CYBERSPACE GOVERNANCE AND INTELLECTUAL PROPERTY (IP) PROTECTION IN INDIA: LEGAL FRAMEWORKS AND CHALLENGES

Maitri Shail Patel, Ph.D. Research Scholar at the School of Doctoral Research and innovation (SDRI), GLS University (Ahmedabad).[1]

Dr. Sonal Raval, Assistant Professor at Faculty of Law (FOL), GLS University (Ahmedabad)[2]

ABSTRACT

This research paper comprises cyberspace governance and intellectual property protection in India when it comes to the existing legal frameworks and challenges related to the same. It's unique in its own way as it talks about one of the most debated topics nowadays in the era of digitalization and technological advancement. This paper is a doctrinal, non-empirical and an exploratory study which has truly summarized that how cyberspace governance and intellectual property protection are interconnected in this digital era.

Keywords: Cyberspace, Cyberspace Governance, Intellectual Property, Protection, Legal Frameworks, and Challenges.

[1] The Author is a Ph.D. Research Scholar at the School of Doctoral Research and innovation (SDRI), GLS University (Ahmedabad).
[2] The Co-Author is an Assistant Professor at Faculty of Law (FOL), GLS University (Ahmedabad) and currently, the Author's Ph.D. Guide also.

I. Background:

Earlier when at global level or even at national level, when there used to be spectacular debates and discussions about the world-wide and enormous spread of the technological advancement with the invention and increased usage of computers, no one ever even imagined that it could get this gigantic as the current situations as well as scenarios are coming up, especially in India. Never had anyone thought that digitalization, globalization, privatization and liberalization would bring out everything into an astonishing reality of the era of 21st century of latest gadgets, electronics, and even the arena of law, especially the criminal law as the offences are committed even on the Internet known as "Cyberspace" which has given to the way for the creation of "Cyberspace Governance", especially, in the context of Intellectual Property (IP) protection all over the globe, especially, in India.

1.1 Introduction:

Nowadays, just like any newspaper is incomplete without a breaking news, a magazine is incomplete without its iconic cover story, or any existing law is absolutely incomplete without its amendments, life nowadays, is absolutely unimaginable without any news, cover story or amendments in criminal law, especially, when it's ambit and frontiers have gone into digital arena.

In India, since the time immemorial, law as well as judiciary has been undergone an evolutionary change through and through especially, when it comes to criminal law as the ambit of offences have widened with the emergence of a virtual space called cyberspace (also commonly known as internet) and intellectual property laws as they have come to be very much interlinked and interconnected in a unique way.

Also, until year 2021 or so, governance was only understood in its literal meaning – which is confined only to the various aspects and tasks related to government formation, governing of a country and its citizens, functioning of legislature, executive as well as judiciary and administration.

But as the offences are being committed increasingly on cyberspace alongwith its utilization in day-to-day life for various works, the new concept termed "cyberspace governance" has come into emergence. So, eventhough, there have been several statutes existing in India regarding

intellectual property protection, cybercrimes, and cyberspace, there needs to be an in-depth study on what challenges have emerged and what are the challenges in the future.

As the intellectual properties are nowadays being stored on various digital platforms as well as digital media and arenas, they are increasingly becoming vulnerable to cybertheft from the company computers, cloud storages, softwares and so on. Hence, it has become a very relevant area of study and in-depth research when digitalization as well as globalization has reached it's peak.

The objectives of this research paper are: (a) to explore the vital interconnection between the cyberspace governance and intellectual property (IP) protection in India; (b) to study the existing statutes on cyberspace governance in the context of IP protection in India and understand the various challenges for coming up with the best solutions possible; and (c) to gather better and insightful inferences as well as useful suggestions as a way forward.

The research study is a theoretical study which has utilized several methodologies including the exploratory, doctrinal, and non-empirical research methodology.

1.2 Cyberspace Governance: Global and Indian Perspectives:

The borderless armature of the Internet has long frustrated classic, home- grounded public- law generalities of sovereignty. The decades-old debate over whether cyberspace is subject primarily to state regulation or to multi-stakeholder "tone- governance" has yielded a realistic answer both. At the global position, three broad governance models now contend. The European Union titleholders a rights-defensive, regulations-heavy frame epitomized by the GDPR and the Digital Services Act. China advances a sovereignty- centric model that foregrounds state control of data flows and content. The United States, still told by its early laissez- faire posture, relies on sector-specific rules buttressed by antitrust enforcement and public- security restrictions on foreign technology. Each model seeks to export its norms through trade deals, development aid, and cyber-diplomacy, producing a fractured "splinternet." Recent U.N. processes the Open-Ended Working Group and the announcement Hoc Committee noncyber-crime — have exposed deep North- South divides over whether being transnational law suffices to regulate State mechanism on the same in cyberspace or whether new covenants are demanded. Developing countries worry about digital colonialism and advocate capacity- structure and indifferent access rather than purely normative

pronouncements.

India, the world's largest open Internet governance, decreasingly positions itself as a swing state among these models. New Delhi's politic white papers emphasize "strategic autonomy" support for an open, secure, and interoperable Internet, tempered by the right of countries to apply domestic law against cross-border platforms.

This balancing act reflects India's binary imperatives — attracting foreign investment in its booming digital frugality while conserving nonsupervisory space to manage misinformation, data localization, and public security pitfalls. At home, India's governance toolkit has expanded well beyond the foundational Information Technology Act, 2000. The 2022 CERT- In Directions dictate 6- hour breach reporting and data retention by VPN providers; draft emendations to the Data Protection Act of 2023 narrow "concurrence fatigue" loopholes; and the forthcoming Digital India Act is anticipated to remake safe- harbor rules, put algorithmic-translucency duties, and introduce canted liability for "significant" interposers.

India's approach to global norm- making glasses its domestic pragmatism. In multinational fora, it aligns with the G-77 in defying binding proscriptions on "obnoxious cyber capabilities," citing asymmetric security challenges. Yet it co-leads capacity- structure enterprise at the Global Forum on Cyber Expertise and has inked the U.S.- led Counter-Ransomware Initiative statement. Regionally, India spearheads the "Global South Data- Flow Principles," calling for interoperable but locally enforceable data- governance norms — an attempt to attune GDPR-style acceptability with sovereignty enterprises.

Civil- society reviews centre on due- process poverties in India's content- blocking governance and the broad description of "fake or deceiving news" under the Information Technology (Central Guidelines and Digital Media Ethics Code) Rules, 2021. Courts have begun to check superintendent overreach in Google v. SMC (2024), the Delhi High Court applied proportionality to limit traceability demands on translated messaging services. analogous judicial engagement encyclopedically — from the CJEU's Schrems II decision to Brazil's Supreme Court rulings on the "Fake News Bill" — demonstrates how indigenous courts can shape cyber-governance when convention processes cube.

Looking ahead, effective cyberspace governance will depend on interoperable "middle-ground" results threat- grounded regulation of critical structure, minimum due- process

guarantees for content restrictions, and reciprocity fabrics for cross-border data. India's trial — combining an ambitious digital-public- goods mound (Aadhaar, UPI, ONDC) with incremental but rights-sensitive regulation — offers a template for other arising husbandry seeking to chart a path between Silicon Valley libertinism and Beijing centralism.

1.3 Meaning and Elements of Cyberspace Governance

With the exponential increase of digital data in cyber environments, security measures have gained more importance.[3] Cybersecurity threats are revealed by national and international units, and the number of these threats is increasing daily. The elimination of cybersecurity risks is possible with an effective cybersecurity strategy which is[4] – Cyberspace Governance. Since the concept of management is not sufficient, the implementation of this strategy is possible with cyber governance, which includes all stakeholders in the management processes.[5]

With the widespread growth of the Internet, a new space – cyberspace – has appeared and has rapidly been integrated into every facet of life and work. It has effectively become the fourth basic living space for human beings.[6] Although cyberspace has become a topic of increasing widespread concern, it is still difficult to understand cyberspace well because of its many definitions, vast and varied content, and differences with other similar spaces.[7]

The term "cyberspace" comes from the word "cybernetics", which is originally derived from the Ancient Greek "kybernetes" and means steersman, governor, pilot, or rudder.[8] The term "cyberspace" was first defined as a concept concerning the digital world created by computers. Specifically, it was described as "a consensual hallucination experienced daily by billions of legitimate operators" and "a graphic representation of data abstracted from the banks of every computer in the human system".[9] Technically, the development of cyberspace could track back to the birth of the world's first computer in 1946.[10] Considering the separation of physical and

[3] S. Savaş & S. Karataş, Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance, 3(1) Int'l Cybersecurity L. Rev. 7 (2022).
[4] *Ibid.*
[5] S. Savaş & S. Karataş, Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance, 3(1) Int'l Cybersecurity L. Rev. 7 (2022).
[6] H. Ning, *A Brief History of Cyberspace* (Auerbach Publications 2022).
[7] H. Ning, *A Brief History of Cyberspace* (Auerbach Publications 2022).
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*

telecommunication infrastructures among different fields, the Cyber-Physical System was proposed to deal with the integration of computation, communication, and physical system.[11]

Cyber governance is sometimes also used as internet governance.[12] The concept of governance has recently been affecting management systems in the world and has come to the fore. [13]Thus, as a reflection of this in cyberspace, the concept of cyber governance emerged as a natural result.[14]

Cyberspace governance involves establishing rules, regulations, and mechanisms for managing the use and development of cyberspace.[15] Key elements include defining the scope of governance, establishing clear roles and responsibilities, and developing policies and procedures.[16] Effective cyber governance also encompasses risk management, incident response, and compliance with relevant regulations and standards.[17]

1.4 Elaboration[18]:

- **Defining Scope[19]:**

Determining what aspects of cyberspace fall under governance, such as cybersecurity, online data privacy, or freedom of expression.

- **Roles and Responsibilities[20]:**

Identifying the actors involved in cyberspace governance, including governments, international organizations, private companies, and civil society.

[11] H. Ning, *A Brief History of Cyberspace* (Auerbach Publications 2022).
[12] S. Savaş & S. Karataş, Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance, 3(1) Int'l Cybersecurity L. Rev. 7 (2022).
[13] *Ibid.*
[14] S. Savaş & S. Karataş, Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance, 3(1) Int'l Cybersecurity L. Rev. 7 (2022).
[15] Online Google Search Result, Key Search Words "Elements of Cyberspace Governance", last visited: 17th May, 2025.
[16] *Ibid. Supra Note 14*
[17] *Ibid. Supra Note 14*
[18] *Ibid. Supra Note 14*
[19] M. Mueller, *Sovereignty and Cyberspace: Institutions and Internet Governance* (Vincent & Elinor Ostrom Memorial Lecture 2018).
[20] Online Google Search Result, Key Search Words "Elements of Cyberspace Governance", last visited: 17th May, 2025.

- **Policies and Procedures[21]:**

Developing and implementing rules and guidelines for cyberspace use, including cybersecurity policies, data protection regulations, and guidelines for online content moderation.

- **Risk Management[22]:**

Identifying, assessing, and mitigating cyber risks, such as cyberattacks, data breaches, and online fraud.

- **Incident Response[23]:**

Establishing plans and procedures for responding to cyber incidents, including data breaches, malware infections, and denial-of-service attacks.

- **Compliance[24]:**

Ensuring that cyberspace activities comply with relevant laws, regulations, and industry standards.

- **Good Governance Principles[25]:**

Applying principles such as accountability, transparency, and rule of law to cyberspace governance.

- **Multi-stakeholder Approach[26]:**

[21] M. Weiss & V. Jankauskas, Securing Cyberspace: How States Design Governance Arrangements, 32(2) Governance 259 (2019).
[22] I. Pernice, *Cybersecurity Governance: Making Cyberspace a Safer Place* (2017). —risk management frameworks & compliance.
[23] A. Shull & A. Boysen, *Governing Cyberspace During a Crisis in Trust* (CIGI 2019). —incident-response coordination & trust-repair mechanisms.
[24] I. Pernice, *Cybersecurity Governance: Making Cyberspace a Safer Place* (2017). —risk management frameworks & compliance.
[25] L.Y. Chang & P. Grabosky, The Governance of Cyberspace, in *Regulatory Theory: Foundations and Applications* 533 (2017). —roles, responsibilities & policy design.
[26] A. Liaropoulos, Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics, 15(4) J. Info. Warfare 14 (2016). —good-governance principles & power dynamics; S.Y. Peng, Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (IR) Relevance of the TBT Regime, 51 Cornell Int'l L.J. 445 (2018). —industry standards & regulatory compliance; and M. Mueller, *Sovereignty and Cyberspace: Institutions and Internet Governance* (Vincent & Elinor Ostrom Memorial Lecture 2018). —scope-setting, sovereignty & multistakeholderism.

Involving a wide range of stakeholders in cyberspace governance, including governments, private sector actors, civil society organizations, and individuals.

- **Adaptability[27]:**

Recognizing that cyberspace is constantly evolving and adapting governance structures and policies accordingly.

1.5 Key Stakeholders in Cyberspace:

Key stakeholders in cyberspace include governments, the private sector, civil society, technical communities, and international organizations.[28] These groups have variety of roles and responsibilities in shaping and maintaining a secure and stable digital environment.[29] Governments play a key role in policy-making and regulation, while the private sector is responsible for infrastructure and technology development. [30]Civil society organizations can advocate for user rights and ethical considerations, and technical communities provide expertise in cybersecurity. [31] Finally, international organizations facilitate cooperation and standardization.[32]

Here's a more detailed description:

1. Governments:

- **Policy-making and regulation[33]:**

Governments set the legal and regulatory framework for cyberspace, including cybersecurity standards, data privacy laws, and national cybersecurity strategies.

---

[27] C.M. Glen, Internet Governance: Territorializing Cyberspace? 42(5) Pol. & Pol'y 635 (2014). —jurisdictional design & accountability.
[28] Online Google Search Result, Key Search Words "Key Stakeholders in Cyberspace", last visited: 17th May, 2025.
[29] *Ibid.*
[30] *Ibid.*
[31] Online Google Search Result, Key Search Words "Elements of Cyberspace Governance", last visited: 17th May, 2025.
[32] *Ibid.*
[33] Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World (Oxford Univ. Press 2006).

- **National security[34]:**

They are responsible for protecting critical infrastructure, national interests, and citizens from cyber threats.

- **Cooperation[35]:**

Governments engage in international collaborations to address global cyber challenges and build trust in cyberspace.

2. Private Sector:

- **Infrastructure and technology development[36]:**

Private companies develop and operate the technology infrastructure of cyberspace, including networks, hardware, and software.

- **Cybersecurity[37]:**

They are responsible for protecting their own systems and data from cyberattacks, as well as providing cybersecurity services to others.

- **Innovation[38]:**

Private sector innovation drives the development of new technologies and approaches to cybersecurity.

3. Civil Society:

- **User rights and ethical considerations[39]:**

[34] Kristen E. Eichensehr, Public-Private Cybersecurity, 95 Tex. L. Rev. 467 (2017).
[35] United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security (2021). U.N. Doc. A/76/135 (July 14, 2021).
[36]World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World (2012).
[37] Kristen E. Eichensehr, Cybersecurity's Sovereignty Gap: Government Responses to the Rise of Private Cybersecurity Companies, 52 U.C. Davis L. Rev. 101 (2018).
[38] Peter Swire, A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?, 3 J. Telecomm. & High Tech. L. 163 (2004).
[39] Laura DeNardis, *The Global War for Internet Governance* (Yale Univ. Press 2014).

Civil society organizations advocate for user rights, privacy, and ethical considerations in cyberspace.

- **Public awareness[40]:**

They raise public awareness about cybersecurity threats and best practices.

- **Advocacy[41]:**

They play a role in shaping public policy and promoting responsible cyber behavior.

4. Technical Communities:

- **Cybersecurity expertise[42]:**

This includes individuals and organizations with technical expertise in cybersecurity, such as cybersecurity researchers, incident responders, and standards organizations.

- **Standards and best practices[43]:**

Technical communities develop and promote cybersecurity standards and best practices.

- **Collaboration[44]:**

They collaborate to share information, respond to incidents, and develop new technologies.

5. International Organizations:

- **Facilitating cooperation[45]:**

Organizations like the United Nations and the ITU play a role in facilitating international

[40] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010).
[41] *Ibid.*
[42] Internet Engineering Task Force (IETF), *Mission Statement*, RFC 3935 (Oct. 2004).
[43] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (Wiley 2015).
[44]National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1, Apr. 2018).
[45] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015).

cooperation and promoting a common understanding of cyber issues.

- **Standards and norms[46]:**

They develop and promote international norms and standards for responsible state behavior in cyberspace.

- **Capacity building[47]:**

They provide technical assistance and capacity building to countries in developing their cybersecurity capabilities.

1.6 International Efforts and Treaties (WIPO, ICANN and ITU)

Cyberspace governance has increasingly become a subject of global cooperation, facilitated by international institutions such as WIPO, ICANN, and ITU. The World Intellectual Property Organization (WIPO) plays a central role in harmonizing rules related to intellectual property (IP) rights in cyberspace, including domain name disputes and copyright protection in digital platforms.[48]

The **Internet Corporation for Assigned Names and Numbers (ICANN)** manages the global Domain Name System (DNS), ensuring stable and secure allocation of IP addresses and domain names.[49] Its multistakeholder model emphasizes inclusiveness, transparency, and accountability in Internet governance. The **International Telecommunication Union (ITU)**, a UN specialized agency, sets global standards for information and communication technologies (ICTs), coordinates spectrum use, and promotes cybersecurity cooperation.[50]

These organizations collaborate to promote a free, open, secure, and interoperable Internet. Their efforts are essential in creating norms, building technical capacity, and addressing cyber threats across borders. In the Indian context, participation in these global forums has helped

[46] International Telecommunication Union (ITU), *Global Cybersecurity Agenda* (2007).
[47] OECD, *Digital Security Policy: Risk Management and Economic and Social Prosperity* (2015).
[48] World Intellectual Property Organization, *WIPO Overview of WIPO's Internet-Related Activities* (2022), https://www.wipo.int/about-wipo/en/internet.html.
[49] Internet Corp. for Assigned Names & Numbers, *About ICANN* (2023), https://www.icann.org/resources/pages/welcome-2012-02-25-en.
[50] Int'l Telecomm. Union, *Overview of ITU's Cybersecurity Work* (2022), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

shape national policies, enhance cyber capabilities, and foster international cooperation on digital governance issues.

1.7 India's Approach to Internet Governance

India's approach to internet governance is shaped by its democratic constitutional values, strategic interests, technological aspirations, and socio-economic diversity. As the world's largest democracy with one of the fastest-growing digital populations, India recognizes the Internet as both a critical enabler of development and a domain that needs secure, inclusive, and accountable governance. India's strategy focuses on four key areas: digital sovereignty, data protection, cybersecurity, and multistakeholder engagement.

India supports a multistakeholder model but with a strong role for the state in regulating content, managing infrastructure, and safeguarding national security.[51] The Information Technology Act, 2000, is India's primary legislation governing cyberspace, addressing cybercrimes, intermediary liability, and data handling practices.[52]

Amendments to the Act and evolving IT Rules, 2021, reflect India's increasing emphasis on content moderation, accountability of social media platforms, and enforcement of digital norms.[53] India's internet governance is also driven by its commitment to data sovereignty, demonstrated by its push for local data storage requirements and the passage of the Digital Personal Data Protection Act, 2023.[54]

This legislation establishes a consent-based data processing regime, empowers the Data Protection Board of India, and aims to strike a balance between innovation and individual privacy rights. On the international front, India participates actively in forums like the Internet Governance Forum (IGF), ICANN, WIPO, and the ITU, asserting its role as a major player in shaping global cyber norms.[55]

[51] Ministry of Electronics & Info. Tech. (MeitY), *India's Position on Internet Governance*, https://www.meity.gov.in (last visited May 16, 2025).
[52] The Information Technology Act, No. 21 of 2000, India Code (2000).
[53] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, https://www.meity.gov.in/content/it-rules-2021.
[54] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[55] Internet Governance Forum (IGF), *IGF Participants List - India*, https://www.intgovforum.org/en (last visited May 16, 2025).

India supports a more equitable global Internet infrastructure, where developing countries have a stronger say in standards and policymaking. This aligns with India's advocacy for digital inclusivity, capacity building, and development-focused internet governance.

India has also launched ambitious programs like Digital India,[56] aimed at transforming the country into a digitally empowered society and knowledge economy. The initiative promotes infrastructure development, digital literacy, and e-governance while embedding cybersecurity principles in digital expansion.

However, India's approach faces challenges, including tensions between regulation and freedom of expression, concerns over surveillance, and balancing innovation with control. Judicial scrutiny and public discourse continue to play a role in shaping India's evolving legal and policy frameworks.

The Supreme Court's landmark decision in ***Justice K.S. Puttaswamy v. Union of India***,[57] which recognized the right to privacy as a fundamental right, continues to influence internet and data governance laws. Overall, India's approach to internet governance seeks to reconcile openness and security, growth and regulation, sovereignty and global collaboration — an approach that reflects both its domestic priorities and its ambition to shape the future of cyberspace governance.

II. Intellectual Property (IP) in the Digital Environment:

The migration of creative and inventive activity from the analog world to networked, data-driven platforms has upended every pillar of classical intellectual-property (IP) doctrine. Copyright's fixation requirement, patent law's enablement standard, trademark's likelihood-of-confusion test, and trade-secret law's "reasonable efforts" rubric were all drafted for tangible media and territorially bounded markets.

Digital technologies—especially generative artificial intelligence (AI), distributed-ledger systems, and extended-reality (XR) interfaces—undermine those premises by permitting

[56] Digital India Programme, Ministry of Electronics & Info. Tech., https://www.digitalindia.gov.in (last visited May 16, 2025).
[57] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

instant, perfect, and global replication of protected subject matter, by de-coupling distribution from geography, and by automating the creation of derivative works at scale.

India's public-digital-goods stack (Aadhaar, UPI, ONDC, and the nascent Digital Public Infrastructure for Health) illustrates how government-backed platforms can nurture innovation while preserving openness. The recently issued "National Deep Tech Startup Policy" offers fast-track patents and sovereign seed funding, but conditions benefit on local data storage—an implicit IP-industrial-policy lever. As Indian courts refine injunction standards and the executive finalizes the Digital India Act, the country may furnish a replicable blueprint for emerging economies that seek to balance creator incentives, user rights, and strategic autonomy.

Digital transformation has not obviated intellectual-property law; it has magnified its stakes and exposed its fault lines. Effective governance in 2025 and beyond will therefore require interoperable, risk-based regulation that (1) clarifies the legality of data inputs for AI, (2) aligns privacy, competition, and IP objectives, and (3) empowers courts to calibrate remedies to technological realities. India's hybrid approach—combining ambitious digital-public infrastructures, data-sovereignty safeguards, and incremental yet rights-conscious reforms—offers a pragmatic template for navigating the uncertainties of IP in the digital environment.

The digital revolution has profoundly transformed the landscape of intellectual property (IP) in India. With the proliferation of digital technologies, the traditional frameworks governing IP rights face unprecedented challenges. Also, the major Ips in cyberspace nowadays include: Copyrights, Patents, Trademarks, and Trade Secrets.

With the digital arena becoming the new normal for storing the intellectual properties, the infinite and borderless nature of the enormously gigantic cyberspace has contributed in making the intellectual property rights enforcement as well as it's protection online very challenging as the other dimensions get involved in every such cybercrime like digital piracy, counterfeiting and domain squatting.

Hence, India needs to work up on its legislation as well as policy-making where it involves Digital Rights Management (DRM) and Technological Protection Measures (TPMs).

III. Legal Framework for IP Protection in India in Cyberspace:

The rapid evolution of digital technologies and the proliferation of cyberspace have significantly altered the intellectual property (IP) landscape across the globe, including India. The internet, with its borderless nature and instantaneous transmission of data, has brought both unprecedented opportunities and profound challenges to the protection and enforcement of IP rights.

In this digital milieu, India has sought to strike a balance between encouraging innovation, facilitating access to knowledge, and safeguarding the proprietary rights of creators. The country's legal infrastructure for IP protection in cyberspace is anchored in a combination of traditional IP statutes, specific digital laws, and judicial pronouncements that interpret and expand upon these statutes to address emerging complexities.

At the core of India's IP legal framework lie the **Copyright Act, 1957**, the **Patents Act, 1970**, the **Trademarks Act, 1999**, and the **Designs Act, 2000**, each of which has undergone amendments to align with technological advancements and the country's obligations under international agreements such as the **TRIPS Agreement** (Agreement on Trade-Related Aspects of Intellectual Property Rights).

Notably, the **Copyright (Amendment) Act, 2012** introduced provisions directly relevant to the digital domain, such as legal recognition of digital rights management (DRM) and protections for the broadcasting of works online.[58] The statute ensures that digital reproduction, transmission, and communication of works without authorization is treated as an infringement, thereby offering a degree of deterrence against online piracy.

Complementing these traditional statutes is the **Information Technology Act, 2000 (IT Act)**, which, though primarily designed to address cybercrime and data security, plays an ancillary but significant role in IP enforcement. Sections such as 66 and 67 of the IT Act penalize cyber-related offences including identity theft, hacking, and transmission of obscene materials, which often overlap with unauthorized exploitation of IP online.[59]

[58] The Copyright Act, No. 14 of 1957, INDIA CODE (2012), https://copyright.gov.in.
[59] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), https://meity.gov.in/writereaddata/files/itbill2000.pdf.

The IT Act's provisions on intermediary liability (Section 79), clarified in the landmark **Shreya Singhal v. Union of India**[60] define the circumstances under which internet service providers, social media platforms, and digital marketplaces may be held accountable for infringing content hosted on their platforms.

Judiciary in India has also contributed to shaping the IP cyberspace framework. Courts have upheld dynamic injunctions and blocking orders to combat digital piracy, especially in copyright cases involving movie releases and streaming content, as seen in **Super Cassettes Industries Ltd. v. MySpace Inc.**[61]. Such judicial interventions have reinforced the adaptability of India's IP regime to digital realities.

However, despite these efforts, challenges such as **anonymous infringement**, **cross-border jurisdiction**, **weak enforcement mechanisms**, and **limited public awareness persist**. As India aspires to become a global digital economy, a robust, agile, and harmonized legal framework for IP protection in cyberspace becomes imperative to ensure that innovation and creativity are effectively incentivized and safeguarded.

IV. Institutional and Regulatory Mechanisms:

India's stewardship of its fast-growing digital ecosystem relies on a lattice of ministries, sectoral regulators, statutory bodies, and specialized adjudicatory fora that together provide the normative and operational bulwark for cyberspace governance and the protection of intellectual-property (IP) rights. The Ministry of Electronics and Information Technology (MeitY) sits at the apex of this architecture, exercising rule-making power under the Information Technology Act, 2000 ("IT Act") and coordinating national policy through instruments such as the National Cyber Security Policy 2013 and its successor Draft National Cybersecurity Strategy 2021.[62]

MeitY's emergency and technical arm, the Indian Computer Emergency Response Team (CERT-In), issues legally binding "Directions" under section 70B of the IT Act; the April 2022 Directions require six-hour breach reporting and extensive data-retention by virtual-private-

[60] (2015) 5 SCC 1
[61] 2011 SCC OnLine Del 2646
[62] Ministry of Electronics & IT, *Draft National Cybersecurity Strategy* (2021), available at https://www.meity.gov.in.

network and cloud providers—measures intended both to harden cyber resilience and to preserve evidentiary trails for IP-infringement investigations.[63]

Parallel authority over data flows now vests in the Data Protection Board of India, constituted by the Digital Personal Data Protection Act, 2023 ("DPDPA"), which can impose compliance orders and monetary penalties that indirectly safeguard proprietary datasets—an increasingly valuable species of trade secret.[64]

Within the commerce portfolio, the Department for Promotion of Industry and Internal Trade (DPIIT) frames macro-level IP policy and represents India at WIPO and WTO TRIPS councils, while the Controller General of Patents, Designs & Trade Marks (CGPDTM) administers registration and opposition proceedings through modernized e-filing systems. For quasi-judicial redress, the erstwhile Intellectual Property Appellate Board has been subsumed into the High Courts under the Tribunals Reforms Act, 2021, thereby streamlining appellate review and aligning IP disputes with the judiciary's evolving cyber-jurisprudence.[65]

Sector-specific regulators also play a pivotal role: the Telecom Regulatory Authority of India (TRAI) prescribes content-delivery network norms that facilitate site-blocking for copyright enforcement; the Securities and Exchange Board of India (SEBI) has issued guidance on non-fungible-token (NFT) marketplaces to curb trademark counterfeits; and the Reserve Bank of India's directives on card-tokenisation underpin fintech IP security. Enforcement capacity is further buttressed by the Dedicated Cyber Crime Investigation & Forensics Division ("I4C") of the Ministry of Home Affairs, which coordinates state police cyber cells and hosts the National Cyber Crime Reporting Portal that channels takedown requests from right-holders.[66]

V. Challenges in IP Protection in Cyberspace in India:

India's aspiration to be a $1-trillion digital economy by 2027 has magnified long-standing fault lines in its intellectual-property (IP) enforcement architecture.[67] The very features that make cyberspace an engine of innovation—borderless reach, low replication cost, anonymity, and real-time distribution—also enable piracy, counterfeiting, database scraping, and trade-secret

[63] Indian Computer Emergency Response Team, *Directions under § 70B(6), IT Act* (Apr. 28, 2022).
[64] Digital Personal Data Protection Act, No. 30 of 2023, § 18, INDIA CODE.
[65] Tribunals Reforms Act, No. 33 of 2021, § 3 (India).
[66] Ministry of Home Affairs, *About Indian Cyber Crime Coordination Centre (I4C)*, https://i4c.mha.gov.in.
[67] Ministry of Electronics & IT, *Digital India Vision 2027* 2 (2024).

exfiltration on a scale that outstrips traditional legal remedies. First, **ubiquitous online piracy persists despite statutory reforms.**[68]

Second, the **anonymity and jurisdictional fluidity of cyberspace** frustrate investigation.[69]

Third, **intermediary liability** sits in a regulatory grey zone.[70]

Fourth, **data-protection and IP interests increasingly collide**.[71]

VI. Suggestions, Way Forward and Conclusion:

India needs to strengthen its legal framework and enforcement. Also, the judicial as well as administrative reforms need to be introduced that can cater to the era of digitalization as well as technological advancement. It also needs to enhance international cooperation alongside working on spreading public awareness and capacity building. India also needs to work on legislative, administrative as well as judicial aspects altogether for encouraging innovation and digital protection tools.

[68] *Star India Pvt. Ltd. v. Jack Telecom*, C.S. (COMM) 92/2023 (Del. H.C. Mar. 3, 2023).
[69] Indian Computer Emergency Response Team, *Directions under § 70B(6), IT Act* (28 Apr. 2022).
[70] Internet Freedom Found., *Automated Filters & Free Speech: Comments on the Draft Digital India Bill* (Sept. 2024).
[71] Digital Personal Data Protection Act, No. 30 of 2023, § 17, INDIA CODE.

References:

1. S. Savaş & S. Karataş, Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance, 3(1) Int'l Cybersecurity L. Rev. 7 (2022).

2. H. Ning, *A Brief History of Cyberspace* (Auerbach Publications 2022).

3. Online Google Search Result, Key Search Words "Elements of Cyberspace Governance", last visited: 17th May, 2025.

4. Online Google Search Result, Key Search Words "Key Stakeholders in Cyberspace", last visited: 17th May, 2025.

5. Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford Univ. Press 2006).

6. Kristen E. Eichensehr, Public-Private Cybersecurity, 95 Tex. L. Rev. 467 (2017).

7. United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security (2021). U.N. Doc. A/76/135 (July 14, 2021).

8. World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World (2012).

9. Kristen E. Eichensehr, Cybersecurity's Sovereignty Gap: Government Responses to the Rise of Private Cybersecurity Companies, 52 U.C. Davis L. Rev. 101 (2018).

10. Peter Swire, A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security? 3 J. Telecomm. & High Tech. L. 163 (2004).

11. Laura DeNardis, The Global War for Internet Governance (Yale Univ. Press 2014).

12. Internet Engineering Task Force (IETF), Mission Statement, RFC 3935 (Oct. 2004).

13. Bruce Schneier, Secrets and Lies: Digital Security in a Networked World (Wiley 2015).

14. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1, Apr. 2018).

15. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

16. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010).

17. International Telecommunication Union (ITU), Global Cybersecurity Agenda (2007).

18. OECD, Digital Security Policy: Risk Management and Economic and Social Prosperity (2015).

19. World Intellectual Property Organization, WIPO Overview of WIPO's Internet-Related Activities (2022), https://www.wipo.int/about-wipo/en/internet.html.

20. Internet Corp. for Assigned Names & Numbers, About ICANN (2023), https://www.icann.org/resources/pages/welcome-2012-02-25-en.

21. Int'l Telecomm. Union, Overview of ITU's Cybersecurity Work (2022), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

22. Ministry of Electronics & Info. Tech. (MeitY), India's Position on Internet Governance, https://www.meity.gov.in (last visited May 16, 2025).

23. The Information Technology Act, No. 21 of 2000, India Code (2000).

24. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, https://www.meity.gov.in/content/it-rules-2021.

25. The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

26. Internet Governance Forum (IGF), IGF Participants List - India, https://www.intgovforum.org/en (last visited May 16, 2025).

27. Digital India Programme, Ministry of Electronics & Info. Tech.,

https://www.digitalindia.gov.in (last visited May 16, 2025).

28. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

29. The Copyright Act, No. 14 of 1957, INDIA CODE (2012), https://copyright.gov.in.

30. The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), https://meity.gov.in/writereaddata/files/itbill2000.pdf.

31. Super Cassettes Industries Ltd. v. MySpace Inc. [2011 SCC OnLine Del 2646]

32. Shreya Singhal v. Union of India [(2015) 5 SCC 1]

33. Ministry of Electronics & IT, Draft National Cybersecurity Strategy (2021), available at https://www.meity.gov.in.

34. Indian Computer Emergency Response Team, Directions under § 70B(6), IT Act (Apr. 28, 2022).

35. Digital Personal Data Protection Act, No. 30 of 2023, § 18, INDIA CODE.

36. Tribunals Reforms Act, No. 33 of 2021, § 3 (India).

37. Ministry of Home Affairs, About Indian Cyber Crime Coordination Centre (I4C), https://i4c.mha.gov.in.

38. Ministry of Electronics & IT, Digital India Vision 2027 2 (2024).

39. Star India Pvt. Ltd. v. Jack Telecom, C.S. (COMM) 92/2023 (Del. H.C. Mar. 3, 2023).

40. Indian Computer Emergency Response Team, Directions under § 70B(6), IT Act (28 Apr. 2022).

41. Internet Freedom Found., Automated Filters & Free Speech: Comments on the Draft Digital India Bill (Sept. 2024).

42. Digital Personal Data Protection Act, No. 30 of 2023, § 17, INDIA CODE.