	
Dimensión	Derecho a ...
1ª	→ Libre acceso y uso de la información y el conocimiento → Interacción simple y completa con ... → las Administraciones Públicas a través de redes telemáticas
2ª	→ Inclusión Digital: → Inserción laboral (colectivos marginales) → Profesionalización y capacitación
3ª	→ Educación ciudadana: → Inserción autónoma a cada país en un mundo globalizado

Nota. Adaptado de Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

Por otro lado, Riofrío (2014) refuerza la noción de que los Derechos Digitales son una extensión de los derechos fundamentales existentes, los cuales han adquirido una nueva dimensión en el contexto de la sociedad de la información. En este sentido, el Consejo de Europa se ha pronunciado sobre la necesidad de proteger los derechos humanos en el entorno digital, recomendando que los derechos que existen en el mundo físico sean igualmente garantizados en el ciberespacio.

Tabla 13.

Derechos digitales según Riofrío Martínez-Villalba

DERECHOS DEL CIBERNAUTA EN EL MUNDO DIGITAL O VIRTUAL Y EN LA SOCIEDAD DE LA INFORMACIÓN			
1	El derecho a existir digitalmente.	6	El derecho al big-reply.
2	El derecho a la reputación digital.	7	El derecho al domicilio digital.
3	La estima digital.	8	El derecho a la técnica, al update, al parche.
4	La libertad y responsabilidad digital.	9	El derecho a la paz cibernética y a la seguridad informática.
5	La privacidad virtual, el derecho al olvido, el derecho al anonimato.	**10**	El derecho al testamento digital.

Nota: Adaptado de Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

Así mismo, Nitsche y Hairsine (2016) argumentan que los Derechos Digitales no son nuevos, sino los mismos que ya existen en el mundo offline, pero con adaptaciones específicas al entorno digital, mientras que otras definiciones (Nitsche, 2016), por otra parte, En el ámbito legislativo, la definición de los Derechos Digitales cobra relevancia en España con la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, que formaliza el reconocimiento de estos derechos en la legislación del país (Ministerio de Asuntos Económicos y Transformación Digital., 2021).

Tabla 14.

Derechos digitales según Consejo de Europa

DERECHOS DE LOS USUARIOS DE INTERNET

1	El derecho al acceso y no discriminación		
2	Libertad de expresión e información.	**6**	Derecho a la educación y conocimientos básicos
3	Derecho de reunión, asociación y participación.	**7**	Derecho de protección y orientación a niños y jóvenes
4	Derecho a la protección de la vida privada y de los datos personales.	**8**	Derecho a disponer de recursos efectivos en caso de restricción y violación de derechos fundamentales.

Nota. Adaptado de Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

Finalmente, la clasificación de los Derechos Digitales varía según el autor y el marco normativo, pero todos coinciden en que se trata de una extensión de los derechos humanos fundamentales que deben ser protegidos en el entorno digital. Estos derechos buscan promover el acceso libre y justo a la tecnología, garantizando la protección y confidencialidad de los usuarios en la red. Sin embargo, en Colombia aún estamos en un proceso de discusión sobre la conformación y reconocimiento de los Derechos Digitales, lo cual implica la necesidad de establecerlos claramente en una legislación adecuada. Este desafío requiere un marco legal robusto que asegure un entorno digital seguro y respetuoso para todos los colombianos, asegurando la protección de los derechos fundamentales en el ciberespacio.

Para realizar un análisis comparado de marcos normativos en derechos digitales, en primer lugar, se escogieron ordenamientos que han desarrollado regulaciones robustas en materia de derechos digitales, ya que permiten observar modelos consolidados y replicables. En segundo lugar, se priorizaron sistemas con cercanía constitucional a Colombia, puesto que comparten estructuras garantistas y modelos de protección de derechos. Finalmente, se eligieron jurisdicciones donde los debates sobre responsabilidad en entornos digitales, autonomía tecnológica y protección frente a la inteligencia artificial han alcanzado mayor desarrollo.

En la Unión Europea, España y Brasil existe un reconocimiento más amplio y sistemático de los derechos digitales, ya que incluyen catálogos explícitos, autoridades

reguladoras fuertes y marcos sancionatorios claros. Estos países han logrado articular norma, institucionalidad y cultura digital, lo que les permite enfrentar desafíos como la automatización, el procesamiento masivo de datos y la inteligencia artificial.

En contraste, Colombia mantiene un modelo fragmentado y reactivo, puesto que no ha incorporado de manera expresa los derechos digitales en su Constitución ni en una ley estatutaria. La protección de estos derechos depende de la acción de tutela y de la interpretación jurisprudencial, lo cual genera incertidumbre, criterios dispares y ausencia de lineamientos unificados.

Tabla 15.

Contraste de jurisdicciones en el ámbito de derecho digital.

Criterio	**Colombia**	**Unión Europea**	**Estados Unidos**
Marco general de derechos digitales	No existe una ley integral de derechos digitales. La protección se deriva de la Constitución (arts. 15, 20, 29, 74) y normas sectoriales.	Reconoce explícitamente los derechos digitales mediante la *Carta de Derechos Fundamentales de la UE* y el *Acervo Digital Europeo*.	No hay un marco federal integral. Los derechos digitales se regulan de forma fragmentada por estados y agencias.
Protección de datos personales	Ley 1581 de 2012, Decreto 1377/2013 y jurisprudencia constitucional. Modelo inspirado en la UE pero menos robusto.	Reglamento General de Protección de Datos (GDPR). Estándar más alto y exigente del mundo.	No existe una ley federal. Destacan CCPA (California), COPPA para menores y regulaciones sectoriales.
Gobernanza algorítmica y IA	No hay ley específica. Existen lineamientos del Gobierno Digital y propuestas legislativas (PL 003/2024).	Ley de Inteligencia Artificial (AI Act), marco obligatorio basado en riesgos.	No existe regulación federal. Enfoque sectorial y "light-touch"; guías de NIST no son obligatorias.
Responsabilidad por decisiones automatizadas	No regulada expresamente. Se acude a principios generales, tutela y control de convencionalidad.	GDPR reconoce el derecho a no estar sometido a decisiones automatizadas sin supervisión humana. AI Act crea obligaciones estrictas	No existe reconocimiento explícito. La responsabilidad depende del caso, reguladores sectoriales y jurisprudencia.

		para sistemas de alto riesgo.	
Blockchain y organizaciones descentralizadas (DAO)	No existe legislación. Se aplican figuras tradicionales como asociaciones de hecho o contratos civiles.	Regulación fragmentaria. Se analizan las DAO bajo normas financieras y de protección al consumidor.	La SEC ha tratado a las DAO como emisores de valores. No hay marco unificado. El caso The DAO generó precedentes inhibitorios y advertencias regulatorias.
Identidad digital	No hay identidad digital estatal unificada. Se avanza en interoperabilidad y servicios digitales.	Existe *Identidad Digital Europea* (EIDAS 2.0) con validez transfronteriza.	No existe identidad digital federal. Cada entidad gestiona sus propios sistemas.
Derechos frente a plataformas digitales	Protección basada en habeas data, tutela y normas sectoriales (comercio electrónico).	Ley de Servicios Digitales (DSA) y Ley de Mercados Digitales (DMA) regulan transparencia, moderación y competencia.	Enfoque de autorregulación y responsabilidad limitada bajo la Sección 230.
Enfoque regulatorio predominante	Reactivo y jurisprudencial, con avances sectoriales del MinTIC.	Preventivo, integral y de alta exigencia técnica.	Sectorial, flexible y descentralizado.
Capacidad institucional para casos complejos (como DAO)	Dificultades por vacíos normativos; podría presentarse inhibición en ciertos casos complejos.	Marcos más sólidos, aunque ciertos casos han generado incertidumbre.	En varios casos se han dado abstenciones o inhibiciones por ausencia de categorías jurídicas aplicables.

Nota. Elaboración Propia, 2025

El análisis de los marcos normativos en derechos digitales evidencia diferencias sustanciales entre Colombia, la Unión Europea y Estados Unidos, diferencias que no solo reflejan sus tradiciones jurídicas, sino también sus prioridades institucionales y el ritmo con el que cada región ha decidido responder a los desafíos tecnológicos contemporáneos.

En primer lugar, la Unión Europea se posiciona como el referente más sólido y coherente, ya que ofrece un marco integral, preventivo y articulado, especialmente visible en el RGPD, el AI Act y el paquete de gobernanza digital compuesto por el DSA y el DMA. Su enfoque parte de la protección de derechos fundamentales y de un control riguroso sobre tecnologías emergentes, lo que permite una mayor seguridad jurídica tanto para ciudadanos como para desarrolladores y operadores tecnológicos.

Por su parte, Estados Unidos mantiene un modelo fragmentado y predominantemente sectorial. Aunque cuenta con agencias fuertes y guías técnicas como las del NIST, la ausencia de una ley federal integral crea brechas importantes de protección. Esto ha generado respuestas regulatorias desiguales entre estados y ha permitido que fenómenos como las DAO o los sistemas algorítmicos se analicen principalmente desde ópticas económicas o financieras, con menor atención sistemática a los derechos digitales. Esta falta de uniformidad explica, en parte, las decisiones inhibitorias en casos como The DAO.

En contraste, Colombia se encuentra en una etapa intermedia caracterizada por avances dispersos, apoyados en jurisprudencia constitucional robusta, pero sin un cuerpo legislativo unificado que aborde la complejidad digital contemporánea. El país opera con normas sectoriales, principios generales del derecho y herramientas de integración normativa, lo que permite resolver algunos casos mediante analogía, aunque sin eliminar la incertidumbre jurídica. Esta situación genera un panorama en el que, ante fenómenos altamente innovadores o estructuralmente descentralizados, las cortes podrían enfrentar dificultades similares a las observadas en los sistemas más avanzados, especialmente cuando no exista un sujeto responsable o categoría jurídica aplicable.

De manera transversal, el estudio comparado muestra que tanto Colombia como Estados Unidos comparten desafíos derivados de la ausencia de leyes integrales en derechos digitales, mientras que la Unión Europea marca la pauta hacia un constitucionalismo digital robusto y adaptado a las exigencias tecnológicas actuales. Esto confirma la necesidad de que Colombia avance hacia una regulación más sistemática y anticipatoria, que permita responder con mayor claridad a fenómenos como inteligencia artificial, blockchain, organizaciones autónomas y toma de decisiones automatizadas, reduciendo así la posibilidad de decisiones inhibitorias y fortaleciendo la protección efectiva de los derechos fundamentales en entornos digitales.

A partir de este análisis, se concluye que un trasplante normativo integral no sería viable, ya que Colombia no cuenta con las capacidades institucionales de la Unión Europea ni con el nivel de despliegue tecnológico de España.

La revisión comparada permite evidenciar que Colombia enfrenta un escenario de vulnerabilidad digital debido a la fragmentación normativa, la debilidad institucional y la ausencia de un marco legal integral. Aunque la jurisprudencia constitucional ha proporcionado avances importantes, sigue existiendo un vacío regulatorio significativo que limita la protección efectiva de los derechos fundamentales en entornos digitales.

Este diagnóstico confirma la necesidad de avanzar hacia un constitucionalismo digital preventivo y de diseñar un modelo normativo propio, tomando como referencia las mejores prácticas observadas en los ordenamientos analizados, ya que estos aportan insumos valiosos para la formulación de políticas públicas y la construcción de un marco regulatorio coherente.

TÍTULO V: PROPUESTA NORMATIVA Y MODELO DE CONSTITUCIONALISMO DIGITAL COLOMBIANO.

El presente capítulo constituye la culminación del diagnóstico crítico realizado en el Capítulo 4, en el que se evidenció que Colombia carece de un marco jurídico integral para enfrentar los desafíos de la quinta revolución industrial y de las tecnologías emergentes como inteligencia artificial, *blockchain,* metaverso y biotecnologías digitales. Dicho vacío normativo se traduce en una desprotección efectiva de los ciudadanos, quienes ven amenazados derechos como la intimidad, la identidad digital y la libertad de expresión en entornos virtuales, sin que exista una respuesta estatal oportuna y coordinada.

Actualmente, el Estado colombiano no está preparado para la velocidad de la transformación digital. La fragmentación normativa y la lentitud de los mecanismos institucionales dejan desprotegidos a los usuarios de nuevas tecnologías, mientras que la Corte Constitucional, aunque garante final de la supremacía constitucional, no puede ser la única responsable de materializar la protección digital. La ausencia de un marco normativo robusto y preventivo hace que la reacción jurídica sea principalmente reactiva, por vía de tutelas, acciones de inconstitucionalidad y pronunciamientos aislados.

En este contexto, el constitucionalismo digital colombiano que propone esta tesis parte de una necesidad urgente: transitar de un modelo reactivo a uno preventivo y sostenible, que combine:

1. Reconocimiento expreso de derechos digitales por conexidad (intimidad, habeas data, igualdad, libertad de expresión, debido proceso).
2. Lineamientos normativos claros para la supervisión de tecnologías emergentes.
3. Un modelo de gobernanza digital institucional, que desconcentre la carga de protección de la Corte Constitucional y la extienda a autoridades especializadas.

La metodología de este capítulo integra tres ejes:

i) Fundamentación doctrinal:

La construcción del constitucionalismo digital colombiano se sustenta en la teoría general del Estado y del derecho constitucional, retomando las aportaciones de Hans Kelsen, quien concibe la jurisdicción constitucional como la garantía última de la supremacía de la Constitución, y de Georg Jellinek y Georges Burdeau, quienes subrayan

que la fuerza normativa de la Constitución requiere instrumentos concretos de protección frente a los cambios sociales y tecnológicos.

En línea con La Salle, la Constitución no solo debe entenderse como un texto jurídico sino como realidad política y social, lo que implica que el marco jurídico debe adaptarse a la dinámica digital para evitar que los derechos fundamentales queden rezagados frente a la innovación tecnológica. Complementariamente, Luigi Ferrajoli, desde su teoría del garantismo, advierte que un derecho sin mecanismos de protección efectiva se convierte en mera declaración, planteamiento que justifica la urgencia de diseñar mecanismos normativos preventivos para derechos digitales.

Desde la perspectiva de los derechos fundamentales y su proyección digital, Gregorio Peces-Barba y Antonio-Enrique Pérez Luño han destacado la necesidad de reconocer los derechos de cuarta generación y su interdependencia con los derechos clásicos, especialmente en materia de privacidad, identidad e integridad digital.

En el ámbito del derecho procesal constitucional, se integran las contribuciones de Héctor Fix-Zamudio y Humberto Nogueira Alcalá, quienes consolidan esta disciplina como instrumento operativo para la defensa de los derechos fundamentales en escenarios de transformación social. Néstor Pedro Sagüés, Eduardo Ferrer Mac-Gregor y Gustavo Zagrebelsky refuerzan la idea de que la protección constitucional en el siglo XXI debe ser proactiva, combinando mecanismos jurisdiccionales efectivos con estructuras normativas que anticipen riesgos derivados de la inteligencia artificial, el big data y las plataformas digitales.

Finalmente, Peter Häberle introduce la noción de una Constitución abierta a la sociedad, que reconoce la interacción entre instituciones, ciudadanía y tecnología, subrayando que la protección digital no puede recaer exclusivamente en la Corte Constitucional. Este enfoque sustenta la propuesta de crear un marco normativo integral y una gobernanza digital preventiva, capaz de proteger de manera eficaz los derechos digitales y de fortalecer la seguridad jurídica ante las tecnologías emergentes.

ii) Derecho comparado:

Se analizan referentes como la Carta de Derechos Digitales de España, el Reglamento General de Protección de Datos (GDPR) y la Ley de Inteligencia Artificial de la Unión Europea, así como la Ley General de Protección de Datos (LGPD) y el Marco

Civil de Internet de Brasil, que materializan estándares internacionales de gobernanza digital y derechos fundamentales.

iii) Diagnóstico normativo nacional:

El capítulo parte de la constatación de que Colombia opera bajo un modelo fragmentado, donde la protección digital depende exclusivamente de reacciones judiciales y medidas sectoriales, sin un marco legal integral. Este vacío justifica la construcción de un modelo de constitucionalismo digital colombiano que articule doctrina, derecho comparado y una propuesta normativa concreta, presentada en este capítulo como proyecto de ley y modelo de gobernanza digital.

Con este enfoque, el Capítulo 4 representa el aporte original de la tesis: ofrecer un marco jurídico preventivo y sostenible que permita a Colombia proteger de manera efectiva los derechos digitales, fortalecer la seguridad jurídica y reducir la dependencia exclusiva de la Corte Constitucional, alineándose con estándares internacionales y anticipando la evolución acelerada de las tecnologías emergentes.

5. Lineamientos para un marco normativo integral de derechos digitales

La digitalización ha transformado radicalmente la interacción humana, la economía y la gobernanza, generando beneficios sociales innegables, como el acceso masivo a la información, la expansión del comercio electrónico y la modernización de los servicios públicos. Sin embargo, también ha creado nuevos escenarios de vulnerabilidad jurídica que amenazan los derechos fundamentales reconocidos en la Constitución de 1991.

En Colombia, la fragmentación normativa y la reacción tardía del Estado frente a tecnologías emergentes han generado una protección insuficiente de los ciudadanos en entornos digitales, trasladando el peso de la defensa de los derechos a la Corte Constitucional, que opera principalmente de manera reactiva. Este modelo es insostenible en la era de la quinta revolución industrial, donde tecnologías como la inteligencia artificial (IA), el big data, el metaverso y la biometría avanzada plantean riesgos inmediatos para la privacidad, la seguridad y la libertad individual.

El constitucionalismo digital colombiano que propone esta tesis parte de un principio esencial: los derechos digitales deben reconocerse como derechos fundamentales por conexidad y contar con mecanismos preventivos y reactivas que garanticen su protección efectiva. A continuación, se desarrollan los lineamientos normativos para cada derecho,

integrando fundamentación doctrinal, jurisprudencia nacional, derecho comparado y propuestas normativas.

El reconocimiento de derechos digitales por conexidad constituye el eje central de los lineamientos para un marco normativo integral de protección. La evolución tecnológica ha generado que garantías clásicas como la privacidad, la libertad de expresión, el acceso a la información, la seguridad digital y la protección frente a la ciberdelincuencia y la vigilancia no autorizada, enfrenten nuevos escenarios de vulnerabilidad que la legislación colombiana aún no logra atender de manera integral. Aunque existen normas como la Ley 1581 de 2012 (protección de datos personales), la Ley 1273 de 2009 (delitos informáticos) y la Ley 1712 de 2014 (acceso a la información), su alcance es fragmentado y reactivo, dejando a los ciudadanos expuestos ante riesgos propios del big data, la inteligencia artificial, el metaverso y la vigilancia digital masiva. En este contexto, resulta indispensable desarrollar cada uno de estos derechos digitales por conexidad para diagnosticar su estado actual, sus vacíos normativos y jurisprudenciales, así como proponer recomendaciones normativas que sienten las bases del constitucionalismo digital colombiano.

a) Derecho a la Protección de la Privacidad

En el contexto digital, la privacidad se enfrenta a retos inéditos, ya que los datos personales de los ciudadanos son recopilados, procesados y compartidos a través de diversas plataformas. Esto plantea el riesgo de vulneraciones de la privacidad de los individuos, lo que exige un marco normativo robusto que regule el manejo de datos personales. En Colombia, la Ley 1581 de 2012 de Protección de Datos Personales establece las bases para la protección de la privacidad en el entorno digital, pero aún hay áreas que requieren fortalecimiento, como el control sobre la recolección y el uso de datos por parte de actores no autorizados.

La Ley 1581 de 2012, que regula la protección de los datos personales en Colombia, representa un paso fundamental en la búsqueda de un marco normativo para salvaguardar la privacidad de los ciudadanos frente al tratamiento de sus datos personales. Sin embargo, esta legislación muestra deficiencias al no adaptarse a las nuevas tecnologías y herramientas emergentes, como el big data, el metaverso, y la inteligencia artificial. Siendo así que la ley no aborda de manera efectiva los nuevos escenarios en los que los usuarios interactúan con plataformas tecnológicas avanzadas, las cuales recopilan y procesan grandes volúmenes de datos personales. En estos contextos, la ley no ofrece directrices claras sobre cómo garantizar que los usuarios puedan otorgar su consentimiento de manera informada y explícita, ni

establece procedimientos para mantener el control sobre la información que se comparte en entornos digitales tan complejos (Becerra, 2018).

Además, los derechos de los usuarios frente a sus datos personales en entornos de tecnologías emergentes son insuficientemente protegidos por la Ley 1581. Mientras que en el mundo físico el usuario puede tener un control directo sobre la recopilación y el tratamiento de sus datos, en el ámbito virtual, especialmente en plataformas como el metaverso y otras aplicaciones de inteligencia artificial, los usuarios se ven desbordados por la opacidad de los procesos tecnológicos que subyacen a la recolección de información. Las políticas de privacidad de estas plataformas no siempre cumplen con los principios de transparencia, lo que dificulta que los usuarios comprendan cómo se utilizan sus datos y qué riesgos conlleva la exposición de estos. En este sentido, se requiere una actualización y fortalecimiento de la Ley 1581, que contemple mecanismos claros y accesibles para que los usuarios sean capaces de tener un control real sobre sus datos, incluso en entornos virtuales complejos.

Finalmente, la seguridad de los datos personales en el marco de tecnologías emergentes presenta un reto adicional debido a la naturaleza global de estas herramientas. Muchas de las plataformas tecnológicas que operan en el metaverso, big data e inteligencia artificial están bajo jurisdicciones extranjeras que pueden no estar alineadas con las regulaciones colombianas sobre privacidad. Esto plantea un escenario de vulnerabilidad para los usuarios, quienes pueden ver sus derechos reducidos al no contar con mecanismos internacionales de protección. La Ley 1581, aunque pionera en la protección de datos, no contempla estos riesgos globales ni la coordinación entre países para garantizar la seguridad y el respeto de los derechos de los ciudadanos en plataformas tecnológicas que cruzan fronteras. Es crucial que Colombia impulse reformas a esta ley para hacerla más robusta frente a las herramientas tecnológicas del futuro y garantizar un marco adecuado de protección para los usuarios en la era digital.

A la fecha, la Corte Constitucional de Colombia no ha abordado de manera directa ningún caso relacionado con los derechos digitales de los usuarios en el contexto de tecnologías emergentes como el big data, el metaverso o la inteligencia artificial. Aunque la Corte ha emitido pronunciamientos sobre la protección de datos personales en el ámbito tradicional, aún no se ha pronunciado de forma explícita sobre los desafíos que surgen con el avance de las nuevas tecnologías, especialmente en lo que respecta a la recopilación, el tratamiento y la gestión de los datos en plataformas digitales complejas. Este vacío jurisprudencial deja a los usuarios sin un marco de protección específico ante los riesgos emergentes derivados del uso

de sus datos en entornos digitales, lo que resalta la necesidad urgente de un pronunciamiento judicial que aclare los derechos y garantías fundamentales en este nuevo contexto tecnológico.

Pese a los avances que trajo la Ley 1581 de 2012, la privacidad digital en Colombia sigue siendo meramente formal y reactiva. La ausencia de regulación específica sobre el consentimiento informado reforzado, la transferencia internacional de datos y la protección en entornos de IA, metaverso y big data, deja a los ciudadanos sin control real sobre su información personal. En la práctica, la seguridad de los datos depende de reacciones judiciales ex post, mientras que la explotación tecnológica de datos avanza sin límites claros. Esta brecha evidencia la urgencia de una ley marco de derechos digitales que garantice autodeterminación informativa y mecanismos preventivos, reduciendo la dependencia de la Corte Constitucional como único garante.

b) Derecho a la Libertad de Expresión

La digitalización ha proporcionado nuevas plataformas para la expresión de ideas y opiniones. Sin embargo, esto también ha dado lugar a nuevos riesgos, como la desinformación, el discurso de odio y la censura en línea. La libertad de expresión es un derecho fundamental protegido por la Constitución Política de Colombia, pero la digitalización ha generado la necesidad de establecer límites que protejan a los usuarios sin afectar su capacidad para expresarse. El reto está en encontrar un equilibrio entre la libre circulación de ideas y la protección contra contenidos dañinos o ilegales.

En la Sentencia T-372 de 2023 de la Corte Constitucional de Colombia, se reafirma la importancia del acceso al servicio de internet como un derecho fundamental. La Corte subraya su rol crucial no solo como medio de comunicación e información, sino también como herramienta esencial para el ejercicio de derechos como a la protesta pacífica y el derecho a la libertad de expresión, especialmente en contextos sociales sensibles como manifestaciones. A continuación, la postura de la Corte:

i. La Corte Constitucional considera que el acceso a internet es indispensable para la materialización de la libertad de expresión. Este derecho, inherente a un sistema democrático, incluye la posibilidad de difundir y recibir información sin restricciones arbitrarias. En el caso en cuestión, la interrupción del servicio de internet durante las protestas afectó la capacidad de los ciudadanos para

comunicarse y denunciar posibles abusos, socavando el pluralismo informativo y limitando el debate público.

ii. En línea con los estándares internacionales, la Corte señala que cualquier limitación al acceso a internet debe cumplir estrictos principios de legalidad, necesidad y proporcionalidad. Las restricciones sin base jurídica clara o que no persiguen fines legítimos, como la protección de derechos fundamentales de terceros, constituyen censura previa, prohibida por la Constitución. Esto es particularmente relevante en el caso de las redes sociales, donde el flujo de información en tiempo real permite el monitoreo ciudadano y la visibilización de injusticias.

iii. La Corte reafirma el principio de neutralidad de la red, que prohíbe a los operadores de internet discriminar o restringir el acceso a contenidos lícitos. Además, recalca que el Estado tiene el deber no solo de abstenerse de bloquear internet arbitrariamente, sino también de garantizar su acceso continuo y libre, especialmente en situaciones críticas como protestas sociales. Esto incluye investigar y prevenir prácticas que puedan limitar el ejercicio de derechos fundamentales mediante cortes de conectividad.

La postura de la Corte no se centra en las tecnologías emergentes de la quinta revolución industrial, sino en garantizar derechos fundamentales mediante un uso adecuado de herramientas ya existentes como internet y redes sociales, vitales en contextos democráticos.

Para lograr una visión integral sobre el impacto de la inteligencia artificial (IA) en la administración de justicia, es fundamental analizar la Sentencia T-323 de 2024 desde una perspectiva tanto nacional como comparada. En este sentido, la Corte Constitucional de Colombia estableció un precedente clave al determinar que la IA no puede sustituir la labor del juez en la toma de decisiones, aunque sí puede servir como herramienta de apoyo. En el caso analizado, se evaluó si el uso de ChatGPT por parte de un juez vulneró el debido proceso, concluyéndose que no hubo sustitución de la función jurisdiccional, ya que el juez ya había tomado la decisión previamente y solo utilizó la IA como referencia adicional. No obstante, la Corte resaltó que el uso de estas tecnologías en el ámbito judicial debe cumplir con principios de transparencia y responsabilidad, advirtiendo sobre la necesidad de regular su implementación para evitar riesgos futuros (Sentencia T-323 del 2024, 2024).

Bajo esta misma línea, la sentencia enfatiza la importancia de establecer un marco regulatorio claro y alineado con principios de imparcialidad y control humano, evitando que

los algoritmos sesgados comprometan la equidad en las decisiones judiciales. Para el ámbito internacional, se destacan referencias como el Reglamento de Inteligencia Artificial de la Unión Europea (2024/1689), que clasifica los sistemas de IA según su nivel de riesgo y restringe su uso en prácticas que puedan atentar contra los derechos fundamentales. La Corte concluye que, aunque la IA puede mejorar la eficiencia y el acceso a la justicia, su implementación debe estar acompañada de mecanismos de supervisión adecuados que garanticen la autonomía del juez y la seguridad jurídica de los ciudadanos, evitando que la tecnología sustituya el análisis crítico y la ponderación de derechos esenciales en la función jurisdiccional (Sierra, 2024)

Otro aspecto relevante de la decisión es la falta de un marco regulatorio claro en Colombia sobre el uso de IA en el sistema judicial. La Corte advierte que la ausencia de normas tanto nacionales e internacionales alineados genera incertidumbre y dificulta la creación de reglas precisas para el uso responsable de esta tecnología. En este punto, la sentencia hace referencia a la necesidad de que el Consejo Superior de la Judicatura establezca lineamientos específicos que orienten a los jueces sobre el uso de herramientas basadas en IA, asegurando que su aplicación no comprometa la independencia ni la imparcialidad judicial. Esta recomendación cobra especial importancia en un contexto donde la digitalización de la justicia es cada vez más acelerada (Sentencia T-323 del 2024, 2024).

La Corte también hace referencia a las normativas más recientes y relevantes sobre el uso de la inteligencia artificial (IA), destacando algunos aspectos clave sin agregar interpretaciones adicionales a lo expresado por esta Corporación.

Uno de los principales marcos regulatorios mencionados es el Reglamento (UE) 2024/1689, aprobado por el Parlamento Europeo y el Consejo el 13 de junio de 2024. Este instrumento busca fortalecer el funcionamiento del mercado interno y fomentar el desarrollo de una IA centrada en las personas, garantizando elevados estándares de protección en áreas como la salud, la seguridad y los derechos fundamentales, incluyendo la democracia, el Estado de Derecho y la conservación del medio ambiente. Asimismo, la normativa promueve la innovación y establece prohibiciones sobre ciertas aplicaciones de IA, como el uso de técnicas subliminales que alteren el comportamiento sin consentimiento informado, la explotación de vulnerabilidades por razones de edad o condiciones socioeconómicas, y la categorización biométrica basada en datos sensibles como raza, religión u orientación sexual, salvo en casos excepcionales. También restringe el uso de la puntuación social, la evaluación de riesgos de

criminalidad basada únicamente en perfiles, la recopilación masiva de imágenes faciales en internet, la inferencia de emociones en entornos laborales o educativos sin justificación médica o de seguridad, y la identificación biométrica en tiempo real en espacios públicos, salvo en circunstancias específicas como la búsqueda de personas desaparecidas o la prevención de actos terroristas.

El reglamento establece un modelo de clasificación basado en el nivel de riesgo asociado a los sistemas de IA. En este sentido, los sistemas de alto riesgo incluyen aquellos vinculados a biometría, infraestructura crítica, educación, empleo, acceso a servicios, aplicación de la ley, migración y justicia, y deben cumplir estrictos requisitos de seguridad y transparencia. Los sistemas de riesgo limitado abarcan aplicaciones como chatbots, donde se exige que los usuarios sean informados de que interactúan con una máquina. Finalmente, los sistemas de riesgo mínimo, como videojuegos o filtros de spam, no requieren medidas regulatorias específicas. Además, el reglamento establece directrices sobre gestión de riesgos, calidad de los datos de entrenamiento, documentación técnica, transparencia, supervisión humana y ciberseguridad para los sistemas de alto riesgo.

En el contexto de la regulación internacional, Estados Unidos ha avanzado en la adopción de instrumentos normativos para el uso seguro de la IA. En 2023, el presidente Joe Biden emitió una Orden Ejecutiva sobre el Desarrollo y Uso Seguro de la IA, basada en un Anteproyecto de Declaración de Derechos de la IA, cuyo propósito es salvaguardar los derechos de los ciudadanos frente a los sistemas automatizados. Esta regulación promueve la seguridad, la equidad, la protección de datos, la transparencia y el derecho de los ciudadanos a decidir si desean o no interactuar con IA en ciertos entornos. Además, EE.UU. ha implementado otras iniciativas regulatorias, como el Plan Nacional de Investigación y Desarrollo de IA, el Marco de Gestión de Riesgos del Instituto Nacional de Estándares y Tecnología (NIST) y diversas directrices de la Oficina de Protección Financiera del Consumidor, enfocadas en evitar la discriminación en decisiones automatizadas y garantizar un uso ético de la IA en el sector financiero y comercia (Sentencia T-323 del 2024, 2024)l.

Finalmente, en esta sentencia se reafirma que la inteligencia artificial no puede sustituir el razonamiento humano del juez, ya que esto vulneraría el debido proceso y la independencia judicial. No obstante, su uso en tareas administrativas y de apoyo es válido siempre que se garantice la transparencia, la supervisión humana y la privacidad de los datos. La Corte insta al Consejo Superior de la Judicatura a establecer lineamientos claros para el uso de IA en la

Rama Judicial, asegurando que su implementación no comprometa la imparcialidad ni la autonomía de los jueces. Además, destaca la importancia de mecanismos de autorregulación y evaluación ética, en línea con principios internacionales que buscan un uso responsable de estas tecnologías (Sentencia T-323 del 2024, 2024).

Si bien la digitalización de la justicia avanza, aún persisten desafíos en la regulación de la IA en Colombia. La evolución tecnológica plantea interrogantes sobre la garantía del debido proceso y el control judicial en un contexto de creciente automatización. Por lo que, la modernización del sistema judicial debe equilibrar la eficiencia tecnológica con la protección de derechos fundamentales, evitando que la IA comprometa la seguridad jurídica y el principio del juez natural en la administración de justicia (Sentencia T-323 del 2024, 2024).

Las sentencias T-372 de 2023 y T-323 de 2024 reflejan la intersección entre derechos fundamentales y avances tecnológicos, evidenciando los desafíos jurídicos que surgen en la era digital. La primera enfatiza la importancia del acceso a internet como un derecho esencial para la libertad de expresión y la participación democrática, mientras que la segunda plantea los límites de la inteligencia artificial en la administración de justicia, estableciendo que esta debe ser una herramienta de apoyo y no un sustituto del juicio humano. Ambas decisiones revelan la necesidad de marcos normativos claros que regulen el uso de la tecnología sin menoscabar derechos fundamentales. En un contexto donde la digitalización avanza a un ritmo acelerado, el desafío radica en encontrar un equilibrio entre la innovación y la protección de garantías esenciales, asegurando que el progreso tecnológico no se convierta en un mecanismo de restricción de libertades o en una amenaza a la autonomía judicial.

La libertad de expresión digital en Colombia enfrenta una protección insuficiente frente a fenómenos como la desinformación masiva, la censura privada ejercida por plataformas y la interrupción arbitraria de servicios de internet, especialmente en contextos de protesta social. Aunque la Corte Constitucional ha avanzado con fallos como la T-372 de 2023, que reconoció el acceso a internet como derecho fundamental, y la T-323 de 2024, que reguló el uso de inteligencia artificial en la función judicial, la respuesta normativa sigue siendo reactiva y casuística. No existe un marco legal integral que regule la moderación de contenidos digitales, garantice la neutralidad de la red y asegure transparencia en los algoritmos que impactan la circulación de ideas. Sin una ley marco de constitucionalismo digital con enfoque preventivo y garantista, la defensa de la libertad de expresión seguirá dependiendo de decisiones judiciales

ex post, manteniendo a los ciudadanos vulnerables ante riesgos tecnológicos y decisiones discrecionales de actores privados.

c) Derecho al Acceso Igualitario a la Información

En Colombia, actualmente no existe un reconocimiento expreso del derecho al acceso igualitario a la información en la legislación, lo que ha perpetuado desigualdades significativas en el acceso a recursos digitales esenciales. Esta omisión afecta especialmente a las comunidades rurales, a las personas con discapacidad y a los sectores más vulnerables, que enfrentan barreras para conectarse, acceder a contenidos educativos, culturales y gubernamentales, y participar plenamente en la sociedad digital. Por ello, se propone establecer este derecho como una prioridad nacional, promoviendo su incorporación en el marco normativo para garantizar igualdad de oportunidades en el entorno digital (Naciones Unidas, 2025).

El derecho al acceso igualitario a la información es un principio fundamental que exige garantizar que todas las personas, sin importar su estatus social, ubicación geográfica o capacidades, puedan acceder a la información en línea de manera equitativa. Este derecho está vinculado a valores esenciales como la igualdad, la inclusión y la libertad de expresión, lo que requiere esfuerzos conjuntos entre los sectores público y privado para superar barreras como la brecha digital, la falta de alfabetización tecnológica y las restricciones arbitrarias de acceso. De acuerdo con la UNESCO es necesario promover políticas públicas que aseguren la conectividad universal, incluyendo la accesibilidad de los contenidos digitales para personas con discapacidad, y proteger el derecho a la información frente a censuras injustificadas (Unesco, 2025).

Los Estados tienen la obligación de implementar políticas públicas que aseguren la conectividad universal y asequible, promover la accesibilidad de los contenidos digitales para personas con discapacidad y proteger el derecho a la información frente a censuras injustificadas (Castells, 2011). Por su parte, el sector privado debe garantizar la neutralidad de la red, desarrollar tecnologías inclusivas y asequibles, y colaborar activamente en iniciativas para reducir las desigualdades digitales, proporcionando herramientas que permitan el acceso a recursos clave como educación, salud y servicios gubernamentales en línea (ITUPublications, 2025).

El acceso igualitario a la información no solo es un derecho humano fundamental, sino también un motor de progreso social y económico. Igualmente, el sector público como el privado deben colaborar de manera coordinada para crear un entorno digital inclusivo, en el que todas las personas puedan participar plenamente. Garantizar este acceso significa cerrar brechas, empoderar comunidades vulnerables y promover una sociedad más justa y democrática, preparada para afrontar los desafíos del siglo XXI (Asamblea General de las Naciones Unidas, 2025).

Es por ello, que se requiere que en Colombia con la digitalización se ofrezca un acceso sin precedentes a la información, pero también ha generado brechas digitales que podrían dejar fuera a grupos vulnerables de la sociedad, como las personas en zonas rurales o con bajos recursos. El derecho al acceso a la información es esencial para el ejercicio de otros derechos, y en el contexto digital, debe garantizarse que todos los ciudadanos puedan acceder a recursos informativos de manera equitativa. La implementación de políticas de inclusión digital se vuelve crucial para cerrar estas brechas y permitir una participación activa en la sociedad de la información.

Como conclusión, es urgente que Colombia adopte una legislación que reconozca de manera expresa el derecho al acceso igualitario a la información, un derecho fundamental que debe ser considerado dentro de la nueva era digital. A pesar de los avances en tecnología, el país sigue enfrentando desigualdades en el acceso a recursos digitales esenciales, lo que afecta particularmente a las comunidades rurales, a las personas con discapacidad y a los sectores más vulnerables. La creación de una ley que contemple este derecho garantizaría la igualdad de oportunidades, promoviendo la conectividad universal, el acceso sin barreras a contenidos educativos, culturales y gubernamentales, y la presencia plena de la ciudadanía en la sociedad digital. Solo a través de la colaboración efectiva entre los sectores público y privado, así como políticas públicas inclusivas, se podrá cerrar la brecha digital y asegurar que todos los colombianos puedan ejercer sus derechos fundamentales en el entorno digital, aportando al avance social y económico del país.

En Colombia, el derecho al acceso igualitario a la información está reconocido en el marco normativo de la Ley de Transparencia y Acceso a la Información Pública (Ley 1712 de 2014), cuyo objetivo es garantizar que todos los ciudadanos puedan acceder a información pública sin discriminación. Sin embargo, a la fecha no existe una discusión jurídica o jurisprudencial específica que desarrolle este derecho desde una perspectiva de igualdad en el

acceso, ni un marco normativo que aborde de manera diferenciada las barreras que ciertos grupos pueden enfrentar. En contraste, en España, la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno establece principios que buscan garantizar un acceso equitativo a la información, con especial atención a colectivos vulnerables. En México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha promovido criterios para asegurar que el acceso a la información sea inclusivo, considerando factores como accesibilidad para personas con discapacidad y la disponibilidad de información en lenguas indígenas. Por su parte, el Tribunal Europeo de Derechos Humanos (TEDH) ha desarrollado una línea jurisprudencial en la que vincula el acceso a la información con la libertad de expresión, destacando que cualquier restricción debe ser proporcional, justificada y no discriminatoria. Este desarrollo internacional pone en evidencia la necesidad de que en Colombia se inicie una discusión más profunda sobre el acceso igualitario a la información, asegurando que toda la ciudadanía, sin importar sus circunstancias sociales, físicas o económicas, puedan ejercer este derecho en igualdad de condiciones.

La brecha digital en Colombia sigue siendo un obstáculo estructural que profundiza la desigualdad social y limita el ejercicio efectivo de derechos fundamentales como la educación, la participación democrática y la libertad de expresión. A pesar de la Ley 1712 de 2014 sobre acceso a la información pública, el país carece de un reconocimiento expreso del acceso igualitario a la información digital como derecho fundamental, así como de políticas robustas de inclusión tecnológica que garanticen conectividad universal, accesibilidad para personas con discapacidad y reducción de las brechas urbano-rurales. Esta omisión mantiene a comunidades vulnerables excluidas de la sociedad digital, generando una inequidad estructural incompatible con los estándares de la ONU y la UNESCO. La adopción de una ley marco de constitucionalismo digital, que incorpore la inclusión digital como principio rector, es indispensable para cerrar estas brechas y garantizar que ningún ciudadano quede al margen de la sociedad de la información.

d) Derecho a la Seguridad en Línea

En Colombia, aunque existen esfuerzos aislados para regular la seguridad digital, actualmente no existe un marco jurídico que reconozca de manera expresa el derecho a la seguridad en línea. La legislación nacional se ha centrado principalmente en la protección de datos personales y la prevención de delitos informáticos.

La Ley 1581 de 2012 sobre la protección de datos personales y la Ley 1273 de 2009, que tipifica delitos informáticos, han sido pasos importantes en la salvaguarda de los datos en el ámbito digital. Sin embargo, estos esfuerzos no abordan de manera integral la seguridad en línea como un derecho fundamental, lo que deja a los ciudadanos vulnerables frente a riesgos como el robo de identidad, el fraude cibernético o los ataques informáticos, sin una base jurídica sólida para exigir su protección (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023).

La falta de un marco normativo explícito que reconozca el derecho a la seguridad en línea implica que la respuesta ante las amenazas digitales sea fragmentada, centrada en sanciones, pero sin estrategias preventivas claras para proteger a los usuarios. En este contexto, es urgente que Colombia implemente una ley de ciberseguridad que no solo regule los delitos informáticos, sino que también establezca una política de protección integral para la seguridad digital. Esto incluiría medidas para garantizar la seguridad de los usuarios frente a ciberataques, el robo de datos y el fraude en línea, así como mecanismos de reparación en caso de ser víctimas de dichos delitos. Según la UNESCO, una legislación clara sobre la seguridad en línea garantizaría la preservación efectiva de los derechos digitales de las personas, promoviendo un entorno de confianza y acceso seguro a la información (Unesco, 2025).

Además, es crucial que se fomente la cooperación internacional en materia de ciberseguridad, ya que las amenazas digitales suelen no respetar fronteras. La participación activa de Colombia en acuerdos internacionales, como la Convención de Budapest sobre delitos informáticos, es fundamental para fortalecer la respuesta global ante el crimen cibernético. De igual forma, el sector privado juega un rol esencial en garantizar la seguridad en línea, desarrollando tecnologías de protección robustas y promoviendo la educación digital de los usuarios. Como señala Castells, la seguridad en línea debe ser considerada como un derecho fundamental que debe ser garantizado a través de la colaboración entre los sectores público, privado e internacional, creando un entorno digital seguro y confiable para todos (Castells, 2011).

Es fundamental que Colombia avance hacia el reconocimiento explícito del derecho a la seguridad en línea mediante la creación de una ley robusta que proteja a los ciudadanos de los riesgos y amenazas del entorno digital. La seguridad en línea no solo es esencial para proteger los datos personales y la integridad de los usuarios, sino también para garantizar la confianza en el uso de la tecnología y la participación de los ciudadanos en la sociedad digital.

Una legislación clara y efectiva en este ámbito permitirá fortalecer la infraestructura de ciberseguridad, promover la educación digital y fomentar una colaboración más efectiva entre el sector público, privado e internacional. El establecimiento de este derecho como parte del marco jurídico colombiano contribuirá a cerrar las brechas de seguridad existentes y asegurará que todos los ciudadanos, independientemente de su condición o ubicación, puedan disfrutar de un entorno digital seguro y libre de riesgos.

El derecho a la seguridad en línea es un tema de creciente relevancia en el ámbito jurídico, aunque su fundamentación teórica y jurisprudencial aún se encuentra en desarrollo. Doctrinariamente, se ha abordado en el contexto de la protección de datos personales y la ciberseguridad. Por ejemplo, la Ley Orgánica 3/2018 de España, en su artículo 82, reconoce el "derecho a la seguridad digital", enfatizando la protección de los datos personales en entornos digitales (Bes, 2025).

En el ámbito internacional, informes como "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta" destacan la interrelación entre la seguridad digital y los derechos humanos, subrayando la importancia de políticas que protejan la privacidad y la libertad de expresión en línea (Sequera & Amalia Toledo, 2018). Jurisprudencialmente, aunque aún es limitado, se han comenzado a sentar precedentes. Por ejemplo, el Tribunal Europeo de Derechos Humanos ha abordado casos relacionados con la seguridad en línea, estableciendo criterios sobre la responsabilidad de los Estados en la protección de los derechos digitales de los ciudadanos (Tribunal Europeo de Derechos Humanos, 2022). A pesar de estos avances, la fundamentación teórica y jurídica del derecho a la seguridad en línea sigue siendo incipiente, lo que evidencia la necesidad de un desarrollo más profundo en este ámbito.

En Colombia, el derecho a la seguridad en línea ha sido objeto de desarrollo normativo y jurisprudencial en los últimos años. La Ley 1273 de 2009 introdujo el delito de "acceso abusivo a un sistema informático", sancionando el ingreso no autorizado a sistemas informáticos protegidos. La Corte Suprema de Justicia, en la Sentencia SP 592 de 2022, analizó y detalló los elementos constitutivos de este delito, estableciendo criterios para su aplicación en el ordenamiento jurídico colombiano (Pérez, 2022).

En el ámbito de la ciberseguridad, el Decreto 338 de 2022 establece lineamientos para fortalecer la gobernanza de la seguridad digital, la gestión de riesgos y la identificación de infraestructuras críticas cibernéticas y servicios esenciales. Este decreto enfatiza la importancia

de proteger los derechos humanos y la libre competencia económica en el entorno digital. Además, la Corte Constitucional ha abordado temas relacionados con la seguridad en línea. En la Sentencia T-372 de 2023, la Corte determinó que la interrupción injustificada del servicio de internet vulnera derechos fundamentales como la libertad de expresión, de asociación y de reunión en el contexto de la protesta social (Sentencia T-372 del 2023, 2023).

Estas normativas y decisiones jurisprudenciales reflejan el compromiso de Colombia en fortalecer la seguridad en línea y proteger los derechos de los usuarios en el entorno digital. El reconocimiento del derecho a la seguridad en línea es un desafío jurídico en evolución que requiere un enfoque integral para su consolidación. Si bien en países como España y México se han adoptado regulaciones específicas para proteger a los ciudadanos en el entorno digital, en Colombia aún no existe un marco normativo robusto que garantice este derecho de manera expresa. La legislación vigente se centra en la tipificación de delitos informáticos y la protección de datos personales, dejando vacíos en la prevención de amenazas cibernéticas y en la garantía efectiva de la seguridad digital como un derecho fundamental. La ausencia de un desarrollo teórico y jurisprudencial sólido evidencia la necesidad de fortalecer la discusión académica y legislativa en torno a este tema.

Por otra parte, la experiencia internacional, en particular los precedentes del Tribunal Europeo de Derechos Humanos, demuestra la importancia de contar con mecanismos jurídicos adecuados para la protección de los derechos digitales. En este sentido, es fundamental que Colombia avance en la formulación de políticas públicas y normativas que no solo castiguen los delitos informáticos, sino que también implementen estrategias preventivas, fomenten la cooperación internacional y garanticen un entorno digital seguro para todos los ciudadanos.

La seguridad digital en Colombia sigue siendo fragmentada y predominantemente reactiva, incluso tras la expedición de la Ley 2502 de 2025, que incorporó agravantes penales frente a la suplantación de identidad mediante inteligencia artificial (deepfakes) y ordenó la formulación de políticas de ciberseguridad y cooperación interinstitucional. Pese a este avance, la normativa vigente —junto con la Ley 1273 de 2009 y el Decreto 338 de 2022— no configura un derecho fundamental explícito a la seguridad en línea ni establece un sistema nacional preventivo capaz de anticipar riesgos derivados de IA, metaverso, big data y ataques transnacionales. La protección ciudadana frente a fraudes, hackeos y robo de identidad sigue dependiendo de sanciones penales posteriores, mientras la confianza en el ecosistema digital permanece frágil. Resulta indispensable que una ley marco de constitucionalismo digital eleve

la seguridad en línea a garantía constitucional y articule una estrategia integral de prevención, supervisión tecnológica y cooperación internacional, superando el enfoque reactivo y mediático de la legislación actual.

e) Protección Frente a la Ciberdelincuencia y la Vigilancia No Autorizada

La ciberdelincuencia es una amenaza creciente que afecta la privacidad, la propiedad intelectual y la seguridad de los usuarios en el entorno digital. La protección frente a la ciberdelincuencia y la vigilancia no autorizada es un derecho que debe ser protegido por el Estado, asegurando que las tecnologías utilizadas para la seguridad no vulneren derechos fundamentales, como la privacidad o la libertad personal. La incorporación de tecnologías emergentes como la inteligencia artificial y el reconocimiento facial plantea nuevos desafíos relacionados con la vigilancia masiva y la protección de los datos personales de los ciudadanos.

A nivel internacional, la ciberdelincuencia y la vigilancia no autorizada se han convertido en amenazas significativas para los derechos humanos, la seguridad nacional y la integridad de los sistemas digitales. La Convención de Budapest sobre delitos cibernéticos, adoptada en 2001 bajo el marco del Consejo de Europa, establece principios fundamentales para la cooperación internacional en la lucha contra el crimen informático, con énfasis en la protección de la confidencialidad y protección en el entorno digital. Esta convención, además, promueve el acceso a la justicia y la cooperación transfronteriza entre los países para enfrentar los delitos informáticos, que no conocen fronteras. En su artículo 2, se abordan delitos como el acceso no autorizado a sistemas informáticos y la vigilancia sin consentimiento, destacando la importancia de la legislación nacional para sancionar estos actos con severidad. A nivel internacional, la ciberdelincuencia y la vigilancia no autorizada se perciben como violaciones graves de la privacidad, la libertad de expresión y la integridad de los sistemas de información, lo que ha motivado la creación de políticas para su prevención y sanción (Consejo de Europa, 2001).

En Colombia, la protección frente a la ciberdelincuencia y la vigilancia no autorizada es aún un desafío significativo. A pesar de la existencia de leyes como la Ley 1273 de 2009, que tipifica los delitos informáticos, y la Ley 1581 de 2012, que regula la protección de datos personales, no existe una legislación integral que aborde de manera clara y específica la protección frente a estas amenazas digitales. La falta de un derecho expreso de protección frente a la ciberdelincuencia y la vigilancia no autorizada en el marco jurídico colombiano deja a los ciudadanos vulnerables frente a delitos como el hurto de datos personales, la coacción

cibernética y la invasión de la intimidad. A pesar de estos avances normativos, la insuficiencia de un enfoque claro y robusto sobre la protección contra la ciberdelincuencia genera vacíos legales que dificultan una respuesta efectiva frente a estos crímenes. Los mecanismos legales existentes son fragmentados y no se ajustan a la evolución constante de las amenazas digitales, lo que ha generado una percepción de impunidad en la ciberdelincuencia y la violación de la privacidad en línea (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025)

En este contexto, es urgente que Colombia adopte una legislación más específica y rigurosa para sancionar la ciberdelincuencia y la vigilancia no autorizada. Esta legislación debe contemplar no solo sanciones penales, sino también sanciones administrativas, como multas y sanciones pecuniarias, para garantizar una respuesta integral ante estos delitos. La implementación de una ley que regule estos aspectos permitirá que los ciudadanos cuenten con un marco jurídico de protección frente a la invasión de su privacidad y el uso indebido de sus datos. Además, la sanción de estos delitos no solo debe ser punitiva, sino también preventiva, mediante la creación de campañas de concienciación y la promoción de buenas prácticas en el entorno digital. Como señala las organizaciones internacionales, los gobiernos deben adoptar políticas de protección en línea que prioricen la seguridad de la información personal y ofrezcan garantías claras sobre la vigilancia y el acceso no autorizado a los sistemas. De esta manera, Colombia podrá fortalecer la confianza en el entorno digital, proteger a sus ciudadanos frente a los riesgos del ciberespacio y garantizar el cumplimiento de los derechos fundamentales en el contexto digital.

En conclusión, la protección frente a la ciberdelincuencia y la vigilancia no autorizada es un área crítica que requiere una respuesta jurídica integral en Colombia. A pesar de los esfuerzos normativos existentes, la falta de un marco claro y actualizado en conjunto con la ciberdelincuencia y la prevalencia de la intimidad en línea deja al país vulnerable ante los constantes avances tecnológicos y las amenazas digitales. La implementación de una legislación robusta que contemple sanciones penales y administrativas es esencial para garantizar la seguridad de los ciudadanos y fortalecer la confianza en el entorno digital. Sin embargo, este desafío se presenta dentro de un contexto más amplio de transformación digital, donde el constitucionalismo digital se enfrenta a nuevos retos. La adaptación de la Constitución y el marco normativo colombiano a las demandas de la era digital, garantizando derechos fundamentales como el acceso a la información, la privacidad y la seguridad en línea, será fundamental para asegurar un equilibrio entre los avances tecnológicos y la protección de los

derechos humanos en el ciberespacio. Este panorama exige un debate continuo sobre cómo modernizar las leyes y garantizar que el marco jurídico colombiano sea lo suficientemente flexible y eficiente para enfrentar los desafíos del constitucionalismo digital en el futuro.

En el ámbito de la ciberseguridad y la lucha contra los delitos informáticos, distintos países han avanzado en la adecuación de sus normativas conforme a estándares internacionales como el Convenio de Budapest. Este convenio, promovido por el Consejo de Europa, busca armonizar las legislaciones nacionales y fortalecer la cooperación internacional en la investigación y persecución del cibercrimen. España, Argentina, Uruguay y Colombia han seguido diferentes caminos en su implementación, reflejando tanto avances significativos como desafíos pendientes. A continuación, se presenta un cuadro comparativo que analiza el desarrollo normativo de cada país en relación con la tipificación de delitos informáticos, la adopción de mecanismos procesales y su grado de compromiso con el Convenio de Budapest.

Tabla 16. Evolución de normas en algunos países

NOMBRE DE PAÍS	EVOLUCIÓN NORMATIVO
España	En 2015, España reformó su normativa penal con dos leyes clave: la Ley Orgánica 13/2015, que reguló medidas de investigación tecnológica y fortaleció garantías procesales, y la Ley 41/2015, orientada a agilizar la justicia penal. Estas normas establecieron el uso de herramientas como agentes encubiertos informáticos, interceptación de comunicaciones y registros remotos en dispositivos electrónicos. España firmó el Convenio de Budapest en 2001 y lo promulgó en 2010 sin reservas, asegurando su incorporación plena en su legislación. Actualmente, se estudia una reforma procesal más profunda para modernizar el sistema judicial.
Argentina	Desde el 2000. se cuenta con una regulación avanzada en protección de datos y desde que se adaptó su legislación al Convenio de Budapest con la Ley 26.388 en 2008, que incorporó delitos informáticos como el acceso ilícito a datos, la interrupción de comunicaciones y el grooming (con la Ley 26.904 en 2013). Sin embargo, su sistema procesal varía

	por ser un Estado Federal. En 2017, el país ratificó el Convenio con reservas en materia de posesión de pornografía infantil, jurisdicción penal internacional y cooperación en investigaciones transnacionales. A pesar de esto, Argentina no ha implementado una adecuación normativa unificada y mantiene proyectos de ley pendientes para fortalecer la regulación del cibercrimen.
Uruguay	Tiene una legislación limitada en ciberdelincuencia, con excepción de delitos como el contacto con menores con intenciones delictivas (artículo 277 bis del Código Penal). En 2017, reformó su Código Procesal Penal, introduciendo normas sobre la interceptación de comunicaciones electrónicas. Sin embargo, el país no ha adherido al Convenio de Budapest ni tiene en trámite su implementación.
Colombia	Regula los delitos informáticos desde 2009 con la Ley 1273, protegiendo la información y los datos. Su Código de Procedimiento Penal permite la recuperación de información de dispositivos electrónicos, y el decreto 1704 de 2012 obliga a los proveedores de internet a colaborar con la Fiscalía. En 2013, Colombia inició el proceso de adhesión al Convenio de Budapest, y en 2018 se aprobó la Ley 1928 de incorporación. No obstante, el ingreso formal aún no se ha concretado. Existen reservas sobre la aplicación de medidas de obtención en tiempo real de datos, pero sin especificar a qué delitos aplica. Actualmente, hay proyectos de ley en trámite para fortalecer la ciberseguridad, incluyendo sanciones por sexting y uso de software malicioso.

Nota. Elaboración propia (2025).

España es el país con mayor avance en la implementación del Convenio, mientras que Argentina y Colombia han ratificado el tratado, pero sin una adecuación total de su legislación. Uruguay aún no ha iniciado el proceso de adhesión. La implementación efectiva del Convenio sigue siendo un desafío en Latinoamérica, donde la modernización de la normativa avanza lentamente en comparación con Europa.

La ciberdelincuencia y la vigilancia digital no autorizada constituyen amenazas directas a la privacidad, la libertad y la seguridad ciudadana, y la respuesta del Estado colombiano sigue siendo insuficiente y fragmentada frente a los riesgos de la era digital. Si bien existen la Ley 1273 de 2009 (delitos informáticos), la Ley 1581 de 2012 (protección de datos personales) y la Ley 2502 de 2025, que introdujo agravantes penales para la suplantación digital mediante inteligencia artificial (deepfakes) tras casos mediáticos de artistas y figuras públicas, estas normas son reactivas y de alcance limitado, sin conformar un régimen integral de prevención, sanción y supervisión tecnológica. Además, la adhesión parcial al Convenio de Budapest mantiene brechas en cooperación internacional, lo que favorece la impunidad en delitos transnacionales y prácticas de vigilancia masiva. Esta situación deja a los ciudadanos vulnerables frente a riesgos complejos y demuestra la urgencia de una ley marco de constitucionalismo digital, que articule prevención, sanción penal y administrativa, control estricto de tecnologías invasivas y cooperación internacional efectiva, garantizando así la seguridad jurídica y la vigencia plena de los derechos fundamentales en el ciberespacio.

5.2. Diagnóstico crítico del impacto de la digitalización en los derechos fundamentales.

La Quinta Revolución Industrial ha transformado radicalmente la interacción entre los ciudadanos, el Estado y los actores privados. Tecnologías como la inteligencia artificial (IA), el big data, el metaverso y la automatización algorítmica han generado oportunidades inéditas para el acceso a la información, la participación social y la eficiencia de los servicios públicos. Sin embargo, estos avances también han creado nuevos escenarios de vulnerabilidad para los derechos fundamentales, frente a los cuales el marco normativo colombiano sigue siendo insuficiente y fragmentado.

Pese a contar con normas como la Ley 1581 de 2012 (protección de datos personales), la Ley 1273 de 2009 (delitos informáticos) y la Ley 2502 de 2025 (suplantación digital y deepfakes), así como una jurisprudencia constitucional creciente, el país carece de una regulación integral que articule prevención, supervisión tecnológica y protección efectiva de los derechos digitales. La respuesta sigue siendo reactiva, apoyada en acciones de tutela y sanciones ex post, mientras los riesgos digitales evolucionan con rapidez.

A continuación, se presentan los derechos fundamentales más impactados por la digitalización, con su análisis crítico:

a) Privacidad y protección de datos personales

El derecho a la privacidad y la protección de datos personales ha sido uno de los más afectados por la digitalización. Si bien la Ley 1581 de 2012 estableció el marco de protección del habeas data, esta norma no cubre adecuadamente los desafíos del tratamiento masivo y transnacional de datos en entornos de IA, big data y metaverso.

La jurisprudencia de la Corte Constitucional ha fijado límites importantes frente a la divulgación de información personal en redes sociales y ha reconocido el derecho al olvido y la responsabilidad de los administradores de plataformas digitales (T-453/2024, T-289/2023). Sin embargo, no se ha pronunciado de manera directa sobre los riesgos complejos que implican tecnologías emergentes como la IA generativa, el seguimiento biométrico y los sistemas predictivos.

La protección de la privacidad sigue siendo formal y reactiva. La falta de consentimiento informado reforzado, de mecanismos de supervisión transnacional y de una ley marco de derechos digitales deja a los ciudadanos sin control efectivo sobre sus datos personales, mientras la explotación tecnológica avanza sin límites claros.

b) Libertad de expresión y acceso a la información en línea

La digitalización ha potenciado la difusión de ideas y el acceso a la información, pero también ha generado riesgos inéditos. Las plataformas internacionales operan con políticas de moderación opacas, aplicando bloqueos o eliminando contenidos sin control jurídico local, lo que vulnera la libertad de expresión y el derecho a la información.

Si bien la Corte Constitucional ha reconocido el acceso a internet como derecho fundamental (T-372/2023) y ha limitado el uso de IA en decisiones judiciales (T-323/2024), aún no existe un marco normativo integral que garantice neutralidad de red, transparencia algorítmica y supervisión estatal eficaz.

La defensa de la libertad de expresión y el acceso a la información en Colombia depende de decisiones judiciales aisladas. Sin una ley marco de constitucionalismo digital que regule contenidos, garantice debido proceso digital y obligue a las plataformas a respetar estándares constitucionales, los ciudadanos seguirán vulnerables ante censura privada y desinformación masiva.

c) Igualdad y no discriminación en el entorno digital

La brecha digital en Colombia perpetúa desigualdades estructurales entre zonas urbanas y rurales, y entre grupos socioeconómicos, limitando el acceso a educación, participación política y servicios públicos digitales.

A esto se suma la discriminación algorítmica, derivada de sistemas de IA entrenados con sesgos raciales, de género o socioeconómicos, que pueden excluir o estigmatizar a poblaciones vulnerables. Las plataformas internacionales no siempre adaptan sus algoritmos al contexto cultural y jurídico colombiano, amplificando desigualdades existentes.

La igualdad digital sigue siendo una promesa no cumplida. Sin políticas robustas de inclusión digital, supervisión de algoritmos y garantía de accesibilidad universal, la sociedad colombiana seguirá enfrentando discriminaciones invisibles en la era digital. Una ley marco de constitucionalismo digital debe reconocer el acceso igualitario y la protección frente a la discriminación algorítmica como derechos fundamentales.

5.3. Retos y desafíos del constitucionalismo digital en Colombia

La digitalización ha transformado de manera profunda la vida social, económica y política en Colombia, impactando la forma en que los ciudadanos interactúan con el Estado, las empresas y entre sí. La quinta revolución industrial, impulsada por tecnologías como la inteligencia artificial (IA), el big data, el metaverso, el blockchain y la automatización algorítmica, ha creado nuevas oportunidades para el desarrollo económico y la inclusión social. Sin embargo, también ha generado retos significativos para el constitucionalismo digital, ya que la protección de los derechos fundamentales no avanza al mismo ritmo que la innovación tecnológica.

Pese a contar con normas como la Ley 1581 de 2012 (protección de datos personales), la Ley 1273 de 2009 (delitos informáticos) y la Ley 2502 de 2025 (suplantación digital y deepfakes), así como diversas políticas públicas de conectividad, la respuesta estatal sigue siendo fragmentada, lenta y reactiva, dejando a los ciudadanos vulnerables frente a riesgos crecientes. Estos desafíos estructurales requieren soluciones inmediatas y efectivas para garantizar una digitalización inclusiva, equitativa y segura.

A continuación, se presentan los cuatro principales retos del constitucionalismo digital en Colombia, que fundamentan la necesidad de un marco normativo integral.

1. Brecha digital y desigualdad en el acceso a TIC

A pesar de los esfuerzos realizados mediante programas como Plan Vive Digital y la expansión de internet en zonas rurales, la brecha digital persiste, afectando principalmente a comunidades rurales, indígenas y personas con discapacidad. La falta de acceso a infraestructura tecnológica y dispositivos adecuados impide que amplios sectores de la población participen plenamente en la economía digital, la educación virtual y la vida democrática en línea.

La exclusión digital perpetúa desigualdades históricas y convierte la ciudadanía digital en un privilegio. Sin políticas robustas de inclusión tecnológica, que combinen conectividad universal, alfabetización digital y accesibilidad para poblaciones vulnerables, el principio de igualdad material en la era digital seguirá siendo una promesa vacía.

2. Regulación insuficiente de tecnologías emergentes (IA, big data, blockchain**)**

El desarrollo acelerado de IA, big data, blockchain y automatización ha abierto oportunidades sin precedentes en la economía y los servicios públicos, pero también ha traído riesgos éticos y jurídicos. La IA plantea dilemas sobre privacidad, sesgos algorítmicos y autonomía humana; el big data sobre vigilancia masiva y explotación comercial de datos; y el blockchain sobre trazabilidad y seguridad de la información.

En Colombia, la legislación vigente no regula de manera específica estas tecnologías. Incluso la Ley 2502 de 2025, aunque relevante frente a la suplantación digital mediante deepfakes, sigue siendo una respuesta parcial y reactiva, sin contemplar mecanismos preventivos, de supervisión y rendición de cuentas frente a riesgos sistémicos.

Mientras Colombia legisle solo como reacción a casos mediáticos, la protección de los ciudadanos seguirá siendo limitada. El país necesita un marco normativo proactivo, que garantice el uso ético y responsable de las tecnologías emergentes, incorporando supervisión algorítmica, transparencia y responsabilidad empresarial y estatal.

3. Protección débil de la privacidad y la seguridad digital

El entorno digital expone a los ciudadanos a filtraciones de datos, ciberataques, vigilancia no autorizada y uso indebido de información personal por empresas nacionales e internacionales. Si bien existen la Ley 1581 de 2012 y la Ley 1266 de 2008 sobre manejo de datos financieros, así como normas penales como la Ley 1273 de 2009, los mecanismos de control y sanción siguen siendo insuficientes frente a los riesgos del mundo digital.

La protección de la privacidad y la seguridad digital en Colombia es débil y reactiva. Mientras la seguridad digital no sea reconocida como derecho fundamental explícito y no exista un sistema integral de ciberseguridad con cooperación internacional, los ciudadanos permanecerán vulnerables ante ciberdelitos, hackeos y vigilancia masiva, debilitando la confianza en el ecosistema digital.

4. Fortalecimiento institucional y gobernanza digital

Un constitucionalismo digital efectivo requiere instituciones sólidas capaces de implementar políticas públicas y supervisar el cumplimiento normativo. Actualmente, entidades como la Superintendencia de Industria y Comercio (SIC) y la Agencia Nacional del Espectro (ANE) carecen de recursos suficientes y de personal especializado para enfrentar los retos tecnológicos.

Además, existe falta de articulación entre el Estado, las plataformas digitales y la sociedad civil, lo que retrasa la implementación de estrategias coordinadas de protección de derechos en línea.

Sin fortalecimiento institucional y gobernanza digital preventiva, el Estado seguirá actuando de manera lenta y reactiva. Es indispensable crear una autoridad nacional de supervisión digital e inteligencia artificial, dotada de recursos tecnológicos y capacidades de cooperación internacional, para garantizar una protección integral y efectiva de los derechos fundamentales en el entorno digital.

Los desafíos descritos reflejan que el constitucionalismo digital colombiano enfrenta cuatro brechas estructurales: exclusión digital, regulación insuficiente, debilidad en privacidad y seguridad, y falta de gobernanza institucional. Mientras la respuesta estatal siga siendo fragmentada y tardía, los ciudadanos permanecerán expuestos a vulneraciones de sus derechos en la era digital. Estos retos justifican la creación de un marco normativo integral, que permita:

1. Cerrar la brecha digital y garantizar inclusión tecnológica.
2. Regular de forma proactiva las tecnologías emergentes.
3. Fortalecer la privacidad y la seguridad digital como derechos fundamentales.
4. Consolidar una gobernanza digital preventiva con capacidad real de supervisión.

Este diagnóstico de retos y desafíos sirve como base directa para la Propuesta de Ley de Constitucionalismo Digital en Colombia, desarrollada en el siguiente subcapítulo.

5.4.Propuesta de Ley de Constitucionalismo Digital en Colombia

El análisis realizado en los apartados anteriores evidencia que el constitucionalismo digital en Colombia enfrenta una protección fragmentada y reactiva frente a los retos de la quinta revolución industrial. La digitalización ha impactado derechos fundamentales como la privacidad, la libertad de expresión, la igualdad y la seguridad digital, mientras que la normativa vigente —Ley 1581 de 2012, Ley 1273 de 2009, Ley 1266 de 2008 y Ley 2502 de 2025— resulta insuficiente y tardía ante fenómenos como la IA generativa, el metaverso, el big data, la suplantación digital y los deepfakes.

En respuesta a este diagnóstico, se propone la Ley de Constitucionalismo Digital de Colombia, concebida como un marco normativo integral y preventivo, que reconozca derechos digitales por conexidad, establezca una gobernanza digital robusta y garantice mecanismos efectivos de protección y supervisión tecnológica.

5.4.1. Objeto y finalidad de la ley

El objeto de la Ley de Constitucionalismo Digital es garantizar la protección efectiva de los derechos fundamentales en el entorno digital colombiano, mediante el reconocimiento expreso de los derechos digitales por conexidad y la creación de un sistema integral de gobernanza tecnológica, que combine mecanismos preventivos, correctivos y de supervisión institucional.

Esta ley se concibe como el instrumento normativo central para transitar de un modelo reactivo, basado casi exclusivamente en la acción de tutela y en sanciones ex post, hacia un modelo preventivo y articulado, en el que Estado, sector privado y ciudadanía compartan responsabilidades para la protección y promoción de los derechos digitales.

La finalidad de esta ley se desarrolla en tres ejes estratégicos:

1. Fortalecer la seguridad jurídica y digital de los ciudadanos, estableciendo reglas claras sobre el tratamiento de datos personales, la supervisión de algoritmos, la neutralidad de la red y la prevención de ciberdelitos, garantizando que la innovación tecnológica se desarrolle dentro de un marco respetuoso de la Constitución.

2. Prevenir vulneraciones derivadas del uso de tecnologías emergentes, mediante la creación de mecanismos normativos y técnicos que anticipen riesgos en entornos como la inteligencia artificial, el metaverso, el big data, el blockchain y la automatización algorítmica, siguiendo estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y el AI Act 2024/1689.

3. Promover una digitalización inclusiva, equitativa y segura, reduciendo la brecha digital y garantizando que todas las personas, sin discriminación, tengan acceso real a los beneficios de la quinta revolución industrial, conforme a los principios de igualdad material, dignidad humana y participación ciudadana consagrados en la Constitución Política de 1991.

En suma, la ley busca armonizar el desarrollo tecnológico con la protección constitucional, generando un marco normativo robusto, preventivo y alineado con estándares internacionales, que permita a Colombia enfrentar los desafíos de la era digital con seguridad jurídica, confianza ciudadana y respeto pleno por los derechos fundamentales.

5.4.2. Principios rectores

La Ley de Constitucionalismo Digital se sustenta en un conjunto de principios rectores que orientan su interpretación, aplicación y supervisión, garantizando que el desarrollo tecnológico en Colombia se realice en armonía con la Constitución y los estándares internacionales de derechos humanos. Estos principios constituyen la base conceptual y normativa para la transición hacia un modelo preventivo de protección digital, en el que los derechos fundamentales se proyectan hacia el ciberespacio.

1. **Dignidad humana:** La dignidad humana es el núcleo axiológico de la Constitución (Art. 1 C.P.) y constituye el límite infranqueable para el uso de tecnologías digitales. Toda innovación, desde la inteligencia artificial hasta el metaverso, debe garantizar que la persona sea fin y no medio, evitando prácticas que cosifiquen, discriminen o vulneren su autonomía. Este principio conecta con la doctrina de Ferrajoli y Zagrebelsky, que destaca la centralidad de la persona frente al poder tecnológico y estatal.

2. **Privacidad y autodeterminación informativa:** Inspirado en el Art. 15 C.P. y en estándares como el GDPR europeo, este principio reconoce que los ciudadanos tienen el derecho a controlar sus datos personales y decidir sobre su uso en entornos digitales. La autodeterminación informativa implica que cualquier tratamiento de datos —incluyendo algoritmos, big data y monitoreo biométrico— debe ser consentido, informado y reversible, evitando prácticas de vigilancia masiva o explotación opaca de la información.

3. **Seguridad digital y prevención de riesgos:** El principio de seguridad digital obliga al Estado y a los actores privados a proteger la integridad de los sistemas tecnológicos y la información de los ciudadanos, garantizando un ecosistema digital confiable. Su dimensión preventiva requiere la anticipación de riesgos mediante políticas de ciberseguridad, protocolos de respuesta ante incidentes y cooperación internacional contra ciberdelitos, conforme a compromisos como el Convenio de Budapest.

4. **Transparencia y neutralidad tecnológica:** La transparencia asegura que los algoritmos, sistemas de IA y plataformas digitales operen bajo reglas claras, auditables y no discriminatorias, permitiendo la rendición de cuentas. La neutralidad tecnológica implica que las plataformas no pueden favorecer o censurar arbitrariamente contenidos lícitos, garantizando la libertad de expresión y el pluralismo informativo (Art. 20 C.P.). Este principio se inspira en experiencias comparadas como la Carta de Derechos Digitales de España (2021).

5. **Inclusión e igualdad digital:** La inclusión digital refleja la obligación estatal de cerrar la brecha tecnológica, asegurando que todas las personas, sin discriminación por origen social, económico, étnico o geográfico, accedan a las oportunidades de la sociedad digital. Conecta con el Art. 13 C.P. (igualdad material) y con los estándares de UNESCO y ONU sobre derecho universal a la conectividad, incorporando además la prevención de sesgos algorítmicos que puedan reproducir discriminaciones estructurales.

6. **Cooperación nacional e internacional:** El constitucionalismo digital requiere un enfoque transnacional, pues los riesgos digitales trascienden fronteras. Este principio obliga a:

    1. Coordinar acciones entre entidades nacionales (MinTIC, SIC, ANE, Fiscalía Cibernética).

2. Participar en mecanismos internacionales de persecución de ciberdelitos y armonización normativa.

3. Adoptar buenas prácticas globales como el AI Act de la UE y la LGPD de Brasil, garantizando que Colombia se inserte en la gobernanza digital mundial.

En conjunto, estos principios rectores no solo dan coherencia a la ley, sino que materializan la transición hacia un modelo preventivo de protección de derechos digitales, en el que la dignidad humana, la inclusión y la seguridad son el eje central de la gobernanza tecnológica en Colombia.

5.4.3. Reconocimiento y protección de los derechos digitales

El reconocimiento de los derechos digitales constituye el pilar central de la Ley de Constitucionalismo Digital propuesta en esta investigación. Dichos derechos representan la proyección y adaptación de los derechos fundamentales al ciberespacio, en un contexto donde la quinta revolución industrial ha trasladado la vida social, económica y política a entornos virtuales, interconectados y transnacionales.

La conexidad constitucional de estos derechos con garantías clásicas —como la intimidad personal y familiar, la libertad de expresión, la igualdad material, la propiedad privada y la inviolabilidad de las comunicaciones— permite que su protección sea inmediata a través de la acción de tutela, instrumento idóneo frente a vulneraciones digitales que evolucionan con mayor rapidez que la legislación tradicional. Con ello, se construye un bloque de constitucionalidad digital preventivo, que fortalece la eficacia y justiciabilidad de los derechos humanos en entornos digitales.

La presente propuesta reconoce dos bloques de derechos digitales, articulados de manera complementaria:

I. Derechos clásicos proyectados al ámbito digital, que actualizan el alcance de garantías constitucionales existentes frente a nuevos riesgos tecnológicos.

II. Derechos innovadores inéditos, creados en el marco de esta tesis doctoral, que responden a vacíos normativos globales y proyectan a Colombia como referente en protección avanzada de derechos digitales.

I. Derechos clásicos proyectados al ámbito digital

Estos derechos constituyen extensiones naturales de garantías fundamentales ya reconocidas, adaptadas al contexto tecnológico contemporáneo. Cada uno de ellos tiene vinculación directa con la Constitución Política de 1991 (Arts. 2, 13, 15, 20, 28 y 74) y permite la protección vía acción de tutela ante su vulneración.

1. Privacidad digital y protección de datos personales (habeas data digital)

Extiende la intimidad personal y familiar al ámbito digital, garantizando que cada individuo mantenga control pleno sobre la recolección, uso, almacenamiento y transferencia de sus datos personales en entornos tecnológicos como plataformas de IA, big data y metaverso. Su vulneración, por explotación indebida, suplantación digital, deepfakes o vigilancia no autorizada, habilita la tutela inmediata.

2. Libertad de expresión y acceso a la información en entornos digitales

Garantiza la difusión de ideas y el acceso a información sin censura algorítmica ni bloqueos arbitrarios de contenidos o cuentas, preservando la neutralidad de la red y la transparencia algorítmica. La tutela procede ante limitaciones desproporcionadas, tanto por actores privados como por autoridades.

3. Acceso igualitario a la información y a la inclusión digital

Reconoce el derecho a participar plenamente en la sociedad digital, con accesibilidad universal, alfabetización tecnológica y prevención de discriminación algorítmica. Su vulneración, especialmente en contextos de brecha digital estructural, afecta derechos conexos como educación, participación ciudadana y acceso a servicios públicos, habilitando tutela inmediata.

4. Seguridad digital y protección frente a ciberdelitos

Garantiza la integridad de los sistemas digitales y la información de los ciudadanos, protegiéndolos frente a fraudes, hackeos, suplantaciones de identidad, ciberacoso y filtraciones de datos. El Estado tiene la obligación de implementar estrategias preventivas y cooperación internacional. La tutela procede ante omisión estatal o negligencia de plataformas tecnológicas que comprometan la seguridad digital.

5. Protección frente a la vigilancia digital no autorizada

Asegura la inviolabilidad de las comunicaciones y actividades digitales, frente a interceptaciones, geolocalización o monitoreo masivo sin autorización judicial. Este derecho protege al ciudadano frente a vigilancia ilegítima ejercida tanto por el Estado como por plataformas privadas internacionales.

II. Derechos digitales innovadores propuestos por esta tesis

Estos derechos surgen como creación doctrinal original de esta tesis doctoral, con el objetivo de cubrir vacíos normativos internacionales y anticipar desafíos emergentes de la quinta revolución industrial. Su reconocimiento ubica a Colombia en una posición pionera dentro de la gobernanza digital.

1. Propiedad intelectual digital

Protege la titularidad moral y patrimonial de obras, software, contenidos digitales, desarrollos de IA y NFTs, frente a plagio, apropiación tecnológica o explotación comercial no autorizada. Garantiza que la economía creativa digital tenga plena protección jurídica.

2. Muerte digital y desconexión post-mortem

Reconoce el derecho de toda persona a definir el destino de sus datos, cuentas y perfiles digitales tras su fallecimiento, incluyendo su eliminación total, memorialización o transferencia de contenidos a herederos, como manifestación de la autodeterminación informativa post mortem.

3. Patrimonios digitales y bienes virtuales

Protege la titularidad, uso y transmisión de activos con valor económico real en entornos digitales, como criptomonedas, activos tokenizados, cuentas monetizadas y bienes en metaversos, asegurando que sean considerados propiedad patrimonial para efectos legales y sucesorales.

4. Sucesión digital

Reconoce que los bienes, contenidos y derechos digitales forman parte de la herencia del titular, permitiendo su transmisión a beneficiarios designados o herederos legales, cerrando la brecha normativa en materia de legado digital.

5. Reserva digital entre el usuario y la plataforma

Crea una esfera privada de confidencialidad digital entre el usuario y las plataformas, asegurando que su actividad, patrones de uso y datos no públicos no puedan ser divulgados, perfilados o cedidos a terceros sin consentimiento expreso, salvo orden judicial.

Todos los derechos digitales aquí reconocidos se consideran derechos fundamentales por conexidad, habilitando su protección inmediata mediante acción de tutela. Esta cláusula consolida un bloque de constitucionalidad digital preventivo, capaz de garantizar respuesta rápida, protección efectiva y armonización entre innovación tecnológica y derechos humanos, contribuyendo a la seguridad jurídica y a la confianza ciudadana en la sociedad digital.

5.4.4. Deberes de las plataformas digitales y los usuarios

La construcción de un constitucionalismo digital preventivo no puede limitarse al reconocimiento de derechos, sino que exige la definición clara de deberes y responsabilidades para todos los actores que participan en el ecosistema digital. En la quinta revolución industrial, caracterizada por la interconexión global, la inteligencia artificial, el big data, el metaverso y la economía de datos, la protección de los derechos digitales depende tanto de las acciones de las plataformas tecnológicas como del comportamiento responsable de los usuarios.

En este contexto, la Ley de Constitucionalismo Digital establece un marco de corresponsabilidad, que reconoce que garantizar la confianza en el ciberespacio es una tarea conjunta entre proveedores de servicios y ciudadanos digitales. Este enfoque busca materializar el principio preventivo del modelo propuesto en esta tesis: anticipar riesgos, generar condiciones de seguridad digital y consolidar una gobernanza tecnológica inclusiva y sostenible.

i. Deberes de las plataformas digitales y proveedores de servicios tecnológicos

Las plataformas digitales y los proveedores de servicios tecnológicos —sean nacionales o internacionales— concentran un poder significativo sobre la información, la interacción social y la economía digital, lo que las convierte en garantes activos de los derechos fundamentales en el ciberespacio. Por ello, la Ley de Constitucionalismo Digital les impone obligaciones de carácter proactivo, que superan la lógica reactiva tradicional:

1. Cumplimiento de los estándares constitucionales colombianos: Toda plataforma que opere en Colombia debe respetar los derechos y principios consagrados en la Constitución Política de 1991, sin que la ausencia de sede física en el país constituya un obstáculo para su exigibilidad.

Esto incluye la protección de la dignidad humana, la privacidad, la libertad de expresión, la igualdad y la seguridad digital.

Su incumplimiento puede generar responsabilidad administrativa, civil e incluso penal, fortaleciendo la soberanía jurídica en el entorno digital.

2. Transparencia algorítmica y notificación de decisiones automatizadas: La creciente dependencia de algoritmos e inteligencia artificial en la moderación de contenidos, la recomendación de información y la toma de decisiones exige reglas claras de transparencia. Las plataformas deben explicar los criterios y efectos de sus algoritmos, especialmente cuando afectan visibilidad de contenidos, acceso a servicios o monetización digital.

Toda decisión automatizada que impacte derechos —como la suspensión de cuentas, la eliminación de contenidos o la limitación de funcionalidades— debe ser notificada oportunamente al usuario, garantizando derecho de defensa y posibilidad de revisión humana. Este principio se alinea con los estándares internacionales sobre IA confiable, como el AI Act de la Unión Europea (2024/1689).

3. Respeto a la neutralidad de la red y la libertad de expresión: Las plataformas deben garantizar igualdad en el acceso y circulación de contenidos lícitos, evitando bloqueos, filtraciones o priorizaciones arbitrarias que puedan distorsionar el pluralismo informativo. La neutralidad tecnológica es condición esencial para que la libertad de expresión y el derecho a recibir información (Art. 20 C.P.) se materialicen en el entorno digital. Solo se permitirá la restricción de contenidos ilegales o nocivos bajo criterios objetivos, proporcionales y auditables, evitando la censura privada descontrolada.

4. Cooperación judicial y administrativa: Las plataformas y proveedores tecnológicos deben colaborar activamente con las autoridades competentes en la prevención, investigación y sanción de vulneraciones de derechos digitales y ciberdelitos.

Deben contar con canales expeditos y seguros para responder a requerimientos judiciales o administrativos, respetando siempre los principios de necesidad, proporcionalidad y protección de datos. Esta obligación es clave para evitar la impunidad en el ciberespacio y garantizar la efectividad del bloque de constitucionalidad digital.

II. Deberes de los usuarios

Si bien las plataformas concentran gran parte de la responsabilidad estructural, la consolidación de un ecosistema digital seguro y confiable también depende de la conducta de los ciudadanos digitales. La Ley de Constitucionalismo Digital fomenta una cultura de corresponsabilidad, estableciendo los siguientes deberes para los usuarios:

1. Uso responsable de las tecnologías digitales

El usuario debe emplear los servicios digitales de forma ética, consciente y segura, absteniéndose de:

- Difundir contenidos ilícitos o que vulneren derechos fundamentales de terceros.

Participar en actividades de suplantación, ciberacoso, desinformación o ataques digitales.

2. Respeto a los derechos de terceros en el entorno digital

La ciudadanía digital implica reconocer y proteger la privacidad, el buen nombre, la honra y la propiedad intelectual de otros usuarios.

- Se prohíbe la difamación, el discurso de odio y la discriminación en línea, favoreciendo un espacio de interacción respetuoso y plural.

3. Colaboración en la denuncia y prevención de incidentes digitales

Los usuarios tienen el deber de informar a las autoridades o a las propias plataformas sobre incidentes de seguridad, fraudes o vulneraciones de derechos digitales, contribuyendo a:

- La detección temprana de riesgos.
- La protección de potenciales víctimas.
- El fortalecimiento de la ciberseguridad nacional.

La definición de deberes para plataformas y usuarios consolida un modelo de corresponsabilidad que materializa el enfoque preventivo del constitucionalismo digital. Las plataformas asumen el rol de garantes proactivos de los derechos digitales, sujetas a supervisión

institucional y responsabilidad jurídica. Los usuarios se reconocen como ciudadanos digitales responsables, llamados a respetar derechos y colaborar en la seguridad del ecosistema digital.

Este esquema permite armonizar innovación tecnológica, seguridad digital y protección de los derechos fundamentales, generando confianza en la sociedad digital y contribuyendo a la efectividad del bloque de constitucionalidad digital colombiano.

5.4.5. Proyecto de Ley para la Regulación de Nuevas Tecnologías, Derechos y Obligaciones, Creación de la ANSDIA, entre otros.

El constitucionalismo digital colombiano requiere una herramienta normativa integral que articule innovación tecnológica, soberanía digital y protección de los derechos fundamentales en el contexto de la quinta revolución industrial. Este proyecto de ley, derivado de los dos años de investigación doctoral, constituye la respuesta normativa preventiva que permitirá a Colombia cerrar vacíos legales, anticipar riesgos tecnológicos y fortalecer su gobernanza digital frente a fenómenos como la inteligencia artificial, el big data, el blockchain, el metaverso, el transhumanismo y otras tecnologías emergentes.

La justificación de esta ley se sustenta en tres elementos fundamentales:

1. La digitalización acelerada ha superado la capacidad regulatoria tradicional, dejando sin cobertura jurídica situaciones críticas como la toma de decisiones algorítmicas, la explotación masiva de datos y los riesgos de sesgo tecnológico.
2. La protección de los derechos fundamentales exige un marco preventivo y articulado, que evite la dependencia exclusiva de la acción de tutela ex post y permita respuestas anticipadas a vulneraciones digitales.
3. La inserción de Colombia en la gobernanza digital internacional requiere normas modernas y coordinadas con estándares globales como el GDPR, la LGPD de Brasil, la Carta de Derechos Digitales de España y el AI Act de la Unión Europea.

i. **Obligaciones y responsabilidades de las empresas tecnológicas nacionales e internacionales**

Las empresas tecnológicas son aquellas organizaciones que diseñan, desarrollan, implementan o comercializan soluciones basadas en tecnologías emergentes, constituyéndose en actores estratégicos de la quinta revolución industrial. Su actividad se centra en la innovación digital y la aplicación de herramientas disruptivas como la inteligencia artificial

(IA), el big data, el blockchain, el internet de las cosas (IoT), la robótica avanzada, el metaverso, la biotecnología digital y la computación cuántica, entre otras. Estas compañías no solo proporcionan servicios y productos tecnológicos, sino que transforman profundamente los entornos sociales, económicos y jurídicos, al intervenir en la producción, gestión y circulación de datos masivos, así como en la automatización de decisiones que pueden impactar directamente en los derechos fundamentales. En el marco del constitucionalismo digital, estas empresas adquieren una doble dimensión: son motor de desarrollo e innovación, pero también potenciales generadores de riesgos, por lo que requieren regulación preventiva, supervisión especializada y obligaciones claras frente a usuarios y al Estado. Las empresas tecnológicas son actores centrales del ecosistema digital y, por tanto, tienen obligaciones duales: con los usuarios y con el Estado colombiano.

- **Obligaciones frente a los usuarios**.

a. Proteger la privacidad y seguridad de los datos personales, cumpliendo las normas nacionales e internacionales aplicables.

b. Evitar sesgos y discriminación algorítmica, garantizando acceso equitativo e inclusión digital.

c. Notificar decisiones automatizadas, asegurando transparencia algorítmica y derecho de defensa de los usuarios.

d. Habilitar canales de reclamación y reparación efectivos, ofreciendo protección real ante vulneraciones de derechos digitales.

- **Obligaciones frente al Estado colombiano**

a. Habilitación de servicios ante la ANSDIA, requisito indispensable para operar en el territorio nacional.

b. Gestión de actos administrativos de registro y operación, presentando el alcance de los servicios, los mecanismos de protección de derechos y los procedimientos de atención de incidentes.

c. Establecer domicilio legal y representación en Colombia, asegurando jurisdicción efectiva y responsabilidad ante autoridades nacionales.

d. Colaborar en la supervisión y fiscalización estatal, facilitando auditorías, reportes periódicos y cooperación para la prevención y persecución de ciberdelitos.

ii. Creación de la Autoridad Nacional de Supervisión Digital y de Inteligencia Artificial (ANSDIA)

La Autoridad Nacional de Supervisión Digital y de Inteligencia Artificial (ANSDIA) se erige como el eje central del modelo de gobernanza digital preventiva propuesto para Colombia, concebida como una entidad descentralizada de carácter técnico, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con autonomía administrativa y presupuestal para garantizar neutralidad, independencia y eficiencia operativa. Su mandato principal consiste en supervisar el cumplimiento normativo de plataformas y proveedores tecnológicos, monitorear algoritmos e inteligencia artificial para prevenir sesgos y riesgos a la igualdad digital, coordinar la cooperación nacional e internacional en la prevención y persecución de ciberdelitos, y emitir lineamientos, auditorías y alertas preventivas en materia de protección de datos y seguridad digital. La ANSDIA dispone de facultades sancionatorias efectivas, que incluyen la imposición de multas proporcionales y disuasorias, la suspensión o limitación de operaciones en casos graves, la adopción de medidas correctivas obligatorias con compensación a las víctimas y la remisión de hallazgos a la fiscalía general de la Nación ante la presunta comisión de delitos informáticos. Este modelo de supervisión se complementa con el fortalecimiento de la Superintendencia de Industria y Comercio (SIC), como órgano de vigilancia de prácticas comerciales digitales y fiscalización de algoritmos, y de la Agencia Nacional del Espectro (ANE), encargada de la gestión del espectro radioeléctrico y de la infraestructura digital crítica, asegurando conectividad segura y estable. Ambas entidades deben contar con herramientas de fiscalización avanzadas, talento humano especializado y mecanismos de cooperación internacional, de manera que la respuesta institucional ante vulneraciones de derechos digitales sea eficaz, coordinada y acorde con los estándares internacionales de protección tecnológica.

Es por ello, que sus principales funciones serán:

1. Supervisar el cumplimiento normativo por parte de plataformas y proveedores tecnológicos.
2. Monitorear algoritmos e IA para prevenir sesgos y riesgos a la igualdad digital.
3. Coordinar cooperación nacional e internacional para la prevención y persecución de ciberdelitos.

4. Emitir lineamientos, auditorías y alertas preventivas en materia de seguridad digital y protección de datos.

Frente a sus facultades sancionatorio estarán:

1. Multas proporcionales y disuasorias.
2. Suspensión o limitación de operaciones en casos graves.
3. Medidas correctivas obligatorias y compensación a víctimas.
4. Remisión de hallazgos a la fiscalía general de la Nación ante posibles delitos informáticos.

En síntesis, la ANSDIA se configura como el órgano rector de la gobernanza digital preventiva en Colombia, con competencias para supervisar el cumplimiento normativo, auditar algoritmos e inteligencia artificial, coordinar cooperación nacional e internacional y emitir lineamientos estratégicos en materia de seguridad y protección de datos. Sus facultades sancionatorias le otorgan la capacidad de imponer multas proporcionales y disuasorias, suspender o limitar operaciones digitales en casos graves, ordenar medidas correctivas con compensación a las víctimas y remitir hallazgos a la Fiscalía General de la Nación ante posibles delitos informáticos. Este modelo se complementa con la SIC, encargada de la protección de datos personales y la vigilancia de prácticas comerciales digitales, y con la ANE, responsable de la gestión del espectro radioeléctrico, la supervisión de la infraestructura digital crítica y la posibilidad de bloquear temporalmente plataformas infractoras para salvaguardar la soberanía tecnológica y los derechos fundamentales. La articulación funcional de estas entidades, dotadas de herramientas avanzadas de fiscalización, talento humano especializado y mecanismos de cooperación internacional, asegura una respuesta institucional coordinada, preventiva y eficaz, alineada con los estándares internacionales de protección tecnológica y constitucionalismo digital.

iii. Fortalecimiento de la Superintendencia de Industria y Comercio (SIC)

En el nuevo modelo de gobernanza digital preventiva, la Superintendencia de Industria y Comercio (SIC) mantiene su papel fundamental en la protección de los datos personales y en la vigilancia de las prácticas comerciales digitales, actuando dentro de las facultades que le otorgan la Ley 1581 de 2012 y el Decreto 1074 de 2015. Su función principal consiste en inspeccionar, verificar y sancionar vulneraciones relacionadas con el tratamiento de datos personales, asegurando la efectividad del habeas data digital y fortaleciendo la confianza de los

usuarios en los entornos tecnológicos. La SIC, a través de sus actuaciones, garantiza que las empresas tecnológicas respeten los principios de legalidad, finalidad, veracidad y seguridad en el uso de los datos, previniendo el uso indebido de la información personal como un paso esencial para la consolidación del constitucionalismo digital en Colombia.

El rol de la SIC se complementa estratégicamente con las funciones de la Autoridad Nacional de Supervisión Digital y de Inteligencia Artificial (ANSDIA), evitando duplicidad de competencias y fortaleciendo una estructura de fiscalización coordinada. Mientras la SIC se concentra en la protección de datos personales y la vigilancia de prácticas comerciales, la ANSDIA asume la supervisión integral de las tecnologías emergentes, los algoritmos y la inteligencia artificial, abordando los riesgos de alto impacto y alcance transnacional. Esta delimitación de competencias permite construir un modelo de gobernanza digital jerárquico y preventivo, en el que cada institución ejerce funciones complementarias para la protección efectiva de los derechos fundamentales en la era digital, asegurando que la innovación tecnológica se desarrolle en armonía con los principios constitucionales.

iv. Fortalezca las funciones Agencia Nacional del Espectro (ANE).

En el marco del constitucionalismo digital colombiano, la Agencia Nacional del Espectro (ANE) desempeña un papel estratégico en la gestión del espectro radioeléctrico y la supervisión de la infraestructura digital crítica, garantizando conectividad estable, segura y equitativa en todo el territorio nacional. Su función tradicional de administración técnica del espectro se amplía dentro del modelo de gobernanza digital preventiva propuesto por esta tesis, al convertirse en un pilar de la soberanía tecnológica, encargado de prevenir riesgos asociados a interrupciones, vulnerabilidades o usos indebidos de la infraestructura digital. En este esquema, la ANE coordina acciones preventivas con la ANSDIA, de manera que el entorno digital colombiano se mantenga resiliente, confiable y conforme a los principios constitucionales.

De manera innovadora, la ANE adquiere la facultad de limitar o bloquear temporalmente el acceso de plataformas digitales en el territorio colombiano, en coordinación con la ANSDIA, cuando se acrediten infracciones graves o reiteradas que afecten la seguridad digital, la soberanía tecnológica o los derechos fundamentales de los usuarios. Esta potestad se ejercerá bajo estrictos principios de legalidad, proporcionalidad y debido proceso, a través de actos administrativos motivados que garanticen que toda restricción sea excepcional, temporal

y reversible, orientada exclusivamente a la protección del interés público. Con estas competencias, la ANE se integra de forma complementaria a la arquitectura institucional del constitucionalismo digital, convirtiéndose en aliada esencial de la ANSDIA para garantizar que las plataformas tecnológicas cumplan con la normativa nacional, fortaleciendo así la soberanía digital y la protección efectiva de los derechos fundamentales en la era de la quinta revolución industrial.

v. Reforma de nuevos delitos penales y sanciones administrativas

El proyecto de Ley de Constitucionalismo Digital propone una modernización integral del marco penal y sancionatorio colombiano, con el propósito de responder a los desafíos de la quinta revolución industrial y garantizar que las conductas ilícitas en el entorno digital tengan una respuesta jurídica eficaz, proporcional y preventiva. La creciente dependencia de tecnologías emergentes, la expansión de la inteligencia artificial, el uso masivo de datos personales y la globalización de las plataformas digitales han generado un escenario de vulnerabilidad para los derechos fundamentales, en el cual tipos penales tradicionales resultan insuficientes para enfrentar nuevas modalidades de ciberdelitos. En este contexto, la reforma penal propuesta busca cerrar vacíos normativos, armonizar la legislación colombiana con estándares internacionales, y reforzar la capacidad de prevención y sanción del Estado frente a delitos que afectan la privacidad, seguridad y patrimonio digital de los ciudadanos.

En primer lugar, la ley contempla la incorporación de nuevos delitos digitales que reflejan la complejidad del ecosistema tecnológico actual, tales como: el robo de datos personales, la apropiación y suplantación de identidad digital, los ataques contra menores de edad en entornos virtuales, la piratería digital, y la difusión maliciosa de contenidos manipulados como los deepfakes. Estas conductas se reconocen como amenazas directas a la dignidad humana, la intimidad, la seguridad informática y la confianza en la sociedad digital, y su tipificación permitirá perseguir penalmente a los responsables, incluso en contextos transnacionales, mediante la cooperación prevista en tratados como el Convenio de Budapest sobre Ciberdelincuencia.

De manera complementaria, la propuesta establece un régimen de sanciones penales y administrativas con efecto disuasorio y preventivo, que incorpora multas proporcionales a la gravedad de la infracción y a la capacidad económica de la empresa infractora o del responsable individual, evitando así escenarios de impunidad corporativa. Además, se establece la

obligación de reparar integralmente a las víctimas y la implementación de protocolos internos de prevención de reincidencia, que incluyen medidas como la mejora de la seguridad digital, la adopción de políticas de gobernanza tecnológica y la supervisión periódica por parte de la ANSDIA. Con este enfoque, la reforma penal y administrativa no solo busca sancionar conductas ilícitas, sino también construir un ecosistema digital seguro, confiable y alineado con los principios del constitucionalismo digital preventivo, fortaleciendo la protección de los derechos fundamentales y la soberanía digital de Colombia.

v. Procedimiento sancionador para empresas que vulneren derechos digitales

El proyecto de Ley de Constitucionalismo Digital establece un procedimiento sancionador integral y garantista, diseñado para garantizar la eficacia en la protección de los derechos digitales sin sacrificar los principios de legalidad, debido proceso y proporcionalidad. En la era de la quinta revolución industrial, donde las empresas tecnológicas nacionales e internacionales ejercen un impacto directo sobre la privacidad, la seguridad digital y la igualdad de los usuarios, resulta imprescindible contar con mecanismos claros de fiscalización y sanción, capaces de responder con rapidez y contundencia ante vulneraciones graves o reiteradas. La finalidad del procedimiento sancionador propuesto no es únicamente castigar las infracciones, sino prevenir su repetición, garantizar reparación efectiva a las víctimas y fortalecer la confianza ciudadana en el ecosistema digital.

El procedimiento sancionador se inicia con la detección o denuncia de la infracción, ya sea a través de auditorías preventivas de la ANSDIA, reportes de la SIC, hallazgos de la ANE o denuncias de los propios usuarios. Una vez identificado el presunto incumplimiento, se abre investigación administrativa formal, en la cual la empresa tecnológica implicada tiene derecho a presentar descargos, aportar pruebas y controvertir las evidencias presentadas, cumpliendo los estándares de debido proceso administrativo. Concluida la fase de investigación, la ANSDIA, en coordinación con la SIC y la ANE cuando corresponda, podrá imponer sanciones proporcionales que van desde multas disuasorias y medidas correctivas obligatorias, hasta la suspensión temporal o limitación de operaciones en el territorio colombiano, en los casos de infracciones graves o reiteradas.

Un elemento innovador de este procedimiento es la obligación de implementar planes de corrección y prevención de reincidencia, que incluyen ajustes en los sistemas de seguridad

digital, fortalecimiento de políticas internas de protección de datos, transparencia algorítmica y capacitación en cumplimiento normativo. Asimismo, se establece que la compensación a las víctimas forma parte esencial de la sanción, de modo que los usuarios afectados recuperen la confianza en el entorno digital. Este procedimiento sancionador articulado, liderado por la ANSDIA y con la colaboración de la SIC y la ANE, materializa un modelo de constitucionalismo digital preventivo, que combina sanción, reparación y prevención, consolidando la soberanía digital de Colombia y garantizando la vigencia real y efectiva de los derechos fundamentales en el ciberespacio.

En conclusión, la propuesta de Proyecto de Ley para la Regulación de Nuevas Tecnologías y los Derechos Digitales constituye una respuesta normativa integral a los desafíos que plantea la quinta revolución industrial en Colombia. Este marco legal no solo redefine la relación entre innovación tecnológica y derechos fundamentales, sino que construye un modelo de constitucionalismo digital preventivo, capaz de anticipar riesgos, cerrar vacíos jurídicos y garantizar la protección real de los ciudadanos en el entorno digital. Al definir con precisión las tecnologías emergentes, imponer obligaciones claras a empresas nacionales e internacionales, reconocer nuevos derechos digitales, fortalecer las competencias de la SIC y la ANE, e incorporar delitos penales, sanciones administrativas y un procedimiento sancionador eficaz, esta ley se proyecta como la solución estructural para consolidar la soberanía digital del Estado colombiano. Su enfoque propositivo y preventivo asegura que el país transite hacia una sociedad digital inclusiva, segura y respetuosa de la dignidad humana, evitando que la rapidez del cambio tecnológico supere la capacidad de reacción del derecho.

5.4.6. Parámetros, criterios y lineamientos del proyecto de ley

El Proyecto de Ley para la Regulación de Nuevas Tecnologías y la Protección de los Derechos Digitales se plantea como una respuesta normativa integral a los desafíos que enfrenta Colombia en el marco de la quinta revolución industrial, caracterizada por la expansión de tecnologías emergentes como la inteligencia artificial (IA), el big data, la blockchain, el metaverso y la automatización avanzada. Su finalidad es garantizar la protección de los derechos fundamentales de los ciudadanos en entornos digitales, promover la soberanía tecnológica del Estado y consolidar un modelo de gobernanza digital preventiva que supere el enfoque reactivo, históricamente basado en la acción judicial ex post.

Este proyecto de ley se sustenta en cuatro parámetros rectores:

1. Protección integral de los derechos digitales, reconociendo su conexidad con la privacidad, la libertad de expresión, la seguridad y el patrimonio digital.

2. Innovación tecnológica con enfoque preventivo, asegurando que el desarrollo y uso de nuevas tecnologías se ajuste a los principios constitucionales y a los estándares internacionales de derechos humanos.

3. Transparencia y responsabilidad digital, mediante la exigencia de claridad en el tratamiento de datos, supervisión algorítmica y auditorías tecnológicas preventivas.

4. Inclusión social y equidad, garantizando acceso equitativo a los derechos digitales, incorporando un enfoque de género y protegiendo a grupos vulnerables, especialmente en materia de educación y seguridad digital.

5.4.6.1.Lineamientos estratégicos del proyecto de ley

Los lineamientos estratégicos del proyecto de ley constituyen la columna vertebral de su diseño normativo, pues definen su alcance, objetivos operativos y enfoque preventivo frente a los desafíos de la quinta revolución industrial. En primer lugar, la propuesta delimita y regula las tecnologías emergentes que marcan esta etapa, incluyendo la inteligencia artificial (IA), el big data, la blockchain, el metaverso y la automatización avanzada, asegurando que su desarrollo se realice bajo principios de legalidad, seguridad y respeto por los derechos fundamentales. En segundo lugar, el proyecto reconoce y protege nuevos derechos digitales, entre ellos la privacidad digital, la seguridad en línea, la libertad de expresión en entornos digitales, la portabilidad de datos, la sucesión y la educación digitales, ampliando el alcance de las garantías constitucionales al ciberespacio. A nivel institucional y regulatorio, la ley impone obligaciones claras a las empresas tecnológicas nacionales e internacionales, tanto frente a los usuarios como al Estado colombiano, que incluyen la habilitación de sus servicios ante la ANSDIA, el establecimiento de domicilio legal y representación en Colombia, y la colaboración activa en procesos de supervisión y fiscalización estatal.

De forma complementaria, el proyecto fortalece el rol de la Superintendencia de Industria y Comercio (SIC) y de la Agencia Nacional del Espectro (ANE) como órganos técnicos coordinados con la ANSDIA, con el fin de garantizar la fiscalización de las prácticas digitales, la protección efectiva de los datos personales y la supervisión de la infraestructura tecnológica crítica. En materia penal y sancionatoria, la ley incorpora nuevos delitos cibernéticos en el Código Penal colombiano, tales como robo de datos personales, suplantación

de identidad digital, ataques contra menores en línea y difusión de deepfakes maliciosos, acompañados de sanciones proporcionales y medidas reparadoras para las víctimas. Asimismo, se crea un Comité Digital Interinstitucional, encargado de impulsar la innovación, coordinar políticas públicas y promover la cooperación entre el sector público y privado, consolidando la gobernanza digital del país. Finalmente, el proyecto establece un procedimiento sancionador claro y preventivo, que contempla multas disuasorias, medidas correctivas obligatorias, compensación integral a las víctimas y, en casos graves o reiterados, el bloqueo temporal de las plataformas infractoras, asegurando así un entorno digital seguro, transparente y alineado con los principios del constitucionalismo digital preventivo.

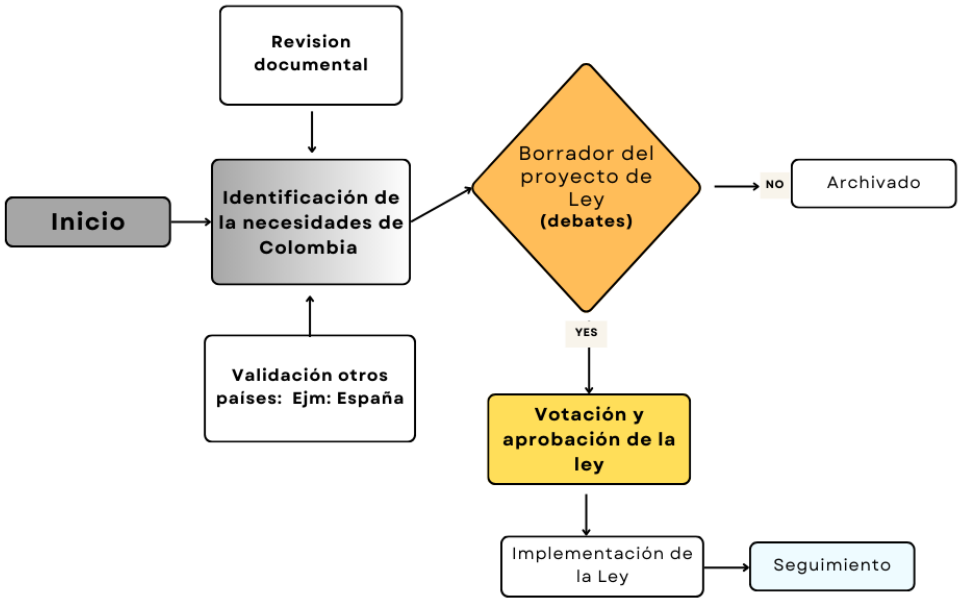
5.4.6.2. Fases de implementación del proyecto de ley

El proceso de implementación de la ley propuesta se concibe como un ciclo preventivo y adaptable, estructurado en siete fases que permiten evolucionar desde la identificación de la necesidad normativa hasta la evaluación continua del marco legal:

1. Inicio: Identificación de la necesidad de regular las nuevas tecnologías en Colombia.
2. Establecimiento del marco normativo: Definición de derechos digitales y alcance de las tecnologías emergentes.
3. Presentación del proyecto de ley: Discusión y análisis en el Congreso de la República.
4. Creación de la Autoridad Nacional de Supervisión Digital y de Inteligencia Artificial (ANSDIA): Consolidación de la entidad encargada de la fiscalización y control preventivo.
5. Revisión e inclusión de delitos cibernéticos: Incorporación de nuevos tipos penales y sanciones proporcionales en el Código Penal.
6. Creación del Comité Digital Interinstitucional: Coordinación de políticas públicas y fortalecimiento de la cooperación público-privada.
7. Seguimiento y Evaluación: Monitoreo permanente de resultados, ajustes normativos y adecuación continua a los avances tecnológicos.

Figura 13.

Flujograma del Proyecto de Ley



Nota: Elaboración propia (2025).

Conforme al flujograma previamente expuesto, el proceso se desarrollará en siete fases, las cuales son las siguientes: 1) Inicio: Identificación de la necesidad de regular las nuevas tecnologías en Colombia; 2) Establecimiento del marco normativo: Definición de las nuevas tecnologías y los derechos digitales; 3) Presentación del Proyecto de Ley: Debate y análisis en el Congreso de la República; 4) Creación de la Autoridad de Protección: Establecimiento de una entidad encargada de garantizar el cumplimiento de los derechos digitales; 5) Revisión de delitos cibernéticos: Inclusión de delitos como el robo de datos personales, ciberdelitos contra menores y piratería digital en el Código Penal; 6) Establecimiento del Comité Digital Interinstitucional: Creación de un comité para impulsar el desarrollo tecnológico y normativo en el país; 7) Seguimiento y Evaluación: Monitoreo de los avances y adaptación del marco normativo a los avances tecnológicos. Finalmente, se alcanzará el Fin, con la implementación de un entorno digital seguro y eficiente para todos los ciudadanos.

La adopción de este proyecto de ley constituye la solución estructural al rezago normativo de Colombia en materia de derechos digitales, pues consolida un constitucionalismo

digital preventivo capaz de anticipar riesgos, proteger a los ciudadanos y garantizar la soberanía tecnológica del Estado. Este marco legal armoniza innovación y protección de derechos humanos, estableciendo mecanismos claros de supervisión, sanción y cooperación interinstitucional, lo que permitirá que Colombia deje de depender exclusivamente de respuestas judiciales reactivas. De aprobarse e implementarse, este proyecto convertiría al país en un referente regional en gobernanza digital, asegurando un entorno tecnológico seguro, inclusivo y sostenible para todos los ciudadanos.

Finalmente, se anexa el proyecto de ley derivado de la revisión realizada en el marco de la investigación, en la que se crearon los derechos digitales. Este proyecto establece un marco normativo para regular el uso de las nuevas tecnologías en Colombia, con el objetivo de proteger los derechos digitales y garantizar una gestión transparente de los datos personales en el contexto de la Quinta Revolución Industrial. La ley abarca varios aspectos clave, entre los que se incluyen la protección de los derechos fundamentales de los ciudadanos en el entorno digital, la creación de derechos digitales, la regulación de tecnologías emergentes como el metaverso, la inteligencia artificial, el big data y la blockchain, así como la creación de una autoridad encargada de supervisar el cumplimiento de sus disposiciones. El proyecto también reconoce derechos esenciales como la privacidad, la seguridad, la libertad de expresión, la portabilidad de los datos y la educación digital. Además, propone la creación de un Comité Digital Interinstitucional, encargado de fomentar la innovación y colaborar con el sector público y privado, para asegurar un entorno digital seguro y justo, e incluye un capítulo especial para la protección de los menores en Internet, así como la inclusión de delitos cibernéticos en el Código Penal Colombiano, con sanciones específicas para ciberdelincuentes.

5.5. Modelo de gobernanza para el constitucionalismo digital

La organización institucional constituye el eje estructural del modelo de gobernanza para el constitucionalismo digital en Colombia, al permitir articular de manera coherente las competencias normativas, técnicas y operativas necesarias para garantizar la protección efectiva de los derechos fundamentales en entornos digitales. Este diseño institucional se estructura en tres componentes estratégicos. En primer lugar, la creación de un Consejo de Constitucionalismo Digital (CCD), concebido como instancia de alto nivel responsable de la definición de lineamientos estratégicos, la evaluación de riesgos constitucionales y la armonización normativa frente a tecnologías emergentes. En segundo lugar, la Autoridad de

Supervisión Digital (ASD), con funciones de inspección, vigilancia y control sobre algoritmos, inteligencia artificial, interoperabilidad de plataformas y protección de datos personales. Y, en tercer lugar, la coordinación interinstitucional entre el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Superintendencia de Industria y Comercio (SIC) y la Fiscalía Cibernética, garantizando respuestas integrales y articuladas ante incidentes digitales, delitos informáticos y vulneraciones de derechos fundamentales. Este esquema busca cerrar los vacíos institucionales que han limitado históricamente la capacidad del Estado colombiano para anticipar riesgos y actuar de manera preventiva frente a los desafíos de la quinta revolución industrial.

Siguiendo la doctrina de Ferrajoli (2020) y Pérez Luño (2019), la protección efectiva de los derechos fundamentales en la era digital no puede limitarse a la expedición de normas aisladas o meramente declarativas; requiere la construcción de instituciones sólidas, políticas públicas coherentes y mecanismos de gobernanza anticipatoria que permitan identificar y mitigar riesgos antes de que se traduzcan en afectaciones irreversibles a la dignidad humana. Esta exigencia resulta especialmente crítica en Colombia, donde la respuesta normativa frente a la innovación tecnológica ha sido tardía, fragmentada y reactiva, generando brechas en seguridad jurídica y protección ciudadana. Mientras que jurisdicciones comparadas, como la Unión Europea, España o Brasil, han consolidado cartas de derechos digitales, reglamentos de protección de datos y marcos éticos para la inteligencia artificial, Colombia continúa operando bajo un esquema disperso, que deja a los usuarios expuestos a la suplantación de identidad, la discriminación algorítmica, la explotación indebida de datos y la vigilancia masiva sin controles claros.

Esta postura negligente y retardada del Estado limita la efectividad de los derechos en entornos digitales y erosiona la confianza ciudadana, afectando actividades cotidianas como transacciones financieras, trámites públicos y participación en redes sociales o plataformas de comercio electrónico. La ausencia de un reconocimiento explícito de los derechos digitales, como los que esta tesis propone —privacidad reforzada, derecho a la autodeterminación informativa, derecho al olvido digital, garantía de neutralidad algorítmica y acceso universal a la conectividad— impide que la ciudadanía perciba que el Estado respalda activamente su seguridad y libertad en el ciberespacio. Frente a este panorama, resulta urgente que Colombia abandone su actitud reactiva y adopte un constitucionalismo digital robusto, capaz de integrar prevención, regulación anticipatoria y educación digital ciudadana. Solo así será posible

garantizar que la dignidad humana, eje del Estado social de derecho, permanezca protegida en un ecosistema donde datos, algoritmos y decisiones automatizadas impactan de manera cada vez más profunda la vida de las personas.

5.5.1. Organización institucional

El modelo de gobernanza propuesto requiere una estructura institucional articulada y especializada, capaz de enfrentar los retos jurídicos, técnicos y sociales de la era digital. En este marco, se propone la creación de un Consejo de Constitucionalismo Digital (CCD) como instancia estratégica de alto nivel, responsable de la formulación de lineamientos, la evaluación de riesgos constitucionales y la armonización normativa frente a tecnologías disruptivas como la inteligencia artificial, el blockchain, el metaverso y los sistemas ciberfísicos. A su vez, la Autoridad de Supervisión Digital (ASD) asumiría funciones de inspección, vigilancia y control, con competencias para certificar algoritmos, exigir transparencia en sistemas automatizados, verificar la interoperabilidad de plataformas y sancionar vulneraciones a los derechos digitales. Esta arquitectura institucional se complementa con la coordinación interinstitucional entre el MinTIC, la SIC y la Fiscalía Cibernética, que permitirá articular la política pública digital, la protección de datos y la persecución de delitos informáticos, cerrando la brecha histórica entre innovación tecnológica y capacidad de respuesta estatal.

5.5.2. Gobernanza digital preventiva

La gobernanza digital preventiva se fundamenta en la capacidad del Estado para anticipar riesgos y proteger los derechos fundamentales frente a afectaciones derivadas de la transformación tecnológica. La supervisión de algoritmos e inteligencia artificial se convierte en un pilar esencial, implementando registros de algoritmos de alto riesgo, auditorías periódicas y evaluaciones de impacto constitucional que aseguren el respeto a la igualdad, la privacidad y el debido proceso. De manera complementaria, la interoperabilidad de plataformas públicas y privadas garantiza la integración segura de datos y servicios, reduciendo la fragmentación administrativa y fortaleciendo la trazabilidad de la información. Finalmente, la coordinación interinstitucional permitirá que las acciones preventivas y de control cuenten con respaldo técnico y jurídico, disminuyendo la vulnerabilidad de los usuarios frente a amenazas digitales complejas.

5.5.3. Sistema de monitoreo y respuesta a ciberamenazas

Como complemento, la propuesta contempla la creación de un sistema integral de monitoreo y respuesta a ciberamenazas, diseñado para identificar, prevenir y mitigar riesgos que comprometan la infraestructura crítica y los derechos fundamentales. Este sistema se articulará con el Centro de Respuesta a Incidentes Cibernéticos (CSIRT) nacional, pero con un enfoque preventivo y constitucional, priorizando incidentes que afecten la dignidad humana, la privacidad y la seguridad jurídica. Para su operación se requerirán plataformas de análisis predictivo basadas en inteligencia artificial, protocolos de reacción inmediata y canales permanentes de coordinación con la Fiscalía Cibernética, la Policía Nacional y la Autoridad de Supervisión Digital. Con este enfoque, Colombia no solo respondería ante incidentes consumados, sino que consolidaría un ecosistema digital seguro, confiable y alineado con los estándares internacionales de ciberseguridad y derechos digitales, fortaleciendo la confianza ciudadana en la era de la quinta revolución industrial.

5.6. Estrategia de implementación

La estrategia de implementación del modelo de gobernanza para el constitucionalismo digital constituye el componente propositivo de esta investigación, articulando los hallazgos sobre vacíos normativos, riesgos constitucionales y debilidades institucionales con un plan integral de acción para el Estado colombiano. Su propósito es que la protección de los derechos fundamentales en entornos digitales deje de ser fragmentada y reactiva, para transformarse en un esquema preventivo, articulado y alineado con los estándares internacionales, que fortalezca la seguridad jurídica, la confianza digital y la legitimidad institucional.

Esta estrategia parte del marco normativo e institucional vigente —la Constitución de 1991 (arts. 15, 20 y 29), la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1377 de 2013, la Política Nacional de Ciberseguridad 2020–2025, la Política de Gobierno Digital del MinTIC y la existencia del CSIRT nacional—, pero lo reorganiza bajo un enfoque constitucional que privilegia la prevención de riesgos y la garantía de derechos digitales explícitos, como los propuestos en esta tesis.

5.6.1. Fases de implementación

La estrategia se desarrolla de forma escalonada en tres fases, lo que permite construir capacidades institucionales y ciudadanas de manera progresiva:

Corto plazo (1–2 años): En la fase inicial se priorizan las acciones fundacionales, que habilitan la operación del modelo:

1. Creación formal del Consejo de Constitucionalismo Digital (CCD) como órgano de coordinación estratégica.
2. Elaboración de un diagnóstico nacional de riesgos constitucionales digitales, que identifique vulnerabilidades en privacidad, ciberseguridad e interoperabilidad estatal.
3. Fortalecimiento de protocolos mínimos de ciberseguridad en las entidades públicas, articulando al CSIRT nacional con la Fiscalía Cibernética para garantizar respuestas inmediatas ante incidentes.

Mediano plazo (3–5 años): Esta fase busca consolidar la operatividad institucional y asegurar que la gobernanza digital sea efectiva y supervisada:

- Puesta en marcha de la Autoridad de Supervisión Digital (ASD), con funciones de inspección, vigilancia y sanción.
- Implementación de un registro nacional de algoritmos de alto riesgo y realización de evaluaciones de impacto constitucional sobre decisiones automatizadas e inteligencia artificial.
- Desarrollo de plataformas interoperables que integren servicios públicos y privados, optimizando la trazabilidad y reduciendo la fragmentación administrativa.

Inicio de programas de alfabetización digital ciudadana, que fortalezcan la cultura constitucional digital y promuevan la seguridad y autodeterminación informativa.

Largo plazo (5–10 años): La fase final busca consolidar el modelo y proyectarlo hacia la gobernanza digital internacional:

- Evaluación del impacto constitucional y social del modelo, con informes que sirvan de base para ajustes normativos y de política pública.
- Integración plena con redes regionales e internacionales de ciberseguridad y protección de derechos digitales, incluyendo la Carta Iberoamericana de Derechos Digitales 2023 y las buenas prácticas del RGPD europeo.

- Reconocimiento formal de los derechos digitales propuestos en esta tesis —privacidad reforzada, derecho al olvido digital, neutralidad algorítmica y acceso universal a la conectividad— como parte del bloque de protección constitucional interna, garantizando que el Estado social de derecho también se proyecte al ciberespacio.

5.6.2. Instrumentos normativos y de política pública

La implementación del modelo se sustenta en una combinación de herramientas jurídicas, institucionales y sociales que aseguran la coherencia entre la regulación y la transformación digital. En el plano normativo, se requieren leyes marco que regulen la inteligencia artificial, los algoritmos y la responsabilidad de las plataformas digitales, con un enfoque de derechos humanos y constitucionalidad preventiva, mientras que decretos reglamentarios deberán asignar competencias claras al Consejo de Constitucionalismo Digital (CCD) y a la Autoridad de Supervisión Digital (ASD), estableciendo procedimientos efectivos de supervisión y sanción. A nivel de política pública, la estrategia implica la integración de la Política de Gobierno Digital, la Política Nacional de Ciberseguridad y los programas de protección de datos y ética tecnológica, articulando esfuerzos dispersos bajo una visión constitucional unificada. Finalmente, la alfabetización digital ciudadana se configura como el componente social esencial, orientada a formar usuarios conscientes de sus derechos digitales, promover hábitos de ciberseguridad y fortalecer la confianza en la interacción con plataformas digitales.

5.6.3. Mecanismos de control y seguimiento

Para asegurar la sostenibilidad y eficacia del modelo, se plantean mecanismos de evaluación permanente:

- Informes periódicos: Publicación anual del Informe Nacional sobre Derechos Digitales y Riesgos Constitucionales, dirigido al Congreso de la República, al Consejo de Constitucionalismo Digital y a la ciudadanía. Divulgación de indicadores clave, como número de incidentes cibernéticos, avances en interoperabilidad y niveles de protección efectiva de derechos digitales.

- Integración con la política de ciberseguridad nacional: Alineación con el Plan Nacional de Ciberseguridad 2020-2025 y la Estrategia de Transformación Digital de MinTIC. Coordinación con el CSIRT nacional, la Fiscalía Cibernética y las redes

regionales, para la gestión de amenazas transfronterizas y la prevención de ciberataques de alto impacto constitucional.

Finalmente, la implementación de esta estrategia se proyecta para su despliegue efectivo una vez el proyecto de ley que materializa esta propuesta sea aprobado como ley de la República, otorgando seguridad jurídica a los órganos creados, asegurando la vinculación obligatoria de entidades públicas y privadas y garantizando que Colombia abandone la postura reactiva que ha caracterizado su regulación tecnológica. De esta manera, la tesis se convierte en una hoja de ruta normativa y operativa que permite al país insertarse en la gobernanza digital regional e internacional, con un modelo preventivo, confiable y respetuoso de los derechos fundamentales.

En perspectiva futura, la consolidación de un constitucionalismo digital robusto en Colombia debe prepararse para un escenario donde ciber-robots, inteligencias artificiales avanzadas, sistemas autónomos y humanos aumentados tecnológicamente interactúen de manera cotidiana en la vida social, económica y jurídica. La emergencia de la "ciudadanía digital de las máquinas" y la participación de agentes inteligentes en procesos decisionales plantean el reto de garantizar que la primacía de la dignidad humana permanezca incuestionable, al tiempo que se asegure un ecosistema digital equilibrado, donde tanto humanos como sistemas tecnológicos avanzados tengan acceso, cuidado y garantías adecuadas. En este marco, el Estado deberá anticipar normas y salvaguardas para proteger al ser humano común, evitando que quienes han potenciado sus capacidades mediante tecnología generen nuevas formas de desigualdad o exclusión digital. Este horizonte refleja el cierre evolutivo de la tesis, proyectando un Colombia preparada para la era de la inteligencia artificial, la robótica social y la convergencia tecnológica, donde la seguridad jurídica, la ética digital y la protección de la persona humana serán la base para una convivencia armónica entre ciudadanos y máquinas inteligentes.

5.7. Impacto esperado

La implementación del modelo de gobernanza para el constitucionalismo digital proyecta un impacto profundo y sostenido en la protección de derechos fundamentales, la seguridad jurídica y la inserción internacional de Colombia, con una visión de futuro a 20 años, anticipando los desafíos de la inteligencia artificial avanzada, la robótica social, la ciudadanía

digital de las máquinas y la convergencia tecnológica. Este impacto se manifiesta en tres dimensiones estratégicas:

Beneficios en la protección de derechos fundamentales
En el horizonte de dos décadas, el modelo permitirá que los derechos fundamentales —como la privacidad, el habeas data, la libertad de expresión, la igualdad y el debido proceso— tengan una protección reforzada y preventiva frente a las amenazas de los entornos digitales. La supervisión de algoritmos e inteligencia artificial y la interoperabilidad de plataformas garantizarán que las decisiones automatizadas se mantengan dentro de un marco de legalidad y no discriminación, incluso en escenarios donde humanos aumentados tecnológicamente, robots sociales e inteligencias artificiales autónomas interactúen con la ciudadanía. En este futuro, la protección de derechos no solo se enfocará en el ser humano común, sino que también velará por reducir las brechas frente a quienes potencien sus capacidades con tecnología, evitando nuevas formas de desigualdad digital y social.

Mejora de la seguridad jurídica y confianza digital
A medida que evolucione la tecnología y se incorporen sistemas autónomos, ciber-robots y agentes inteligentes a la vida cotidiana, la seguridad jurídica y la confianza digital se consolidarán como pilares del ecosistema nacional. La existencia de un marco normativo claro, instituciones especializadas y mecanismos de supervisión en tiempo real permitirá que ciudadanos, empresas y entidades públicas interactúen con tecnologías emergentes sin incertidumbre ni riesgos jurídicos excesivos. En 20 años, este modelo proyecta un país donde la confianza digital no solo fortalezca el comercio electrónico y los servicios públicos en línea, sino también la convivencia entre humanos y máquinas inteligentes, bajo principios de responsabilidad, trazabilidad y ética tecnológica.

Cumplimiento de estándares internacionales y compromisos regionales
En su proyección a dos décadas, el modelo situará a Colombia como un referente latinoamericano en gobernanza digital, alineado con los principios de la Carta Iberoamericana de Derechos Digitales 2023, las directrices de la Unión Europea sobre inteligencia artificial y los marcos regionales de ciberseguridad y protección de datos. Esta inserción internacional facilitará la cooperación transfronteriza frente a ciberamenazas, la armonización normativa para el desarrollo ético de nuevas tecnologías y la participación en la discusión sobre la ciudadanía digital de las máquinas y los derechos asociados a la interacción humano-tecnología. El impacto esperado trasciende el ámbito jurídico: en 20 años, Colombia podría ser

un país donde la dignidad humana, la innovación tecnológica y la seguridad digital convivan armónicamente, consolidando un ecosistema de confianza entre personas y sistemas inteligentes.

En conjunto, la implementación de este modelo y su proyección futura buscan garantizar que la revolución tecnológica no erosione la centralidad del ser humano, sino que permita un equilibrio entre innovación, ética y derechos fundamentales, asegurando que Colombia esté preparada para la era de los ciber-robots, la inteligencia artificial avanzada y la ciudadanía digital del futuro.

5.8. Defensa del proyecto de ley (Doctorando)

La propuesta de Proyecto de Ley para la Regulación de Nuevas Tecnologías y la Protección de los Derechos Digitales constituye el aporte original y propositivo de esta tesis doctoral al constitucionalismo digital colombiano, sustentado en la doctrina, el derecho comparado y un análisis crítico del contexto nacional. Esta iniciativa se erige como jurídicamente posible, urgente y estructural para garantizar la protección de los derechos fundamentales en la era digital, en la que la quinta revolución industrial —marcada por la expansión de la inteligencia artificial, el big data, la blockchain, el metaverso y la automatización avanzada— transforma aceleradamente la sociedad, la economía y las relaciones jurídicas.

Colombia enfrenta actualmente un vacío normativo estructural frente a los desafíos de estas tecnologías emergentes. A diferencia de países que han desarrollado cartas de derechos digitales y regulaciones proactivas —como el GDPR en Europa, la Carta Digital de España, la LGPD de Brasil o el AI Act de la Unión Europea 2024/1689—, el país ha mantenido un enfoque reactivo, confiando casi exclusivamente en la acción de tutela y en la intervención eventual de la Corte Constitucional para la protección de derechos en entornos digitales. Tal como lo advierte Humberto Nogueira, el derecho procesal constitucional no puede ser la única herramienta de garantía frente a riesgos tecnológicos complejos, porque los mecanismos ex post llegan tarde ante vulneraciones masivas y transnacionales. En la misma línea, Peter Häberle y Gustavo Zagrebelsky sostienen que los derechos fundamentales contemporáneos exigen estructuras normativas preventivas, capaces de anticiparse al riesgo tecnológico y materializar un constitucionalismo activo, no meramente defensivo.

El Estado colombiano se encuentra desbordado por la velocidad de la transformación digital, y la ausencia de regulación integral deja a los ciudadanos expuestos a suplantación digital, explotación de datos personales, discriminación algorítmica y ciberataques transnacionales. Esta propuesta no es un ejercicio académico abstracto, sino una respuesta normativa concreta que busca cerrar la brecha estructural, transformando el modelo reactivo en un sistema preventivo y articulado, conforme con la Constitución de 1991 y con los estándares internacionales de derechos humanos y gobernanza digital.

La viabilidad institucional de esta iniciativa se materializa en un modelo jerárquico y preventivo de gobernanza digital, en el que cada entidad cumple un rol específico y complementario. La ANSDIA (Autoridad Nacional de Supervisión Digital y de Inteligencia Artificial) se proyecta como órgano técnico central, con facultades de supervisión, monitoreo algorítmico, auditorías preventivas y potestad sancionatoria, incluyendo la suspensión de operaciones tecnológicas que vulneren derechos digitales. La Superintendencia de Industria y Comercio (SIC) mantiene su papel en la protección de datos personales y en la vigilancia de prácticas comerciales digitales, en armonía con la Ley 1581 de 2012, actuando como aliada técnica de la ANSDIA. Por su parte, la Agencia Nacional del Espectro (ANE) refuerza la soberanía digital mediante la gestión de infraestructura crítica y la facultad de bloquear temporalmente plataformas infractoras, garantizando que ninguna empresa tecnológica quede fuera de la jurisdicción nacional. A estas entidades se suma el Comité Digital Interinstitucional, que fomenta la cooperación público-privada y la innovación tecnológica, asegurando que el desarrollo digital avance de la mano con la protección de derechos humanos y la inclusión social. Este modelo preventivo, inspirado en buenas prácticas internacionales pero adaptado al contexto colombiano, permite supervisión proactiva, sanción proporcional, reparación efectiva a las víctimas y prevención de reincidencia, rompiendo el ciclo de impunidad tecnológica y vulneración masiva de derechos.

La originalidad de este proyecto radica en la creación de derechos digitales inéditos, ausentes en la legislación colombiana y regional, que fortalecen un bloque de constitucionalidad digital preventivo. Entre ellos destacan la muerte y la sucesión digitales, que permiten al ciudadano decidir el destino de sus cuentas y patrimonios digitales post-mortem; la reserva digital entre usuario y plataforma, que protege la esfera privada frente a la profilación y el uso no consentido de datos; y los patrimonios digitales y bienes virtuales, que reconocen el valor económico y la transmisibilidad jurídica de los activos digitales. Estos derechos,

acompañados de la reforma penal y sancionatoria propuesta, articulan innovación tecnológica, soberanía estatal y protección efectiva de la dignidad humana en el ciberespacio. Además, el proyecto integra un enfoque inclusivo y de género, alineado con la Agenda Digital de la ONU y la OCDE, reconociendo que la brecha digital impacta con mayor intensidad a mujeres, minorías y comunidades rurales, y que, sin políticas de equidad tecnológica, la digitalización corre el riesgo de profundizar desigualdades estructurales.

Como autor de esta propuesta, sostengo que el proyecto de ley presentado en esta tesis doctoral constituye la solución estructural que Colombia necesita para fortalecer su soberanía digital, garantizar los derechos fundamentales en el entorno tecnológico y transitar hacia un constitucionalismo digital robusto, preventivo e inclusivo. Su adopción permitiría superar la dependencia de respuestas judiciales reactivas, ofreciendo un sistema legal e institucional moderno, capaz de dialogar con estándares internacionales y de proteger de manera eficaz a la ciudadanía frente a los riesgos de la quinta revolución industrial. De implementarse, esta ley convertiría a Colombia en un referente regional en gobernanza digital, promoviendo seguridad jurídica, confianza tecnológica e inclusión social, y sentando las bases de un modelo sostenible donde la innovación tecnológica se armonice con la dignidad humana y el Estado de derecho.

Conclusiones

La presente investigación doctoral confirma que el constitucionalismo colombiano, tal como está diseñado, carece de un marco integral capaz de responder a los retos jurídicos, políticos y sociales derivados de la Quinta Revolución Industrial. Aunque la Constitución de 1991 ofrece una robusta carta de derechos, su estructura responde a un paradigma analógico que limita su eficacia frente a riesgos emergentes como la vigilancia masiva, la discriminación algorítmica, la explotación transnacional de datos o la afectación del debido proceso en contextos de decisión automatizada.

El análisis evidenció vacíos normativos sustanciales, entre ellos la ausencia de un reconocimiento formal de los derechos digitales como categoría autónoma, la fragmentación de la legislación sobre protección de datos y ciberseguridad, y la insuficiente articulación jurisprudencial en torno a los entornos tecnológicos. Esta brecha entre norma y realidad tecnológica deja a los ciudadanos en una situación de vulnerabilidad frente a actores privados globales y sistemas algorítmicos que operan fuera del control democrático tradicional. Particularmente, se evidenció que la regulación dispersa y la falta de coordinación institucional dificultan la protección de derechos como la privacidad, la libertad de expresión y el acceso a la información, generando un escenario donde decisiones automatizadas pueden afectar directamente la vida cotidiana de los individuos sin que existan mecanismos claros de reparación o supervisión efectiva.

El aporte central de esta investigación radica en la formulación de un modelo de constitucionalismo digital colombiano que articula principios como la dignidad humana, la eficacia de los derechos fundamentales, la transparencia algorítmica, la soberanía de los datos y la responsabilidad compartida entre Estado, plataformas digitales y desarrolladores tecnológicos. Este modelo propone un enfoque que trasciende la mera adaptación normativa, orientándose hacia la integración de estándares internacionales con prácticas locales, garantizando que los derechos fundamentales no solo se reconozcan en el papel, sino que se hagan efectivos en la práctica cotidiana de los ciudadanos en entornos digitales. Asimismo, incorpora herramientas preventivas y reactivos normativos, incluyendo protocolos de auditoría algorítmica, mecanismos de control ciudadano y lineamientos de diseño ético de sistemas tecnológicos, con el fin de reducir riesgos de vulneración y fortalecer la confianza en la gobernanza digital.

Desde una perspectiva académica, esta tesis contribuye al debate doctrinal sobre la necesidad de constitucionalizar el entorno digital, evidenciando que la protección de los derechos fundamentales no puede limitarse al ámbito físico ni depender exclusivamente de la regulación estatal. La investigación sitúa a Colombia en el contexto de la discusión global sobre gobernanza tecnológica, comparando experiencias con países que han avanzado en la creación de derechos digitales, regulación de algoritmos y supervisión de plataformas privadas, demostrando la pertinencia y urgencia de una reforma constitucional que contemple las particularidades del ciberespacio.

En el plano social, la investigación ofrece herramientas jurídicas y conceptuales para fortalecer la defensa de los ciudadanos frente a vulneraciones derivadas del uso de tecnologías disruptivas. La inclusión de los principios de transparencia y responsabilidad compartida permite generar un marco que no solo protege al individuo frente a actores privados, sino que también promueve la equidad y la participación ciudadana en la configuración de políticas y normas tecnológicas. Esto resulta especialmente relevante en un contexto donde la concentración de datos y el control de la información por parte de conglomerados tecnológicos puede incidir directamente en derechos como la igualdad, la autonomía y la libertad de decisión.

En el ámbito institucional, el estudio consolida una línea de investigación que integra Derecho público, ética digital y gobernanza tecnológica, generando un referente para futuras reformas legislativas, políticas públicas y proyectos de regulación regional. Al articular estos campos, la investigación demuestra que un constitucionalismo digital no es un lujo académico, sino una necesidad estratégica para garantizar la vigencia del Estado social de derecho frente a los desafíos de la era digital, fortaleciendo la capacidad del Estado para intervenir y regular de manera efectiva en la esfera tecnológica sin obstaculizar la innovación.

En síntesis, el trabajo concluye que la única forma de preservar la vigencia del Estado social de derecho en la era digital es mediante un constitucionalismo que reconozca, regule y garantice de forma efectiva los derechos fundamentales en entornos tecnológicos, evitando que la innovación se convierta en un vector de desigualdad y consolidando a Colombia como referente regional en la defensa jurídica de la persona en la sociedad digital. Este enfoque integral y proactivo no solo asegura la protección de los ciudadanos, sino que también establece un precedente para la construcción de marcos normativos adaptativos, capaces de anticipar riesgos futuros y de fomentar un ecosistema digital que sea seguro, equitativo y transparente.

El análisis histórico y doctrinal confirma que la transición del constitucionalismo clásico al neoconstitucionalismo, y de este hacia el constitucionalismo digital, no ha sido un proceso lineal ni estrictamente técnico. Responde a una reconfiguración del poder en el marco de una sociedad global e hiperconectada, donde actores privados transnacionales y el poder algorítmico alteran los límites tradicionales del control constitucional. Esta transformación obliga a superar la visión estrictamente vertical Estado–ciudadano para avanzar hacia un modelo horizontal y transnacional de garantías, en el que los derechos fundamentales encuentren protección también frente a particulares con capacidad de incidir en la esfera pública.

El análisis evidencia que la insuficiencia de los marcos constitucionales nacionales frente a riesgos contemporáneos no se limita a problemas teóricos. Fenómenos como la censura ejercida por plataformas digitales, la discriminación algorítmica en servicios financieros o educativos, la manipulación de información y la vigilancia masiva demuestran cómo la ausencia de regulación digital integral impacta directamente en la vida cotidiana de los ciudadanos. Esto revela una brecha creciente entre la normatividad vigente y la realidad tecnológica, en la que la falta de reconocimiento explícito de derechos digitales y de mecanismos de supervisión efectiva deja a los individuos en situación de vulnerabilidad frente a actores privados con poder desproporcionado en el ciberespacio.

Propositivamente, se plantea la necesidad de un constitucionalismo digital latinoamericano que integre la experiencia nacional con los estándares internacionales, proyectando los valores constitucionales hacia los entornos digitales y algorítmicos. Este modelo no solo busca garantizar la protección de los derechos fundamentales frente al Estado, sino también frente a los actores privados que operan a escala transnacional. La adopción de principios como la dignidad humana, la transparencia algorítmica, la responsabilidad compartida y la soberanía de los datos emerge como estrategia clave para asegurar la eficacia real de los derechos en contextos digitales complejos.

Finalmente, el capítulo concluye que la vigencia del Estado social de derecho en la era digital depende de una reformulación de los marcos constitucionales que reconozca la naturaleza híbrida del poder contemporáneo. Sin un constitucionalismo adaptado al ciberespacio y a los sistemas automatizados, la innovación tecnológica corre el riesgo de consolidarse como un vector de desigualdad, limitando el acceso equitativo a derechos esenciales. Así, la construcción de un constitucionalismo digital no es solo una necesidad

jurídica, sino una estrategia para fortalecer la democracia, la justicia social y la protección de los ciudadanos en un mundo interconectado, donde los límites tradicionales del derecho deben expandirse para responder a desafíos inéditos.

La Quinta Revolución Industrial profundiza la convergencia entre lo físico, lo digital y lo biológico, consolidando un poder tecnológico que se comporta como una nueva fuerza constituyente, capaz de generar asimetrías sociales, económicas y jurídicas. Herramientas como Big Data, inteligencia artificial, blockchain y metaverso, aunque ofrecen oportunidades significativas de innovación, desarrollo económico y transformación de servicios públicos y privados, también implican riesgos inéditos. Entre estos destacan la pérdida de privacidad, la despersonalización, la concentración de información, la discriminación algorítmica y la erosión de la autonomía individual.

La experiencia histórica de revoluciones industriales anteriores demuestra que el derecho, si no actúa de manera anticipada, tiende a reaccionar con retraso, lo que reduce su capacidad de control frente a dinámicas sociales y tecnológicas emergentes. En el contexto actual, esta reacción tardía puede traducirse en vulneraciones masivas de derechos fundamentales, inequidades en el acceso a recursos digitales y dependencia de sistemas tecnológicos que operan fuera del alcance de la supervisión democrática. Así, se evidencia que los marcos normativos tradicionales, concebidos en paradigmas industriales y analógicos, resultan insuficientes para abordar los desafíos de un entorno hiperconectado, globalizado y automatizado.

Por ello, este capítulo subraya la urgencia de integrar de manera simultánea la perspectiva ética, tecnológica y constitucional en un modelo de constitucionalismo digital. Este modelo debe priorizar la protección de la dignidad humana, la seguridad digital, la transparencia algorítmica y la justicia social, asegurando que la innovación tecnológica no se traduzca en nuevas formas de exclusión o desigualdad. Asimismo, la investigación propone que la regulación no se limite a la acción estatal, sino que contemple la responsabilidad compartida de los actores privados, incluyendo plataformas digitales, desarrolladores de software y proveedores de servicios tecnológicos, quienes ejercen un poder creciente sobre la vida cotidiana de los ciudadanos.

En términos prácticos, el constitucionalismo digital en la Quinta Revolución Industrial requiere mecanismos preventivos y reactivos: auditorías algorítmicas, estándares de privacidad

y protección de datos, protocolos de acceso equitativo a tecnologías críticas, y marcos de rendición de cuentas que integren supervisión pública y participación ciudadana. Esto no solo fortalece la protección de derechos fundamentales, sino que también fomenta la confianza social en la gobernanza tecnológica y la legitimidad de las instituciones frente a actores privados con influencia global.

En síntesis, la protección de los derechos fundamentales en la era digital no puede ser una respuesta reactiva: demanda un modelo proactivo y anticipatorio, que reconozca las complejidades de la Quinta Revolución Industrial y asegure que el desarrollo tecnológico sea inclusivo, ético y orientado al bienestar colectivo. Solo mediante un constitucionalismo digital adaptativo se podrá garantizar que la innovación tecnológica no se convierta en un factor de desigualdad, consolidando un marco normativo que equilibre progreso, justicia social y respeto por la dignidad humana en un mundo cada vez más interconectado.

El análisis del ordenamiento jurídico y la jurisprudencia colombiana revela un marco normativo disperso, reactivo y anclado en paradigmas analógicos, insuficiente para regular los entornos digitales complejos. Si bien la Constitución de 1991 y la Corte Constitucional han realizado adaptaciones relevantes, incluyendo pronunciamientos sobre protección de datos, privacidad y libertad de expresión en plataformas digitales, subsisten vacíos significativos en la regulación de tecnologías emergentes como la inteligencia artificial, el metaverso, la tokenización y la responsabilidad derivada de sistemas autónomos. Esta desconexión entre norma y realidad tecnológica genera escenarios donde los ciudadanos quedan expuestos a vulneraciones de derechos sin contar con herramientas jurídicas eficaces para su defensa.

La dispersión normativa se manifiesta también en la fragmentación de la legislación sectorial, que aborda la ciberseguridad, la protección de datos y la economía digital de manera aislada, sin garantizar coherencia ni articulación institucional. Esta situación se agrava frente a la influencia de actores privados transnacionales y algoritmos que operan más allá del control del Estado, afectando derechos fundamentales como la privacidad, la igualdad, la libertad de información y el debido proceso. Casos recientes sobre filtración de datos, decisiones automatizadas sesgadas y manipulación de contenidos muestran que los mecanismos de protección actuales resultan insuficientes para responder a la velocidad e impacto de la innovación tecnológica.

Propositivamente, la investigación sostiene que Colombia requiere una reforma integral que articule principios de ciberseguridad, ética algorítmica, soberanía digital y eficacia horizontal de los derechos fundamentales, consolidando así un verdadero constitucionalismo digital. Este enfoque no solo implica la actualización normativa, sino también la creación de marcos institucionales capaces de supervisar, auditar y regular la actividad tecnológica, garantizando la rendición de cuentas de actores públicos y privados por igual. Además, la incorporación de estándares internacionales y experiencias comparadas puede fortalecer la protección de los derechos digitales y permitir la anticipación de riesgos asociados a tecnologías disruptivas.

En síntesis, el capítulo evidencia que el desarrollo de un constitucionalismo digital colombiano no es una cuestión opcional, sino una necesidad estratégica para preservar la efectividad de los derechos fundamentales en un entorno cada vez más digitalizado y globalizado. Solo mediante un marco normativo integral, articulado y adaptativo, será posible garantizar que la innovación tecnológica se desarrolle de manera ética, segura y equitativa, consolidando la confianza de los ciudadanos en las instituciones y protegiendo la dignidad humana frente a los desafíos de la era digital.

Los retos identificados muestran que el constitucionalismo colombiano atraviesa una crisis de eficacia frente al poder digital transnacional. La ausencia de políticas integrales de gobernanza tecnológica, sumada a la persistente brecha digital y a la dependencia de soluciones judiciales ex post, limita gravemente la capacidad del Estado para garantizar la protección de los derechos fundamentales. Este déficit normativo y estructural evidencia la falta de una estrategia nacional coherente que articule los ámbitos jurídico, ético y tecnológico, lo cual impide responder de manera oportuna a los desafíos generados por la automatización, la inteligencia artificial, el uso masivo de datos y la desinformación digital.

El desplazamiento progresivo de la toma de decisiones hacia sistemas automatizados y actores ajenos al control democrático erosiona la legitimidad del Estado social de derecho. Plataformas privadas y arquitecturas algorítmicas gestionan información, definen criterios de visibilidad, condicionan comportamientos y determinan oportunidades sociales y económicas, todo ello sin mecanismos efectivos de rendición de cuentas. Este escenario pone en cuestión la soberanía jurídica del Estado y la vigencia de principios constitucionales como la igualdad, la transparencia y la participación ciudadana. El derecho constitucional, concebido para limitar el poder político estatal, enfrenta hoy la necesidad de extender su alcance hacia un poder

tecnológico distribuido y opaco, cuyo control requiere nuevas herramientas normativas, institucionales y pedagógicas.

Frente a este panorama, se propone que Colombia asuma un papel de liderazgo regional mediante la creación de un sistema de gobernanza digital constitucionalizado. Dicho sistema debe sustentarse en tres pilares estratégicos:

i) Responsabilidad jurídica clara para plataformas y sistemas autónomos, que incluya criterios de imputación, transparencia y supervisión de decisiones algorítmicas, así como la posibilidad de control judicial efectivo sobre actos tecnológicos con efectos jurídicos o sociales.

ii) Reconocimiento y protección efectiva de nuevos derechos digitales, como el derecho a la identidad digital, la autodeterminación informativa, la protección frente a sesgos algorítmicos y el derecho a la desconexión tecnológica, asegurando que la innovación se oriente al bienestar y no a la explotación o vigilancia del individuo.

iii) Cooperación internacional orientada a la gestión de riesgos globales y a la preservación de la soberanía jurídica, entendida no como aislamiento, sino como capacidad de los Estados para participar activamente en la definición de estándares éticos, normativos y técnicos que regulen el ecosistema digital de manera justa y equitativa.

Además, este modelo debe promover la formación ética y tecnológica de funcionarios públicos, juristas y ciudadanos, reconociendo que la alfabetización digital es condición necesaria para la participación democrática en el siglo XXI. El Estado debe transformarse en garante activo de la confianza digital, articulando políticas de innovación con estrategias de protección de derechos y fortaleciendo la cooperación público-privada bajo parámetros de transparencia y control social.

En síntesis, el capítulo demuestra que el constitucionalismo digital colombiano se enfrenta a un punto de inflexión: o se redefine para responder al poder tecnológico global o se resigna a su pérdida progresiva de relevancia y legitimidad. La construcción de un marco de gobernanza digital constitucionalizado no solo permitirá asegurar la eficacia de los derechos en entornos digitales, sino que también posicionará a Colombia como referente regional en la defensa jurídica, ética y social de la persona en la era tecnológica, contribuyendo a una transformación democrática acorde con los desafíos de la Quinta Revolución Industrial.

El modelo propuesto demuestra que el constitucionalismo digital no es una aspiración teórica ni un ideal lejano, sino una necesidad urgente para garantizar la vigencia, la eficacia y la legitimidad de la Constitución en el contexto de la Quinta Revolución Industrial. En un entorno donde los algoritmos, las plataformas digitales y los sistemas inteligentes se han convertido en mediadores del ejercicio de derechos, cualquier propuesta que permanezca anclada a esquemas analógicos carecerá de capacidad para responder a la velocidad, complejidad e impacto social de la innovación tecnológica.

El modelo de constitucionalismo digital colombiano planteado en esta investigación articula los principios del constitucionalismo clásico, como la dignidad humana, la igualdad, la libertad y la solidaridad, con la configuración de nuevos derechos digitales indispensables en la sociedad hiperconectada. Entre ellos se destacan el derecho a la identidad digital, la soberanía sobre los datos personales, la protección frente a decisiones automatizadas, el derecho a la desconexión tecnológica y la transparencia algorítmica como dimensión del debido proceso digital. Estos derechos emergentes no sustituyen los tradicionales, sino que los expanden hacia el ciberespacio, garantizando su eficacia en entornos donde el poder ya no reside exclusivamente en el Estado, sino también en corporaciones tecnológicas globales con capacidad de condicionar la vida social, económica y política.

El modelo propuesto establece además mecanismos de responsabilidad jurídica diferenciada para actores privados globales, que incluyen obligaciones de transparencia, auditoría y rendición de cuentas sobre el diseño, uso y efectos de sistemas algorítmicos. Esto busca superar la asimetría entre los ciudadanos y los operadores tecnológicos, promoviendo una relación más equitativa y compatible con los principios del Estado social de derecho. En este sentido, la soberanía de los datos se erige como eje central de la justicia digital, al reconocer que el control efectivo de la información es condición esencial para la autonomía, la privacidad y la autodeterminación individual.

El proyecto de ley presentado como anexo constituye un instrumento operativo inicial para materializar este paradigma. Su estructura combina tres dimensiones esenciales: la regulación preventiva, que busca anticipar riesgos mediante principios éticos y estándares técnicos; la protección efectiva de derechos, que fortalece los mecanismos de tutela y reparación ante vulneraciones digitales; y el fomento de la innovación tecnológica responsable, que incentiva el desarrollo de inteligencia artificial y tecnologías emergentes bajo criterios de transparencia, equidad y sostenibilidad. En conjunto, estas medidas adaptan el marco jurídico

colombiano a las exigencias de la sociedad digital contemporánea, proyectándolo como modelo de equilibrio entre innovación y derechos.

La investigación confirma que la Quinta Revolución Industrial representa un desafío constitucional profundo, en el que la dignidad humana, la autonomía y la igualdad se ven tensionadas por poderes digitales que operan más allá del alcance tradicional del Estado. La velocidad de la transformación tecnológica exige una respuesta jurídica flexible, dinámica y articulada, capaz de anticipar riesgos y de garantizar que la tecnología se mantenga al servicio de la persona y no a la inversa. El constitucionalismo clásico y el neoconstitucionalismo, sin una extensión explícita al ámbito digital, resultan insuficientes para asegurar la vigencia real de los derechos fundamentales.

Por tanto, la defensa de los derechos en la era digital exige un cambio cultural, jurídico e institucional, sustentado en la ética digital, la cooperación internacional y la educación tecnológica. La ética digital actúa como principio transversal que orienta el diseño y la aplicación de las tecnologías conforme al respeto por la dignidad y la justicia social; la cooperación internacional garantiza la capacidad del Estado para enfrentar fenómenos transnacionales como la desinformación, la vigilancia masiva o el cibercrimen; y la formación ciudadana digital se convierte en pilar de una democracia informada y participativa.

En suma, esta tesis plantea una hoja de ruta para la consolidación de un constitucionalismo digital colombiano, que armoniza la tradición jurídica del Estado social de derecho con las exigencias de la nueva era tecnológica. El modelo aspira a proyectar a Colombia como referente regional en la protección de los derechos fundamentales en entornos algorítmicos y transnacionales, consolidando una visión del derecho que no se limite a reaccionar frente a la tecnología, sino que la oriente éticamente al servicio del ser humano, de la equidad y del bien común. Solo a través de este enfoque será posible preservar la supremacía constitucional y asegurar que la innovación tecnológica contribuya a una sociedad más justa, libre y humana.

Referencias Bibliográficas.

Aguilar Calahorro, A. y. (2017). Derechos fundamentales y democracia en el constitucionalismo digital. . *Marcial Pons*.

Aibar, E. (2019). *Revoluciones industriales: un concepto espurio.* Oikonomics[en línea].

Ajay Agrawal, J. G. (2019). *Prediction Machines.* Barcelona - España: Editorial Reverté, S. A.

Alcañiz, M. (2008). Cambios demográficos en la sociedad global. *Papeles de población, 14(57)* , 227-255.

Allen, R. (2009). *The British Industrial Revolution in Global Perspective (New Approaches to Economic and Social History).* Prensa de la Universidad de Cambridge.

Alva-Arroyo, N. V.-G.-A.-E. (2022). Transhumanismo. . *Medicina Interna de México*, 38(4), 741-751.

Amaya Cogollo, G. S. (2024). Implicaciones legales y desafíos en la persecución de fraudes, estafas y otros delitos cibernéticos en el comercio electrónico en Colombia.

AMG Metalmecánica Gallega . (28 de agosto de 2024). *La Segunda Revolución Industrial: Transformación y Avances Tecnológicos*. Obtenido de https://www.amgmetalmecanica.com/la-segunda-revolucion-industrial/

Antón, J. H. (2021). Fundamentos tecnologicos de los criptoactivos, criptoactivos. retos y desafios normativos. *AAVV*.

Armstrong, M. (16 de octubre de 2024). *The Future Of A.I.* Obtenido de The Statistics Portal: https://www.statista.com/chart/6810/the-future-of-ai/

Asamblea General de las Naciones Unidas. (10 de enero de 2025). *Declaración Universal de Derechos Humanos. Artículo 19*. Obtenido de https://www.un.org/es/.

Aranda, V. T. (2004). Historia y evolución de Internet. *Autores científico-técnicos y académicos*, *33*(1), 22-32.

Argote, J. G., Maldonado, E., & Maldonado, K. (2025). Algorithmic Bias and Data Justice: ethical challenges in Artificial Intelligence Systems. *EthAIca: Journal of Ethics, AI and Critical Analysis*, (4), 5.

Arencibia, M. G. (2023). El lado oscuro del Big Data como un problema social. *Serie Científica de la Universidad de las Ciencias Informáticas*, *16*(9), 1-27.

Allevato, G., & Pastor-Merchante, F. (2021). The Google Ireland Case and the Legal Battle over Digital Taxes in the European Union. *Review of European Administrative Law*, *14*(1), 209-220.

Acquier, A., Daudigeos, T., & Pinkse, J. (2017). Promises and paradoxes of the sharing economy: An organizing framework. *Technological Forecasting and Social Change*, *125*, 1-10.

Amnistía Internacional (2019). *Surveillance giants: how the business model of Google and Facebook threatens human rights*. Amnistía Internacional Ltd. Londres, UK. https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

Amnistía Internacional (2025). *Breaking up with Big Tech a human rights-based argument for tackling big tech's market power*. Amnistía Internacional Ltd. Londres, UK. https://www.amnesty.nl/content/uploads/2025/08/Breaking-Up-Big-Tech-Report.pdf.

Amnistía Internacional (2015). *7 maneras en que el mundo ha cambiado gracias a Edward Snowden*. [Sitio web]. https://www.amnesty.org/es/latest/campaigns/2015/06/7-ways-the-world-has-changed-thanks-to-edward-snowden/.

American Civil Liberties Union; Center For Democracy & Technology. (2015). *"Secret Surveillance: Five Large-Scale Global Programs".* [sitio web] https://cdt.org/wp-content/uploads/2014/09/cdt-aclu-upr-9152014.pdf..

Aguado, J. M. (2020). *Mediaciones ubicuas: ecosistema móvil, gestión de identidad y nuevo espacio público*. Gedisa Editorial.

AWS (s.f.). ¿Qué es un bot?. [sitio web]. https://aws.amazon.com/es/what-is/bot/.

Aznar, E. (2024). Desafíos legales y estructuras de las Organizaciones Autónomas Descentralizadas (DAOs): Un breve análisis para el marco jurídico actual. [Sitio web]. *Blog de Legal Cripto by BAES*. https://www.baeslegalcripto.eu/legalcripto/desafios-legales-y-estructuras-de-las-daos/.

Baca, D. V. (2023). .La Constitución digital en Perú: a propósito de sus treinta años de vigencia.

Balkin, J. M. (2015). The path of robotics law. Calif. L. Rev. *Circuit, 6*, 45.

Ball, M. (2022). El metaverso. Y cómo lo revolucionará todo. *Deusto*, 392.

Ball, M. (2022). *Metaverso.* Milano: Garzanti.

Banco de Desarrollo de América Latina. (2021). *La economía digital y las industrias digitales basadas en el conocimiento.* Corporación Andina de Fomento.

Barrilao, J. F. (2022). CONSTITUCIONALISMO DIGITAL: ENTRE REALIDAD DIGITAL, PROSPECTIVA TECNOLÓGICA Y MERA DISTOPÍA CONSTITUCIONAL. *da AJURIS–Porto Alegre*, 397-398.

Barrilao, J. F. (2023). derecho constitucional hoy: entre realidad, prospectiva y distopía digital. *Thomson Reuters Aranzadi*, 19-37.

Becerra, J. C.-H.-A.-Á.-V. (9 de enero de 2018). Marco teórico y aproximación jurídica al Big Data: algoritmos, inteligencia artificial y transformación digital. . Bogotá, Colombia: Universidad Católica.

Blanqui, J. A. (1837). *Histoire de l'économie politique en Europe depuis les anciens jusqu'à nos jours.* .

Bostrom N. (2005). In defense of posthuman dignity. Bioethics, 1. 2.–2. (2005). In defense of posthuman dignity. *Bioethics*, 202–214.

Botella, C. R. (2007). La utilización de las nuevas tecnologías de la información y la comunicación en psicología clínica. *Revista sobre la societat del coneixement.*

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *Calif. L. Rev.*, *104*, 671.

Bachs, L. (2025). AI Act: timeline para la aplicación del Reglamento Europeo de Inteligencia Artificial. [sitio web]. *AURIS legal*. https://auris.legal/ai-act-timeline-para-la-aplicacion-del-reglamento-europeo-de-inteligencia-artificial/.

Barría Huidobro, C. D. (2024). Alucinaciones de la inteligencia artificial: impacto en tecnología, política y sociedad. *Revista Estrategia Poder y Desarrollo, 3*(5), 47-64. https://dx.doi.org/10.25062/2955-0289.4847.

Balkin, J. M. (2018). Free speech is a triangle. *Colum. L. Rev.*, *118*, 2011.

Brewer Carias, A. (2007). Notas sobre la situación general de la acción de amparo contra particulares en el derecho latinoamericano. *Revista Iberoamericana de Derecho Constitucional 109* (72).

BBC News. "Yahoo hit by Big gest data breach in history." (2016). https://www.bbc.com/news/technology38301594.

Bird & Bird. (2025). *European Union Artificial Intelligence Act: a guide*. [Sitio web].https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Braun, M., Vallery, A., Benizri, I. (2024). What Are High-Risk AI Systems Within the Meaning of the EU's AI Act, and What Requirements Apply to Them?. [Sitio web]. *Wilmerhale*. https://www.wilmerhale.com/api/sitecore/module/pdfgeneration?itemurl=%2fen%2finsights%2fblogs%2fwilmerhale-privacy-and-cybersecurity-law%2f20240717-what-are-highrisk-ai-systems-within-the-meaning-of-the-eus-ai-act-and-what-requirements-apply-to-them&itemid=%7b5cadfc15-1cde-4873-9f35-a5c254481456%7d.

Brownsword, R. (2019). *Law, technology and society: reimagining the regulatory environment*. Routledge.

Callejón, F. B. (19 de abril de 2024). *La Constitución del algoritmo*. Obtenido de Fundación Giménez Abad: https://www.fundacionmgimenezabad.es/sites/default/files/Publicar/actividades/documentos/2021/

Camacho, S. (2017). La subjetividad "cyborg". En Navarro, S. (Dir.). Inteligencia artificial: tecnología Derecho. *Editorial Tirant to Blanch*, pp- 231-252).

Canals, J. (2000). Crecimiento empresarial: personas y tecnología en la nueva economía. *Revista Empresa Y Humanismo*, 337-370.

Carmona, J. L. (2023). Trabajar en la Industria 4.0 Medición del Impacto Ocupacional ocasionado por la transformación digital de las empresas en el sector manufacturero español.

Castells, M. (2006). *La era de la información economía, sociedad y cultura.* España: Alianza.

Castells, M. (2010). *The Rise of the Network Society.* Offices.

Clavijo, S. N. (2018). El ciborg humano. *Comeras*, 2.

Coleman, D. C. (1992). Myth, History and the Industrial Revolution. Londres: A&C Black.

Carbonell, M. (2007). *Teoría del neoconstitucionalismo: ensayos escogidos*. Trotta Editorial.

Castillo, A. L. (2025). *Constitucionalismo crítico en tiempo real: el proceso constituyente en Chile* (Vol. 1). Editorial Universitas.

Cámara de Comercio España (2020). *¿Qué es una startup?*. https://www.camara.es/blog/creacion-de-empresas/que-es-una-startup.

Celeste, E. (2018). What is digital constitutionalism?. *Alexander Von Humboldt Institut Für Internet Und Gesellschaf.* https://www.hiig.de/en/what-is-digital-constitutionalism/.

Centeno, A. (2019). *Deep learning*. Trabajo de grado para optar al título de matemático. Universidad de Sevilla, España.

Centro Latinoamericano de Investigación Periodística (CLIP). (2025). *La Mano Invisible de las Big Tech: Introducción*. [Sitio web]. https://www.elclip.org/la-mano-invisible-de-las-big-tech-introduccion/.

Comanducci, P. (2002). Formas de (neo) constitucionalismo: un análisis metateórico. *Isonomía*, (16), 89-112.

Cadwalladr, C. (2018). The Cambridge Analytica Files. The Guardian. https://www.theguardian.com/news/series/cambridge-analytica-files.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridgeanalytica-facebook-influence-us-election.

Cronología de la regulación de la IA en Europa y España. (7 de mayo de 2025). [Sitio web]. IA ON. https://www.ia-on.es/regulacion-internacional/cronologia-de-la-regulacion-de-la-ia-en-europa-y-espana/.

Coroado, S. (2023). *Leviathan vs Goliath or States vs Big Tech and what the digital services act can do about it*. Working Papers, Forum Transregionale Studien. https://www.reconstitution.eu/fileadmin/bilder/re_constitution/WP_25-2023_Coroado_final.pdf.

Cova-Fernández, E. J. (2022). Derechos humanos y derechos digitales en la sociedad de la información. *Revista DH/ED: derechos humanos y educación*, (6), 61-80.

Comisión Europea (1998). *Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales*. Documento de trabajo DG XV D/5057/97: Evaluación de la autorregulación industrial: ¿en qué casos realiza una contribución significativa al nivel de protección de datos de un país tercero? Adoptado el 14 de enero de 1998.

Concepto. (15 de mayo de 2024). *Tercera revolucion industrial*. Obtenido de Editorial Etecé: https://concepto.de/tercera-revolucion-industrial/#:~:text=Puntos%20clave-,La%20Tercera%20Revoluci%C3%B3n%20Industrial%20fue%20un%20proceso%20de%20transformaci%C3%B3n%20tecnol%C3%B3gica,la%20b%C3%BAsqueda%20de%20energ%C3%ADas%20renovables.

Cueva, R. V. B. (2019). A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. *Lei Geral de Proteção de Dados–e suas repercussões no Direito brasileiro*, *2*, 83-96.

Custers, B.H.M. *(2018)* Data Mining and Profiling in Big Data, in B.A. Arrigo (ed.) *The SAGE Encyclopedia of Surveillance, Security, and Privacy, p. 277-279*- Thousand Oaks: SAGE Publications, Inc.

Cuzcano-Chavez, X., & González-Véliz, C. (2025). Análisis del abuso de aplicaciones deepfake y su impacto en la violencia digital de género en América Latina y el Caribe. *Veritas*, (61), 32-67.

Crawford, K. (2016). Can an algorithm be agonistic? Ten scenes from life in calculated publics. *Science, Technology, & Human Values*, *41*(1), 77-92.

Comisión Económica para América Latina y el Caribe (CEPAL) (2020). *Red de Políticas de Internet y Jurisdicción, Elementos principales del informe sobre el estado de la jurisdicción de Internet en América Latina y el Caribe*. (LC/TS.2020/68). Santiago, Chile.

Corvalán, J. G., Davila, L. D., & Simari, G. I. (2021). *Inteligencia artificial: Bases conceptuales para comprender la renovación de las revoluciones"*. Buenos Aires: Ciudad autonoma de Buenos Aires.

de Oliveira Fornasier, M. (2021). Artificial intelligence and democratic rule of law. Revista de Estudos Constitucionais, *Hermenêutica e Teoria do Direito (RECHTD),* 13(3), 351-369.

De Vroey, M. (2009). El liberalismo económico y la crisis. *Lecturas de Economía , (70),* , 11-38.

Deckers, J. L. (2021). *Más (que) humanos: Biotecnología, inteligencia artificial y ética de la mejora.* . omercial Grupo ANAYA, SA.

Departamento Nacional de Planeación. (8 de Enero de 2024). *Departamento Nacional de Planeación*. Obtenido de https://dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-economia-y-transformacion-digital.aspx

Departamento Nacional de Planeación. (8 de enero de 2025). *Plan Nacional de Desarrollo 2022-2026*. Obtenido de https://www.dnp.gov.co/plan-nacional-desarrollo/pnd-2022-2026

Díez Estella, F. &. (2023). La nueva Carta de Derechos Digitales en España, y los nuevos reglamentos comunitarios DSA, DMA e IA: ¿hacia un constitucionalismo digital? CEFLegal. *Revista práctica de derecho* .

Domènech, C. B., & Esteve, J. S. (2022). Los derechos fundamentales ante las aporías de la era digital. *Cuestiones constitucionales*.

Dominguez, A. G. (2023). *Constitucionalismo Digital.* Buenos Aires: Ediar.

Diccionario panhispánico del español jurídico (2025). *Definición "neoconstitucionalismo"*. http://dpej.rae.es/lema/neoconstitucionalismo.

De Gregorio, G. (2022). Digital Constitutionalism: An Introduction. *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society(pp. 1–37). Cambridge University Press.* https://doi. org/10.1017/9781009071215.002.

Del Campo, A. (2025). Digital Constitutionalism in Latin America. *CELE Research Paper*, (65).

De la Sierra, S. (2022). Una introducción a la Carta de derechos digitales. *La carta de derechos digitales, Tirant Lo Blanch*.

Docusign (2025). Ley Federal de Protección de Datos: ¿qué es y cuándo es aplicable?. [SITIO WEB]. https://www.docusign.com/es-mx/blog/proteccion-de-datos-personales.

Dhingra, M., & Mudgal, R. K. (2019). Historical evolution of social media: An overview. In *International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India*.

Díaz Senés, J. P. (2024). *Panorámica internacional de la regulación de la Inteligencia Artificial: Reglamento Europeo de Inteligencia Artificial* (AI ACT). Revista CESCO de Derecho de Consumo, ISSN-e 2254-2582, Nº. 49, 2024, págs. 117-130

El Pais. (7 de enero de 2025). *Ediciones EL PAÍS*. Obtenido de Apostar por la digitalización de nuestra democracia: https://elpais.com/chile/2024-11-22/apostar-por-la-digitalizacion-de-nuestra-democracia.html?utm_source=chatgpt.com

Emst-Slavit, G. (2001). La Teoría de las Inteligencias Múltiples de Gardner. *Revista de Psicología de la PUCP. Vol. XIX, 2, 2001*, 321.

Escobar, R. M. (2003). Reseña de "La sociedad del riesgo global" de Ulrich Bech. *Revista Española de Investigaciones*, 279-283.

Escudero, W. S. (2021). *Big data siglo XXI.* Buenos Aires: Ciudad Autónama de Buenos Aires.

Estenssorio, A. C. (2011). *Los Desafíos del Crecimiento y Desarrollo en el Contexto del Cambio Climático.* Chile: Frasis.

Espinoza, J. J. T., & Hidalgo, J. C. (2022). El neoconstitucionalismo: orígenes, desarrollo y su importancia dentro del Ecuador como estado constitucional de derechos. *Polo del Conocimiento*, *7*(9), 1783-1800.

Erdogan, I. (2023). Transparency in the Face of New Technologies: Information Rights under the Law Enforcement Directive. *Jean Monnet Network on EU Law Enforcement Working Paper Series.* https://jmn-eulen.nl/wp-content/uploads/sites/575/2023/06/5.-WP-Erdogan.pdf.

F, S. B. (2020). Riesgos y seguridad a comienzos del siglo XXI (y una coda al. *AA.VV. Los derechos fundamentales ante las crisis económicas*, p. 311-313.

Fernández, L. E. (2012). *Breve historia de la Revolución Industrial. Nowtilus.*

Ferrer, A. (2022). *Historia de la globalización II: La Revolución Industrial y el segundo orden mundial* . Argentina: Fondo de Cultura Económica Argentina.

Filosofia & co. (10 de junio de 2024). *Heidegger y la técnica en el mundo moderno*. Obtenido de https://filco.es/heidegger-tecnica/

Finquelievich. (s.f.). *Finquelievich, S. i-polis ebook. pdf.* i-polis ebook. .

Flores, R. (2020). Segunda Revolución. En Imperialismo capitalista . *Portal Académico del CCH, UNAM.* . Obtenido de https://portalacademico.cch.unam.mx/historiauniversal2/imperialismo-capitalista/segunda-revolucion#:~:text=La%20segunda%20revoluci%C3%B3n%20industrial%20impuls%C3%B3,caso%20con%20nuevos%20territorios%20colonizados.

Friedman, M. (1995). La Segunda Revolución Industrial. *Ciencia política: Revista trimestral para América Latina y España, (38)*, 49-56.

Ferrajoli, L. (2010). *Democracia y Garantismo*. Madrid, España: Trotta.

Farid, H. (2022). Creating, using, misusing, and detecting deep fakes. *Journal of Online Trust and Safety*, *1*(4).

Flores, M. (2023). Qué es la LGPD y cómo cumplir con la Ley de Protección de Datos Personales en Brasil. *Delete Technology* [SITIO WEB]. https://www.deletetechnology.com/blog/qu%C3%A9-es-la-lgpd-y-c%C3%B3mo-cumplir-con-la-ley-de-protecci%C3%B3n-de-datos-personales-en-brasil.

Fernandez, R., Adriaans, I., Klinge, T. J., & Hendrikse, R. (2020). The financialisation of big tech. *SOMO (Stichting Onderzoek Multinationale Ondernemingen)*, *1*(1), 12-21.

Forero, F. (27 de abril de 2023). *¿Quién es el autor de las obras creadas por Inteligencia Artificial?*. Conferencia en el marco de la FilBo. Bogotá, Colombia

Frazão, A., & Mulholland, C. (Eds.). (2020). *Inteligência Artificial e Direito: ética, regulação e responsabilidade*. Revista dos Tribunais (2). ISBN 9786556142210.

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*(1), 1-3.

García, M.A. (2023). *Apoyo de investigación en la línea de Tecnología, Transparencia y Derechos Humanos en la Organización Dejusticia*. Trabajo de Grado para Optar al Título de Abogada. Universidad Industrial de Santander. Bucaramanga, Colombia.

García Jaramillo, L. (2010). Buenos tiempos para el neoconstitucionalismo (sobre la aparición de El examen de proporcionalidad en el derecho constitucional). *Vniversitas*, (120), 317-332.

García Jaramillo, L. (2012). El neoconstitucionalismo en el contexto de la internacionalización del derecho: El caso colombiano. *Boletín mexicano de derecho comparado*, *45*(133), 93-118.

Gavilán, C. T. (2025). La digitalización jurídica en Colombia: de la ley a la práctica. Análisis crítico de las normas sobre el uso de las nuevas tecnologías antes, durante y después de la pandemia. *Estudios Socio-Jurídicos, 27*(2).

Gravett, W. (2020). The dark side of artificial intelligence: challenges for the legal system. *Southern African Public Law, 35*(1), 30-pages.

Gardbaum, S. (2003). The" Horizontal Effect" of Constitutional Rights. *Michigan Law Review*, *102*(3), 387-459.

Gargarella, R. (2018). Sobre el Nuevo Constitucionalismo Latinoamericano, *Revista Uruguaya de Ciencia Politica 27*, 1 (2018) http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S1688499X2018000100109.

Gaitán, I. D. (2024). Derechos humanos, derecho animal y crítica de la violencia especista: el lugar de la sintiencia. . *Análisis Jurídico-Político, 6(11),* , 15-32.

Gamarra, R. (2022). El futuro del trabajo y la necesidad de un nuevo estilo de liderazgo . *(Doctoral dissertation, Universidad Nacional de Luján).*

Gaos, J. (2022). *Filosofía de la técnica.* México.: Herder .

García, J. J. (2012). BIOÉTICA PERSONALISTA Y BIOÉTICA. *Cuadernos de Bioética*, 67-76.

García, M. D. (7 de enero de 2025). *Constitucionalismo ciborgiano: la necesidad de pensar y re-pensar en un derecho fundamental a la mejora y otras cuestiones*. Obtenido de en Blog Revista Derecho del Estado: Marco David Camacho García, “Constitucionalismo ciborgiano: la necesidad de pensar y re-pensar en un derecho fundamental a la mejora y otras cuestiones” en Blog Revista Derecho del Estado, 2 de noviembre de 2023. Disponible en: https://blogrevistaderechoe

García, R. J. (2023). *Retos actuales del derecho real de dominio en Colombia. 9(1), 75-88.* Legem.

Gayozzo, P. (2019). *¿Qué es el transhumanismo?* Lima: IET.

Gobierno de Colombia. (7 de enero de 2025). *Estrategia Nacional Digital de Colombia 2023 - 2026*. Obtenido de Departamento Nacional de Planeación:

https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf

González, A. G. (2022). El auge del Constitucionalismo digital en México. Retos y Perspectivas.

González, L. O. (2018). Fintech, blockchain y big data. In 4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital. *Thomson Reuters Aranzadi.*, 106.

Golia Jr, A. (2022). Critique of digital constitutionalism: Deconstruction and reconstruction from a societal perspective. *GlobCon*, *13*, 488.

González-Páramo, J. M. (2021). En torno a la regulación de las Bigtech en finanzas. *Anales De La Real Academia de Ciencias Morales y Políticas* (pp. 247-266). Ministerio de Justicia.

González, A. G. (2022). El auge del Constitucionalismo digital en México. Retos y Perspectivas. *REVISTA INTERNACIONAL & COMPARADA DE DERECHOS HUMANOS*, 99.

Gorgoni, G. (2021). Special Section introduction: Identity and Citizenship in the Algorithmic Society. *Journal of Ethics and Legal Technologies*, *3*(2), 1-13.

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*(3), 291-323.

Goodman, C. C. (2019). AI/Esq.: Impacts of artificial intelligence in lawyer-client relationships. *Okla. L. Rev.*, *72*, 149.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2020). Generative adversarial networks. *Communications of the ACM*, *63*(11), 139-144.

Giovannini, C. J. (2023). DAOs: Unlocking the Full Potential of Blockchain Technology for the Real Physical World by Exploring Self-Organizing and Self-Regulating Decentralized Systems by Applying Smart Contracts and First Attempts of Applying

AI. *International Journal of Law in Changing World, Special Issue NFTs*, 80-117. DOI: https://doi.org/10.54934/ijlcw.v2i3.59.

Han, B. C. (2013). *La sociedad de la transparencia.* Berlin: Herder.

Han, B. C. (2022). *Infografia. La Digitalización y la Crisis de la democracia.* Buenos Aires: Taurus.

Han, B.-C. (2012). *La sociedad del cansancio.* Barcelona: Heder.

Han, B.-C. (2018). Hiperculturalidad. 18.

Hobsbawm, E. J. (1968). *Industry and Empire: The Birth of the Industrial Revolution.* . Pelican Books.

Hassan, S. & De Filippi, P. (2021). Decentralized Autonomous Organization. *Internet Policy Review, 10*(2). https://doi.org/10.14763/2021.2.1556

Hutchinson, A. (Mayo 12, 2023). Meta Outlines Its Evolving AI Ad Targeting Process, Which Is Improving Ad Performance. *Social Media Today*. [SITIO WEB]. https://www.socialmediatoday.com/news/meta-outlines-evolving-ai-ad-targeting-process-improving-ad-/650225/.

Haitsma, L. M. (2025). From Risk Regulation to Risk Governance:: Examining the Dutch Public Policy Approach to Addressing Discrimination in Algorithmic Profiling. *Technology and Regulation*, *2025*, 404-423.

Helmus, T. C. (2022). *Artificial intelligence, deepfakes, and disinformation: A primer*. RAND National Security Research Division. California, Estados Unidos. https://www.rand.org/pubs/perspectives/PEA1043-1.html.

Herrera Lima, Fernando F.. (2012). La migración a Estados Unidos: una visión del primer decenio del siglo XXI. *Norteamérica*, *7*(2), 171-197. Recuperado en 04 de diciembre de 2025, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35502012000200006&lng=es&tlng=es.

IBM. (28 de Septiembre de 2024). *¿Qué es Big Data?*. . Obtenido de http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/]

Infobae. (10 de JUNIO de 2023). *Adelanto de "Constitucionalismo digital", el nuevo libro de Andrés Gil Domínguez*. Obtenido de https://www.infobae.com/judiciales/2023/06/11/adelanto-de-constitucionalismo-digital-el-nuevo-libro-de-andres-gil-dominguez/

ITUPublications. (10 de Enero de 2025). *International Telecommunication Union*. Obtenido de Measuring digital development Facts and figures 2021: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf.

IONOS (2020). ¿Qué es un HTTP?. IONOS Digital Guide. https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/protocolo-http/.

Isin, E., & Ruppert, E. (2020). *Being digital citizens*. Rowman & Littlefield.

IMMERSIA (2025). La "Caja Negra" en la Inteligencia Artificial. [SITIO WEB]. https://www.immersia.eu/recursos/blog/la-caja-negra-en-la-inteligencia-artificial.

Information Commissioner's Office [ICO] (8 de octubre de 2025). *UK Upper Tribunal hands down judgment on Clearview AI Inc*. [SITIO WEB]. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/10/uk-upper-tribunal-hands-down-judgment-on-clearview-ai-inc/.

Jimenez Retana, R. (2018). Perfeccionamiento Humano: Envejecimiento en la era de la tecnociencia. *InterSedes [online]*.

Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Xu, Y., ... & Fung, P. (2023). Survey of hallucination in natural language generation. *ACM Computing Surveys, 55*(12), 1-38.

Johnson, M. (2023). Decentralized Autonomous Organization Laws across the U.S. *Stinson: news & insights*. https://www.stinson.com/printpilot-publication-decentralized-autonomous-organization-laws-across-the-us.pdf?1764630236.

Karnow, C. E. (2016). The application of traditional tort theory to embodied machine intelligence. In *Robot law* (pp. 51-77). Edward Elgar Publishing.

Kotliar, D. M. (2021). Who gets to choose? On the socio-algorithmic construction of choice. *Science, Technology, & Human Values*, *46*(2), 346-375.

Kouzy, R., Abi Jaoude, J., Kraitem, A., El Alam, M. B., Karam, B., Adib, E., ... & Baddour, K. (2020). Coronavirus goes viral: quantifying the COVID-19 misinformation epidemic on Twitter. *Cureus*, *12*(3).

Kluger, E. (2020). Inteligencia artificial – *¿Cómo funciona el aprendizaje automático?***.** Siemens Stiftung. [sitio web]. https://crea-portaldemedios.siemens-stiftung.org/inteligencia-artificial-como-funciona-el-aprendizaje-automatico-101289.

Karbiner, M. N. (9 de dicimbre de 2024). Diseño de modelo de negocios descentralizados antifrágiles basados en tecnología blockchain. *(Bachelor's thesis).* Bucaramanga, Santander, Colombia: MBA - Maestría en Administración de Empresas.

La BBC. (12 de octubre de 2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). *BBC*.

La Republica . (13 de julio de 2023). La ruta digital: la Nao de China. *La ruta digital: la Nao de China*.

Landes, D. S. (1969). *The Unbound Prometheus: Technical Change and Industrial Development in Western Europe from 1750 to the Present.* Cambridge University Press.

La Rue, F. (2011). Libertad de expresión de los pueblos indígenas, minorías y grupos vulnerables. *Ávila, María et al*, 243-252.

Lewis, N. (2019). *Should AI be used to catch shoplifters?* CNN Bussines. London, UK. https://edition.cnn.com/2019/04/18/business/ai-vaak-shoplifting/index.html.

Lehmann, E. L., & Lehmann, E. L. (2011). Model specification: the views of Fisher and Neyman, and later developments. In *Selected Works of EL Lehmann* (pp. 955-963). Boston, MA: Springer US.

Lozada, A. (2019). ¿Qué es un algoritmo?. [SITIO WEB]. *EDteam*. Recuperado de: https://ed.team/comunidad/que-es-un-algoritmo.

Manyika, J. (2011). The next frontier for innovation, competition, and productivity. *McKinsey Global Institute*.

Marx, K. &. (1848). *Manifesto of the Communist Party.* Moscú: Progress Publishers.

Mendes, G. F. (2020). Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Justiça do Direito*, 6-51.

Mendes, G. y. (2020). Constitucionalismo digital e jurisdição constitucional: una agenda de pesquisa para el caso brasileño. Revista Brasileira de Directo . *Revista Brasileira de Directo* .

Ministerio de Tecnologías de la Información y las Comunicaciones. (8 de enero de 2025). *Ministerio de Tecnologías de la Información y las Comunicaciones*. Obtenido de Política de Gobierno Digital: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Mokyr, J. (1990). *The Lever of Riches: Technological Creativity and Economic Progress.* Oxford University Press.

Molina Gavidia, M. V. (2024). *Estudio documental sistemático sobre las tecnologías blockchain y su aplicación a la ciberseguridad 2024 (Bachelor's thesis, .* Universidad Estatal de Bolívar.

Montero, E. R. (2020). *Industria 4.0 Conceptos, tecnologias habilitadoras y retos.* Pirámide.

Mayer-Schönberger, V & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mahesh, B. (2019). *Machine Learning Algorithms- A Review*. 10.21275/ART20203995

Mangini Pérez, G., & Serrano Miquel, E. (2021). *La falta de regulación del Big Tech ¿amenaza para libertad de expresión?*. Tesina de grado. Universidad de Valparaíso.

Maté Jiménez, C. (2014). " Big data". Un nuevo paradigma de análisis de datos. In *Anales de mecánica y electricidad* (Vol. 91, No. 6, pp. 10-16).

March, J. G., Schulz, M., & Zhou, X. (2000). *The dynamics of rules: Change in written organizational codes*. Stanford University Press.

Murcia, M. J., & Suddaby, R. (2024). A layered governance approach to regulating Big Tech. *Long Range Planning*, *57*(4), 102453.

Mukul, M. (2025). Deepfakes and Legal Accountability: A Threat to Evidence and Reputation. *International Journal for Multidisciplinary Research (IJFMR) 7* (4). E-ISSN: 2582-2160.

Montalban, M., Frigant, V., & Jullien, B. (2019). Platform economy as a new form of capitalism: a Régulationist research programme. *Cambridge Journal of Economics*, *43*(4), 805-824.

Moncau, L. F. M., & Arguelhes, D. W. (2020). *The Marco Civil da Internet and digital constitutionalism*. Oxford University Press.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., ... & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology (JCIT)*, *21*(1), 19-32.

Ministerio de Asuntos Digitales (2024*). El rol de las Big Tech en la Infraestructura digital.* Gobierno Danés. Copenhagen, Dinamarca. https://www.english.digmin.dk/Media/638736628110392217/The%20role%20of%20big%20tech%20as%20digital%20infrastructure.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC]. (2021). Glosario. Definición 'neutralidad tecnológica'. https://www.mintic.gov.co/portal/inicio/Glosario/N/6515:Neutralidad-Tecnologica.

Morant, R. H. (2023). Las organizaciones autónomas descentralizadas (DAO): descripción y papel en el futuro del capital-riesgo. *Anuario de Capital Riesgo*, (2023), 13-38.

Moreno, A. (2025). Esperanza Gómez vs. Meta: nuevas reglas para la libertad de expresión en redes. *La Silla Vacía* [sitio web]. https://www.lasillavacia.com/red-de-expertos/red-de-

democracia-y-tecnologia/esperanza-gomez-contra-meta-nuevas-reglas-para-la-libertad-de-expresion-en-redes/.

Navarreto Barrero, O. (2006). El papel del juez comunitario andino en la tutela de los derechos de los ciudadanos (Vol. 6). *Quito, Pichincha, Ecuador: Revista de Derecho*. Universidad Andina Simón Bolívar.

Naciones Unidas. (10 de enero de 2025). Obtenido de https://www.ohchr.org/en/ohchr_homepage

Naciones Unidas. (2020). *Revolución tecnológica e inclusion social Reflexiones sobredesafíos y oportunidades para la politica social en América Latina.* Santiago: sNaciones Unida.

Naya, S. (2018). Naya, S. (2018). Nuevo paradigma de big data en la era de la industria 4.0. Revista electrónica de terapia ocupacional Galicia, TOG, (27), 2. *Naya, S. (2018). Nuevo paradigma de big data en la era de la industria 4.0. Revista electrónica de terapia ocupacional Galicia, TOG, (27), 2.*, 2.

Negrete, J. F. (26 de enero de 2022). Estado y constitucionalismo digital. *La República*.

Negrón, M. E. (2021). Reflexiones sobre evolución tecnológica y sociología política. . *Perspectivas para interpretar los cambios sociales. Opción, 37(96),*, 186-214.

Newman, V., & Ángel, M. P. (2019). *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*. Dejusticia.

Nieto, J. A. (2022). Una introducción al metaverso: conceptualización y alcance de un nuevo universo online. . *adComunica*, 41-56.

Oneto, M. L. (2020). *Fundamentos para un derecho de la inteligencia a artificial. ¿Queremos seguir siendo humanos?* Valencia: Tirant lo Blanch.

Ordóñez, L. (2007). El desarrollo tecnológico en la historia. *Areté, 19(2*, 187-210.

Orozco, L. H. (9 de septiembre de 2023). *ibericonnect.blog*. Obtenido de https://www.ibericonnect.blog/2023/01/los-peligros-del-constitucionalismo-digital/.

Olhede, S. C., & Wolfe, P. J. (2018). The growing ubiquity of algorithms in society: implications, impacts and innovations. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 20170364.

OCDE (2018). Responsible Innovation in Action: Enabling Responsible Business Conduct in Emerging Technologies. OECD Publishing.

OCDE. (2018). Perspectivas de la OCDE sobre el desarrollo de la inteligencia artificial. https://www.oecd.org/goingdigital/ai/ai-policy-observatory.htm.

O'neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Palomo Garrido, A. (2024). Apuntes teóricos para el estudio de la Globalización desde la perspectiva de las Relaciones Internacionales. . *CONfines de relaciones internacionales y ciencia política*, 69-109.

Parga, R. E., & Barrios, J. E. (2016). ¿Qué es Tecnología? Una aproximación desde la Filosofía: Disertación en dos movimientos. *humanidades, vol. 6, núm. 1,*, 243-285.

Pagallo, U., Corrales, M., Fenwick, M., & Forgó, N. (2018). The rise of robotics & AI: technological advances & normative dilemmas. *Robotics, AI and the Future of Law, 1*-13.

Pollicino, O. (20 de septiembre de 2020). *Ya no estamos "viviendo nuestras vidas".* Obtenido de Universidad de La Sabana: https://www.unisabana.edu.co/portaldenoticias/paso-en-la-sabana/retos-y-ensenanzas-para-el-aprendizaje-unisabana/por-que-ya-no-estamos-viviendo-nuestras-vidas/

Ponce, L. E. (2023). *Regulación de Smart Contracts en Blockchain según normativas europeas y americanas.* Mendoza.

Páez, N. A. R. (2012). La doctrina del estado de cosas inconstitucional en Colombia: novedades del neoconstitucionalismo y "la inconstitucionalidad de la realidad". *Revista Derecho Público Iberoamericano*, (1), 243-264.

Palmiotto, F., & González, N. M. (2023). Facial recognition technology, democracy and human rights. *Computer Law & Security Review*, *50*, 105857.

Prieto Sanchís, L. (2001). Neoconstitucionalismo y ponderación judicial. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid (AFDUAM),* (5), 201-228. http://afduam.es/wp-content/ uploads/pdf/5/6900111(201-228).

Privacy International (2019). To hide: Exposing the sources of risks to your rights online. https://privacyinternational.org/report/2647/no-place-hide-exposing-sources-risks-your-rights-online.

Privacy International. (2018). *Mass Surveillance: The Case Against*. https://privacyinternational.org/advocacybriefing/1742/mass-surveillance-case-against.

Privacy International. (2018). Teach 'em to Phish: The Growing Sophistication of Malicious Phishing. https://privacyinternational.org/advocacy-briefing/2015/04/teach-em-phish-growing-sophistication-maliciousphishing.

Privacy International. (2019). No place to hide: Exposing the sources of risks to your rights online. https://privacyinternational.org/report/2647/no-place-hide-exposing-sources-risks-your-rights-online.

Prince, R. (2016). Microsoft is deleting its AI chatbot's incredibly racist tweets. *Business Insider*. https://www.businessinsider.com/microsoft-deletes-racist-genocidal-tweets-from-ai-chatbot-tay-2016-3.

Peeters, R., & Schuilenburg, M. (2020). The algorithmic society: An introduction. In *The algorithmic society* (pp. 1-15). Routledge.

¿Por qué me piden aceptar o rechazar las cookies de las webs?. [SITIO WEB]. *Grupo SCImago*. https://www.scimagoepi.com/por-que-me-piden-aceptar-o-rechazar-las-cookies-de-las-webs/.

Ponomarov, K. (2024). The EU AI Act Overview: What's Coming for Businesses. Legal Nodes [SITIO WEB]. https://www.legalnodes.com/article/eu-ai-act-overview#high-risk-ai-systems.

Reche, F. H. (2019). La Industrialización por Sustitución de Importaciones (ISI): usos y sentidos de una expresión polisémica. . *Folia Histórica del Nordeste, (35)*, 27-50.

Richta, R. (1970). *Progreso técnico y democracia.* Alberto Corazón.

Rodríguez, V. P.-D. (23 de OCTUBRE de 2024). *Coloquio sobre el futuro del trabajo. Encuentro celebrado en la Fundación*. Obtenido de https://frdelpino.es/investigacion/wp-content/uploads/2020/04/EP2_el_futuro_del_trabajo-vf1.pdf

Rojas, M. E. (2015). Una mirada a la inteligencia artificial. *Revista Ingeniería, Matemáticas y Ciencias de la Información*, 27-31.

Rouhiainen, L. (2018). *Inteligencia artificial.* Madrid: Alienta Editorial.

Rubio, J. C. (2022). Tecnología educativa y enfoque sociocrítico en enseñanza de la Historia.¿ Dónde estamos?¿ Hacia dónde vamos? *Con-ciencia social: Segunda Época*, 143-160.

Rueda-López, J. J. (2007). LA TECNOLOGÍA EN LA SOCIEDAD DEL SIGLO XXI: ALBORES DE UNA NUEVA REVOLUCION INDUSTRIAL. *revista de ciencias sociales*, 1-28.

Redeker, D., Gill, L., & Gasser, U. (2018). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazette*, *80*(4), 302-319.

Real Academia Española: *Diccionario de la lengua española*, 23.ª ed., [versión 23.8 en línea]. <https://dle.rae.es> [Consultado en: 26/11/2025].

Rayón, A. (2024). *En la era digital, una respuesta es evolución y una pregunta, revolución*. Colección 'Erronkak' Bilduma.Secretaría General de Transición Social y Agenda 2030. https://www.euskadi.eus/contenidos/informacion/docs_interes_transicionsocial/es_def/adjuntos/Erronkak-4-ES.pdf.

Rochet, J. C., y Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association 1* (4), pp. 990-1029 (https://doi.org/10.1162/154247603322493212).

Rolla, G. (2012). La evolución del constitucionalismo en américa latina y la originalidad de las experiencias de justicia constitucional. *Anuario iberoamericano de justicia constitucional*, (16), 329-351.

Rodríguez, A. (2023). *Declaración europea sobre los derechos y principios digitales para la década digital: retos y oportunidades para las agendas públicas. Centro de Estudios Políticos y Constitucionales*. [sitio web]. https://www.cepc.gob.es/blog/declaracion-europea-sobre-los-derechos-y-principios-digitales-para-la-decada-digital-retos-y.

Rikap, C. (2022). From global value chains to corporate production and innovation systems: exploring the rise of intellectual monopoly capitalism. *Area Development and Policy*, *7*(2), 147-161.

Rincón, E. (2006). *Manual de derecho de comercio electrónico y de Internet*. Centro Editorial Universidad del Rosario.

Reyes, C. L., Geslevich Packin, N., & Edwards, B. P. (2017). Distributed governance. *Wm. & Mary L. Rev. Online*, *59*, 1.

Sadin, É. (2021). *La silicolonización del mundo. La irresistible expansion del liberalismo digital.* Buenos Aires: Caja Negra.

Sánchez, J. J. (2015). ¿ Qué es el Yo? De la Antropología filosófica a la Psicología.

Secretaría de Estrategias Industriales. (30 de agosto de 2024). *industria.ccoo.es.* Obtenido de https://industria.ccoo.es/4290fc51a3697f785ba14fce86528e10000060.pdf

Secretaría General Iberoamericana (SEGIB). (9 de enero de 2025). *Secretaría General Iberoamericana (SEGIB)*. Obtenido de https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf

Sergio Arboleda. (2 de septiembre de 2024). *CUARTA REVOLUCIÓN INDUSTRIAL: ¿QUÉ ES EL MUNDO 4.0?* Obtenido de https://www.usergioarboleda.edu.co/noticias/cuarta-revolucion-industrial-que-es-el-mundo-4-0/

Shokri, R. y. (2015). *Aprendizaje automático que preserva la privacidad: amenazas y soluciones.* Simposio IEEE sobre seguridad y privacidad.

Sobchack, V. (2016). The Scene of the Screen: Envisioning, Photographic, Cinematic, and Electronic “Presence”. En: Shane Denson y Julia Leyda (eds). *Post-Cinema: Theorizing 21st-Century Film, Brighton: Reframe Books, 88-128.*, 88-128.

Sucari, Y. V. (2022). El ensayo: impactos del metaverso en la sociedad. Waynarroque. *Revista deficiencias sociales aplicadas*, 103-109.

Salvi, C. (2024). *Deepfake Evidence in Criminal Proceedings: Procedural hurdles and forensic challenges*. Criminal Law and Digital Justice. University of Liverpool, UK.

https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/SALVI-8.711-Deepfake-evidence-Salvi-Crim-AI.pdf.

Stoller, M. (2019). *Goliath: the 100-year war between monopoly power and democracy*. Simon & Schuster.

Steiner, C. & Uribe, P. (2014). *Convencion Americana sobre Derechos Humanos Comentario*. Eudeba Editores.

Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, *4*(3), 2056305118787812.

Sued, G. E. (2022). Culturas algorítmicas: conceptos y métodos para su estudio social. *Revista Mexicana De Ciencias Políticas Y Sociales*, *67*(246). https://doi.org/10.22201/fcpys.2448492xe.2022.246.78422

Sánchez-Cartas, J. M., y León, G. (2021), Multi-sided platforms and markets: A survey of the theoretical Literature, *Journal of Economic Surveys, 35* (2), pp. 452-487 (https://doi. org/10.1111/joes.12409).

Saavedra, G. A., & de Aguiar Borges, G. O. (2022). Constitucionalismo digital brasileiro. *Revista da AJURIS-Qualis A2*, *49*(152), 157-180.

Schwarz, O. (2021). *Sociological theory for digital society: The codes that bind us together*. John Wiley & Sons.

Schwarz, O. (2025). The Post-Choice Society: Algorithmic Prediction and the Decentring of Choice. *Theory, Culture & Society*, 02632764251322062.

Schuett, J. (2024). Risk management in the artificial intelligence act. *European Journal of Risk Regulation*, *15*(2), 367-385.

Shin, Don D.H. (2019). Socio-Technical Design of Algorithms: Fairness, Accountability, and Transparency, 30th European Conference of the International Telecommunications Society (ITS): "*Towards a Connected and Automated Society*". Helsinki, Finland, 16th-19th June, 2019, International Telecommunications Society (ITS), Calgary.

Taleb, N. N. (2021). Bitcoin, Currencies, and Fragility. . *Quantitative Finance. vol.21, n°8. Londres:Taylor and Francis*, 1-6.

The Flash Co. . (11 de abril de 2024). *Tecnología digital: Concepto y ventajas.* Obtenido de The Flash Co. : https://theflashco.com/tecnologia-digital-concepto-y-ventajas/#:~:text=La%20definici%C3%B3n%20de%20tecnolog%C3%ADa%20digital,generan%2C%20procesan%20o%20almacenan%20informaci%C3%B3n.

Trujillo Valdiviezo, G. R. (2022). Transformación digital en América Latina: una revisión sistemática. . *Revista Venezolana de Gerencia* .

Trujillo, B. Z. (2014). Reflexión sobre la teoría de la sociedad del riesgo. *Temas Sociales no.35*.

Thrun, S. & Anderson, C. (2017). *What AI is -- and isn't*. [Video]. TED talk on Youtube. https://www.youtube.com/watch?v=J6tgYBMXR6s.

Torres Muñoz, J. (2016). *Conceptos e Introducción, Principales servicios del Internet, la WWW, el Internet y la educación, los navegadores y buscadores*. Universidad Nacional de Educación Enrique Guzmán y Valle. Disponible en: https://repositorio.une.edu.pe/handle/20.500.14039/11116.

The New York Times. (2017). Equifax Says Cyberattack May Have Affected 143 Million in the U.S. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Teichmann, C. (2017). Digitalisierung und Gesellschaftsrecht, Zeitschrift für die gesamte Privatrechtswissenschaft 2, P. 247- 272.

Toyama, K., & Kindersley, N. (2018). The Human Cost of Automated Hiring Practices. *Communications of the ACM*, 61(11), 34-36. doi: 10.1145/3272139

Teece, D. J. (2023). Big tech and strategic management: How management scholars can inform competition policy. *Academy of Management Perspectives*, *37*(1), 1-15.

The Guardian. "*McDonald's hit with #MeToo class action over sexual harassment*." (2019). https://www.theguardian.com/business/2019/may/21/mcdonalds-hit-with-metoo-class-action-over-sexualharassment.

Tripathi, S. (2019). Women and online harassment. *Feminist Dissent*, (6), 133-158. https://doi.org/10.31273/fd.n6.2022.1265.

Unesco. (10 de enero de 2025). *Indicadores de desarrollo universal de internet: Un marco para evaluar la universalidad del internet*. Obtenido de https://www.unesco.org/en/internet-universality-indicators/roam-x

UNIR - Universidad Internacional de La Rioja . (9 de 1 de 2025). *Los derechos digitales buscan garantizar el libre acceso a internet y proteger los derechos fundamentales de las personas en la web.* Obtenido de https://colombia.unir.net/actualidad-unir/derechos-digitales/

Unisabana. (9 de septiembre de 2023). *¿Por qué ya no estamos "viviendo nuestras vidas"?* . Obtenido de https://www.unisabana.edu.co/portaldenoticias/paso-en-la-sabana/retos-y-ensenanzas-para-el-aprendizaje-unisabana/por-que-ya-no-estamos-viviendo-nuestras-vidas/

Universidad en Internet. (25 de septiembre de 2024). *La quinta revolución industrial o Industria 5.0: el futuro llama a la puerta*. Obtenido de https://www.unir.net/empresa/revista/quinta-revolucion-industrial/

Vargas, R. A. (2011). Las universidades y el desarrollo de la investigación científica y tecnológica en México: Una agenda de investigación. *Rev. educ. sup vol.40 no.158 Ciudad de México*.

Vivas, F. (2021). *¿ Cómo piensan las máquinas?: Inteligencia artificial para humano.* Buenos Aires: Editorial Galerna.

Valadéz, D. (2005). *Gobernabilidad y constitucionalismo en América Latina*. UNAM, Instituto de Investigaciones Jurídicas, México. https://www.scielo.org.mx/pdf/cconst/n15/1405-9193-cconst-15-357.pdf.

Vergne, J. P. (2020). Decentralized vs. distributed organization: Blockchain, machine learning and the future of the digital platform. *Organization Theory*, *1*(4), 2631787720977052.

Watkins, E. A. (2014). From the here and now to the everywhere and Forever. *The Enemy, n°1*.

Wenz, V. B. (2022). BYUNG-CHUL HAN: LA SOCIEDAD TRASPARENTE DIGITAL O EL INFIERNO DE LO IGUAL. *Revistas-UCV*.

World History Publishing . (15 de mayo de 2024). *cambios-sociales-de-la-revolucion-industrial*. Obtenido de https://www.worldhistory.org/trans/es/2-2229/cambios-sociales-de-la-revolucion-industrial-brita/.

Wachter, S. (2023). Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond. *Yale JL & Tech.*, *26*, 671.

West, D. M., & Allen, J. R. (2018). How artificial intelligence is transforming the world. *Brookings Institution. URL: https://www. brookings. edu/research/howartificial-intelligence-is-transforming-the-world/(дата обращения: 07.04. 2021). Научное издание*.

World Affairs Council of Philadelphia. (2021). Briefing Paper – Big Tech and Social Media Regulation. *2021 Model Senate on Science and Technology*. https://wacphila.org/uploads/attachments/ckvazxi900pl60hqubf7ceokg-big-tech-and-social-media-briefing-paper.pdf.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents: Introduction. *International journal of Communication*, *10*.

Wittenberg, C., Epstein, Z., Berinsky, A. J., & Rand, D. G. (2024). Labeling AI-generated content: promises, perils, and future directions. *An MIT exploration of generative AI*, *27*.

Weber, R.H. (2020) *The digital future of human rights*. Oxford University Press

Youtube - . (16 de octubre de 2024). *Youtube* . Obtenido de Artificial Intelligence - Q&A with Sebastian Thrun: June 2017: https://youtu.be/gyEyBZdUjCo?si=9fxJlJjPGtTf-8ld

Zuboff, S. (2019). *La era del capitalismo de la vigilancia. .* Madrid: Paidós.

Ziewitz, M. (2016). Governing algorithms: Myth, mess, and methods. *Science, Technology, & Human Values, 41*(1), 3-16. doi: 10.1177/0162243915608948.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1), 1-20.

Referencias bibliográficas jurídicas y resoluciones administrativas.

Congreso General de los Estados Unidos Mexicanos (20 marzo 2025). *Ley Federal De Protección de Datos Personales en posesión de los particulares*. Ciudad de México, México.

Constitución Política de la República de Chile. (2010). Senado de la República de Chile.

Court southern District of New York (2023). *Mata v. Avianca, Inc*. No. 1:2022cv01461 - Document 54 (S.D.N.Y. 2023). https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/.

California Federal Court. (2024). Samuels *v.* Lido DAO. No. 3:23-cv-06492. https://www.courtlistener.com/docket/68095676/samuels-v-lido-dao/.

California Consumer Privacy Act [CCPA]. (2018). https://oag.ca.gov/privacy/ccpa.

Corte Constitucional (1992). Sentencia T-426. M.P. Eduardo Cifuentes Muñoz.

Corte Constitucional (2011). Sentencia C-748. M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional (2013). Sentencia T-040. M. P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional (2014). Sentencia T-020. M.P. Luis Guillermo Guerrero.

Corte Constitucional (2015) Sentencia T-277. M. P. María Victoria Calle Correa.

Corte Constitucional (2017). Sentencia T-063ª. M. P. Jorge Iván Palacio Palacio.

Corte Constitucional (2021). Sentencia SU-139. M. P. Jorge Enrique Ibáñez Najar.

Corte Constitucional (2024). Sentencia T-323. M.S. Juan Carlos Cortés González.

Corte Constitucional (2025). Sentencia T-256. M.P. Natalia Ángel Cabo.

Congreso de la Republica. (9 de Enero de 2025). *Secretaria General de la República*. Obtenido de http://www.secretariasenado.gov.co/.

Congreso de la República. (1991). *Constitución Política de Colombia.* Bogotá: Secretaria del Senado.

Ley Estatutaria 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales*. Octubre 18 de 2012. D.O. 48.587 http://www.secretariasenado.gov.co/senado/basedoc/ ley _1581_2012.html.

Ley 1341 de 2009. *Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las*

Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Julio 30 de 2009. D.O. 47.426.

Ley 1712 de 2014. *Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*. Marzo 06 de 2014. D.O. 49.084. http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html.

Ministerio secretaría general de la presidencia (5 junio 2018). Ley 21096. *Proyecto de reforma constitucional: Consagra el derecho a protección de los datos personales*. Santiago, Chile.

Missouri Court of Appeals Decisions. (2024). *Molly Kruse, Respondent, vs. Jonathan R. Karlen, et al., Appellant*. https://law.justia.com/cases/missouri/court-of-appeals/2024/ed111172.html.

Presidência da República (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Lei Nº 13.709. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

European Parliament and The Council Of The European Union (2016). *General Data Protection Regulation* [GDPR]. Version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. Consultado: 27/11/2025.

European Parliament and of the Council. (13 de Junio 2024). *Regulation (EU) 2024/1689 "Artificial Intelligence Act"*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

European Comission [Comisión de la Unión Europea]. (2025). *AI act*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

Supreme Court (2020). *People v. Jeremy FOREMAN*. Número: 2017-1565 K CR. https://caselaw.findlaw.com/court/spr-crt-apl-ter-new-yor/2060305.html.

Superintendencia de Industria y Comercio de Colombia (2016a). Concepto 14- 218349-4-0, del 3 de marzo de 2016.

Superintendencia de Industria y Comercio de Colombia (2016b). Concepto 16- 172268-00001-0000 del 9 de agosto de 2016.

Superintendencia de Industria y Comercio de Colombia (2019). **Resolución 1321 del 24 de enero de 2019. https://sedeelectronica.sic.gov.co/transparencia/normativa/resolucion-1321-del-24-de-enero-de-2019.**

Tribunal de Justicia de la Unión Europea (2014). *Caso Google Spain, S.L., y Google Inc., vs. Agencia Española de Protección de Datos y Costeja González*, 13 de mayo de 2014.

Diccionario de Términos Tecnológicos y Jurídicos

Big Data:

Conjunto masivo de datos estructurados, semiestructurados y no estructurados que requieren herramientas avanzadas de almacenamiento, procesamiento y análisis para extraer patrones, correlaciones y valor predictivo. En el ámbito jurídico, plantea retos en protección de datos personales, privacidad, discriminación algorítmica y vigilancia masiva, pues el uso no regulado de datos puede vulnerar derechos fundamentales como la intimidad (art. 15 C.P.) y la igualdad.

Blockchain:

Tecnología de registro distribuido, descentralizado e inmutable que permite almacenar transacciones en bloques enlazados criptográficamente, garantizando integridad, trazabilidad y resistencia a la manipulación sin necesidad de un intermediario central. Sus implicaciones legales incluyen la validez de contratos inteligentes (*smart contracts*), la tokenización de activos digitales, la trazabilidad de operaciones y posibles conflictos con el derecho al olvido o la revocatoria del consentimiento de datos.

Habeas Data:

Derecho fundamental reconocido en la Constitución colombiana (art. 15), que otorga a toda persona la facultad de conocer, actualizar, rectificar y solicitar la supresión de la información personal que sobre ella repose en bases de datos públicas o privadas. Es la herramienta central de protección frente a vulneraciones en entornos digitales, especialmente en sistemas de Big Data, blockchain y plataformas de redes sociales.

Inteligencia Artificial (IA):

Conjunto de sistemas informáticos capaces de ejecutar tareas que requieren inteligencia humana, tales como aprendizaje automático, razonamiento, predicción y reconocimiento de patrones. Su expansión genera retos jurídicos relacionados con:

- Sesgo algorítmico y discriminación.
- Responsabilidad civil y penal ante fallos de sistemas autónomos.

- Toma de decisiones automatizadas que pueden afectar el debido proceso y la igualdad.
- Necesidad de ética algorítmica y transparencia para garantizar derechos fundamentales.

Metaverso:

Entorno virtual tridimensional, inmersivo y persistente, donde los usuarios interactúan mediante avatares en actividades sociales, educativas, comerciales y culturales.

Riesgos jurídicos asociados:

- Identidad digital y suplantación.
- Propiedad y comercio de activos virtuales (NFTs y bienes digitales).
- Acoso, delitos virtuales y responsabilidad de plataformas.
- Protección de datos y privacidad, ya que las interacciones generan grandes volúmenes de información personal sensible.

Neutralidad de la Red:

Principio del derecho digital que establece que los proveedores de servicios de Internet no pueden bloquear, ralentizar o priorizar contenido de manera arbitraria. Es esencial para garantizar la libertad de expresión, igualdad en el acceso a la información y competencia justa en el ecosistema digital.

Personas Ciborg:

Individuos que incorporan dispositivos tecnológicos al cuerpo humano para restaurar, mejorar o ampliar sus capacidades biológicas, cognitivas o sensoriales. Ejemplos: prótesis biónicas, implantes neuronales, antenas sensoriales. Desafíos jurídicos:

- Reconocimiento de la autonomía morfológica.
- Regulación de la responsabilidad por fallos o interferencias tecnológicas.
- Protección de datos biomédicos y privacidad corporal.

Proyecto de Ley:

Instrumento normativo que busca crear, modificar o derogar disposiciones jurídicas para

regular una situación social o tecnológica específica. En el marco de esta tesis, el proyecto de ley propuesto pretende:

1. Establecer un modelo de constitucionalismo digital colombiano.
2. Crear mecanismos de protección de derechos digitales.
3. Regulares responsabilidades de plataformas y tecnologías emergentes.

Sintiencia Digital:

Estado avanzado de ciertos sistemas tecnológicos o robots autónomos que les permite percibir el entorno, adaptarse a estímulos y ejecutar acciones con un grado de decisión simulada. Su desarrollo plantea:

- Debate ético sobre si deben considerarse sujetos de derechos.
- Vacíos legales en responsabilidad civil y penal por acciones de sistemas autónomos.
- Desafíos para el constitucionalismo digital en cuanto a la protección de la dignidad humana frente a máquinas con "decisión propia".

Tokenización:

Proceso mediante el cual un activo físico o derecho real o personal se representa como un token digital en blockchain, permitiendo su fraccionamiento, transferencia o comercialización segura. Implica retos en propiedad, tributación, trazabilidad y prevención de delitos financieros.

Ciberseguridad:

Conjunto de estrategias, normas y herramientas tecnológicas y jurídicas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información digital frente a amenazas como ciberataques, filtraciones de datos o intrusiones no autorizadas.

Derecho al Olvido Digital:

Derecho derivado del habeas data que permite a una persona solicitar la eliminación o desindexación de información personal que ha perdido relevancia pública, protegiendo la dignidad y reputación en entornos digitales. Genera tensiones con la libertad de expresión y el derecho a la información.

Ciber-robótica y Robótica Avanzada:

Campo tecnológico que integra IA, sensores, conectividad y automatización en máquinas capaces de realizar tareas físicas complejas de manera autónoma o semiautónoma. Sus implicaciones jurídicas incluyen responsabilidad por daños, certificación de seguridad y supervisión estatal.