ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

GLOBAL CYBERSPACE GOVERNANCE: HARMONIZING AI REGULATIONS ALONG WITH IPR PROTECTION AND HUMAN RIGHTS ENFORCEMENT IN THE DIGITAL REALM

AUTHOR'S NAME – Maitri Shail Patel, Ph.D.

INSTITUTION NAME – Research Scholar, GLS University, Gujarat.

AUTHOR'S NAME – Dr. Sonal Raval, Ph.D.

AFFILIATION OF AUTHOR – Assistant Professor, GLS University, Gujarat.

Received on 28 July 2025, Accepted on 14 July 2025, Published on 17 July 2025

ABSTRACT:

The rise of artificial intelligence (AI) has triggered transformative changes across sectors, redefining innovation, artistic expression, and the contours of legal rights, particularly in the realms of intellectual property and privacy.[1] Simultaneously, the exponential growth of cyberspace has rendered it a global common operating beyond traditional sovereign boundaries, raising complex jurisdictional and regulatory questions.[2]

This expansion, however, is accompanied by increasing fragmentation in global governance over digital technologies, with divergent national frameworks, conflicting standards, and limited multilateral consensus undermining cohesive regulation.[3] These developments collectively underscore the urgency for harmonized, inclusive, and adaptive governance mechanisms to manage emerging techno-legal paradigms. The disjointed and siloed regulation of Artificial Intelligence (AI), Intellectual Property (IP), and Human Rights (HR) presents a critical challenge in the digital age, as fragmented legal frameworks fail to adequately address the complex, overlapping issues arising at their intersection. These challenges are further exacerbated by inconsistencies between national laws and the realities of global digital interdependence, where data, innovation, and digital expression transcend territorial boundaries. The absence of enforceable global standards or comprehensive multilateral treaties further undermines efforts to establish cohesive governance, leading to regulatory uncertainty, rights violations, and barriers to equitable technological advancement.

[1] WIPO, https://www.wipo.int/publications/en/details.jsp?id=4386 (last visited on July 1, 2025).

[2] Jack L. Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Columbia Law School (July 1, 2025, 8:00 P.M.) https://scholarship.law.columbia.edu/books/175/.

[3] UN digital library, https://digitallibrary.un.org/record/3865925?ln=en&v=pdf (last visited on July 1, 2025).

This research's objectives include:

- To critically analyze existing global AI governance frameworks
- To evaluate intersections of IPR and human rights in AI applications
- To identify barriers to harmonization
- To propose a framework for unified cyberspace governance

This research attempts to answer the following Questions:

Q.1 How do AI, IPR, and human rights intersect in cyberspace?

Q.2 What are the key global, regional, and national legal instruments in these domains?

Q.3 What are the challenges in harmonizing these laws across jurisdictions?

Q.4 What role can international organizations and treaties play?

Q.5 What legal and policy models can support integrated governance?

After all, it's true that: "A harmonized global framework integrating AI regulations with IPR and human rights protection will lead to better enforcement, innovation governance, and ethical technological development in cyberspace."

Important Concepts:

Digital constitutionalism seeks to graft foundational constitutional values—such as free speech, rule of law, equality, privacy, participation, and checks and balances—onto the architecture and governance of the digital space, thereby translating "thick" constitutional norms into cyberspace institutions, both public and private.[4] In parallel, Commons Theory reconceptualizes cyberspace as a regulated global commons, advocating governance frameworks that emphasize shared stewardship, equitable access to resources (like data and algorithms), and collective mechanisms to counteract monopolistic capture and knowledge enclosure. Building on this, a Human Rights–Based Approach (HRBA) to AI insists that all AI systems must be designed, deployed, audited, and governed through the prism of human rights—grounded in principles of dignity, non-discrimination, transparency, and accountability—to safeguard individuals against algorithmic bias, privacy infringements, and threats to autonomy. The Innovation-Regulation Equilibrium Theory offers a complementary

[4] Edoardo Celeste, *Digital constitutionalism: a new systematic theorisation*, Taylor & Francis (July 1, 2025, 8:00 P.M.) https://www.tandfonline.com/doi/abs/10.1080/13600869.2019.1562604

policy lens, arguing for a calibrated balance that simultaneously nurtures technology and safeguards rights, encouraging regimes that are neither excessively permissive nor excessively prohibitive, but dynamically pivot based on sectoral risk assessments and emergent harms.[5] Finally, Comparative Governance Models reveal distinct regional strategies: the EU's precautionary risk-based AI Act and GDPR-style data protections foreground rights and pre-emptive assessments; the US favours decentralized, market-driven, sector-specific regulation that values innovation agility; and China pursues cyber-sovereignty—centrally planned, state-led AI development aligned with national security and "core socialist values." [6] These models each embody different trade-offs: the EU privileges human-centric safeguards, the US prioritizes innovation and economic dynamism, and China emphasizes strategic control and social stability. At their intersection, these normative and theoretical frameworks illuminate both shared aspirations and deep tensions in digital governance. Digital constitutionalism offers values and structural guardrails; Commons Theory emphasizes the collective stewardship of cyberspace; HRBA ensures rights are non-negotiable; Innovation-Regulation Equilibrium demands adaptive, evidence-informed calibration; and comparative models expose the fragmented nature of global digital governance, underlining the urgent need for a principled, inclusive, and interoperable framework to reconcile sovereignty, public interest, and technological advancement in an increasingly interconnected world. Digital constitutionalism represents a normative movement that seeks to embed core constitutional values—such as free expression, privacy, democratic participation, rule of law, and checks and balances—into digital spaces governed by both state and private actors. As defined by Celeste, digital constitutionalism is "the ideology that adapts the values of contemporary constitutionalism to the digital society," and it encompasses a plural array of transnational responses, including private norms and binding legal instruments.[7] Suzor elaborates that this constitutionalist project scrutinizes and seeks to legitimize private governance structures, such as platform terms, by applying legal principles like transparency and accountability. Closely related, Commons Theory, derived from the political-economic analysis of global commons, reconceives cyberspace—including shared infrastructures, data resources, and AI platforms—as a regulated

[5] Nicolas Suzor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, Sage Journals (July 1, 2025, 8:00 P.M.) https://journals.sagepub.com/doi/10.1177/2056305118787812

[6] *Id* at 2350.

[7] *Id at 2350.*

global common outside traditional sovereign control.[8] This framework invokes mechanisms of collective resource stewardship, equitable access, and shared governance, cautioning against monopolistic enclosure of digital public goods. These conceptual foundations inform a robust Human Rights–Based Approach (HRBA) to AI. Leading scholars argue that AI systems must be developed, deployed, audited, and governed through human rights–compatible frameworks rooted in dignity, non-discrimination, fairness, transparency, and remedy. This HRBA prioritizes the mitigation of algorithmic harms—bias, privacy intrusions, autonomous decision-making without due process—and centers the assessment of AI systems on their impact on rights holders. Bridging these normative dimensions is the Innovation-Regulation Equilibrium Theory—an emergent policy framework which posits that regulation should strike a calibrated balance: supporting innovation's dynamic growth while safeguarding rights and societal values. It rejects polar approaches—either unbounded technological libertarianism or regulation-driven stasis—and promotes adaptive, risk-sensitive regulatory regimes. Such frameworks allow incremental responses grounded in empirical impact assessments, prioritizing sectoral risk thresholds and human rights protections. Together, the interplay of digital constitutionalism, commons theory, HRBA, and innovation-regulation equilibrium offers a guiding framework to address the fragmentation of global digital governance. Yet the existing landscape also reveals divergent comparative models of jurisdictional control over AI and the internet. In the European Union, the GDPR-style data protection regime and the flagship AI Act embody digital constitutionalism in action, anchoring privacy, explainability, fairness, and systemic risk regulation into binding law.[9] The EU's approach is precautionary and rights-centric, with robust enforcement mechanisms aligned with constitutional values. In contrast, the United States favors a decentralized, sectoral regulatory model. It relies on market-driven innovation, pragmatic rule-making, and patchwork governance, anchored in a strong First Amendment tradition and economic constitutionalism that prioritizes free enterprise and minimal precaution. This model encourages rapid AI diffusion but leaves key protection gaps, relying on claims of market self-regulation and innovation spillover. China embodies a third paradigm of cyber-sovereignty: state-led, centralized, and strategically oriented. Its model advances AI under strict governmental control, enforcing data localization, content regulation, and centralized algorithmic oversight framed by national security, economic planning, and

[8] Wikipedia, https://en.wikipedia.org/wiki/Global_commons (last visited on July 1, 2025).

[9] Oreste Pollicino & Federica Paolucci, *Digital Constitutionalism and the EU AI Act*, SSRN (July 1, 2025, 8:00 P.M.) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5098492.

"core socialist values." This system privileges strategic control and social stability over individual autonomy. These three models—the EU's rights-based approach, US techno-capitalism, and China's state-driven data authoritarianism—illustrate profound normative and institutional divergences. They highlight tensions between universal human rights standards and the assertion of sovereign autonomy in digital governance. The EU model leans toward constitutional convergence, the U.S. model champions regulatory pluralism, and China's model asserts sovereign digital boundary-making. This fragmentation carries deep implications for governing innovation and protecting rights in a digitally interconnected world. Without convergence, global AI regulation remains vulnerable to regulatory arbitrage, geopolitical decoupling, and protectionist technology silos, undermining collective responses to transnational challenges like algorithmic bias, cross-border profiling, and digital suppression. To reconcile these divergent trajectories, a synthesis is necessary: digital constitutionalism supplies the normative foundation and articulates principles; commons theory underscores the definition of cyberspace as shared public infrastructure; HRBA ensures that emerging technologies respect universal freedoms; and innovation-regulation equilibrium offers flexible, evidence-driven policy design. The comparative analysis of governance models, meanwhile, underscores the challenges and necessity of interoperability: rights-based safeguards must operate across different sovereignty regimes, avoiding techno-economic containment while fostering cooperative standards. Bringing these strands together points toward a pluralistic yet interoperable global digital governance architecture—one grounded in shared constitutional values, structured as a managed digital common, reliant on human-rights impact assessments, informed by risk-calibrated innovation-regulation balance, and flexible enough to coexist with diverse governance regimes. Such a framework can help channel AI development and digital interdependence toward outcomes that are both innovative and rights-respecting, ensuring that technology enhances democratic resilience, legal accountability, and collective well-being in the global digital ecosystem.

Introduction to Cyberspace Governance:

From its early utopian beginnings in the 1990s, when cyberspace was imagined as a stateless "electronic frontier," legal concerns soon arose as states and private actors recognized the need to inscribe boundaries and responsibilities in this new domain. John Perry Barlow's 1996 *"Declaration of the Independence of Cyberspace"* epitomized the dream of a borderless, autonomous digital sphere. Yet, as cyberspace matured, governments, multinational corporations, technical bodies, and civil society emerged as stakeholders asserting jurisdictional authority.[10] The establishment of ICANN in 1998 under U.S. Commerce Department oversight and the release of the 2013 *Tallinn Manual* on cyber warfare signalled that sovereignty, international humanitarian law, and non-intervention doctrines were being repurposed to map cyberspace.[11] Meanwhile, international treaties such as the 2001 Budapest Convention formalized cross-border cooperation to combat cybercrime, though enforcement remains uneven6. Throughout the 2000s and 2010s, jurisdictional clashes intensified: national data localization rules, privacy statutes like the EU GDPR, India's Digital Personal Data Protection Act, and China's "cyber-sovereignty" laws all sought to assert territorial control over digital flows18. The Internet & Jurisdiction Policy Network (founded in 2012) emerged to discuss legal interoperability amid the "legal arms race."[12] Parallel multistakeholder efforts—like the Global Commission on the Stability of Cyberspace and UN Group of Governmental Experts meetings—began defining norms on state behavior, cyber-attack thresholds, and due diligence in cyberspace.[13] The rise of AI in the 2010s added layers of complexity to this multi-actor, multi-jurisdictional landscape. AI tools now routinely cross borders via cloud platforms, data analytics, and algorithmic services, blurring the separation between national regulation and global deployment.[14] It has spawned new forms of online harm—automated disinformation, deep-fake campaigns, algorithmic bias, facial recognition misuses—raising urgent accountability questions under existing cyberlaw frameworks.[15] Existing treaties and conventions, designed for traditional cybercrime and state-led aggression, lack clarity on autonomous AI threats.[16] This governance gap prompted the creation of new initiatives: the Global Partnership on AI (2020), advocated by G7 countries for human-rights-

[10] Goldsmith & Tim Wu, *Who Controls the Internet?* (2006); and "Can the Internet Be Governed?" *New Yorker* (July 1, 2025, 8:00 P.M.) https://www.newyorker.com/magazine/2024/02/05/can-the-internet-be-governed.

[11] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), EFF (July 1, 2025, 8:00 P.M.), https://www.eff.org/cyberspace-independence.

[12] *Id at 2353.*

[13] *Id at 2353.*

[14] *Id at 2353.*

[15] Negrea Petru-Cristian, Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies in Contemporary Geopolitics, research gate (July 1, 2025, 8:00 P.M.), https://www.researchgate.net/publication/378334428_Cyber_Conflict_and_International_Relations_A_Comprehensive_Analysis_of_Cyber_Deterrence_Strategies_in_Contemporary_Geopolitics

[16] Shrishti Sharma, "Transformation of State Sovereignty in the Age of Cyberspace," CRIL (2025) (July 1, 2025, 8:00 P.M.), https://cril.nliu.ac.in/2025/04/15/transformation-of-state-sovereignty-in-the-age-of-cyberspace/

aligned AI norms.[17]; the Council of Europe's Framework Convention on AI (Sept. 2024)—the first binding intergovernmental AI treaty[18]And proposals for international institutions or "AI regulators" akin to the IPCC or WTO, to harmonize technical standards across jurisdictions.[19] Yet jurisdictional fragmentation persists. The EU's AI Act and product safety regime embed digital constitutionalism and precaution, but face challenges in enforcement harmonization across member-states.[20] The U.S. continues to rely on sectoral regulation, innovation first, leaving rights enforcement to follow.[21] China emphasizes centralized, state-led AI sovereignty, with data localization, algorithm registration, and digital ethics framed in terms of national security and social harmony.[22] These different legal orders not only co-exist but frequently collide as firms and data streams traverse them. Export control regimes further fragment AI governance, especially for dual-use and foundational models, exacerbating "splinternet" outcomes.[23] This evolving landscape reflects a broader paradox: cyberspace and AI are fundamentally transnational, yet embedded within nation-state-derived legal regimes.[24] Classical sovereignty principles—sovereignty, non-intervention, attribution—are stretched by digital federalism demands, but full coordination remains elusive.[25] Public–private partnerships, technical standards bodies, and hybrid institutions like the Internet & Jurisdiction Network, the Global Partnership on AI, and multistakeholder forums have mitigated some conflicts. Yet binding accountability for algorithmic harms, state-sponsored cyber operations, and cross-border data misuse still lags behind the pace of technological diffusion. In sum, the legal evolution of cyberspace has proceeded in waves: initial legal ambiguity giving way to formal cyberlaw and domain control; growing recognition of global jurisdictional fragmentation as states and the private sector assert overlapping authority; and, finally, the advent of AI, which amplifies the demand for coherent, interoperable transnational governance. While multilateral treaties like the Budapest Convention and the Council of Europe AI

[17] Jack L. Goldsmith & Tim Wu, *Who Controls the Internet?*: Illusions of a Borderless world, Columbia Law School (July 1, 2025, 8:00 P.M.), https://scholarship.law.columbia.edu/books/175/

[18] Veale & Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" Cornell university (July 1, 2025, 8:00 P.M.), https://arxiv.org/abs/2107.03721.

[19] *Wikipedia, https://en.wikipedia.org/wiki/Tallinn_Manual* (last visited on July 1, 2025).

[20]Jack L. Goldsmith & Tim Wu, *Supra note 17* at.

[21] Jeffrey Biller, "The Evolution of International Law in Cyberspace," Lieber institute (July 1, 2025, 8:00 P.M.), https://lieber.westpoint.edu/year-ahead-coming-years-evolution-law-cyber-operations/

[22] Shristhi sharma, *Supra Note 16* at.

[23] Wikipedia, https://en.wikipedia.org/wiki/Framework_Convention_on_Artificial_Intelligence (last visited on July 1, 2025).

[24] Wikipedia, https://en.wikipedia.org/wiki/Internet_%26_Jurisdiction_Policy_Network (last visited on July 1, 2025).

[25] Jack L. Goldsmith & Tim Wu, *Supra note 17* at 2354.

Convention begin to address these challenges, emerging institutional proposals—from global AI regulatory agencies to digital Socratic platforms—signal a recognition of the need for concerted international legal architecture. Yet, persistent divergence between EU, U.S., and Chinese models, along with slower action by Global South states, risks legal balkanization. Without an inclusive, layered governance ecosystem—grounded in accountable state action, flexible multistakeholder standards, and enforceable treaty instruments—cyberspace and AI will remain legal grey zones, subject to conflict, fragmentation, and unaddressed externalities—imperilling individual rights, democratic governance, and global security in the digital age.

Regulation of Artificial Intelligence:

Artificial intelligence (AI) encompasses a diverse set of machine-based systems capable of performing tasks that traditionally require human intelligence—such as perception, learning, reasoning, and decision-making—by processing inputs and generating outputs to influence physical or virtual environments, with varying levels of autonomy and adaptiveness post-deployment. According to the OECD, an "AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. The Financial Times glossary further defines AI as “machines performing tasks needing human intelligence,” spanning subdomains such as deep learning, natural language processing, computer vision, generative AI, and LLMs.[26] These classifications include supervised, unsupervised, and reinforcement learning; white-box versus black-box models (distinguished by explainability); generative adversarial networks (GANs); and large transformer-based models. XAI (Explainable AI), according to Avrieta et al., emphasizes transparency, interpretability, and explainability of these complex models—an essential dimension in ethical and accountable AI.[27] National and international regulatory frameworks have arisen in response to AI’s transformative potential and risks. The **EU Artificial Intelligence Act** adopts a risk-based, sector-specific governance model, classifying AI systems

[26] FINANCIAL TIMES WEBPAGE, https://www.ft.com/ (last visited on July 1, 2025).

[27] Wikipedia, https://en.wikipedia.org/wiki/Artificial_intelligence#:~:text=Artificial%20intelligence%20(AI)%20is%20the,perception%2C%20and%20decision%2Dmaking. (last visited on July 1, 2025).

into unacceptable risk (e.g., social scoring, real-time biometric identification, banned unless exempted), high-risk (healthcare, education, credit, employment, critical infrastructure, law enforcement), limited-risk (requiring transparency obligations), and minimal-risk (unregulated).[28] It mandates Fundamental Rights Impact Assessments (FRIAs), human oversight, technical robustness, continuous post-market monitoring, and conformity assessments—either via self-assessment or third-party audits—administered through a European AI Office and European AI Board.[29] The Act thus embeds constitutional values—privacy, fairness, non-discrimination, accountability—into binding law, establishing pan-EU harmonization and rigorous safeguards. In the **United States**, the **Blueprint for an AI Bill of Rights**, published by the White House Office of Science and Technology Policy, articulates five non-binding principles: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternatives, consideration, and fallback.[30] It applies to "automated systems that have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources."[31] Unlike the EU's legally binding structure, the Blueprint functions as policy guidance, incorporating transparency and fairness ideals akin to GDPR, but lacks enforcement mechanisms and risk-tiered classification.[32] Critics note ambiguities in surveillance boundaries and concerns about compliance with marginalized communities. Its technical companion includes checklists for designers, policymakers, and organizations to embed equity, oversight, and transparency in AI design.[33] On the global stage, the **OECD Principles on Artificial Intelligence**, adopted in May 2019 and updated in 2024, serve as the first intergovernmental standard, emphasizing five complementary values-based principles—innovative growth and well-being; human rights and democratic values including fairness and privacy; transparency and explainability; robustness, security and safety; and accountability—as well as five recommendations for policymakers (invest in R&D, foster inclusive ecosystems, shape

[28] Eur-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689#:~:text=The%20purpose%20of%20this%20Regulation,in%20accordance%20with%20Union%20values%2C (last visited on July 1, 2025).
[29] *Id at 2356.*
[30] *Id at 2356.*
[31] *Id* at 2356.
[32] *Artificial Intelligence,* https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence#:~:text=Opened%20for%20signature%20on%205,to%20technological%20progress%20and%20innovation. (last visited on July 1, 2025).
[33] Management Solution, https://www.managementsolutions.com/sites/default/files/publicaciones/eng/blueprint-for-an-ai-bill-of-rights.pdf (last visited on July 1, 2025).

interoperable governance, build human capacity, and promote international cooperation).[34] These principles inform national policies: OECD countries use their AI system definition as foundational to their respective AI laws or guidelines. OECD's adoption signals consensus on AI's cross-border management and interoperability, paralleling WTO or IPCC analogies.

Further, in September 2024, the **Council of Europe's Framework Convention on Artificial Intelligence**—also known as the AI Convention—was signed by over 50 countries, including the U.S., U.K., and EU member states, marking the first legally binding international AI treaty. It mandates accountability for AI harms, protection of user data, and adherence to democratic and rule-of-law principles. While its enforcement leans on monitoring, its entry into force rhythm requires ratification by five signatories.[35] The *regulatory trilogy*—EU Act, U.S. Blueprint, and OECD Principles / CoE Convention—presents different governance typologies:

- **EU**: Binding foundational framework, precautionary risk tiers, strong rights protection; enforcement through conformity assessments and centralized oversight.
- **US**: Flexible, sector-agnostic guidance rooted in civil rights and innovation; non-binding, reliant on voluntary adoption.
- **OECD/CoE**: International standards promoting trust, interoperability, and human-centric AI; a mix of principles and treaty obligations.

These models reflect varying priorities: balancing innovation vs regulation, sovereignty vs global coordination, economic competition vs ethical safeguards.

Underlying these regulatory lacunae are persistent **ethical risks**:

1. **Bias & Discrimination** — AI trained on biased or non-representative data can systematically disadvantage race, gender, age, or disability groups. Mehrabi et al. identify multiple fairness taxonomy gaps; the US Blueprint requires equity assessments and disparity testing; the EU AI Act mandates assessments for high-risk systems.[36]
2. **Surveillance & Privacy Intrusion** — Widespread use of facial recognition, behavioral profiling, and predictive surveillance threatens autonomy and privacy. The Blueprint calls for opt-out mechanisms and context-based surveillance restraint. But the EU bans real-time biometric identification absent exemptions, whereas U.S. limits are fuzzier;

[34] OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449, (last visited on July 1, 2025).

[35] *Id at 2357.*

[36] *Id at 2357.*

China expressly allows surveillance for national security, illustrating varied ethical thresholds.[37]

3. **Opacity & Explainability** — Black-box AI (e.g., deep neural networks, LLMs, GANs) resists human interpretability. XAI research strives to bridge this gap: transparency, interpretability, and explanations are now regulatory focal points. The OECD and EU demand explainability; the US Blueprint requires plain-language notice and explanations. Continued opacity undermines accountability.
4. **Autonomous Harm & Safety** — High-stakes deployment in health, transport, finance, or militarization entails safety risks from malfunction, adversarial attacks, or misuse. The EU's high-risk category includes safety measures; OECD ensures robustness; the US addresses safety loosely through the "safe and effective" principle.
5. **Accountability & Redress** — Lack of clarity about responsibility for algorithmic harms—e.g., who is liable when AI causes misdiagnosis or wrongful arrest? The EU's conformity regime enforces traceability; OECD declares accountability imperative; the US Blueprint emphasizes fallback and human oversight, but enforcement is voluntary.

Other risks include environmental impacts from massive computing, misinformation proliferation via generative AI, erosion of labor rights, and misuse for autonomous weapons—all noted in ethics scholarship. The multifaceted legal, ethical, and regulatory landscape reflects a dynamic tension: ensuring AI's promise—efficiency, innovation, social progress—without sacrificing human rights, democracy, fairness, and safety. Harmonization across jurisdictional models is emerging through treaties and OECD alignment, yet divergence persists in enforcement, risk categorization, and cultural values around privacy and surveillance. The imperative remains: to design adaptive, interoperable governance architectures that bridge binding and voluntary instruments, foster international cooperation, and embed ethical safeguards across the AI lifecycle. Only through such pluralistic but coherent governance can AI be harnessed responsibly, with trust and accountability, in service of humanity.

Intellectual Property Rights in the AI Era:

The emergence of advanced AI systems—from generative text and image models to autonomous design tools—has revealed critical tensions in traditional intellectual property (IP)

[37] *Id at 2358.*

frameworks, particularly in copyright, patent law, authorship, ownership, licensing, and enforcement across a borderless digital realm.

Copyright in AI-Generated Content:

Under classical copyright doctrine, protection attaches only to human-authored original works fixed in a tangible medium. AI tools, including large language models and generative art platforms, challenge this paradigm by producing expressive output without direct human creative control. Commentators note that copyright depends on human originality and judgment exercised by the author, raising the urgent question: Who, if anyone, is the author of AI-generated content?[38] In the United States, courts have consistently denied copyrightability to non-human creations. The U.K. Copyright Designs and Patents Act allocates rights to the person making the necessary arrangements for computer-generated works, but many jurisdictions remain silent. Scholar Pamela Samuelson proposes allocating such rights to the user who initiates and configures the AI (i.e., the "author" in contract terms), pointing to the need for legislative adaptation.[39] The training of AI models on massive copyrighted corpora—without explicit licensing—also generates legal friction. While defenders invoke the U.S. fair use doctrine to justify training, arguments persist that outputs closely mimicking copyrighted sources might infringe if they compete legitimately or replicate substantial expression.

Patentability of AI Inventions:

AI's role in inventing independently—or in collaboration—has sparked debate over patentability. The key inquiries are whether inventions are deemed patent-eligible and who qualifies as the inventor.

Recent legal decisions, including *Thaler v. Vidal*, clarify that only humans can be legally recognized as inventors in patent law. Patent offices worldwide—from the U.S. Patent and Trademark Office (USPTO) to the European Patent Office (EPO), UK IPO, and Japan—uniformly reject AI-only inventorship.[40] Patent eligibility under statutes like 35 U.S.C. § 101 requires inventive concepts beyond abstract ideas, algorithms, or mathematical formulas. Precedents like *Alice Corp. v. CLS Bank* and *Bilski v. Kappos* set the standard for abstractness

[38] Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works*, Wikipedia (July 1, 2025, 8:00 P.M.) https://en.wikipedia.org/wiki/Pamela_Samuelson.

[39] *Id at 2359.*

[40] Taylor Wessing, https://www.taylorwessing.com/ (last visited on July 1, 2025).

and inventive implementation. AI-generated outputs may face rejection unless tied to concrete technical applications.[41] Patent offices have begun providing guidance. The USPTO's 2024 update treats AI-assisted inventions as patent-eligible, so long as named human inventors made a significant contribution, even if AI played a role. Meanwhile, entities seeking patents in software-heavy jurisdictions like Europe, Japan, Korea, and India must demonstrate a "technical effect"—a real-world practical implementation beyond algorithms alone.[42] Challenges remain, especially with "black-box" AI. To satisfy sufficiency or enablement, patent applications must disclose how inventions work. If an AI model functions opaquely, that may fail disclosure standards unless accompanied by explainable designs or modules.[43] Ethically, granting exclusive rights to AI-generated inventions poses concerns of entrenched dominance by large tech firms, limiting access and innovation in a winner-takes-all patent landscape.

Authorship, Ownership, and Licensing:

With AI-generated content and inventions blurring lines of authorship and inventorship, IP ownership becomes contested territory:

- **Copyright**: Without clear rules, ownership may fall to the AI user, programmer, or data trainer, depending on jurisdiction or contractual terms—but clarity is lacking.
- **Patents**: Legally, inventorship must fall on a person. However, an AI system's "owner" might be listed as the applicant, as the U.K.'s DABUS case suggests, conferring rights even when AI isn't officially the inventor, though outcomes vary.[44]
- **Licensing**: AI models licensed with opaque terms may constrain rights downstream, raising issues of fair use, resale rights, and integration by third parties.

The lack of uniformity on ownership and licensing contracts—including ambiguity on moral rights, resale digital rights, or derivative works—complicates adoption and commercialization,

[41] *Alice Corp.* v. CLS Bank, 573 U.S. 208 (2014)

[42] De penning, Understanding The USPTO's New Guidance On Patent-Eligible AI Inventions, Mondaq (July 1, 2025, 8:00 P.M.) https://www.mondaq.com/india/patent/1564112/understanding-the-usptos-new-guidance-on-patent-eligible-ai-inventions

[43] Aaron Hayward, Anna Vandervliet, Byron Turner, Bryce Robinson, Rachel Montagnon, Heather Newton, Maximilian Kuecking, Peng Lei and Alex Wang, The IP in AI – Can patents protect AI-generated inventions?, Herbert Smith Freehills Kramer (July 1, 2025, 8:00 P.M.) https://www.hsfkramer.com/insights/2023-05/the-ip-in-ai/can-patents-protect-ai-generated-inventions.

[44] TaylorWessing, https://www.taylorwessing.com/en/expertise/services/patents-and-innovation (last visited on July 1, 2025).

making investment and innovation unpredictable. Standardized rights frameworks and contractual clarity are thus urgent needs.

Enforcement Challenges in Borderless Cyberspace:

Cyberspace enables seamless global dissemination of AI outputs, complicating IP enforcement:

1. **Jurisdictional complexity**: A copyrighted AI-generated image hosted in one country is instantly copied and reposted worldwide. Enforcement may require a patchwork of actions across diverse laws and courts, each interpreting authorship, fair use, and safe harbour differently.
2. **Cross-border infringement**: Digital platforms often escape the same territorial boundaries as users. While international conventions like the Berne Convention and TRIPS require national treatment, enforcement remains rights holder-driven and inconsistent.
3. **Automated infringing distribution**: Bots and scraping tools exacerbate infringement, mass-distributing unlicensed copies of AI-generated works, making detection and takedown a losing battle.
4. **Patent trolls and fragmented eligibility**: Patent landscape uncertainties—arising from no AI-inventor patents, evolving subject matter criteria, and jurisdictional differences—can lead to abusive patent assertion, forum shopping, and inconsistent injunctions.[45]
5. **Platform liability and notice regimes**: The effectiveness of safe-harbor provisions (DMCA, E-Commerce Directive) varies: rights holders must often provide notice and track takedown across jurisdictions. AI engines may not always recognize rights, resulting in inconsistent compliance.

Toward Solutions: Policy Responses and Harmonization:

To address these challenges, several reform pathways are emerging:

A. Legislative reform and sui generis IP rights:

Some propose new forms of rights, such as neighbouring rights, sui generis frameworks for AI-generated content or inventions, or contractual presumptions favouring the tool user unless

[45] Reuters, https://www.reuters.com/ (last visited on July 1, 2025).

assigned elsewhere. The DABUS precedent suggests rights to AI output may align with ownership/control rather than human-created origins.

B. Updated patent and copyright doctrines:

USPTO reforms and legislative proposals—like the Patent Eligibility Restoration Act in the U.S.—seek to clarify patent standards for AI-assisted inventions, enabling balanced protection for machine-driven innovation. Copyright legislation may soon need to define “author” to include humans directing AI processes.

C. International cooperation:

Harmonization under TRIPS and WIPO is still nascent. Coordinated treaties or interpretive guidance could align inventorship definitions, fair-use thresholds for training, and global enforcement mechanisms for AI outputs.

D. Private ordering and technology solutions:

Licensing schemes—such as model cards, data lineage labels, and blockchain-based attribution—can help trace rights and usage. Additionally, standardized license templates (Creative Commons, machine-friendly licenses) could streamline licensing for AI models and outputs.

E. Ethical and balanced IP norms:

IP regimes should balance incentive paradigms with fairness. Overbroad IP rights could stifle innovation and limit public access; under-protection could disincentivize investment. As John Alty notes, “copyright legislation … must strike a careful balance” between creator benefit and public domain enrichment.[46]

CONCLUSION: A Dynamic IP Ecosystem for the AI Age:

The AI era challenges all pillars of IP law—copyright, patent, authorship, ownership, licensing, and cross-border enforcement. Traditional frameworks based on human creativity, human inventorship, territorial jurisdiction, and static licensing are rapidly fragmenting.

Reform requires a multi-pronged response:

- **Legal updates**: Legislate for AI authorship and patent eligibility based on human direction.
- **Contractual clarity**: Clarify ownership and licensing terms for AI-generated outputs.

[46] John Alty, Lex World, Financial Times (July 1, 2025, 8:00 P.M.) https://www.ft.com/stream/fdcbf7c7-7197-4a87-987a-020202ea9c80.

- **International convergence**: Coordinate inventorship, training use, and enforcement standards.
- **Technology transparency**: Deploy technical attribution tools and open licensing norms.
- **Principled balancing**: Design IP regimes that promote innovation while preserving accessibility and fairness.

Only through such a holistic and interoperable approach can IP law maintain relevance, incentivize AI-driven creativity, and safeguard individual and collective interests in a borderless digital environment. This treatment integrates legal developments, doctrinal analysis, policy trends, and normative considerations, fully supported by precise academic and legal sources.

Human Rights in the Digital Age:

In the digital age, foundational human rights—such as privacy, freedom of expression, and the right to information—face unprecedented challenges and opportunities. The **International Covenant on Civil and Political Rights (ICCPR)**, notably Articles 17 (privacy) and 19 (expression/information), provides binding frameworks that protect individuals from "arbitrary or unlawful interference" and safeguard speech, subject only to narrowly tailored restrictions for public order or national security.[47] These norms underpin the development of digital rights instruments like the **UN Guiding Principles on Business and Human Rights**, which obligate both states and corporations to prevent abuses, especially in data collection, digital profiling, and algorithmic decision-making. The **International Principles on Communications Surveillance** (also known as the "Necessary and Proportionate" principles), adopted in 2013, further embed international norms, stipulating that any digital surveillance must be lawful, necessary, proportionate, and subject to independent oversight.[48] Yet, technologies of **algorithmic discrimination, misinformation proliferation, and surveillance capitalism** threaten to erode these rights. The phenomenon of surveillance capitalism—coined and analysed by Zuboff—describes industry-wide harvesting and commodification of personal data

[47] Aishwarya Agrawal, Human Rights in the Digital Era, Law Bhoomi (July 1, 2025, 8:00 P.M.) https://lawbhoomi.com/human-rights-in-the-digital-era/.

[48] Wikipedia, https://en.wikipedia.org/wiki/International_Principles_on_the_Application_of_Human_Rights_to_Communications_Surveillance (last visited on July 1, 2025).

to predict and shape behavior, often without meaningful user consent or oversight.[49] This infrastructure creates expansive opportunities for intrusive profiling and monitoring that bypass traditional privacy safeguards. In the workplace, for example, gig-economy platforms employ algorithmic management tools—so-called "robo-bosses"—that can lead to unfair deactivations and discriminatory outcomes, as seen in Uber's controversial dismissal of drivers based solely on algorithmic flags.[50] **Algorithmic bias and discrimination** have also become systemic threats. Studies demonstrate that facial recognition systems misidentify people of colour at dramatically higher rates than white individuals, undermining equality and due process. Algorithmic decision-making in hiring, sentencing, lending, and welfare often embeds historical biases—automating inequality unless rigorous fairness frameworks are adopted.[51] The **Toronto Declaration (2018)** urges states and private actors to apply binding standards to machine learning systems to protect equality and non-discrimination, calling for meaningful remedies when violations occur.[52] Further, scholarship warns of "algorithmic arbitrariness" in content moderation: automated systems may inconsistently flag or remove speech, threatening freedom of expression under Article 19 of the ICCPR.[53] The propagation of **misinformation**—often accelerated by AI-driven recommendation algorithms—has undermined democratic discourse, public trust, and informed consent. Truth and falsehood alike are commodified, with engagement-sustaining false content reigniting societal divisions and proliferating hate speech, as seen during elections and public health crises. Legal responses have emerged to protect core digital rights. The **EU's General Data Protection Regulation (GDPR)** sets global benchmarks for data privacy and subject autonomy, enabling rights like access, rectification, erasure, and portability, and requiring transparent and lawful processing of personal data. GDPR also enforces a "right to explanation" for automated decision-making that significantly affects individuals, embedding transparency as a legal principle.[54] Regionally, the ECHR's

[49] UPSC GUIDE, https://upscguide.in/surveillance-capitalism-privacy-regulation (last visited on July 1, 2025).
[50] Reddit, https://www.reddit.com/r/ObscurePatentDangers/comments/1ixxd37/aipowered_surveillance_capitalism_in_the_workplace/ (last visited on July 1, 2025).
[51] Kenneth Lipartito, Surveillance Capitalism: Origins, History, Consequences, MDPI (July 1, 2025, 8:00 P.M.) https://www.mdpi.com/2409-9252/5/1/2
[52] Wikipedia, https://en.wikipedia.org/wiki/Toronto_Declaration, (last visited on July 1, 2025).
[53] Theresa Adie, Harnessing Technology to Safeguard Human Rights: AI, Big Data, and Accountability, Human Right (July 1, 2025, 8:00 P.M.) https://www.humanrightsresearch.org/post/harnessing-technology-to-safeguard-human-rights-ai-big-data-and-accountability.
[54] Bryce Goodman, Seth Flaxman, European Union regulations on algorithmic decision-making and a "right to explanation", Cornell University (July 1, 2025, 8:00 P.M.) https://arxiv.org/abs/1606.08813

Article 8 and African Charter mirror these protections, while India's Supreme Court and the new DPDP Act (2023) similarly affirm privacy as a constitutional right under Article 21.[55] Nonetheless, enforcement gaps persist. Surveillance technologies outpace legal reforms, creating chilling effects on free expression. The **New Orleans facial recognition case**, where police used real–time scans without oversight, exemplifies algorithmic surveillance's real-world danger.[56] Meanwhile, workplace algorithmic management and automated profiling contribute to economic and social inequalities, often eluding regulatory scrutiny.[57] Addressing these threats necessitates a **human rights-based approach** to digital governance—integrating human rights assessments into policy and technological design. The **UN Guiding Principles on Business and Human Rights** require companies to conduct due diligence, assess impacts, and provide effective remedies for rights violations. The **Necessary and Proportionate Principles** demand that surveillance infrastructures be transparent, limited, and subject to judicial review.[58] The **Toronto Declaration** calls for equality impact assessments and accountability mechanisms for discriminatory systems.[59] Policy reforms are advancing: the **EU's Digital Services Act** and Online Safety Act in the UK impose new transparency obligations on platforms, particularly concerning content moderation and algorithmic governance.[60] In the U.S., the proposed AI Civil Rights Act (Markey, 2024) and other legislative initiatives seek to mitigate bias and algorithmic discrimination.[61] Civil society, including EFF, Access Now, and Amnesty, continues to advocate for robust legal standards, independent oversight, user empowerment, and accountability. Yet significant challenges remain. Transnational digital platforms complicate jurisdictional enforcement, landscapes remain fragmented, and authoritarian governments continue to exploit AI for censorship and surveillance. The digital divide further deepens the inequitable distribution of rights and protections, disproportionately affecting marginalized communities. In sum, safeguarding human rights in the digital age demands a **pluralistic, rights-centered governance**

[55] Aishwarya, *Supra Note 47* at 2365.

[56] Kenneth Lipartito, *Supra Note 51* at 2365.

[57] Alina Wernick, Anna Artyushina, Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies, Internet Policy Review (July 1, 2025, 8:00 P.M.) https://policyreview.info/articles/analysis/future-proofing-the-city

[58] Wikipedia, https://en.wikipedia.org/wiki/International_Principles_on_the_Application_of_Human_Rights_to_Communications_Surveillance (last visited on July 1, 2025).

[59] Wikipedia, https://www.en.wikipedia.org/ (last visited on July 1, 2025).

[60] Bryce Goodman, *Supra Note 54* at 2365.

[61] Theresa, *Supra Note 53* at 2365.

architecture—one that enshrines fundamental freedoms in law, ensures accountability for discrimination and misinformation, restrains surveillance capitalism, empowers individuals with control over their data, and fosters multistakeholder cooperation. This requires harmonizing binding international treaties with emerging regional standards and implementing human rights due diligence across corporate and governmental actors. Only through such comprehensive digital human rights frameworks can we ensure that technology enhances—not erodes—the dignity, autonomy, and democratic values at the heart of our global society.

The Intersections: AI, IPR, and Human Rights:

Artificial Intelligence at the nexus of surveillance, intellectual property, and human rights reveals deep-seated conflicts and emerging convergence points. In China, AI-enabled surveillance systems—powered by firms like iFlytek, Megvii, and SenseTime—have been deployed in regions such as Xinjiang to monitor and detain Uighur Muslims, employing massive voiceprint databases and real-time facial recognition checkpoints as part of an authoritarian compliance infrastructure.[62] These systems illustrate a direct tension between state priorities for security and the erosion of privacy, freedom of movement, and the right to information. In the realm of AI-generated art, the *Zarya of the Dawn* case in the U.S. and debates in India/EU regarding AI as co-creator have spotlighted divergences in copyright regimes. The U.S. Copyright Office's revocation of a Midjourney-generated comic's protection confirms the legal insistence on human authorship.[63] In India, the Copyright Office briefly recognized an AI tool as a co-author but later withdrew the registration, reflecting uncertainty under the Copyright Act's "computer-generated works" clause.[64] Meanwhile, in the EU, proposals for "AI authorship" signal shifting attitudes toward adapting IP frameworks.[65] These conflicts highlight how innovation in AI art challenges conventional notions of authorship, ownership, and licensing. Finally, AI-driven content moderation by platforms like Meta and X manifests further tensions: content moderation algorithms remove or downrank speech globally based on differing national standards. Automated takedowns—

[62] John Burgess, How a Chinese AI Giant Made Chatting-and Surveillance, Wired (July 1, 2025, 8:00 P.M.) https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/

[63] Nishant, Artworks Produced by Creative Robots and Copyright Protection, legal service India (July 1, 2025, 8:00 P.M.) https://www.legalserviceindia.com/legal/article-11868-artworks-produced-by-creative-robots-and-copyright-protection.html

[64] SCRIBD, https://www.scribd.com/document/847594202/ARTIFICIAL-INTELLIGENCE-AND-COPYRIGHT-LAW-IN-INDIA1-1 (last visited on July 1, 2025).

[65] *Id* at 2366.

some biased against minority voices—show algorithmic opacity and lack clear accountability, clashing with freedom of expression rights.[66] These systems span across jurisdictions where a single piece of content may be legal in one country but illegal in another, triggering takedown demands and platform compliance dilemmas. Across these domains, conflicts emerge: state-driven surveillance infringes privacy and civil liberties; AI-generated content unsettles IP regimes and artists' rights; and algorithmic moderation limits expression through opaque processes. Yet, convergence is possible by aligning policy frameworks—for example, applying human rights impact assessments to surveillance systems, updating copyright laws to reflect AI-assisted authorship, and embedding transparency and appeal rights in platform governance. Ultimately, all three sectors reveal a tension between innovation and rights enforcement—innovation offers efficiency, cultural creation, and social control, but often at the cost of privacy, authorship clarity, and speech freedom. The challenge lies in crafting interoperable, rights-based regulatory architectures—regional and global—that balance innovation's promise with robust protections for fundamental rights in our digitally mediated world.

Comparative Analysis of Global Models:

The comparative landscape of digital governance reflects profound divergences among the EU, the United States, China, and India. The European Union advances a rights-centric, precautionary model epitomized by the **General Data Protection Regulation (GDPR)**, which establishes data minimization, purpose limitation, and data subject rights enforceable through significant penalties (Regulation (EU) 2016/679). The **Digital Services Act (DSA)** further regulates online platforms' obligations to remove illegal content transparently while upholding freedom of expression (Regulation (EU) 2022/2065). The **AI Act** (Regulation (EU) 2024/1689) adopts a tiered risk-based approach, imposing stringent conformity assessments and prohibiting certain high-risk AI applications, including social scoring and untargeted biometric surveillance[67] In contrast, the United States maintains a sectoral, innovation-driven regime: privacy is governed by fragmented statutes such as the **Health Insurance Portability and Accountability Act (HIPAA)** for health data and the **Children's Online Privacy Protection Act (COPPA)** for minors, while broader AI regulation remains policy-oriented. The **Blueprint for an AI Bill of Rights** articulates principles on fairness, transparency, and accountability but

[66] The leaflet, https://theleaflet.in/digital-rights/art-artificial-intelligence-and-the-law (last visited on July 1, 2025).

[67] EU Artificial Intelligence, https://artificialintelligenceact.eu/article/5/ (last visited on July 1, 2025).

is nonbinding (White House OSTP, Blueprint for an AI Bill of Rights, 2022). This approach privileges technological growth and self-regulation, relying heavily on Federal Trade Commission enforcement and state legislation, such as the California Consumer Privacy Act.[68] China, by contrast, operationalizes a model of cyber-sovereignty and authoritarian governance. The **Cybersecurity Law of 2016**, the **Data Security Law of 2021**, and the **Personal Information Protection Law (PIPL) of 2021** centralize control over data flows, impose localization mandates, and facilitate extensive state surveillance (PIPL, arts. 3–4). China's AI regulation, including the 2023 Generative AI Measures, requires providers to align outputs with socialist values and submit algorithms for state registration, prioritizing security and ideology over privacy or free expression. India's emerging digital legal ecosystem occupies a hybrid space. The **Digital Personal Data Protection Act, 2023 (DPDP Act)** enshrines consent-based processing, data fiduciary duties, and user rights, but is narrower than GDPR.[69] Simultaneously, the **National Data Governance Framework Policy** advances data-sharing infrastructure and AI development, reflecting a developmentalist posture. Collectively, these models illustrate contrasting trade-offs between innovation, human rights, and state control, shaping the global contest over digital governance norms.

International Institutions and Their Role:

International institutions are central to shaping global digital governance, balancing innovation with rights protection. The **World Intellectual Property Organization (WIPO)** has spearheaded dialogues on AI and IP, convening multi-stakeholder discussions—such as the "WIPO Conversation on IP and AI"—and developing an AI & IP "Strategy Clearing House" to assist member states in adapting IP frameworks to AI, including copyright, patent, and data rights policy considerations.[70] This work complements WIPO's role in harmonizing global IP norms under treaties like the Paris Convention and the WIPO Copyright Treaty. The **UN Human Rights Council (UNHRC)** has increasingly advocated for digital rights, urging states to honor ICCPR protections like privacy (Art. 17) and expression (Art. 19) in the digital realm. The Council's Special Rapporteurs have called for strict oversight of mass surveillance and algorithmic decision-making, emphasizing human rights due diligence for both governments

[68] Leginfo, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100 (last visited on July 1, 2025).
[69] *The Digital Personal Data Protection Act*, 5, No. 22 of 2023, Act of Parliament (India).
[70] WIPO, https://www.wipo.int/en/web/frontier-technologies/ai_and_ip (last visited on July 1, 2025).

and tech companies. **UNESCO** has advanced one of the first intergovernmental ethical frameworks for AI. In November 2021, UNESCO's General Conference adopted the *Recommendation on the Ethics of Artificial Intelligence*, built on pillars including human rights, fairness, transparency, accountability, and do-no-harm obligations. It further promotes tools such as Ethical Impact Assessments and supports capacity-building, underscored by partnerships with LG AI Research and the launch of the Global AI Ethics Observatory.[71] Meanwhile, the **International Telecommunication Union (ITU)** facilitates technical standards and supports AI-for-Good initiatives alongside WIPO. The **World Trade Organization (WTO)** ensures that emerging digital and AI regulations align with TRIPS obligations, promoting non-discrimination and incentivizing innovation. The **Internet Governance Forum (IGF)**—a multi-stakeholder space rooted in the World Summit on the Information Society process—fosters inclusive dialogue among governments, industry, and civil society, shaping norms through peer exchange rather than binding mandates. While none of these bodies independently enforces digital governance, their combined efforts create a layered institutional ecosystem. WIPO sets IP policy precedents; UNHRC reinforces human rights obligations; UNESCO guides ethical AI development; ITU and WTO anchor technical and trade compatibilities; and the IGF fosters normative convergence. Together, they represent a mosaic of soft-law, treaty mechanisms, technical standards, and multi-stakeholder collaboration—each contributing to interoperable frameworks. The central challenge remains crafting coherent coalitions across these institutions to deliver accountability, consistency, and actionable protections in a fast-evolving digital landscape.

Proposals for Harmonized Global Governance:

Efforts toward harmonized global governance of digital technologies have increasingly emphasized **norm-building and soft-law mechanisms**, recognizing the limitations of rigid treaty-making in fast-evolving digital ecosystems. Instruments like the **OECD AI Principles** (2019) and **UNESCO's Recommendation on the Ethics of Artificial Intelligence** (2021) exemplify consensus-driven soft-law frameworks guiding states and corporations toward transparency, accountability, and rights-based AI development (OECD, AI Principles (2019); UNESCO, AI Ethics Recommendation (2021)). Scholars and policymakers have proposed a

[71] UNESCO, https://www.unesco.org/en/articles/unesco-and-lg-ai-research-forge-landmark-partnership-promote-ethics-artificial-intelligence (last visited on July 1, 2025).

Model Treaty on Digital Governance, integrating cross-cutting norms for privacy, algorithmic accountability, and platform responsibility under a unified framework (Floridi & Cowls, 2021). Further, calls for a **Digital Governance Charter** or a **Multilateral Convention on Digital Rights** have been advanced by UN bodies and civil society coalitions, aiming to consolidate normative alignment under instruments akin to the ICCPR but tailored to cyberspace. Multi-Stakeholderism remains a cornerstone, as exemplified by the **Internet Governance Forum (IGF)** and **Global Digital Compact** consultations, where **governments, tech corporations (e.g., Meta, Google), and civil society** co-develop frameworks balancing innovation and fundamental rights (UN, Global Digital Compact). These initiatives collectively signal a shift toward inclusive, principles-based digital constitutionalism across jurisdictions.

CONCLUSION AND SUGGESTIONS:

In conclusion, the intersection of AI, Intellectual Property Rights, and Human Rights reveals critical tensions between innovation, regulation, and fundamental freedoms. While global models vary—from the EU's rights-based approach to China's state-centric controls—harmonized governance remains feasible through soft-law instruments, multi-stakeholder frameworks, and interoperable principles. A global digital governance charter, underpinned by ethical AI norms and human rights obligations, offers a viable roadmap. Future research must explore enforcement mechanisms, AI explainability, cross-border data governance, and participatory model design, ensuring inclusive digital ecosystems that safeguard creativity, autonomy, and equity in the rapidly evolving technological landscape.