

CONSTITUCIONALISMO DIGITAL: Derechos, algoritmos y el futuro de la democracia

PRIMERA EDICIÓN DIGITAL

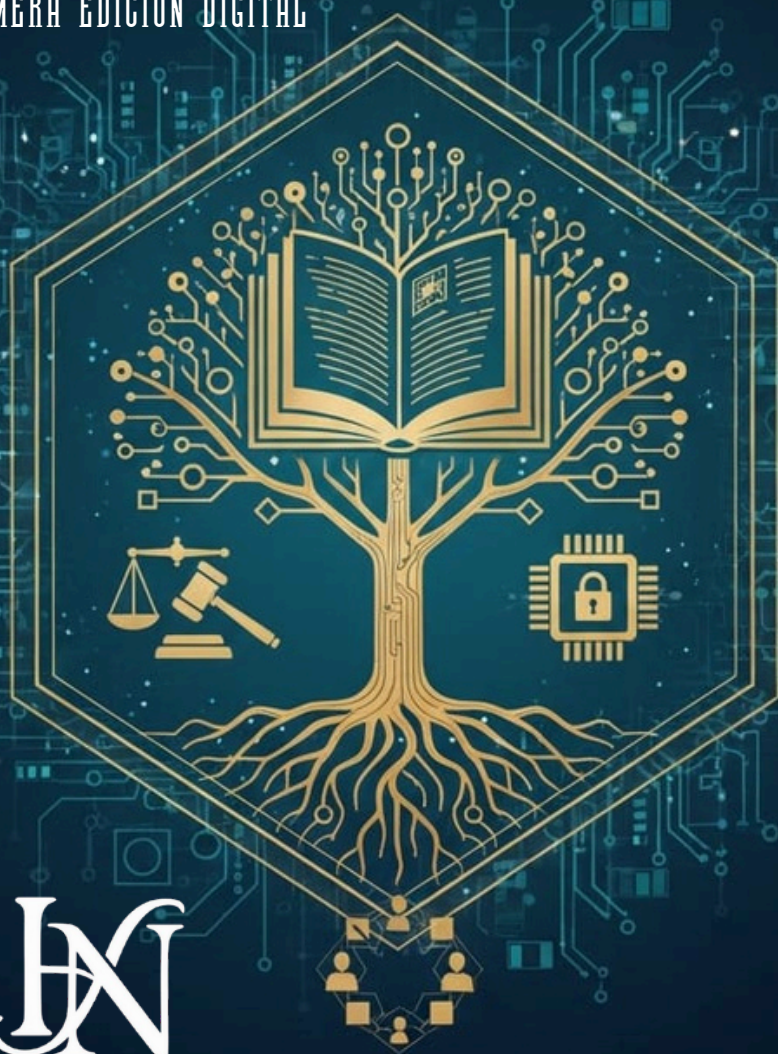


HN
HoNexus
EDITORIAL

Raul Roosevelt,
Chaname Orbe

CONSTITUCIONALISMO DIGITAL: Derechos, algoritmos y el futuro de la democracia

PRIMERA EDICIÓN DIGITAL



HN
HoNexus
EDITORIAL

Raul Roosevelt,
Chaname Orbe

CONSTITUCIONALISMO DIGITAL

Derechos, algoritmos y el futuro de la democracia

© Raul Roosevelt Chaname Orbe.

Editor de contenido: Natalia Beltran Choque

Diseño de cubierta: Ho Nexus

1ª edición digital, diciembre 2025

Editado por:

© HO NEXUS E.I.R.L.

Dirección legal: Urb. Paseo del Mar Mz L4, Lt 33 Nuevo

Chimbote, Santa, Ancash - Perú

Correo electrónico; ed.honexus@gmail.com Teléfono:

978 653 152

<https://books.honexus.org>

DOI: <https://doi.org/10.70504/978-612-99189-9-0>

Reservados todos los derechos de publicación en cualquier idioma; siendo su contenido protegido por la Ley vigente que establece penas de prisión y/o multas a quienes intencionadamente reprodujeren o plagiaran, en todo o en parte, una obra literaria, artística o científica.

Depósito Legal: 2025-14229

ISBN: 978-612-99189-9-0

Revisión por pares:

Este libro (o monografía) fue sometido a evaluación de pares mediante el sistema de doble ciego (doubleblinded review), garantizando la calidad, pertinencia, ética y rigor académico de la obra, conforme a los estándares internacionales de revisión científica y las políticas editoriales de Ho Nexus.

ÍNDICE GENERAL

PRÓLOGO	4
RESUMEN	5
INTRODUCCIÓN	7
Capítulo 1 – Un Réquiem por el Constitucionalismo Analógico	10
Capítulo 2 – La Sociedad Digital y el Nuevo Paradigma	14
Capítulo 3 – La (In)Eficacia de los Derechos Fundamentales en el Mundo Digital	20
Capítulo 4 – Hacia una Carta Magna Digital	33
Capítulo 5 – Legislación Global Digital: Un Panorama Comparado	37
Capítulo 6 – El Caso Peruano: Avances y Desafíos	43
BIBLIOGRAFÍA	48

PRÓLOGO

Vivimos en una época de transformación sin precedentes. La tecnología ha irrumpido en cada aspecto de nuestra vida: cómo nos comunicamos, trabajamos, aprendemos, amamos e incluso cómo ejercemos nuestros derechos. Sin embargo, mientras el mundo avanza a la velocidad de un clic, nuestras leyes y constituciones parecen haberse quedado ancladas en el pasado.

Este manuscrito nace de una pregunta urgente: ¿cómo garantizamos que los derechos fundamentales que tanto costó conquistar sigan vigentes en un mundo dominado por algoritmos, inteligencia artificial y plataformas digitales? No se trata de rechazar el progreso, sino de guiarlo con los valores que nos definen como sociedad: la libertad, la igualdad, la privacidad y la dignidad humana.

A lo largo de estas páginas, exploraremos cómo la revolución digital está desafiando los pilares del constitucionalismo moderno, desde la identidad hasta la privacidad, desde la propiedad intelectual hasta la propia noción de democracia. También veremos cómo países como Perú ya están dando pasos importantes, como la Carta Peruana de Derechos Digitales, y cómo la Unión Europea está liderando esfuerzos globales con su Ley de Inteligencia Artificial.

Este no es un manuscrito solo para juristas o tecnólogos. Es una invitación a todos los ciudadanos a entender los cambios que estamos viviendo y a participar en la construcción de un futuro digital que respete y fortalezca nuestros derechos. Porque, al final, la tecnología es solo una herramienta. Lo que importa es el mundo que decidamos construir con ella.

RESUMEN

La revolución digital ha generado una transformación profunda y acelerada en la estructura social, económica y política, planteando uno de los retos más complejos para el Estado constitucional de derecho del siglo XXI: la obsolescencia del paradigma jurídico analógico. Este libro de investigación analiza la transición necesaria hacia un constitucionalismo digital, argumentando que las constituciones liberales, diseñadas para regular un mundo físico y territorial, han quedado desbordadas por una realidad virtual, global y algorítmica.

A través de un análisis sistemático, se diagnostica la brecha de eficacia que sufren los derechos fundamentales en el entorno digital. Se examinan casos concretos donde derechos como la identidad, la privacidad, la igualdad, la propiedad intelectual y el debido proceso son vulnerados por nuevas dinámicas como la economía de los datos, la inteligencia artificial generativa, los fake news, el ciberacoso y la vigilancia masiva. El texto evidencia cómo el poder se ha desplazado parcialmente de los Estados tradicionales hacia las Big Tech y los algoritmos, creando esferas de regulación privada y anómica.

Frente a este escenario, la obra propone una doble vía: constitucionalizar los algoritmos (someter la tecnología a los valores constitucionales) y digitalizar la constitución (adaptar la norma fundamental al nuevo contexto). Se revisan las respuestas regulatorias a nivel global, destacando el liderazgo de la Unión Europea con su Ley de Inteligencia Artificial, y se analiza en profundidad el caso peruano, evaluando la Carta Peruana de Derechos Digitales de 2022 como un avance significativo, aunque aún insuficiente por su carácter no vinculante.

La conclusión central sostiene que la supervivencia de la democracia y la garantía de los derechos humanos exigen la construcción de un nuevo derecho público para la era digital. Esto implica no solo una actualización normativa, sino también el fortalecimiento de instituciones como la Defensoría del Pueblo, la consolidación de mecanismos procesales como el habeas data y, potencialmente, una reforma constitucional que ancle los derechos digitales en la máxima jerarquía normativa. El libro se presenta como una contribución fundamental para académicos, operadores jurídicos, legisladores y ciudadanos interesados en forjar un futuro tecnológico que sea compatible con la libertad, la dignidad y la justicia.

Palabras Clave: Constitucionalismo Digital; Derechos Fundamentales; Algoritmos; Gobernanza Digital; Inteligencia Artificial (IA); Reforma Constitucional

INTRODUCCIÓN

Del papel a los algoritmos: por qué necesitamos un constitucionalismo digital

“La tecnología es un sirviente útil, pero un jefe peligroso.”

— Christian Lous Lange

“Cuando creíamos que teníamos todas las respuestas, de pronto, cambiaron todas las preguntas.”

— Mario Benedetti

Vivimos en un mundo que se transforma más rápido de lo que podemos asimilar. Hace apenas tres décadas, internet era un lujo académico; hoy, es el sistema nervioso de la sociedad global. La inteligencia artificial, que parecía ciencia ficción, hoy redacta textos, diagnostica enfermedades y hasta resuelve consultas legales. Los datos se han convertido en el nuevo petróleo, y los algoritmos en los arquitectos invisibles de nuestra realidad.

Pero hay algo que no ha cambiado al mismo ritmo: nuestras leyes.

La Constitución, ese pacto social que durante siglos ha definido nuestras libertades y límites, fue pensada para un mundo tangible, lento y predecible. Nació para proteger a las personas de los abusos del poder estatal en un contexto donde la vida transcurría en plazas, mercados y parlamentos. Hoy, sin embargo, gran parte de nuestra existencia se desarrolla en espacios digitales donde las reglas las escriben empresas tecnológicas, donde la privacidad es un bien de cambio y donde un algoritmo puede decidir qué información vemos, qué oportunidades tenemos e incluso cómo nos entendemos a nosotros mismos.

Un desfase peligroso

Este divorcio entre el derecho y la realidad digital no es solo teórico. Tiene consecuencias profundas en nuestra vida cotidiana:

- ¿Puede una plataforma Facebook o X (antes Twitter) suspender tu cuenta — tu identidad digital, tu medio de trabajo— sin derecho a defensa?
- ¿Es justo que tu proveedor de internet ralentice ciertos servicios porque no pagas una tarifa premium?
- ¿Quién responde si una inteligencia artificial genera una obra artística o comete un error que perjudica a alguien?
- ¿Cómo ejercer el derecho al olvido en un mundo donde todo queda registrado para siempre?

Estas preguntas no son futuras. Son presentes urgentes que nuestras leyes no están respondiendo de forma clara y coherente.

Ni apocalípticos ni integrados

Este manuscrito no es un manifiesto en contra de la tecnología. Tampoco una celebración ingenua del progreso técnico. La digitalización ha traído beneficios extraordinarios: acceso al conocimiento, facilidades comerciales, democratización de la creatividad y herramientas para la organización social. Pero también ha creado nuevos mecanismos de exclusión, vigilancia, manipulación y vulneración de derechos.

Como bien señala el documento original que inspira este trabajo, la tecnología es un medio, no un fin. Su dirección depende de las manos —y los valores— que la guíen. Por eso, el gran desafío de nuestro tiempo no es detener la innovación, sino constitucionalizarla: asegurar que los principios de dignidad, libertad, igualdad y justicia que dieron sentido al Estado de derecho sigan vigentes en la era digital.

El viaje que nos espera

En las páginas que siguen, exploraremos cómo el mundo digital está redefiniendo lo que significa ser ciudadano, tener privacidad, expresarse libremente y participar en la democracia. Hablaremos de inteligencia artificial, propiedad intelectual, desinformación, ciberacoso y derecho al olvido. También revisaremos las respuestas que se están gestando alrededor del mundo, desde la pionera Ley Europea de Inteligencia Artificial hasta la innovadora Carta Peruana de Derechos Digitales.

Este manuscrito es, en cierto modo, una carta de amor al constitucionalismo: una invitación a revitalizarlo, a llevarlo del papel a los algoritmos, de las cortes a las plataformas, de la letra muerta a la vida digital.

Porque, al final, no se trata de elegir entre tecnología y derechos.

Se trata de construir un futuro donde la primera esté al servicio de los segundos.

Capítulo 1 – Un Réquiem por el Constitucionalismo Analógico

1.1. La brecha entre la Constitución y la realidad digital

El constitucionalismo liberal, surgido en el siglo XVIII con el noble propósito de reconocer y proteger las libertades individuales frente al poder absoluto del Estado, ha demostrado ser una estructura jurídica resiliente, pero no inmune al cambio. En el pasado, enfrentó y se adaptó a desafíos profundos, como el advenimiento del modelo industrial y la sociedad de masas, que dieron paso al constitucionalismo social en el siglo XIX. Sin embargo, el desafío que presenta la era digital es de una magnitud y naturaleza distintas (Francisco & Barrilao, 2022).

En las últimas décadas, el mundo hiperglobalizado ha experimentado una transformación radical impulsada por la implementación de tecnologías disruptivas. La tecnología digital ha permeado cada aspecto de nuestra realidad, a menudo de manera imperceptible, modificando de forma inexorable nuestras vidas, relaciones y, fundamentalmente, el ejercicio de nuestras libertades. El problema central que identificamos es que el texto constitucional, tal como lo conocemos, ha quedado sustancialmente desfasado de este nuevo contexto (Fundamentais & Justiça | Belo Horizonte, 2021).

Los factores tangibles y reales del mundo digital no se ajustan a las previsiones constitucionales e internacionales concebidas para un mundo físico. La normativa actual se muestra deficitaria para regular una realidad que, en buena parte, ya no existe, quedando rezagada frente a las innovaciones y los nuevos paradigmas que surgen a un ritmo acelerado. Si la Constitución es la depositaria de los valores fundamentales de una sociedad y el marco sobre el cual se construye el Estado de Derecho, no puede permanecer ajena ni excluida del marco de la era digital contemporánea. Su

desconexión de la realidad virtual y algorítmica la convierte, en el mejor de los casos, en una herramienta insuficiente y, en el peor, en una mera declaración retórica de intenciones.

1.2. La tecnología: ¿herramienta útil o jefe peligroso?

Al adentrarnos en este nuevo panorama, es crucial realizar una precisión fundamental: el avance tecnológico de la sociedad digital del siglo XXI no presenta, prima facie, un componente intrínsecamente "positivo" o "negativo". Desde una perspectiva ética, no es inherentemente "correcto" o "incorrecto". La tecnología es, en esencia, un instrumento (Alva et al., 2023).

Esta herramienta ha traído consigo facilidades extraordinarias y ventajas indudables. Ha fortalecido las relaciones sociales, impulsado el progreso económico y democratizado la circulación de la información, coadyuvando a un desarrollo del conocimiento en niveles nunca antes imaginados. El uso de las Tecnologías de la Información y la Comunicación (TIC) en entornos laborales, educativos, familiares y judiciales es un testimonio elocuente de su potencial positivo (Valdez et al., 2021).

No obstante, estos mismos avances han creado mecanismos potenciales para vulnerar prerrogativas constitucionales, la soberanía nacional y los derechos conexos a las libertades individuales. El uso abusivo y malintencionado de estas herramientas puede conculcar libertades con una eficacia y escala nuevas. Esta dualidad queda perfectamente encapsulada en la advertencia del historiador **Christian Lous Lange**: "La tecnología es un sirviente útil, pero un jefe peligroso".

La relación entre la tecnología y la persona debe entenderse, en línea de principio, como una de medio a fin, y no a la inversa. El direccionamiento de la herramienta ya sea para el bien común o para la lesión de derechos, depende última y exclusivamente

del sujeto operador. La tecnología carece de una voluntad propia; su componente ontológico no es nocivo. El desafío jurídico y ético, por tanto, no reside en la tecnología en sí, sino en el marco de valores y regulaciones que los humanos construimos para dirigirla.

1.3. El punto de no retorno: IA, algoritmos y el poder del dato

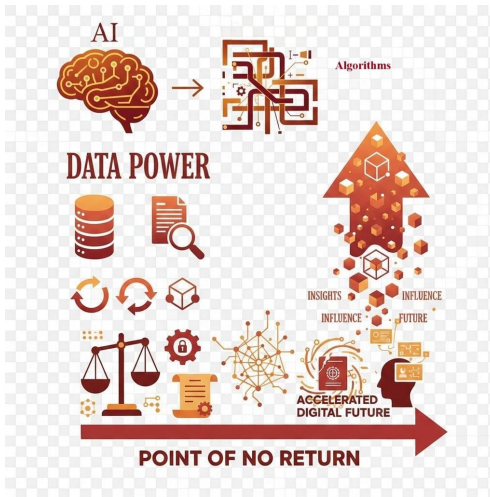
La humanidad ha alcanzado un punto sin retorno. La automatización, la robótica y, de manera prominente, la Inteligencia Artificial (IA) han superado las expectativas y, en muchos aspectos, los esquemas de control humano sobre el medio tecnológico. Si bien algunos de estos fenómenos no son completamente novedosos –basta recordar los autómatas del siglo XIX o los primeros sistemas expertos–, la convergencia, la escala y la autonomía actuales marcan un antes y un después (Zamora Varela & Mendoza Encinas, 2023).

La humanidad ha tomado conciencia del poder del dato (digital). Es en este punto donde cristalizan los novísimos e intrincados retos para la vigencia del Estado Constitucional de Derecho. Los datos son el combustible que alimenta a los algoritmos, y estos se perfeccionan mediante el ejercicio constante de sus operaciones. Modelos de Lenguaje de Gran Escala (LLM, por sus siglas en inglés) de código abierto, como los desarrollados por Open AI (ChatGPT) y el emergente DeepSeek de China, dotan a las máquinas de una capacidad antes impensable (Martín Romero & Gómez, 2025).

A través de un simple diálogo con un chatbot, estas IA pueden producir contenido espontáneo: desde imágenes y material audiovisual hasta respuestas a consultas complejas, clasificación de fuentes e incluso la imitación o creación de voces humanas. Esta tecnología "aprende" de su constante uso, refinando su forma de interactuar con el usuario en una suerte de "ensayo y error" a escala masiva.

La extensión de los usos de estas herramientas inteligentes es tal que ha irrumpido en el campo del derecho. Un ejemplo emblemático es **Juztina**, una IA especializada para abogados que absuelve consultas legales a nivel nacional, apoyándose en un amplio repertorio de documentos legales y jurisprudenciales estructurados en su base de datos.

Si bien la evolución de la IA es todavía temprana y sus productos requieren, por el momento, de la revisión continua del especialista humano para discernir lo útil de lo erróneo, una interrogante crucial se plantea en el camino: ¿es asertivo el término "inteligencia" artificial en una sociedad digital que aún podemos considerar primitiva? La pregunta no es solo semántica; obliga a una reflexión profunda sobre la naturaleza de la inteligencia, la conciencia y la singularidad humana, y sobre cómo el derecho debe abordar entidades que, sin ser humanas, simulan y hasta superan ciertas capacidades cognitivas humanas. Estamos, sin duda, en el umbral de una nueva era que exige un nuevo pacto constitucional.



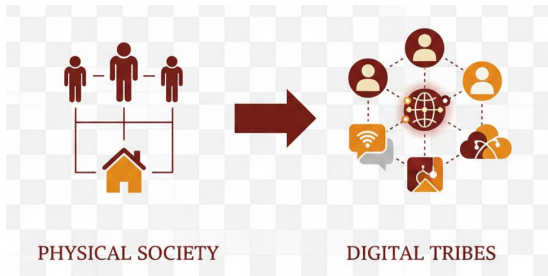
IA, algoritmos y el poder del dato

Capítulo 2 – La Sociedad Digital y el Nuevo Paradigma

2.1. De la sociedad física a las tribus digitales

Tradicionalmente, la sociología ha concebido la sociedad como la integración de un conjunto de individuos con intereses comunes que coexisten en un espacio físico determinado (García Toma, 2010). A diferencia del Estado, la sociedad no se rige exclusivamente por mandatos positivos o leyes formalmente válidas. Su origen reside en la comunión voluntaria y en las reglas del trato social, inherentes al ser humano como ente gregario, dando forma a comunidades tradicionalistas basadas en valores compartidos.

Esta concepción experimenta una ruptura radical en la era digital. Asistimos a un fenómeno singular: la fragmentación de la "realidad social" en dos facetas binarias: la realidad física y la realidad virtual. Surge así un mundo paralelo y hasta entonces desconocido, donde el ser humano puede asociarse, interactuar y construir lazos sin necesidad de contacto físico alguno. En este ecosistema digital emergen las redes sociales, las comunidades virtuales, las realidades híbridas y las tribus digitales (Marín Jódar & Ángel Juan, 2010). Estos grupos comparten un ambiente globalizado, ideas y desarrollos puramente virtuales, desafiando las nociones clásicas de territorialidad y presencia física que durante siglos han definido las relaciones humanas.



De la sociedad física a las tribus digitales

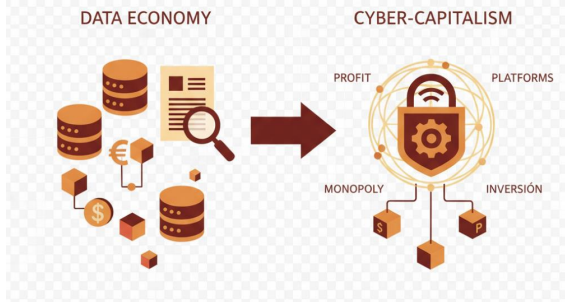
2.2. La economía de los datos y el cibercapitalismo

Aforísticamente se dice que, en la sociedad digital, los datos son el nuevo petróleo. Esta analogía subraya su papel como recurso fundamental para la economía del siglo XXI, tal como lo fue el crudo para la economía industrial. El motor de esta "sociedad digital" son los algoritmos, procesos computarizados centrados en el tratamiento masivo de datos para resolver problemas y predecir comportamientos (Candón Mena, 2012).

Estos algoritmos no solo organizan información; también perciben y analizan tendencias del usuario digital: sus gestos virtuales, aficiones, preferencias, simpatías y antipatías. Su presencia es omnímoda en todas las dinámicas informáticas, desde una simple reacción en Instagram hasta una búsqueda compleja en Google. Esta nueva forma de socialización, que une a personas y grupos que posiblemente nunca se verán las caras, ha dado paso a un nuevo modelo económico: el cibercapitalismo.

A diferencia de la sociedad física, esta nueva realidad trasciende las organizaciones estatales, sus fronteras políticas, económicas y jurídicas, quedando estas últimas materialmente obsoletas ante un fenómeno digital-global donde todo está interconectado. La economía digital, con sus criptomonedas, mercados digitales y transacciones desprovistas de control estatal, deja en vilo conceptos constitucionales tan fundamentales como el de soberanía nacional.

LA ECONOMÍA DE LOS DATOS Y EL CIBERCAPITALISMO



2.3. El concepto "glocal": lo global y local en simultáneo

El cibercapitalismo supone una experiencia simultánea entre lo global y lo local, un fenómeno que ha servido de base para la construcción de un revelador neologismo: "glocal" (Marín Jódar & Ángel Juan, 2010). Este término designa aquella situación en la que convergen factores de las realidades globales y locales.

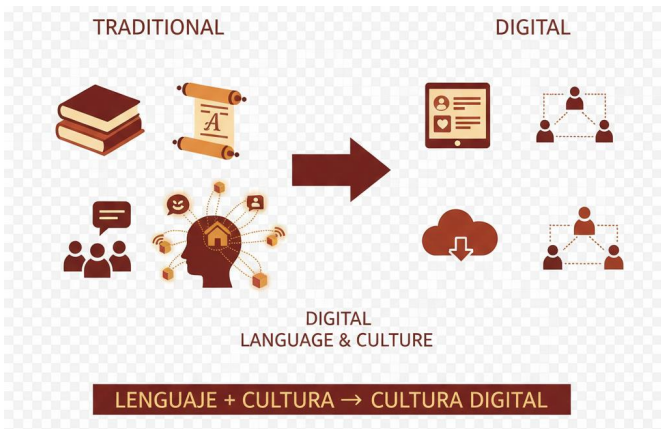
En la práctica, esto significa que una persona que navega por la red se encuentra, ciertamente, dentro de los límites físicos de un territorio determinado, sujeto a las reglas de un Estado en particular. Sin embargo, al mismo tiempo, su desenvolvimiento en el ciberespacio se lleva a cabo en una dimensión que tiene incidencias globales e instantáneas. Esta dualidad presenta un obstáculo formidable para la regulación, ya que las estrategias de defensa de los derechos y la soberanía deben, de igual forma, concebirse con una perspectiva global para ser efectivas.

2.4. La mutación del lenguaje y la cultura

La tecnología, como factor cultural, ha modificado profundamente los hábitos y la forma de desenvolverse de las personas. La lectura, por ejemplo, ya no se asocia exclusivamente a libros de hoja y tinta, sino a formatos digitales como audiolibros o

epub, maximizando y masificando el acceso al conocimiento. Nuestra propia percepción del tiempo se ha alterado; el efecto acelerado del desarrollo tecnológico nos da la impresión de vivir a una velocidad precipitada, acostumbrándonos a obtener cualquier producto o información en cuestión de minutos o segundos. Este fenómeno de eficiencia, estandarización y control es lo que el sociólogo **George Ritzer (2023)** denominó críticamente como "La Macdonalización de la sociedad" (Giugovaz, n.d.).

El lenguaje también ha mutado, trascendiendo de ser una expresión identitaria de naciones particulares a convertirse en una mezcla de códigos globales y mixtos (por ejemplo, el espanglish), producto de la proliferación de herramientas digitales anglosajonas. Pero la transformación lingüística más radical se manifiesta ahora en los lenguajes de programación, los códigos binarios y los algoritmos computarizados que rigen el intercambio digital moderno. Atendiendo a este nuevo desafío, se considera urgente la implementación de políticas nacionales de alfabetización digital para formar a los "ciudadanos digitales" del mañana.



Mutación del lenguaje y la cultura

2.5. Hegemonía digital: la nueva guerra híbrida

La digitalización y la globalización han trastocado sustancialmente lo que entendíamos por hegemonía, es decir, la capacidad de un Estado, empresa o comunidad para influir en el mundo y promover políticas favorables a sus intereses particulares. Este poder ya no depende exclusivamente, como en el pasado, de la presión militar o económica (Gambarte, 2023).

En la actualidad, es posible generar movimientos o cambios en las orientaciones políticas de los países sin necesidad de realizar operaciones físicas dentro de sus fronteras. La estructura política y comercial de una nación puede ser condicionada mediante mecanismos propios de la guerra híbrida, que incluyen la inteligencia artificial militar, las redes neuronales artificiales, los ciberataques y el terrorismo digital. Esto genera un menoscabo indiscutible a la seguridad y soberanía de los estados, ya que, en muchos casos, solo es necesario "moldear" las preferencias de la sociedad digital mediante la manipulación de la información y, para ser más exactos, mediante el uso de la "inteligencia artificial".

2.6. El transhumanismo y los límites de la naturaleza humana

El cambio de paradigmas alcanza incluso la propia forma de concebir al ser humano, su antropología, anatomía y capacidades. El transhumanismo emerge como una corriente de pensamiento que promueve la superación de los límites biológicos naturales de la humanidad por medio de la tecnología (Roel Alva et al., 2025). Sus defensores plantean preguntas fundamentales: ¿Qué nos hace humanos? ¿Tenemos una esencia inmutable? ¿Por qué debemos aceptar nuestros límites anatómicos si la tecnología ofrece la posibilidad de "mejorarnos"?

La industria médica ya permite modificar genéticamente al ser humano, y la Inteligencia Artificial, con su acelerado desarrollo, podría pronto implantarse dentro de las personas para brindar ventajas físicas (como superar limitaciones visuales) y

psicológicas (como mejorar la capacidad de decisión). El transhumanismo presenta formidables retos bioéticos al situar al ser humano como manipulador de su propia naturaleza, desdibujando la línea entre lo humano y lo artificial. A este ritmo, el derecho y la constitución podrían enfrentarse pronto a la necesidad de tutelar no solo a "personas", sino a híbridos computarizados, lo que redefine por completo el concepto de dignidad humana y la razón de ser del derecho mismo: la persona humana.

Capítulo 3 – La (In)Eficacia de los Derechos Fundamentales en el Mundo Digital

Los "derechos fundamentales" constituyen el núcleo esencial del sistema jurídico en un Estado Constitucional de Derecho y democracia. En su dimensión objetiva, forman la matriz de todo el ordenamiento; en su dimensión subjetiva, protegen las libertades esenciales de la persona natural y, en los casos aplicables, de la persona jurídica (Solozábal Echavarría, 1991). Su goce es una condición indispensable para la vida en sociedad.

El Derecho, como conjunto de reglas, principios y valores objetivados en normas, traduce los mandatos y fines que la sociedad requiere. Estos principios, como señala (Peces-Barba et al., 2014), se sustentan en una moralidad y, según **Häberle** (2000) mencionado en (López González, 2001), cristalizan una cultura determinada que informa a todo el sistema. Sin embargo, al manifestarse como enunciados amplios, indeterminados y orientadores —a menudo carentes de un presupuesto de hecho concreto—, dejan un margen considerable de discreción al operador de justicia constitucional. Este margen se enfrenta hoy a situaciones cada vez más diversas y aceleradas por los cambios tecnológicos, que no guardan correspondencia con la concepción clásica del orden constitucional.

El mundo digital ha maximizado las posibilidades del ser humano, tanto para un ejercicio óptimo de sus derechos como para su vulneración. Los derechos que la Constitución ampara en esta "revolución tecnológica" corren el riesgo de devenir en mera retórica normativa (Celeste & Santarém, 2022). Para optimizar su protección, es imperativo que las disposiciones se reformen o, al menos, se (re)interpreten adecuándolas a la nueva esfera de desenvolvimiento de la persona: la "vida digital". Como expresara **Schönfeld** (citado en (Larenz, 2023)), "solo en la interpretación se concreta el Derecho en su plena realidad". Esta tarea es difícil, pues ni el legislador más creativo puede prever el devenir de una sociedad de la información en

permanente cambio. Ya lo advertía **Thomas Macaulay**: "mientras las naciones avanzan al trote, las constituciones van a pie" (Josué Vasquez Villanueva et al., 2023).

A continuación, exploraremos las principales vulneraciones y desafíos que enfrentan los derechos fundamentales en el entorno digital.

3.1. Identidad Digital

El derecho a la identidad y al libre desarrollo de la personalidad adquiere una relevancia especial en el entorno digital. La personalidad como expresión individualizadora se refleja en los actos cotidianos, y en el mundo virtual construimos una identidad a través de preferencias publicadas, fotos, comentarios, opiniones y patrones de consumo. Toda esta información forma parte de la identidad digital del usuario.

Incluso puede darse el caso de que una persona se identifique con mayor arraigo en la red que en la realidad física, construyendo una reputación e imagen en plataformas virtuales mediante la creación de contenido. Esta identidad cobra especial relevancia cuando la actividad en estos medios se convierte en el principal medio de ingresos económicos del usuario. Por lo tanto, debe existir una tutela de la identidad en este ámbito digital, que, aunque no sea la forma primigenia, forma parte integral del individuo, tal como señala nuestro ordenamiento constitucional y la jurisprudencia del Tribunal Constitucional peruano (STC N° 05829-2009-PA/TC ; (Tribunal Constitucional, 2009)).

Un escenario común actualmente es la suspensión unilateral de una cuenta de usuario por parte de una plataforma. Si un usuario ha construido una marca personal y un medio de vida en dicha plataforma, esta acción no solo podría constituir una restricción arbitraria a la libertad de expresión, sino también una vulneración a su

identidad digital. Cuando una persona invoca su identidad, lo hace para distinguirse del colectivo, y en el entorno digital esta distinción puede depender de referentes complejos vinculados a una notoriedad construida y asentada en su ejercicio permanente en estas plataformas.

Otra problemática es la suplantación de identidad en redes sociales. Las **Big Tech** han intentado remediarlo con mecanismos de verificación (como la "marca azul"), pero la cualidad de usuario adquiere una condición universal en el ámbito de estas compañías, sobreponiéndose frecuentemente a la protección nacional.

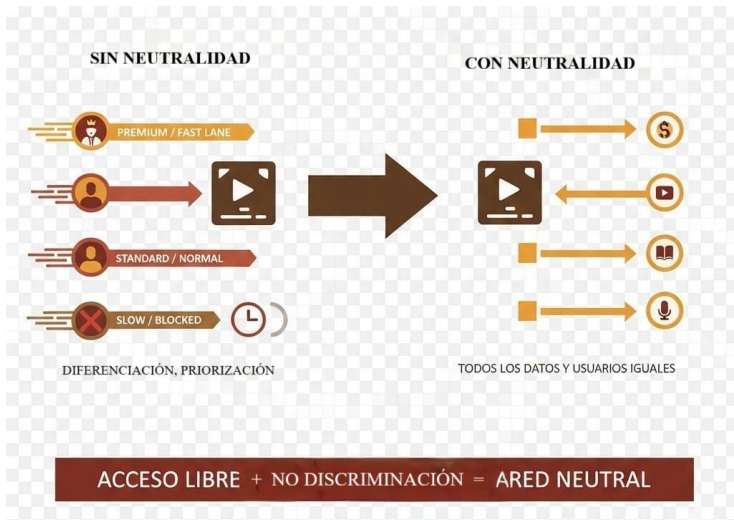
3.2. Igualdad y Neutralidad de la Red

El principio-derecho de igualdad, que postula que los individuos merecen idéntico trato en el ejercicio de sus facultades, enfrenta un desafío específico en la era digital: el acceso a Internet. Reconocido en la constitución peruana como un servicio básico, en teoría se garantiza su acceso igualitario. Sin embargo, fenómenos como el "internet a dos velocidades" exponen una forma de discriminación.

Este fenómeno, observado en 2017 con proveedores como Verizon, consistía en bloquear o ralentizar la velocidad de conexión en función del precio pagado por el cliente o de la página web visitada, favoreciendo así a servicios propios o de aliados. Evitar esta "ralentización" requería pagar una comisión extra. Este escenario atenta contra el acceso igualitario a portales digitales.

Para combatir esto se ha conceptualizado el principio de "Neutralidad de la red", que impide comportamientos desiguales por parte de los proveedores de Internet. En EE.UU., la Comisión Federal de Comunicaciones (FCC) sancionaba estas prácticas, exigiendo transparencia. No obstante, los detractores argumentan que estas regulaciones son excesivas y lastran la innovación, una postura que tuvo fuerza cuando

la administración Trump levantó dichas prohibiciones. Esta disputa simboliza la pugna eterna entre los derechos de igualdad y libertad en el entorno digital.



Igualdad y Neutralidad de la Red

3.3. Propiedad Intelectual en la Era de la IA Generativa

La generación de obras y contenido por tecnologías de creación espontánea, como las IA generativas, plantea serias cuestiones sobre el derecho fundamental a la propiedad intelectual. La duda central recae en si los contenidos generados por estas herramientas, al ser obra "no-humana", escapan del amparo de los derechos morales de paternidad e integridad.

Este problema no es completamente nuevo. Un precedente curioso es el caso *Naruto vs. Slater*, donde una organización protectora de animales (PETA) demandó a un fotógrafo en representación de un mono que se había "autofotografiado", alegando

la vulneración de su copyright. El tribunal consideró que, si bien el mono era presunto autor, no podía ser titular de derechos, por lo que la imagen quedó en dominio público.

Con las IA generativas, el problema se vuelve más intrincado. En el caso **Thaler vs. Perlmutter (2023)**, un tribunal de EE.UU. resolvió unánimemente que el arte generado por IA no está protegido por derechos de autor, puesto que estos exigen "autoría humana", un requisito basado en siglos de jurisprudencia y en la propia Constitución estadounidense. La jueza Baryl A. Howell rechazó también la teoría del trabajo por encargo, pues esta también requiere un creador humano (Iviandy Aquino & Oscar Flores, 2024).

Este fallo abre un debate crucial. Si el trabajo de conducir a una IA con comandos complejos resulta en una creación inédita y valiosa, ¿no es razonable que el operador humano deba hacer suyo algún derecho sobre aquella creación? El análisis de este punto requiere una óptica amplia de las posibilidades digitales, y no solo ceñirse a una repetición literal de la norma.



Propiedad Intelectual en la Era de la IA Generativa

3.4. Vida Digital y el Derecho a la Desconexión

La vida física es temporal, pero la vida digital tiende a la permanencia. Toda la información que una persona genera en el ambiente virtual se mantiene perenne y encriptada en la nube. El registro digital de nuestra navegación nos acompaña indefinidamente, haciendo presente un pasado que a menudo se desearía olvidar. La creación de universos virtuales como el Metaverso, con avatares y herramientas de realidad aumentada, consolida esta vida digital como una genuina forma de existencia.

Hoy, tener una vida digital no es solo una opción, sino una necesidad para el desenvolvimiento en ámbitos familiares, educativos y, especialmente, laborales. En este último, donde la mayor parte de la comunicación se realiza por plataformas digitales, el manejo experto de estas herramientas es indispensable.

Sin embargo, esta hiperconexión genera desgaste. Por ello, así como se reconoce el derecho a acceder a la red, debe plantearse el "derecho a la desconexión digital". Este derecho, ya reconocido por varias multinacionales y países como Francia, es polidrico. Entre sus beneficios se cuenta la mejora de la salud física y psicológica, evitando patologías como el estrés laboral, agotamiento mental y problemas visuales por la exposición continua a pantallas. Entre sus perjuicios potenciales está el aislamiento de la sociedad global y la incomunicación en casos de emergencia.

3.5. La Buena Muerte Digital y el Derecho al Olvido

La muerte también tiene una dimensión digital. Surgen preguntas sobre el "patrimonio virtual" del usuario fallecido: sus archivos en la nube, cuentas en redes sociales, blogs y páginas web. ¿Qué hacer con esa información? ¿Se debe respetar su deseo de trascendencia o de anonimato?

Para ello, se han innovado variantes del "testamento vital" o "voluntades anticipadas" digitales, donde la persona puede especificar qué hacer con su información personal en línea. En este ámbito, el "derecho al olvido" actúa como un límite a la vida eterna en el espacio digital, facultando a la persona a solicitar la eliminación, desindexación o bloqueo de información personal en internet por ser inexacta, irrelevante o lesiva para su privacidad. Legislaciones como la española ya reconocen a los "herederos digitales".

En Perú, el derecho al olvido posee reconocimiento legal y jurisprudencial dentro de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), en un marco de razonabilidad y proporcionalidad, y en armonía con otros derechos como el de información (STC Exp. N° 03041-2021-PHD/TC) (Revista Peruana de Derecho Constitucional, 2022).

Paradójicamente, la manipulación digital de registros estatales (como el Reniec o Sinadef) puede llevar a que una persona viva figure como fallecida en plataformas digitales, impidiéndole realizar trámites bancarios o administrativos, lo que evidencia la precariedad de los sistemas de ciberseguridad y la gravedad de estas vulneraciones.

3.6. Juicios Mediáticos y Lawfare

Las plataformas digitales ejercen a menudo una "condena social perpetua" sobre personas imputadas o condenadas por delitos, contradiciendo abiertamente los fines constitucionales del sistema penitenciario: la reeducación, rehabilitación y reincorporación del penado a la sociedad (Art. 139.22 Constitución Peruana) (Congreso Constituyente, 2025).

¿Cómo garantizar la resocialización de un condenado que ha cumplido su pena si sigue siendo objeto de criminalización permanente en las redes digitales? Este

fenómeno afecta no solo al condenado, sino incluso al imputado que es posteriormente sobreseído. Esta situación ha revitalizado el debate sobre el derecho al olvido.

El auge de los medios digitales les ha otorgado atribuciones de facto para actuar como jueces o verdugos, exacerbando métodos tradicionales y filtrando información reservada durante procesos judiciales. Como adelantaba (Ferrajoli et al., 2000), el proceso se convierte en un instrumento de estigmatización pública antes de la condena.

Dentro de estos fenómenos se inscribe el Lawfare o "guerra jurídica", que es el uso estratégico de la ley y el proceso judicial para desprestigiar a adversarios políticos. Estrategias como publicar encuestas en redes sociales sobre la culpabilidad de un imputado, ejercer presión mediática sobre el juez o utilizar bots para crear narrativas masivas, suponen una grave vulneración al derecho al debido proceso y a la presunción de inocencia, síntomas de un estado donde el "cuarto poder" digital se superpone a las garantías jurisdiccionales.

3.7. Ciberacoso y el Derecho a un Ambiente Digital Pacífico

El derecho a disfrutar de un ambiente pacífico debe trasladarse al mundo digital. La convivencia en redes se vuelve conflictiva, manifestándose en fenómenos como el ciberbullying y el acoso digital, que atentan contra un entorno saludable y se relacionan con el derecho al honor y la buena reputación. En casos extremos, esto puede desembocar en suicidio.

Este derecho queda en vilo por el anonimato digital y acciones como el ciber secuestro (robo de datos para exigir un rescate), o el uso de bots y ciborgs (cuentas parcialmente automatizadas) para emitir descalificativos, injurias y difundir datos sensibles. Por el

referido anonimato, poco se puede hacer para remediar el daño a la imagen del agraviado y su familia.

La implementación de una ciberseguridad adecuada es vital. La proliferación de ciberdelitos como vishing, spyware, phishing, malware, grooming, sexting, ransomware, entre otros, son producto de esta irrupción informática. Medidas como el registro con correos o números de teléfono reales son paliativos insuficientes.

El reto se complejiza con la IA, que imita con facilidad rostros, voces e identidades. Esta tecnología puede usarse para reconstruir personajes históricos o generar conferencias de ponentes no disponibles, pero también para dañar la imagen de personas o empresas mediante deepfakes (audios, fotos o grabaciones falsas hiperrealistas), dificultando enormemente la calificación de su falsedad y configurando delitos patrimoniales y contra el honor.



Ciberacoso y el Derecho a un Ambiente Digital Pacífico

3.8. Secreto de las Comunicaciones y Ciberseguridad

El derecho al secreto y a la inviolabilidad de las comunicaciones, protegido penalmente (Art. 161 CP), ha devenido en una suerte de "pieza de museo" ante la tecnología. Ahora es posible, por ejemplo, leer cartas cerradas mediante microtomografía de rayos X y algoritmos de reconstrucción en 3D, inaplicando los supuestos de hecho del delito (PCM - Presidencia de Consejo de ministros, 2019).

Además, el objeto tradicional del delito (la carta) está en peligro de extinción, reemplazado por mensajería instantánea (correo electrónico, WhatsApp). Una interpretación extensiva del tipo penal que incluye "otro documento de naturaleza análoga" es acertada para proteger estas nuevas formas de comunicación. No obstante, estas también son vulnerables a ser "leídas" sin abrirse mediante malware o "virus informáticos".

La regulación que combate el malware y la extracción ilegal de información es precaria. Aunque el **Código Penal peruano** contempla delitos como la posesión de equipos para interceptación (Art. 162-A) o la interferencia de comunicaciones electrónicas (Art. 162-B), las tecnologías emergentes burlan estos candados, vulnerando incluso entornos de máxima seguridad como los procesos judiciales (PCM - Presidencia de Consejo de Ministros, 2019).

Una consecuencia peligrosa es el "fruto del árbol envenenado": la prueba obtenida vulnerando derechos fundamentales, situación facilitada por técnicas digitales que quebrantan la ciberseguridad. Esto también facilita el lavado de activos y la evasión digital.

3.9. Comercialización Ilícita de Datos Personales

La información privada y la intimidad están constitucionalmente tuteladas. Sin embargo, en el mundo digital persiste una vulneración permanente de la privacidad mediante la extracción de datos a partir de la actividad en Internet. Casos como los "altavoces inteligentes" que se activan para recabar información bajo la excusa de "mejorar el servicio" son emblemáticos.

Ocurre el fenómeno de la "vulneración consentida", propia de los contratos masivos de adhesión (los llamados ciber-Drittwirkung por (Gomes Canotilho, 2009)). ¿Quién lee las condiciones de uso antes de usar una app? La despreocupación de los nativos digitales por su privacidad se explica por la seducción de la notoriedad pública que brindan estas aplicaciones. Su indignación surge solo cuando el producto recibido es deficitario.

El sistema de las tecnologías de la información se desmoronaría sin seguridad, pero lo cierto es que la información personal recolectada es circulada por las compañías tecnológicas con fines comerciales. El escándalo de Cambridge Analytica ilustra esto a gran escala: la venta indebida de datos de 50 millones de usuarios de Facebook a una empresa que los utilizó para análisis psicológicos y campañas de desinformación durante las elecciones de EE.UU. en 2016. **Como afirmó el científico de datos Christopher Wylie**, esto constituye "una violación básica de la autonomía para tomar decisiones libres".

3.10. Posverdad y Fake News: ¿Democracia o Infocracia?

Lo más pernicioso del nuevo agente "mediático" digital es el uso de la desinformación como arma de control. Las fake news permiten que cualquier persona divulgue información sin reparar en su veracidad, con efectos devastadores cuando son replicadas por medios "calificados". La rigurosidad de la información está incluida dentro del derecho fundamental a la información veraz.

La desinformación se ha convertido en una nueva forma de desestabilización y conflicto entre Estados, siendo objeto de alarmas por amenaza a la seguridad nacional. Sin embargo, resulta peligroso otorgar un poder "orwelliano" a una persona o grupo para decidir qué es "verdadero" y "falso", a fortiori cuando ese "verificador" es el propio Estado. Históricamente, información tachada de "conspiración" ha resultado veraz (ej., WikiLeaks, MK-Ultra, Tuskegee).

El derecho fundamental a la información veraz ha perdido sustancia, distorsionado por el bombardeo constante de información. Para las compañías tecnológicas, las noticias son solo datos dentro de un modelo de intercambio comercial. La novedad radica en la capacidad de las redes sociales para convertir noticias falsas en tendencias mayoritarias, ocupando un espacio fundamental del ámbito público.

Como remedio, en el campo constitucional se plantea el "derecho a la verdad" como manifestación de la voluntad de la sociedad digital de acceder a "calidad informativa" más que a "cantidad informativa".

3.11. El Derecho a la Privacidad Digital

¿Qué tan vigilados estamos? ¿Tenemos privacidad en el siglo XXI? La Unión Europea ha debatido la diáda: "¿promover los mensajes encriptados o vetarlos?". La encriptación refuerza la privacidad, pero también puede "camuflar actuaciones delictivas". Las Conclusiones del Consejo Europeo sobre ciberseguridad reflejan esta ambigüedad, admitiendo los desafíos para las autoridades pero subrayando que una encriptación fuerte es vital para la confianza digital y el respeto a los derechos humanos.

Casos reales ilustran este conflicto. En 2022, un ciudadano británico, Aditya Verma, fue arrestado tras escribir en un grupo privado de Snapchat (como broma) que iba "a volar el avión" (El Clarín, 2024). Un caza español interceptó el vuelo. ¿Cómo accedieron las autoridades a un mensaje privado? Este caso no es insólito; situaciones similares han ocurrido con mensajes de WhatsApp.

La discusión se extiende al plano laboral: ¿puede una empresa vigilar las herramientas digitales que provee a sus trabajadores sin límite? El Tribunal Europeo de Derechos Humanos, en el caso *Barbulescu vs. Rumanía*, estableció que la vigilancia empresarial requiere un aviso previo, consentimiento informado sobre la amplitud de la medida y una motivación reforzada con "razones legítimas", debiendo priorizarse métodos menos intrusivos (Grand Chamber, 2017).

Podríamos decir que el poder de la sociedad digital ha dejado en indefensión al derecho fundamental a la privacidad. Nunca sabremos con certeza hasta qué punto se nos han recortado libertades en este nuevo ambiente.



Derecho a la Privacidad Digital

Capítulo 4 – Hacia una Carta Magna Digital

4.1. Constitucionalizar el algoritmo, digitalizar la constitución

El advenimiento de lo que Karl Popper denominaba "La Sociedad Abierta" da lugar a la concepción de una "Constitución Abierta", entendida como un órgano vivo y en constante evolución. La aparición de esferas digitales "anómicas" y los profundos cambios descritos exigen repensar el derecho constitucional, condicionado por los nuevos paradigmas de esta era (Francisco & Barrilao, 2022).

Para responder a este enrevesado desafío, es necesario diseñar un "nuevo derecho público" que adapte su contenido con el fin de propugnar la eficacia de los derechos y la coherencia de los principios constitucionales en la realidad del siglo del algoritmo. Según el constitucionalista **Francisco Balaguer Callejón (2023)** (mencionado en (Palombino, 2023)), el camino implica una doble vía: por un lado, constitucionalizar los algoritmos, es decir, someter la nueva realidad del mundo digital a los principios y valores constitucionales; y por otro, digitalizar la constitución, adaptando la propia norma fundamental a las condiciones de un mundo nuevo que no puede gobernarse plenamente con los instrumentos de la constitución analógica.

En este sentido, el "constitucionalismo digital" puede definirse como el conjunto de reglas, principios, valores y jurisprudencia constitucional que buscan aplicarse a las controversias intersubjetivas en la era digital, con el objetivo de optimizar las libertades y los derechos humanos en el siglo XXI. La constitución analógica es ajena a un mundo digital que es, en buena medida, virtual, codificado, impersonal, transnacional y global. Problemas como la concentración digital monopolística, la seguridad informativa, la garantía de los derechos en la red y la canalización de conflictos políticos en las plataformas sociales son solo ejemplos de los desafíos que una "sociedad del cambio" plantea al derecho tradicional.

4.2. Las cinco rupturas del constitucionalismo tradicional

La crisis del constitucionalismo en la era digital se manifiesta a través de cinco rupturas fundamentales que redefinen su esencia:

- Ruptura entre la modernidad y la posmodernidad: El proyecto racional, universalista y de progreso lineal de la modernidad choca con la fragmentación, el relativismo y la incredulidad hacia los grandes relatos que caracterizan a la posmodernidad digital.
- Ruptura entre la realidad física y la realidad virtual: Se consolida un dualismo donde la primera se regula principalmente por el Estado a través del derecho público, mientras que la segunda, de alcance global, se ordena esencialmente por compañías tecnológicas a través del derecho privado.
- Integración entre lo nacional y lo mundial: Las soberanías nacionales se ven desbordadas por fenómenos digitales que operan en una escala global, exigiendo respuestas normativas que trasciendan las fronteras.
- La mutación de los derechos fundamentales como límite al poder: El objeto del límite se desplaza. Los derechos ya no operan solo como freno al poder del Estado (el Leviatán tradicional), sino que deben erigirse como el límite al poder de los algoritmos y de las entidades privadas que los controlan.
- La mutación del constitucionalismo analógico en el constitucionalismo digital: El paradigma jurídico mismo debe evolucionar de uno basado en lo tangible, presencial y nacional, a otro capaz de dar cuenta de lo virtual, remoto y global.

Estas rupturas difieren de las revoluciones constitucionales clásicas (inglesa, americana, francesa), que fueron respuestas ante el totalitarismo o el gobierno absoluto dentro del Estado. En cambio, las rupturas actuales se sitúan ajenas al Leviatán, configurando un mundo donde el poder público estatal no alcanza a una gran parte de la realidad que antes ordenaba. Este nuevo escenario se hizo patente en crisis mundiales como la financiera de 2008 y la sanitaria por la COVID-19, y se evidencia hoy en las guerras comerciales y digitales entre potencias globales.

4.3. El poder de las Big Tech y la necesidad de límites

La potencialidad de los "factores reales de poder" de los que hablaba Ferdinand Lassalle se ha evidenciado plenamente en la era digital. La capacidad de las Big Tech o gigantes tecnológicos (como Meta, Alphabet/Google, Apple, Amazon y Microsoft) para configurar los procesos comunicativos y el espacio público a través de aplicaciones de Internet ha significado el reemplazo parcial del poder material por un poder digital. La estrategia de estas compañías y de los Estados se centra en el control de datos, un recurso que evoluciona en paralelo a las plataformas de servicios que monopolizan el nuevo valor digital.

Difícilmente estos grandes conglomerados opten por autolimitarse voluntariamente respecto a los valores constitucionales. Sin embargo, el factor cultural es un agente determinante poderoso. Un referente histórico es el código Hays de Hollywood, un conjunto de lineamientos que, reflejando la cultura de su época (décadas de 1930 a 1960), prescribía cómo debían ser representados los personajes y las historias. Si trasladamos esta enseñanza al ámbito digital, fomentar una "cultura digital sana" acorde a los principios de libertad, igualdad y autodeterminación podría tener un efecto similar, guiando el comportamiento en los ecosistemas virtuales.

Lamentablemente, esta aspiración choca con un obstáculo mayúsculo: la concentración monopólica del orden digital en manos de las Big Tech. Algunas de estas compañías, como Apple Inc., han alcanzado un valor bursátil que supera el PIB de países como Italia o Brasil. Este poder económico per se no es reprochable; el problema surge cuando someten a lesiones permanentes de los derechos constitucionales, como en la venta de datos, la violación del secreto de las comunicaciones o la injerencia en procesos democráticos. Estas compañías globales, por sí mismas, no tienen interés en la regulación y menos en una "constitución" que actúe como dique a los usos abusivos de la tecnología. Por ello, es imperativo fijar límites a estos agentes, lo que obliga a reconsiderar los principios del derecho de la

competencia y a revivir la "responsabilidad social" de las empresas, tanto extra muros (en la sociedad) como intra muros (dentro de su organización).

4.4. Hacia un nuevo Derecho Público para la era digital

El poder soberano y, sobre todo, los juristas, parecen haberse adormecido ante el ineluctable efecto transformador de los espacios digitales en el fuero del individuo y en el derecho público. En gran medida, nos encontramos indefensos frente a estas nuevas tecnologías. La solución, sin embargo, no consiste únicamente en regular las tecnologías para garantizar los derechos. La regulación es importante para establecer una base legal sobre la que operen los mecanismos de control, pero no es suficiente (Palombino, 2023).

Es imprescindible el desarrollo de estructuras y procedimientos que hagan posible un control efectivo, basado en la salvaguarda de la persona como principio y fin del sistema. Autores clásicos como Hans Kelsen o Costantino Mortati prestaron atención en su época a los "factores reales de poder" y a su incidencia sobre la constitución, intentando someter el poder político al Derecho en el contexto del Estado nacional. Ahora nos toca a nosotros redibujar los límites al poder, esta vez en el mundo digital, un espacio que se sitúa fuera de los confines del poder estatal tradicional.

Queda claro que, para evitar que la constitución se convierta definitivamente en una "hoja de papel mojada en tinta" –como temía Lassalle–, se requiere un esfuerzo monumental de adecuación normativa y cultural. Diferentes instituciones ya han sostenido la urgencia de una nueva carta política, al advertir que la aplicación de la constitución y la vigencia de los derechos fundamentales se ve amenazada por un nuevo orden digital que, esta vez, se sitúa deliberadamente fuera del Estado. La tarea es ardua, pero el camino está trazado: hacia un constitucionalismo reinventado, capaz de garantizar la democracia y la dignidad humana en la era de los algoritmos.

Capítulo 5 – Legislación Global Digital: Un Panorama Comparado

5.1. Iniciativas Internacionales (ONU, OCDE)

La preocupación internacional por establecer un marco regulador que contemple los desafíos de la vida digital y garantice una tutela efectiva de los derechos no es nueva. Desde hace décadas, organizaciones multilaterales han intentado sentar principios básicos para la gobernanza digital.

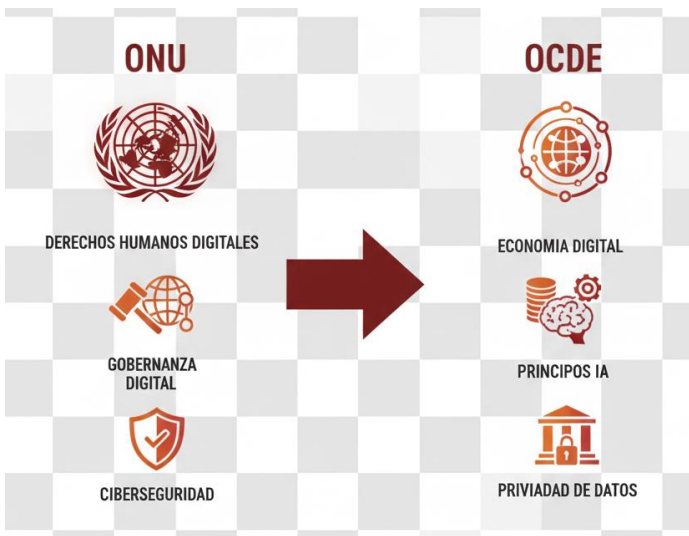
En el ámbito de la **Organización de las Naciones Unidas (ONU)**, ya en 1990 la Asamblea General aprobó la Resolución 45/95, conteniendo los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales (ONU, 1995). Este documento temprano reconocía la necesidad de proteger la privacidad frente al tratamiento automatizado de datos. Posteriormente, en 2013, la Asamblea General reafirmó esta preocupación con la resolución 'The right to privacy in the digital age, subrayando que los derechos humanos deben protegerse tanto en línea como fuera de línea.

La **Organización para la Cooperación y el Desarrollo Económicos (OCDE)**, por su parte, adoptó en 1980 sus Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. Estas directrices, aunque no vinculantes, han servido como modelo fundamental para la legislación nacional sobre protección de datos en muchos países, estableciendo principios como la limitación de la recolección, la garantía de calidad de los datos y la seguridad de la información (OCDE, 2002).

A nivel regional, el **Consejo de Europa** marcó un hito con el **Convenio 108**, adoptado el 28 de enero de 1981 (mencionado en (gavrilovic, 1981)) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter

personal. Este fue el primer tratado internacional jurídicamente vinculante en esta materia, sentando las bases para el posterior y más robusto **Reglamento General de Protección de Datos (RGPD)** de la (Unión Europea, 2025) .

Estos instrumentos iniciales demostraron una visión prospectiva, pero su carácter generalmente declarativo o su limitado alcance los hizo insuficientes para regular la explosión digital del siglo XXI.



Iniciativas Internacionales (ONU, OCDE)

5.2. El Liderazgo Regulatorio de la Unión Europea

Frente a la ambigüedad de muchas declaraciones internacionales, la Unión Europea (UE) ha emergido como el actor global más proactivo y ambicioso en la construcción de un marco regulatorio digital basado en valores. Su enfoque ha pasado de las declaraciones de principios a la legislación vinculante de alto impacto.

El interés de la UE por regular la **Inteligencia Artificial (IA)** se manifestó tempranamente. En 2017, la **Asamblea Parlamentaria del Consejo de Europa** en Estrasburgo aprobó el primer Informe Europeo sobre máquinas inteligentes, abordando temas pioneros como la responsabilidad civil de los robots (especialmente los coches autónomos), la creación de una agencia reguladora, la privacidad de los datos y la posibilidad de establecer un impuesto a la automatización (Unión Europea, 2020). Este informe abrió el debate sobre la necesidad de una gobernanza ética de la tecnología.

Posteriormente, en 2019, la Comisión Europea publicó las Directrices Éticas para una IA Fiable, un conjunto de principios (como la supervisión humana, la robustez técnica, la privacidad y la transparencia) destinados a guiar un desarrollo responsable de la IA. Estas directrices allanaron el camino para una regulación más estricta.

El compromiso político se plasmó en declaraciones conjuntas de los Estados miembros. La **Declaración de Berlín** sobre sociedad y gobierno digitales basado en valores (diciembre de 2020) incidió en el papel fundamental de los poderes públicos para asegurar que la transformación digital se asiente en valores como la participación social y la educación digital (Comisión Europea, 2020). Poco después, la Declaración de Lisboa sobre una democracia digital con propósito reafirmó tres objetivos clave: 1) equilibrar el desarrollo tecnológico con principios éticos y derechos humanos, 2) promover la cooperación digital internacional, y 3) fomentar una economía digital verde que favorezca la cohesión social.

Un hito simbólico fue la proclamación de la **Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital** (Comisión Europea, 2022). Su considerando 3 expresa de manera categórica: "La transformación digital no debe implicar un retroceso en los derechos. Lo que es ilegal fuera de línea, es ilegal en línea". Este principio de equivalencia, junto con la adopción del Programa estratégico de la Década Digital para 2030, demostró la determinación de la UE de

liderar una transformación digital protegida, segura y sostenible, alineada con sus valores constitucionales.

5.3. La Ley Europea de Inteligencia Artificial (AIA)

La culminación (hasta el momento) del esfuerzo regulatorio europeo es la **Ley de Inteligencia Artificial (AIA)**, formalmente adoptada por el (Parlamento Europeo, 2023). Este macroproyecto, que parte de la propuesta de la Comisión de abril de 2021 y se enmarca en la Década Digital 2030, constituye el primer marco regulatorio integral del mundo destinado a gobernar el desarrollo y uso de la IA de manera ética y responsable.

La Ley AIA establece las bases para un uso seguro y responsable de la IA en el espacio europeo, con estricto respeto a los derechos fundamentales. Su novedad más destacada es la adopción de un enfoque basado en el riesgo, clasificando los sistemas de IA en cuatro niveles, cada uno con obligaciones distintas:

1. **Riesgo Inaceptable (Prohibidos):** Sistemas de IA considerados una clara amenaza para la seguridad, los medios de subsistencia y los derechos de las personas. Incluye, en principio, la vigilancia masiva mediante reconocimiento facial biométrico remoto en espacios públicos con fines policiales, así como sistemas que manipulen el comportamiento humano para eludir su libre albedrío.
2. **Riesgo Alto (Supervisión rigurosa):** Sistemas de IA empleados en áreas críticas que gestionan procesos judiciales, formación profesional, servicios públicos esenciales (agua, energía), y procesos democráticos. Estos sistemas están sujetos a una evaluación de conformidad antes de su comercialización, requisitos de alta calidad de los datos, trazabilidad, supervisión humana y transparencia hacia el usuario.

3. **Riesgo Limitado (Obligaciones de transparencia):** Sistemas como los chatbots tienen el deber de informar al usuario de que está interactuando con una IA, para que pueda tomar una decisión informada. También se incluyen aquí obligaciones específicas de etiquetado para contenido generado por IA (como deepfakes en audio, video o texto) publicado con fines de información pública.
4. **Riesgo Mínimo (Normas generales):** La gran mayoría de los sistemas de IA actuales (filtros de spam, videojuegos con IA) entran en esta categoría, sujeta únicamente a normas generales de seguridad y buenas prácticas, permitiendo su uso gratuito.

La Ley AIA representa un modelo ambicioso que busca convertir a la UE en el estándar global para la regulación ética de la IA, equilibrando la innovación con la protección de los ciudadanos.



Ley Europea de Inteligencia Artificial (AIA)

5.4. Cartas de Derechos Digitales en Latinoamérica

Paralelamente a los esfuerzos europeos, en Latinoamérica han surgido iniciativas, principalmente desde la sociedad civil y algunos gobiernos, para reconocer y plasmar los derechos digitales. Estas "Cartas" o "Declaraciones" suelen ser documentos de carácter orientador y no vinculante, pero constituyen un primer paso crucial para visibilizar la problemática y presionar por futuras legislaciones. Entre ellas destacan:

- **Carta de Derechos de Internet para Guatemala (2017):** Una de las pioneras en la región, que buscaba establecer principios para un internet libre, abierto y accesible (Embajada Británica en la Ciudad de Guatemala, 2017).
- **Contract for the Web (2019):** Propuesta global del inventor de la Web, Tim Berners-Lee, que incluye principios como el acceso para todos, la construcción de una Web que sirva al interés público y el respeto a la privacidad (Contract for the Web, 2019). Aunque no es exclusivamente latinoamericana, ha tenido eco en la región.
- **Carta Magna de Derechos Digitales para Chile (2022):** Un esfuerzo por sistematizar los derechos de los ciudadanos en el entorno digital, reconociendo desafíos específicos de la región (Álvarez Valenzuela & Miralles, 2022).

Estas iniciativas encuentran su fundamento en principios básicos como la neutralidad de la red, el acceso universal, la seguridad de los datos personales, la libertad de expresión y la exigencia de estándares técnicos para las TIC. Si bien carecen de la fuerza coercitiva de una ley como la AIA europea, cumplen un rol pedagógico y político esencial: sentar las bases discursivas y normativas para que, en el futuro, los países latinoamericanos puedan desarrollar marcos regulatorios propios, adecuados a sus realidades y que eviten quedar a merced de estándares diseñados en otras latitudes. Su existencia evidencia que, aunque a un ritmo distinto, la preocupación por un constitucionalismo digital es un fenómeno global.

Capítulo 6 – El Caso Peruano: Avances y Desafíos

6.1. La Carta Peruana de Derechos Digitales

En el año 2022, Perú dio un paso significativo para posicionarse en el debate constitucional digital con la publicación oficial de la **Carta Peruana de Derechos Digitales** por parte de la Secretaría de Gobierno y Transformación Digital de la (PCM - Presidencia de Consejo de Ministros, 2022). Este documento representa un avance crucial, aunque preliminar, en la sistematización y reconocimiento de los derechos fundamentales adaptados al contexto digital peruano .

La Carta no es una ley ni un reglamento vinculante; es un documento de carácter orientador y programático. Su valor reside en ser el primer esfuerzo oficial por plasmar de manera integral cómo los derechos constitucionales se configuran y deben protegerse frente a las tecnologías informáticas. Se estructura como un listado de 24 derechos (y correlativas obligaciones) agrupados en seis bloques temáticos, delineando la responsabilidad del Estado en su protección:

- **I. Derechos relacionados con la protección de la persona en entornos digitales:** Incluye la Identidad Digital (Art. 1), la No discriminación (Art. 2), la Protección de datos personales (Art. 3), la Privacidad (Art. 4) y el derecho a Gozar de un ambiente digital equilibrado y adecuado (Art. 5).
- **II. Derechos que se ejercen en entornos o por medios digitales:** Aquí se reafirman derechos clásicos cuyo ejercicio se ha trasladado a la esfera virtual: Libertad de expresión e información (Art. 6), Acceso a la información pública (Art. 7), Acceso a la cultura y el conocimiento (Art. 8), Participación política (Art. 9), Reunión pacífica (Art. 10) y Asociación libre (Art. 11).
- **III. Habilitadores:** Contiene derechos que son condición para el ejercicio de los anteriores: Acceso a Internet libre, abierto y seguro (Art. 12), Neutralidad de la Red (Art. 13), Anonimato (Art. 14) y el derecho a beneficiarse de Tecnologías emergentes (Art. 15).

- **IV. Derechos específicos para niñas, niños y adolescentes:** Reitera y especializa para este grupo vulnerable los derechos a la Educación digital (Art. 16), a un Ambiente digital equilibrado (Art. 17), a la Protección de datos (Art. 18) y a la Privacidad (Art. 19).
- **V. Derechos relacionados con la Administración Pública:** Establece derechos frente al Estado digital: Salud digital (Art. 20), Educación digital (Art. 21), Justicia digital (Art. 22) y el derecho a Relacionarse por canales digitales con la Administración pública (Art. 23).
- **VI. Derechos específicos para el entorno laboral:** Reconocimiento del Derecho a la desconexión digital (Art. 24) y regulación del Teletrabajo (Art. 25).

Esta estructura evidencia un esfuerzo comprehensivo por abordar el fenómeno digital desde múltiples ángulos: el individuo, el ciudadano, el niño, el usuario de servicios públicos y el trabajador.

6.2. La Secretaría de Gobierno y Transformación Digital

La creación de la **Secretaría de Gobierno y Transformación Digital de la PCM**, establecida mediante **Decreto Legislativo 1412**, constituye el principal esfuerzo institucional del Estado peruano para liderar la modernización digital del país. Este ente rector está encargado de articular los esfuerzos del sector público, privado, la academia y la sociedad civil en materia de gobierno digital, confianza y transformación digitales (Presidencia del Consejo de Ministros, 2018).

Sus funciones son amplias y estratégicas, comprendiendo la regulación y supervisión de aspectos clave como las tecnologías digitales, la identidad digital, la interoperabilidad entre sistemas estatales, los servicios digitales, la seguridad y la arquitectura digital. Además, diseña y ejecuta la política nacional de transformación

digital, estableciendo normas, planes y lineamientos para garantizar su implementación correcta en toda la administración pública.

La existencia de esta Secretaría es un reconocimiento oficial de que la transformación digital no es un tema meramente técnico, sino una cuestión de política de Estado que requiere gobernanza, planificación y una visión de largo plazo. Su desempeño será fundamental para cerrar la brecha digital, modernizar trámites, mejorar la ciberseguridad nacional y, en última instancia, crear las condiciones de infraestructura y confianza necesarias para que los derechos consagrados en la Carta puedan ejercerse plenamente.

6.3. El Habeas Data y el rol de la Defensoría del Pueblo

La protección concreta de los derechos digitales en Perú requiere no solo de declaraciones, sino de mecanismos procesales efectivos. En este ámbito, el habeas data, regulado en el **Nuevo Código Procesal Constitucional** ((TC - Tribunal Constitucional, 2021)), se erige como la herramienta jurídica fundamental. Como afirma el profesor **Antonio Pérez Luño en** (Martín Ostos, 2017), el habeas data es "un cauce procesal para salvaguardar la libertad de la persona en la esfera informática". Este proceso constitucional es la vía idónea para tutelar la autodeterminación informativa —el derecho de cada persona a controlar el uso de sus datos personales— y los derechos conexos en las nuevas plataformas.

La efectividad del habeas data y de la tutela digital en general podría potenciarse significativamente con el fortalecimiento del rol de la **Defensoría del Pueblo**. Como institución nacional de derechos humanos, la Defensoría está llamada a tener un "protagónico lugar", tal como se sugiere en las conclusiones del documento original, en esta nueva etapa del constitucionalismo digital. Más que una mera "defensoría de los datos", se requiere que la Defensoría del Pueblo en su conjunto asuma la defensa y promoción de los derechos digitales como parte integral de su mandato.

Esto implicaría desarrollar expertise especializada en Ciberderechos, realizar supervisiones a las entidades públicas y privadas que manejen grandes volúmenes de datos, emitir recomendaciones sobre políticas digitales, orientar a la ciudadanía sobre el ejercicio de sus derechos en línea y actuar como un órgano de alerta temprana ante nuevas formas de vulneración digital. En un contexto donde el ciudadano común se siente abrumado por el poder de las plataformas tecnológicas, la Defensoría podría convertirse en un contrapeso esencial y un puente entre la sociedad civil y el Estado en la defensa de los derechos en el ciberespacio.

6.4. Perspectivas de futuro: ¿Hacia una reforma constitucional?

La situación jurídico-digital en Perú es todavía incipiente. La Carta Peruana de Derechos Digitales es un excelente punto de partida, pero su carácter no vinculante limita su impacto real. El gran desafío futuro reside en transitar de la **declaración de principios a la normativa exigible**.

Un camino posible y necesario es la potencial reforma constitucional para incorporar expresamente los derechos digitales. Un precedente alentador es la incorporación del **Artículo 14-A a la Constitución Política mediante la Ley 31878 (2023)**, que declara: "El Estado garantiza, a través de la inversión pública o privada, el acceso a internet libre en todo el territorio nacional...". Este es un primer y fundamental paso que reconoce el acceso a Internet como un derecho-habilitador (Diario Oficial El Peruano, 2023).

El siguiente paso lógico sería una reforma más amplia que pueda consagrar un núcleo duro de derechos digitales directamente en el texto constitucional, dándoles la máxima jerarquía y estabilidad. Esto podría incluir, como mínimo, el derecho a la protección de datos personales (autodeterminación informativa), el derecho a la identidad digital, el principio de neutralidad de la red y el derecho a la desconexión digital. Una

constitución digitalizada enviaría una señal poderosa sobre la prioridad que el Estado otorga a estos temas.

Paralelamente, es urgente desarrollar leyes de desarrollo constitucional específicas que regulen con detalle los principios de la Carta. Una **Ley de Transformación Digital integral, una actualización de la Ley de Protección de Datos Personales (Ley 29733)** (Congreso de la República, 2011) a estándares modernos como el RGPD europeo, y una legislación que aborde los vacíos en materia de responsabilidad por daños causados por algoritmos e IA, son piezas legislativas indispensables.

El éxito de este proceso dependerá de una adecuada interpretación y aplicación por parte de las autoridades, especialmente del **Tribunal Constitucional**, que tendrá el rol protagónico de realizar la adecuación interpretativa de los derechos clásicos a los nuevos contextos digitales, y del compromiso permanente de la sociedad civil para vigilar y exigir que estos derechos se respeten y fortalezcan en el cambiante entorno digital. El futuro del constitucionalismo peruano pasa, inexorablemente, por su capacidad de digitalizarse.

BIBLIOGRAFÍA

- Alva, R., Andrés, L., Jesús, E., Ravina, C., Milagros, P., & Pariona, S. (2023). Las nuevas tecnologías y el daño al derecho a la autodeterminación informativa y derechos conexos. la IA como nueva amenaza a los derechos fundamentales. *ACTA JURÍDICA PERUANA*, 6(2), 64–80. <https://doi.org/10.56891/AJRV6I2.412>
- Álvarez Valenzuela, D., & Miralles, D. Z. (2022). *Una constitución digital para Chile - Revista Chilena de Derecho y tecnología*. <https://doi.org/10.5354/0719-2584.2022.67657>
- Candón Mena, J. (2012). *Soberanía tecnológica en la era de las redes*. <http://www.bea.org.ar/>
- Comisión Europea. (2020, December 8). *Berlin Declaration on Digital Society and Value-based Digital Government | Configurar el futuro digital de Europa*. <https://digital-strategy.ec.europa.eu/es/node/479>
- Comisión Europea. (2022, December 15). *Declaración Europea sobre Derechos y Principios Digitales | Configurar el futuro digital de Europa*. <https://digital-strategy.ec.europa.eu/es/library/european-declaration-digital-rights-and-principles>
- Congreso Constituyente, E. (2025). *Constitución Política del Perú*.
- Congreso de la República. (2011, July 3). *Ley N.º 29733 - Normas y documentos legales - Congreso de la República - Plataforma del Estado Peruano*. <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733>
- Contract for the Web. (2019). *Contrato Para La Web Un plan de acción global para que nuestro mundo en línea sea seguro y empoderador para todos y todas*. <https://contractfortheweb.org/es/>
- Diario Oficial El Peruano. (2023). *Ley 31878: reconocen como derecho constitucional el acceso a internet*.
- El Clarín. (2024, January). *Dijo que iba a “volar el avión”, pero la broma pesada le salió muy mal*. https://www.clarin.com/internacional/dijo-iba-volar-avion-broma-pesada-salio-mal_0_Z3Rjk75oF3.html
- Embajada Británica en la Ciudad de Guatemala. (2017, February 22). *Guatemaltecos participan activamente en definición de sus derechos digitales - GOV.UK*. <https://www.gov.uk/government/news/guatemalans-actively-participate-to-define-their-digital-rights.es-419>
- Ferrajoli, Luigi., Pisarelo, Gerardo., Estrada, A. Julio., & Díaz Martín, J. Manuel. (2000). *El garantismo y la filosofía del derecho*. 198. https://books.google.com/books/about/El_Garantismo_y_la_filosof%C3%ADa_de_L_derech.html?hl=es&id=iyWjDwAAQBAJ
- Francisco, J., & Barrilao, S. (2022). Constitucionalismo Digital, Prospectiva Tecnológica y Mera Distopía Constitucional. *Revista Da AJURIS - Qualis A2*, 49(152), 395–418. <https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/1318>

- Fundamentais, D., & Justiça | Belo Horizonte, &. (2021). Constitucionalismo Digital. *Revista Brasileira de Direitos Fundamentais e Justiça*, 15(45), 63–91. <https://doi.org/10.30899/DFJ.V15145.1219>
- Gambarte, M. M. A. (2023). Constitucionalismo en crisis. *Constitucionalismo En Crisis*. <https://doi.org/10.2307/JJ.1895814>
- García Toma. (2010). *Teoría del Estado y Derecho Constitucional*.
- gavrilovic. (1981). *Convenio Para las Personas con respecto al Tratamiento Automatizado de Datos de Caracter Personal*. Estrasburgo, 28.I.1981.
- Giugovaz, E. (n.d.). *Ritzer George - La Mcdonalizacion De La Sociedad*. Retrieved November 30, 2025, from https://www.academia.edu/32927049/Ritzer_George_La_Mcdonalizacion_De_La_Sociedad
- Gomes Canotilho, J. J. (2009). *De las constituciones de los derechos a la crítica de los derechos § 10 DE LAS «CONSTITUCIONES DE LOS DERECHOS» A LA CRÍTICA DE LOS DERECHOS EN LAS CONSTITUCIONES*.
- Grand Chamber. (2017, September). *Barbulescu vs. Romania*. <https://hudoc.echr.coe.int/fre#%22itemid%22:%222001-177082%22>]
- Iviandy Aquino, & Oscar Flores. (2024). *El Caso Thaler y la Autoría de Obras Creadas por Inteligencia Artificial | Foro Jurídico*. <https://forojuridico.mx/el-caso-thaler-y-la-autoria-de-obras-creadas-por-inteligencia-artificial/>
- Josué Vasquez Villanueva, I., Nacional, U., De, M., & Marcos, S. (2023). Propedéutica constitucional peruana y disquisición de teoría del estado (1823-1993). *PRIUS - Revista de Derecho y Ciencia Política*, 1(2), 59–83. <https://doi.org/10.5281/ZENODO.11187418>
- Larenz, Karl. (2023). *Metodología de la ciencia del derecho*. 1–504.
- López González, J. L. (2001). *Häberle, Peter: Teoría de la Constitución como ciencia de la cultura Tecnos*, Madrid, 2000, 161 págs.
- Marín Jódar, & Ángel Juan. (2010). *La era digital: nuevos medios, nuevos usuarios y nuevos profesionales*. www.razonypalabra.org.mx
- Martín Ostos, J. de los Santos. (2017). *Pérez-Luño Robledo, Enrique César "El prodecimiento de habeas data. El derecho procesal ante las nuevas tecnologías"*. Editorial Dykinson, Madrid, 2017, 333 Páginas (ISBN: 978-84-9148-213-0).
- Martín Romero, Enrique., & Gómez, Ángel. (2025). *Inteligencia artificial y defensa El impacto en los ejércitos*. https://books.google.com/books/about/Inteligencia_artificial_y_defensa.html?hl=es&id=R9uYEQAQBAJ

- OCDE. (2002). *Directrices de la OCDE que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos personales (23 de septiembre de 1980)*. <http://publicaciones.administracion.es>
- ONU. (1995). *Resoluciones Aprobadas por la Asamblea General durante el 45° Periodo de Sesiones*. <https://www.un.org/es/documents/ag/res/45/list45.htm>
- Palombino, G. (2023). Balaguer Callejón, F. (2022). La constitución del algoritmo. Zaragoza: Fundación Manuel Giménez Abad. ISBN: 9788412448757. 206 páginas. *De Legge Ferenda*, 1, 167–171. <https://doi.org/10.30827/DLF.1.2023.28576>
- Parlamento Europeo. (2023, December 9). *Ley de Inteligencia Artificial: acuerdo sobre normas integrales para una IA fiable*. <https://www.europarl.europa.eu/news/es/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>
- PCM - Presidencia de Consejo de Ministros. (2019). *Decreto Legislativo N.º CÓDIGO PENAL - Normas y documentos legales - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Plataforma del Estado Peruano*. <https://www.gob.pe/institucion/indecopi/normas-legales/3462306-codigo-penal>
- PCM - Presidencia de Consejo de Ministros. (2022, July 27). *Carta Peruana de Derechos Digitales - Informes y publicaciones - Presidencia del Consejo de Ministros - Plataforma del Estado Peruano*. <https://www.gob.pe/institucion/pcm/informes-publicaciones/3302991-carta-peruana-de-derechos-digitales>
- Peces-Barba, Gregorio., Asís, R. de., Fernández Liesa, C. R. ., & Llamas Cascón, Angel. (2014). *Curso de derechos fundamentales : teoría general*.
- Presidencia del Consejo de Ministros. (2018, September 13). *Decreto Legislativo N.º 1412 - Normas y documentos legales - Presidencia del Consejo de Ministros - Plataforma del Estado Peruano*. <https://www.gob.pe/institucion/pcm/normas-legales/289706-1412>
- Revista Peruana de Derecho Constitucional. (2022). *Código Procesal Constitucional*.
- Roel Alva, L., Chocano Ravina, E., & Salazar Pariona, P. (2025). Los nuevos retos del derecho a la identidad en el Perú: desde la heteroasignación hacia la autodeterminación. *Persona y Familia*, 9, 221–242. <https://doi.org/10.33539/PERYFA.2020.N9.2340>
- TC - Tribunal Constitucional. (2021). *Nuevo Código Procesal Constitucional*.
- Tribunal Constitucional. (2009, January). *SENTENCIA DEL TRIBUNAL CONSTITUCIONAL*. <https://www.tc.gob.pe/jurisprudencia/2010/03052-2009-AA.html>
- Unión Europea. (2025, March 3). *Protección de Datos conforme al reglamento RGPD*. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
- Unión Europea. (2020, February 19). *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*.

<https://op.europa.eu/en/publication-detail/-/publication/4ce205b8-53d2-11ea-aece-01aa75ed71a1/language-es>

- Valdez, R., Elena, M., Vallejo, U. C., Beymar, P., & Solis Trujillo, P. (2021). Los efectos positivos y negativos en el uso de las Tecnologías de la Información y Comunicación en educación. *HAMUT'AY*, 8(1), 23–32. <https://doi.org/10.21503/HAMU.V8I1.2233>
- Zamora Varela, Y., & Mendoza Encinas, M. del C. (2023). La Inteligencia artificial y el futuro de la educación superior. *Horizontes Pedagógicos*, 25(1), 1–13. <https://doi.org/10.33881/0123-8264.HOP.25101>

Dirección legal: Urb. Paseo del Mar
Nuevo Chimbote, Santa, Ancash
Correo electrónico: ed.honexus@gmail.com
Teléfono: 978653152



ISBN: 978-612-99189-9-0



9 786129 918990